МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Н.Э. БАУМАНА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)"

«БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

ДЕВЯТАЯ
ВСЕРОССИЙСКАЯ
НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

(Москва, 4-5 декабря 2018 года)

СБОРНИК ТРУДОВ КОНФЕРЕНЦИИИ

МГТУ им.Н.Э.Баумана
НУК «Информатика и системы управления»
МОСКВА-2018

УДК 003.26.7:004.09
ББК 32.937.202
Б31

Б31

Безопасные информационные технологии. Сборник трудов Девятой всероссийской научно-технической конференции – М.: МГТУ им. Н.Э.Баумана, 2018. 214 с. – илл.

ISBN 978-5-9906630-9-1

Сборник содержит тезисы докладов, представленных на Девятой всероссийской научно-технической конференции "Безопасные информационные технологии" (БИТ-2018), проходившей 4-5 декабря 2018 г. в Москве в МГТУ им. Н.Э. Баумана.

Тезисы публикуются в редакции научных руководителей или в авторской редакции при наличии ученой степени.

УДК 004.056.5

Проектирование и разработка экспертно-аналитической системы «Система анализа трафика» для исследования алгоритмов классификации трафика мобильных устройств под управлением операционной системы Android

Барков В.В.[1]

В настоящей работе описаны проектирование и разработка экспертно-аналитической системы «Система анализа трафика». Рассмотрены этапы проектирования базы данных, включая концептуальный, логический и физический. Приведено описание таблиц, их связей. Разработана Web-служба для доступа к базе данных. Собраны данные, необходимые для обучения классификаторов.

Ключевые слова: *база данных, Web-служба, классификация, машинное обучение, алгоритмы, сетевой трафик, приложение, пакет, поток, протокол, сеть, мобильные приложения.*

Введение

Классификация сетевого трафика является актуальной задачей, решение которой позволит обнаруживать трафик вредоносных и нежелательных приложений в общем потоке трафика [1, 2]. Классификация сетевого трафика может быть использована в системах обнаружения вторжений, для фильтрации вредоносных и нежелательных приложений, блокировки заданных приложений, передающих зашифрованный трафик. Очень часто для решения задачи классификации используют методы машинного обучения, которые требуют данные для обучения.

В настоящее время все больший интерес представляет трафик мобильных приложений. В случае классификации трафика мобильных приложений данными для обучения является набор потоков сетевого трафика, в котором для каждого потока заранее известно генерирующее его приложение.

В рамках исследования трафика мобильных устройств важное место занимает формирование экспериментальной базы данных сетевого трафика выбранных мобильных приложений.

Целью является провести инфологическое, даталогическое и физическое проектирование базы данных [5, 6] трафика мобильных устройств и наполнить базу данных. Источником трафика являются мобильные приложения под управлением ОС Android [7].

Анализ предметной области

Для автоматизации процесса исследования алгоритмов классификации трафика мобильных приложений требуется разработка программного комплекса, позволяющего в автоматическом режиме собирать с мобильных устройств пакеты сетевого трафика и сохранять их в базу данных; группировать пакеты сетевого трафика в потоки; по запросу пользователя формировать наборы данных с заданными характеристиками (количество потоков конкретного приложения: наличие фонового трафика; формирование набора данных на основе уже созданного набора с добавлением новых потоков, исключая повторения) [3, 4].

[1] Барков Вячеслав Валерьевич, аспирант, Московский технический университет связи и информатики, Москва, viacheslav.barkov@gmail.com

Программный комплекс должен:

• вычислять характеристики (признаки) потока с возможностью легкого добавления новых вычисляемых характеристик (признаков);

• создавать и обучать классификаторы сетевого трафика с заданными набором данных, признаками и алгоритмом обучения;

• использовать кросс-валидацию;

• использовать online классификацию;

• применять алгоритмы выбора признаков;

• единообразно работать со сторонними библиотеками машинного обучения (такими как WEKA, MOA и т.п.) и собственными алгоритмами машинного обучения;

• получать численные результаты оценки эффективности классификаторов;

• создавать кластеризаторы сетевого трафика с заданными набором данных, признаками и алгоритмом;

• получать численные результаты оценки эффективности кластеризаторов;

• осуществлять управление процессом исследования с помощью мобильного клиента и Web-браузера;

• получать с помощью Web-браузера информацию о наборах данных, классификаторах, кластеризаторах, их числовых и графических характеристиках;

• в автоматическом режиме определять приложение-источник по пакетам сетевого трафика.

Взаимодействие приложений с базой данных показано на рисунке 1.

Рис.1. Взаимодействие приложений с базой данных

На основании сформулированных требований можно выделить следующие сущности создаваемого ПО:

• Пакет – хранит информацию о пакетах сетевого трафика

• Поток – хранит информацию о потоке сетевого трафика

• Приложение – хранит информацию о мобильном приложении

• Набор потоков – хранит информацию о наборе потоков, которые в дальнейшем будут использованы для обучения и проверке классификатора

• Атрибут – хранит информацию об атрибутах классификации (кластеризации), которые могут быть вычислены

• Кеш атрибутов – хранит информации о значении атрибутов классификации (кластеризации) для потоков. Используется для сокращения времени вычисления атрибутов

• Набор атрибутов – хранит информацию об атрибутах, используемых при классификации или кластеризации для описания потока сетевого трафика

• Сеанс фильтрации атрибутов – хранит информацию о сеансах фильтрации атрибутов классификации (кластеризации)

• Параметры – хранит информацию о значениях параметров алгоритма выбора признаков, алгоритма оценки, используемого при фильтрации признаков, алгоритма классификации и кластеризации

• Обработчик трафика – общая сущность для классификаторов и кластеризаторов

• Матрица ошибок – хранит матрицы ошибок всех проведённых экспериментов

• Ячейка матрицы ошибок – составная часть матрицы ошибок

• Эксперимент – хранит информацию о проведённых экспериментах (классификация, кластеризация трафика)

• Пользователь – хранит информацию о пользователях системы

• Сеансы пользователя – хранит информацию обо всех активных сеансах пользователей

Сеанс фильтрации атрибутов может иметь несколько параметров алгоритма фильтрации признаков и несколько параметров алгоритма оценки, указывает на один или несколько начальных атрибутов и на результирующий набор атрибутов, связан с набором потоков и имеет владельца.

Каждый обработчик трафика (классификатор или кластеризатор) может иметь несколько параметров, относящиеся к алгоритму классификации или алгоритму кластеризации, связан с набором атрибутов и имеет владельца.

Поток может включать в себя один или несколько пакетов, связан с приложением и имеет владельца.

Набор потоков включает в себя один или несколько потоков сетевого трафика, а также может включать несколько потоков фонового трафика и имеет владельца.

Каждый пакет сопоставлен с приложением.

Набор атрибутов включает в себя один или несколько атрибутов и имеет владельца.

Кэш атрибутов связан с потоком и атрибутом.

Каждый эксперимент включает в себя один или несколько обработчиков трафика (классификатор или кластеризатор), набор потоков и имеет владельца.

Матрица ошибок состоит из одной или нескольких ячеек и сопоставлена с набором данных и процессором (классификатором или кластеризатором). Каждая ячейка матрицы ошибок ссылается на ожидаемое и полученное в результате классификации приложение. Каждый пользователь может иметь одну или несколько сессий.

Инфологическое проектирование

На основании анализа предметной области построена инфологическая модель предметной области, включающая 15 сущностей и 29 связей. ER-диаграмма, описывающая сущности, атрибуты сущностей и связи сущностей представлена на рис. 2.

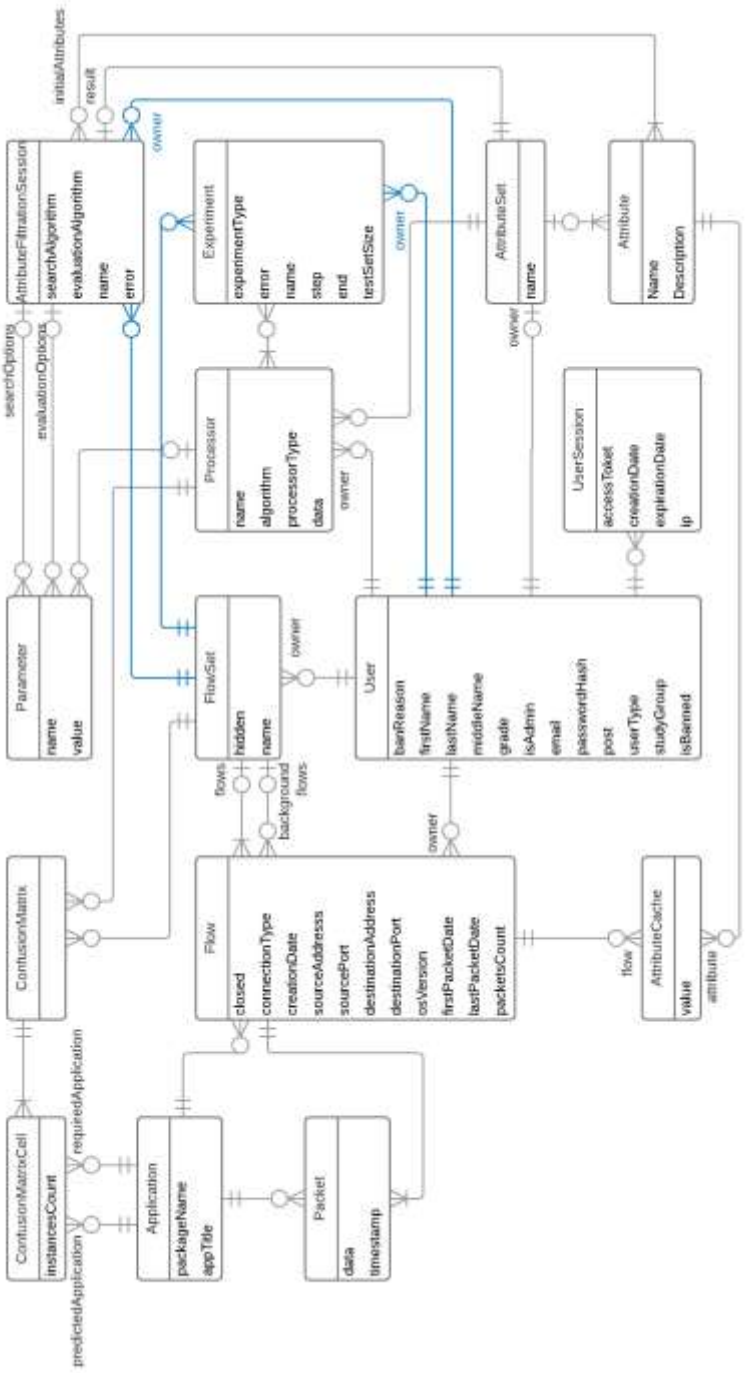


Рис.2. Инфологическая модель предметной области

Сущность ConfusionMatrix (Матрица ошибок) хранит информацию наборе потоков и обработчике трафика, для которых данная матрица ошибок была получена, а также о наборе ячеек.

Сущность ConfusionMatrixCell (Ячейка матрицы ошибок) представляет ячейку матрицы ошибок и хранит информацию о количестве потоков, которые были классифицированы как принадлежащие приложению, указанному в поле predictedApplication, но на самом деле принадлежат приложению, указанном в поле requiredApplication.

Сущность Application (Приложение) хранит информацию о названии

приложения, которое взято из магазина приложений Google Play и имени пакета – уникальном строковым идентификатором приложения.

Сущность Flow (Поток) хранит информацию о дате создания потока, IP-адресе и порте источника и назначения, версии операционной системы клиента, типе соединения (мобильная сеть или сеть Wi-Fi), временных метках первого и последнего пакетов в потоке, количестве и наборе пакетов, информацию о приложении, которому принадлежит данный поток, владельце потока, а также признак, указывающий активно соединение или уже закрыто.

Сущность Packet (Пакет) хранит бинарное представление IP-датаграмы, приложение, которому принадлежит пакет, а также временную метку, по которой можно определить дату и время генерации датаграмы.

Сущность FlowSet (Набор потоков) хранит название набора данных, признак, с помощью которого можно определить, является ли набор скрытым или нет, набор потоков, набор потоков, играющих роль фонового трафика, а также о владельце набора потоков.

Сущность Processor (Обработчик трафика) хранит название обработчика трафика, тип (классификатор или кластеризатор), алгоритм классификации или кластеризации, данные, полученные в результате обучения, набор атрибутов, по которым осуществляется обучение и тестирование, параметры алгоритма классификации, данные о владельце обработчика трафика.

Сущность ConfusionMatrix (Матрица ошибок) хранит информацию наборе потоков и обработчике трафика, для которых данная матрица ошибок была получена, а также о наборе ячеек.

Сущность ConfusionMatrixCell (Ячейка матрицы ошибок) представляет ячейку матрицы ошибок и хранит информацию о количестве потоков, которые были классифицированы как принадлежащие приложению, указанному в поле predictedApplication, но на самом деле принадлежат приложению, указанном в поле requiredApplication.

Сущность Application (Приложение) хранит информацию о названии приложения, которое взято из магазина приложений Google Play и имени пакета – уникальном строковым идентификатором приложения.

Сущность Flow (Поток) хранит информацию о дате создания потока, IP-адресе и порте источника и назначения, версии операционной системы клиента, типе соединения (мобильная сеть или сеть Wi-Fi), временных метках первого и последнего пакетов в потоке, количестве и наборе пакетов, информацию о приложении, которому принадлежит данный поток, владельце потока, а также признак, указывающий активно соединение или уже закрыто.

Сущность Packet (Пакет) хранит бинарное представление IP-датаграмы, приложение, которому принадлежит пакет, а также временную метку, по которой можно определить дату и время генерации датаграмы.

Сущность FlowSet (Набор потоков) хранит название набора данных, признак, с помощью которого можно определить, является ли набор скрытым или нет, набор потоков, набор потоков, играющих роль фонового трафика, а также о владельце набора потоков.

Сущность Processor (Обработчик трафика) хранит название обработчика трафика, тип (классификатор или кластеризатор), алгоритм классификации или кластеризации, данные, полученные в результате обучения, набор атрибутов, по которым осуществляется обучение и тестирование, параметры алгоритма классификации, данные о владельце обработчика трафика.

Сущность AttributeFiltrationSession (Сессия фильтрации атрибутов) хранит информацию о названии сессии, об алгоритме отбора признаков и алгоритме оценки, о параметрах алгоритмов отбора признаков и оценки, наборе потоков, на котором производится фильтрация атрибутов, список начальных атрибутов, результирующий набор атрибутов, информация о владельце набора атрибутов, а также информация об ошибках.

Сущность Parameter (Параметры) хранит информацию о паре ключ-значение, используется для хранения параметров алгоритмов отбора признаков, оценки и классификации.

Сущность AtributeSet (Набор атрибутов) хранит информацию о названии набора атрибутов, входящих в состав набора атрибутах и владельце набора атрибутов.

Сущность Attribute (Атрибут) хранит название и описание атрибута.

Сущность AttributeCache (Кэш атрибутов) хранит вычисленное значение конкретного атрибута для конкретного потока.

Сущность Experiment (Эксперимент) хранит информацию о наборе потоков, с которым проводится эксперимент, обработчике трафика, владельце эксперимента, названии и типе эксперимента, наличии ошибок, размере тестовой выборки, общие числовые характеристики, зависящие от типа эксперимента, такие как шаг и конечное значение изменяемого параметра.

Сущность User (Пользователь) хранит информацию о пользователе системы: фамилию, имя, отчество, ученую степень, роль пользователя (студент или преподаватель), группу для студентов, занимаемую должность для преподавателей, адрес электронный почты и хеш пароля для осуществления процесса аутентификации, признак того, что пользователь является администратором, признак того, что пользователь заблокирован и причина блокировки.

Сущность UserSession (Сеансы пользователя) хранит информацию о текущем сеансе пользователя: информация о пользователе, дата начала и окончания сеанса, IP-адрес, с которого был установлен сеанс связи и токен доступа.

Даталогическое проектирование

В ходе даталогического проектирования базы данных для реализации связей многие ко многим и связей с необязательным классом принадлежности с обеих сторон были созданы вспомогательные сущности. Общее число сущностей увеличилось до 21. Перечень сущностей представлен в таблице 1.

Таблица 1

Сущности базы данных

№	Сущность	Назначение
1	apps	Хранит информацию о приложениях
2	confusionmatrices	Хранит информацию о матрицах ошибок
3	confusionmatrixcells	Хранит информацию о ячейках матрицы ошибок
4	evaluationoptions	Хранит информацию о значениях параметров алгоритма оценки, используемого при фильтрации признаков
5	experimentresultpoints	Хранит информацию о точках экспериментов
6	experiments	Хранит информацию об экспериментах
7	flows	Хранит информацию о потоках
8	flowsinset	Хранит информацию о связи потоков и наборов потоков
9	flowssets	Хранит информацию о наборах потоков
10	optionvalue	Хранит информацию о значениях параметров
11	packets	Хранит информацию о пакетах
12	processoroptions	Хранит информацию о связи классификаторов (кластеризаторов) и значений параметров

13	processors	Хранит информацию о классификаторах и кластеризаторах
14	processorsinexperiments	Хранит информацию о связях экспериментов и классификаторов
15	searchoptions	Хранит информацию о связях сеансов фильтрации атрибутов и значений параметров алгоритма отбора атрибутов
16	user	Хранит информацию о пользователях
17	usersession	Хранит информацию о сессиях пользователей
18	attributesfiltrationsessions	Хранит информацию о сеансах фильтрации атрибутов
19	attributevalues	Хранит информацию о значения атрибутов для потоков
20	backgroundflows	Хранит информацию о связях фоновых потоках и наборах потоков
21	attributesset	Хранит информацию о наборах атрибутов

За хранение пакетов сетевого трафика мобильных приложений и наборов данных отвечают сущности apps, flows, flowsinset, flowsets, packets, backgroundflows.

Физическое проектирование

Для развёртывания программного комплекса был выбран сервер IMB под управлением операционной системы Microsoft Windows Server 2016 Standard. В качестве сервера базы данных была выбрана бесплатная СУБД MySQL 5.7.

На рисунке 3 показана схема базы данных.

Для взаимодействия с разработанной базой данных с использованием технологий Java Enterprise Edition было разработано корпоративное приложение, обеспечивающие возможность накопление пакетов и потоков трафика выбранных мобильных приложений, управления наборами потоков и проведения экспериментов. В ходе разработки приложения, по инфологической модели предметной области были созданы классы-сущности, и Web-сервис, с помощью которого с приложением могут удалённо взаимодействовать клиенты. Перечень поддерживаемых HTTP-запросов представлен в таблице 2.

Весь функционал, описанный в таблице 2 реализован с использованием EJB-компонентов, организующих получение и сохранение сущностей из базы данных. Обучение и тестирование классификаторов и кластеризаторов осуществляется с использованием библиотек WEKA и MOA. Разработанные абстракции классификаторов и кластеризаторов позволяют использовать любые другие библиотеки, в том числе написанных на других языках программирования, либо реализовывать собственные алгоритмы классификации и кластеризации.

Сбор трафика на мобильном устройстве осуществляется с помощью разработанного клиентского программного обеспечения. Перехват пакетов сетевого трафика осуществляется с помощью прикладного программного интерфейса для построения виртуальных частных сетей. Определение приложения, которому принадлежит трафик, производится в два этапа. На первом этапе с помощью псевдофайлов /proc/net/tcp и /proc/net/udp, предоставляемые операционной системой Linux, определяется идентификатор пользователя Linux, которому принадлежит сетевое подключение. На втором этапе с помощью класса PackageManager, входящего в Android API, по идентификатору пользователя Linux определяется приложение (имя пакета и название). Собранная информация отправляется на сервер с использованием описанного выше REST API.

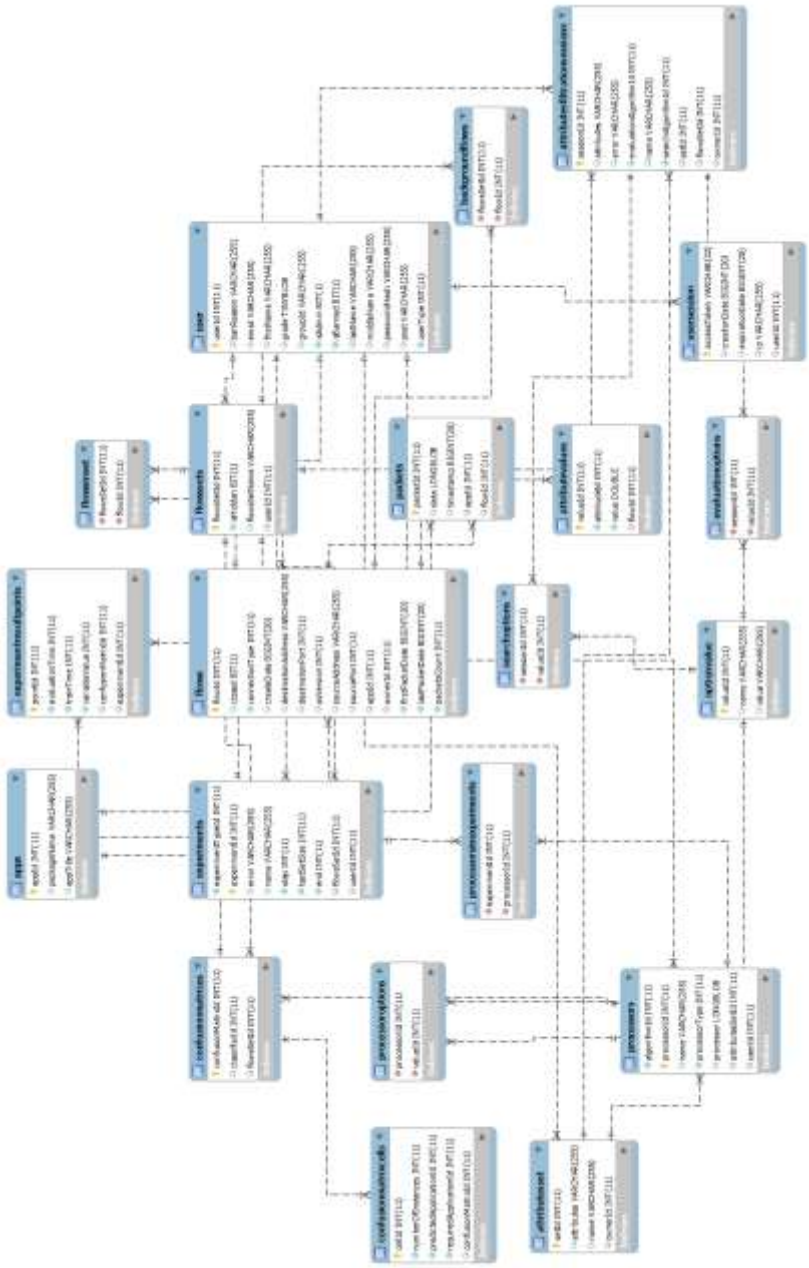


Рис.3. Схема базы данных

Таблица 2

Перечень поддерживаемых запросов к Web-службе

Метод	Путь	Назначение
Администрирование		
PUT	/admin/ban	Блокировка доступа к API заданному пользователю
GET	/admin/users	Получение информации о всех зарегистрированных пользователях
Управление пользователями		
POST	/register	Регистрация пользователя
POST	/auth	Авторизация пользователя
GET	/users/current	Получение информации о текущем пользователе

Работа с атрибутами (признаками)		
GET	/attributes	Получение всех признаков
GET	/attributes/filtration/sessions	Получение списка сеансов фильтрации признаков текущего пользователя
DELETE	/attributes/filtration/sessions/{id}	Удаление сессии фильтрации атрибутов с идентификаторов id
POST	/attributes/sets	Создание набора признаков
GET	/attributes/sets	Получение наборов атрибутов текущего пользователя
DELETE	/attributes/sets/{id}	Удаление набора атрибутов с идентификаторов id
GET	/attributes/sets/all	Получение всех наборов признаков, принадлежащих указанному пользователю
POST	/attributes/sets/filter	Фильтрация признаков
GET	/evaluation-algorithms	Получение алгоритмов оценки признаков
GET	/search-algorithms	Получение всех доступных для использования алгоритмов выбора признаков
Работа с пакетами и потоками		
GET	/flows/count	Получение информации о количестве соединений по всем приложениям
GET	/flows/count/{appId}	Получение количества потоков по приложению с идентификаторов appId
GET	/flows/count/filter	Получение количества потоков по приложениям с учетом минимального количества пакетов в потоке
PUT	/packet	Точка приема перехваченного трафика
GET	/packets/count	Получение информации о количестве IP-дейтаграмм по всем приложениям
Работа с наборами данных		
GET	/applications	Получение списка собранных приложений
PUT	/dataset	Создание набора данных
DELETE	/dataset/{id}	Удаление уже созданных наборов данных с идентификаторов id
GET	/datasets	Получение наборов данных текущего пользователя
GET	/datasets/all	Получение всех созданных наборов данных всех пользователей
Работа с классификаторами		
POST	/classifiers	Создание классификатора
GET	/classifiers/algorithms	Получение алгоритмов классификации
Работа с кластеризаторами		
POST	/clusterers	Создание кластеризатора
GET	/clusterers/algorithms	Получение всех доступных для использования алгоритмов кластеризации
Работа с классификаторами и кластеризаторами		
GET	/processors	Получение списка классификаторов или кластеризаторов
DELETE	/processors/{id}	Удаление классификатор или кластеризатора с идентификаторов id
Работа с экспериментами		
GET	/experiments	Получение списка экспериментов

DELETE	/experiments/{id}	Удаление уже созданного эксперимента с идентификаторов id
GET	/experiments/{id}	Получение информации об эксперименте с идентификаторов id
GET	/experiments/all	Получение созданных экспериментов пользователя
POST	/experiments/cross-validation	Создание эксперимента кросс-валидации
POST	/experiments/one-set-many-processors	Создание эксперимента "Один набор - много алгоритмов"
POST	/experiments/one-set-one-processor	Создание эксперимента "Один набор - один алгоритм"
POST	/experiments/packets-incrementation	Создание эксперимента "Увеличение пакетов"
GET	/experiments/status	Получение состояний выполнения всех экспериментов
GET	/experiments/status/{id}	Получение статуса эксперимента с идентификаторов id
DELETE	/experiments/stop/{id}	Остановка эксперимента с идентификаторов id

База данных сетевого трафика мобильных приложений

С использованием разработанного программного комплекса в течение одного месяца был собран трафик 110 мобильных приложений, включающий 95 447 потоков и 7 119 169 пакетов. 71 667 потоков и 6 989 991 пакетов составляют 18 основных приложений. В таблице 2 показано количество собранных потоков для каждого приложения.

Таблица 3

Количество собранных потоков

№	Название приложения	Шифрование	Имя пакета	Количество потоков	Количество пакетов
1	Московский комсомолец	нет	com.mobilein.mk	5335	107202
2	Пикабу – юмор и новости	да	ru.pikabu.android	5329	265071
3	Годвилль	нет	ru.godville.android	5016	61343
4	Instagram	да	com.instagram.android	4979	1916363
5	НТВ: новости, видео, передачи	нет	ru.ntv.client	5908	233982
6	Фишки с FiReader – юмор, демотиваторы, посты	нет	com.kirik88.fireader	5422	576581
7	Booking.com бронь отелей	частично	com.booking	5326	552606
8	Коммерсантъ	частично	com.nsadv.kommersant	5325	338327
9	Скайп – бесплатные мгновенные сообщения и видеозв.	да	com.skype.raider	5244	232510
10	WolframAlpha	нет	com.wolfram.android.alpha	5190	61140
11	Яндекс.Браузер – с Алисой	частично	com.yandex.browser	5132	139595
12	Сбербанк Онлайн	да	ru.sberbankmobile	5110	241235
13	ПиццаСушиВок - доставка еды	нет	ru.itsilver.pizzaempire	5097	64460
14	Почта Mail.Ru	да	ru.mail.mailapp	5070	246184
15	Hearthstone	да	com.blizzard.wtcg.hearthstone	5028	227688
16	Badoo – Новые знакомства	частично	com.badoo.mobile	4976	581212
17	4PDA	частично	ru.fourpda.client	4974	524215
18	Google Chrome: быстрый браузер	частично	com.android.chrome	3865	620277

Выводы

В ходе работы была спроектирована, реализована и наполнена база данных.

В ходе инфологического и даталогического проектирования выделено 21 сущность, 6 из которых (apps, flows, flowsinset, flowsets, packets, backgroundflows) используются для непосредственного хранения данных трафика. В ходе физического проектирования был выбран сервер баз данных MySQL 5.7 и создана 21 таблица. Для доступа к базе данных с применением технологии Java Enterprise Edition было создано корпоративное приложение, прдоставляющее доступ с помощью REST API. Для сбора трафика с мобильных устройств под управлением операционной системы Android было разработано приложение, которое с помощью прикладного программного интерфейса для создания виртуальных частных сетей, собирает пакеты сетевого трафика, идентифицирует приложение-источник и отправляет их по протоколу HTTP серверному программному обеспечению. С использованием клиентского и серверного программного обеспечения созданная база данных была наполнена трафиком 18 основных приложений. В ходе сбора данных было получено 71 667 потоков и 6 989 991 пакетов.

Литература

1. Шелухин О.И., Ерохин С.Д., Ванюшина А.В. Под редакцией Шелухина О.И. Классификация IP –трафика методами машинного обучения. М., Горячая-линия – Телеком, 2018, 284 с.

2. Шелухин О.И., Ванюшина А.В., Габисова М.Е. Фильтрация нежелательных приложений интернет-трафика с использованием алгоритма классификации Random Forest // Вопросы кибербезопасности. 2018. № 2 (26). С. 44-51.

3. Шелухин О. И., Барков, В.В. Разработка инфраструктуры для классификации сетевого трафика мобильных приложений с применением алгоритмов машинного обучения . В кн.: Труды международной НТК Телекоммуникационные и вычислительные системы – 2017 – 22 ноября 2017 г -М. «Горячая линия-Телком» - 2017.- 300с (стр.180)

4. Шелухин О.И., Барков В.В. Методы сбора сетевого трафика с мобильных устройств под управлением операционной системы android с целью классификации по типам приложений. Сборник трудов XII Международной научно-технической конференции «Технологии инфор-мационного общества». Москва, Московский технический университет связи и информатики (МТУСИ), 14-15 марта 2018 г. В 2-х томах. Том 2. М.: ИД Медиа Паблишер», 2018. 384 с.

5. Советов, Б. Я. Базы данных: теория и практика/ Б. Я. Советов, В. В. Цехановский, В. Д. Чертовский. – М. : Высш. шк., 2005. – С. 436.

6. Карпова И.П. Базы данных. Курс лекций и материалы для практических занятий. – Учебное пособие. – Издательство "Питер", 2013. – 240 с.

7. Коматинэни С., Маклин Д., Хэшими С. Google Android: программирование для мобильных устройств = Pro Android 2. — 1-е изд. — СПб.: Питер, 2011. — 736 с. — ISBN 978-5-459-00530-1.

Научный консультант: Шелухин Олег Иванович, д.т.н., профессор, заведующий кафедрой «Информационная безопасность» Московского технического университета связи и информатики, sheluhin@mail.ru

Design and Development of the Expert Analytical System “Traffic Analysis System” for Researching of the Algorithms for the Classification of the Traffic Generated by Mobile Devices Running on Android OS

Barkov V.V.[2]

Abstract. This work describes design and development of the expert analytical system “Traffic Analysis System”. The stages of database design, including conceptual, logical and physical, are considered. It is shown tables and their relationships. Web service to access the database was developed. The data necessary for training classifiers are collected.

Keywords: Database, Web service, classification, machine learning, algorithms, network traffic, application, packet, flow, protocol, network, mobile applications

[2] Barkov Viacheslav, postgraduate student, Moscow Technical University of Communication and Informatics, Moscow, viacheslav.barkov@gmail.com

УДК 621.392

Алгоритм функций устройств абонентского доступа имитатора сети ПД категории специального назначения, подлежащих реализации на специально разработанных аппаратно-программных устройствах

Бельфер Р. А. [3], **Борисов С. М.** [4], **Макаров И. М.**[5]

Предложены алгоритмы выполнения функций участка абонентского доступа имитатора объединенной сети передачи данных из нескольких частных (изолированных) сетей с высокими требованиями к информационной безопасности, надежности и другим характеристикам. Отечественная разработка таких сетей для разных государственных ведомств является актуальной и проводится на кафедре "Информационная безопасность" МГТУ им. Н.Э.Баумана в научно-практическом плане создания имитатора сети передачи данных в рамках учебного лабораторного стенда. Назначением предлагаемых алгоритмов является их использование для работ студентов по созданию аппаратно-программного имитатора такой объединенной сети.

Ключевые слова: *информационная безопасность (Information Security), надежность (reliability), сеть передачи данных (data transmission networks).*

Введение

Настоящая статья посвящена продолжению работ [1-8] по созданию в рамках учебного лабораторного стенда (УЛС) имитатора сети ПД специального назначении, выполняемого преподавателями и студентами кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана. В отличие от другого доклада на данной конференции по этому направлению (“Алгоритм формирования маршрутизации от источника в имитаторе сети ПД категории специального назначения”) задача настоящей работы разработать алгоритм некоторых функций устройств абонентского доступа имитатора сети ПД, который подлежит реализации на специально разработанных для этого аппаратных средствах имитатора сети. Используется та же конфигурация имитатора сети ПД (рис. 1) с тем же примером пучка маршрутов коммутируемого виртуального канала (КВК) с четырьмя путями маршрутизации, дополненная единым удостоверяющим центром (УЦ).

[3] Бельфер Рувим Абрамович, к.т.н., доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, a.belfer@yandex.ru

[4] Борисов Сергей Михайлович, студент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, geniusser@mail.ru

[5] Макаров Илья Михайлович, студент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, ipost.mim@gmail.com

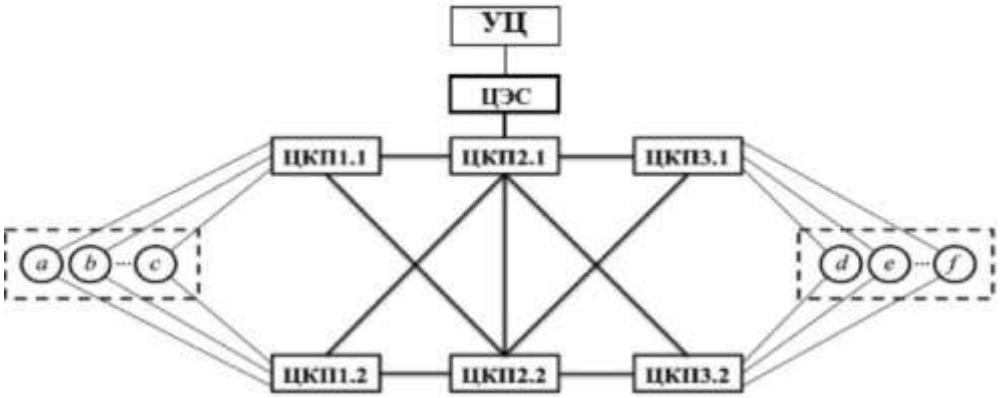


Рис. 1. Конфигурация имитатора сети ПД с четырьмя путями маршрутизации, центром эксплуатации сети и единым удостоверяющим центром.

Каждый путь маршрутизации включает три из шести центров коммутации пакетов (ЦКП). Четыре из них – граничные - ЦКП 1.1 (адрес 11), ЦКП 3.1 (адрес 31), ЦКП 1.2 (адрес 12), ЦКП 3.2 (адрес 32) с подключенными к ним оконечными пунктами ОП - (*a,b,…,c*) и (*d,e,...,f*), а ЦКП 2.1 (адрес 21), и ЦКП 2.2 (адрес 22) являются транзитными. подключен к определенной частной (изолированной) подсети. Имитатор сети ПД представляет объединение частных изолированных сетей, каждая из которых согласно Закону “О связи” предназначена определенных функций ОПК, МВД и некоторых других государственных ведомств. Соединения КВК, как правило, устанавливается с последующей передачей данных между оконечными пунктами одной частной подсети. Согласно изложенному в работе [7] положению в объединенной сети предусмотрена возможность установления КВК для определенных оконечных пунктов разных частных сетей ПД. Такое соединение будем называть смешанным.

В настоящей работе алгоритм реализации такого смешанного соединения КВК на разрабатываемых аппаратных средствах имитатора сети ПД не рассматривается.

На примере двух частных сетей объединенного имитатора сети ПД категории специального назначения приводится описание последовательно исполняемых программ на специально созданных аппаратных средствах по реализации функций на устройствах абонентского доступа для частных сетей 1(ЧС1) и 3 (ЧС3) и смешанного соединения оконечных пунктов этих сетей. При этом рассматривается упрощение использование разработанных алгоритмов в работах учебного лабораторного стенда [1-8]. Например, шифрование заменяется сложением по модулю 2. Полная реализация алгоритмов всего имитатора сети ПД категории специального назначения проводится в рамках УЛС на одном компьютере по разработанному программному обеспечению. Взаимная аутентификация и управление ключами приводится в работе [8].

Частная сеть 1

Приняты исходные данные: физический адрес оконечного пункта (ОП) источника установления КВК - 101, физический адрес оконечного пункта назначения - 601, логический адрес ОП - LCN=809.

1. ОП ------- >11. Формирование в ОП сообщение МХ1, включающее множество типов характеристик информационной безопасности (ИБ). Передача в ЦКП 1.1 (физический адрес 11).
2. ОП < ------- 11. Прием МХ1 в 11. Коррекция МХ1 и создание МХ2. Определение логического адреса ОП (с адресом 101) LCN=809. Шифрование согласованным алгоритмом в МХ2 с канальным ключом абонентского доступа K_{101} сообщения МХ2, идентификатора ассоциации безопасности $SA_{101.}$ и LCN. Передача в ОП.
3. ОП ------- >11. Прием в ОП. Дешифрация согласованным алгоритмом в МХ2 ключом K_{101} сообщения МХ2 с SA_{101} и LCN.

   Составить сообщение на установление соединения (УС) - тип (установление КВК), физический адрес оконечного пункта источника соединения (в примере – 101). физический адрес оконечного пункта назначения (в примере – 601). Зашифровать сообщение УС и сквозные ключи шифрования и целостности $K1_{101601,}$ $K2_{101601,}$ $K3_{101601,}$ $K4_{101601}$ канальным ключом $K_{101.}$ Передача в 11.
4. 21 < ------- 11. Составить в 11 сообщение запрос цепочек маршрутизации (ЗЦМ) - тип сообщения, физический адрес ЦКП абонентского доступа оконечного пункта источника установления КВК, физический адрес оконечного пункта абонентского доступа назначения установления КВК, путь маршрутизации сообщений ЗЦМ в ЦЭС [9]. Путь маршрутизации сообщений ЗЦМ включает участки от ЦКП 1.1 между смежными ЦКП 1.1 и ЦКП 2.1, между ЦКП 2.1 и ЦЭС. Зашифровать сообщение ЗЦМ согласованным алгоритмом шифрования ассоциацией безопасности с канальным ключом $K1_{1121.}$между ЦКП 1.1 и ЦКП 2.1 частной сети 1. Передача зашифрованного ЗЦМ в 21.
5. ЦЭС < ------- 21. Дешифрация сообщения ЗЦМ в 21 согласованным алгоритмом шифрования ассоциацией безопасности с ключом $K1_{1121.}$ Зашифровать сообщение ЗЦМ согласованным алгоритмом шифрования ассоциацией безопасности с канальным ключом частной сети 1 ($K1_{ЦЭС}$) между ЦКП 2.1 и ЦЭС [8]. Передача ЗЦМ в ЦЭС.
6. ЦЭС. Дешифрация сообщения ЗЦМ в ЦЭС согласованным алгоритмом шифрования ассоциацией безопасности с канальным ключом частной сети 1 - $K1_{ЦЭС.}$

   Сформировать в ЦЭС сообщения цепочек маршрутизации (ЦМ) в соответствии с форматом. Формат сообщений ЦМ включает следующие поля: тип сообщения; адреса ЦКП абонентского доступа, запрашивающих цепочки физических адресов каждого из четырех путей маршрутизации принятых в примере работ по имитатору сети [7]; пути маршрутизации КВК; цепочки маршрутизации КВК; цепочки маршрутов ЦМ. Передача зашифрованных сообщений ЦМ четырех путей маршрутизации обратно в ЦКП 1.1 и ЦКП 1.2. В ЦКП 1.1 передаются цепочки маршрутизации первого пути (11-21-31) и третьего пути (11-22-31). В ЦКП 1.2 передаются цепочки маршрутизации второго пути (12-22-32) и четвертого пути (12-21-32). На каждом из участков между смежными ЦКП с помощью канальных ключей производится шифрование/дешифрация сообщений ЦМ [8].
7. В граничных ЦКП 1.1 (11) и ЦКП 1.2 (12) абонентского доступа источника установления КВК сформировать сообщение “Запрос Вызова” (ЗВ) на

установление КВК. Формат сообщения “Запрос Вызова” на установление КВК состоит из следующих полей для каждого сообщения – состояние КВК – установление соединения "1", номер пути маршрута, физический адрес исходящего оконечного пункта (в примере – 101), физический адрес оконечного пункта назначения (в примере - 601), цепочка физических адресов ЦКП каждого пути маршрутизации от источника, LCN, номер частной сети. Зашифровать сообщение ЗВ согласованным алгоритмом шифрования ассоциацией безопасности с канальным ключом $К1_{1121.}$между ЦКП 1.1 и ЦКП 2.1частной сети 1.

8. Формирование части строки таблицы маршрутизации, относящейся к исходящему сообщению ЗВ (и других типов сообщений) из ЦКП абонентского доступа устанавливаемого КВК. Для этого из очереди $О_{1свн1112}$ используется LCN=802. Для подготовки к передаче сообщения ЗВ от ЦКП абонентских доступов (в примере ЦКП 1.1 и ЦКП 1.2) в транзитные ЦКП 2.1 и ЦКП 2.2 необходимо LCN, стоящий первым в очереди $О_{1свн1112}$ LCN=802. Заменить в сообщении ЗВ LCN=809 на полученный из очереди $О_{1свн1112}$ LCN=802 для всех путей маршрутизации. Как видно из таблицы 1 части строк, относящиеся к исходящему сообщению по всем четырем путям маршрутизации, включают следующие параметры (характеристики): адрес поступления сообщения из ЦКП 1.1 или ЦКП 1.2 (транзитные ЦКП 2.1 и ЦКП 2.2. с адресами соответственно 21 и 22); LCN этого сообщения (в данном случае – 802); производилось ли назначение этого LCN в данном ЦКП (в данном случае – да). Для упрощения значение LCN=802 принято одинаковым для всех четырех путей маршрутизации КВК.
9. Эти и последующие таблицы маршрутизации в остальных ЦКП сети ПД составляются при установлении КВК для маршрутизации в сети ПД по логическим адресам служебных сообщений (при подтверждении установления или разъединении КВК и др.), при передаче пакетов данных. Сформированная строка в табл. 1 обеспечивают передачу сообщений только в одном направлении (в примере от оконечного пункта 101 в оконечный пункт 601). Для передачи сообщений в противоположном направлении в таблицы маршрутизации для каждого пути маршрутизации вводится еще одна строка. Как видно из таблицы 1, эта строка для другого направления составляется на основе первой.

Создание строк таблиц маршрутизации для передачи сообщений противоположного направления производится при установлении КВК во всех ЦКП сети ПД.

Табл. 1.

Таблица маршрутизации частной сети 1по логическим адресам в ЦКП1.1 и ЦКП 1.2

		Входящее сообщение в ЦКП 1.1			Исходящее сообщение из ЦКП 1.1		
Номер КВК	Номер пути маршрутизации	Адр. источн. сообщ. в ЦКП 1.1	LCN	Освн	Адрес поступлен. сообщ. из ЦКП 1.1	LCN	Освн
1	1	101	809	да	21	802	да
	1	21	802	да	101	809	да
	3	101	809	да	22	802	да
	3	22	802	да	101	809	да
		Входящее сообщение в ЦКП 1.2			Исходящее сообщение из ЦКП 1.2		
Номер	Номер пути	Адр. источн.	LCN	Освн	Адрес	LCN	Освн

КВК	маршрутизации	сообщ. в ЦКП 1.2			поступлен. сообщ. из ЦКП 1.2		
1	2	101	809	да	22	802	да
	2	22	802	да	101	809	да
	4	101	809	да	21	802	да
	4	21	802	да	101	809	да

Частная сеть 3.

Приняты исходные данные: физический адрес оконечного пункта (ОП) источника установления КВК - 2101, физический адрес оконечного пункта назначения - 2601, логический адрес ОП - LCN=2809.

Приведем отличие частной сети 3 от приведенного выше описания для частной сети 1:

- адресация физических и логических адресов;
- ключи, выполняющие функции механизмов ИБ;
- Таблица маршрутизации частной сети 1по логическим адресам в ЦКП1.1 и ЦКП 1.2.

Выводы

Приведенный алгоритм функций устройств абонентского доступа имитатора сети ПД учебного лабораторного стенда позволяет его использовать для создания аппаратных средств, на которых планируется реализация имитация некоторых функций объединенной сети специального назначения.

Список литературы

1. Бельфер Р.А., Матвеев В.А., Кравцов А.В. Анализ технологий построения сети передачи данных с высокими требованиями по информационной безопасности, надежности и задержке. Электросвязь №5, 2017. С.46-49

2. Бельфер Р.А., Матвеев В.А., Басараб М.А, Кравцов А.В., Мерзляков Д.И. Алгоритм функционирования УЛС защищенной сети ПД на базе виртуальных каналов с высокими требованиями к качеству обслуживания, Электросвязь №8, 2017, С.57-62

3. Бельфер Р.А., Глинская Е.В., Амелин В.В., Механизмы информационной безопасности в имитаторе сети передачи данных учебного лабораторного стенда, Сборник трудов Восьмой всероссийской научно-технической конференции. Безопасные информационные технологии под. ред. М.А. Басараба – М.: - МГТУ им. Н.Э.Баумана, 2017, С.40-44.

4. Бельфер Р.А., Куянов М.С., Мерзляков Д.И., Использование отечественных криптографических алгоритмов на макете аппаратной реализации абонентского доступа сетей ПД, Сборник трудов Восьмой всероссийской научно-технической конференции. Безопасные информационные технологии под. ред. М.А.Басараба – М.: - МГТУ им. Н.Э.Баумана, 2017, С. 35-39.

5. Бельфер Р.А., Басараб М.А., Глинская Е.В., Кравцов А.В., Алгоритм по установлению КВК-соединения на абонентском доступе сети ПД с учетом обеспечения ИБ, Первая миля №8, 2017, С.64-69

6. Бельфер Р.А., Глинская Е.В., Кравцов А.В., Алгоритм программного обеспечения аутентификации абонентского доступа имитатора сети ПД учебного лабораторного стенда, Первая миля №1, 2018, С.64-68

7. Басараб М.А., Бельфер Р.А., Кравцов А.В. Алгоритмы коррекции таблицы маршрутизации в имитаторе сети ПД с обеспечением высокой надежности и безопасности, Электросвязь №6, 2018, С.63-66.

8. Басараб М.А., Бельфер Р.А., Кравцов А.В. Алгоритм аутентификации и управления ключами в имитаторе объединенных частных сетей ПД специального назначения. Первая миля №1, 2018, (в печати).

9. Бельфер Р., Макаров И., Никулина. Алгоритм формирования маршрутизации от источника в имитаторе сети ПД категории специального назначения. (настоящий сборник).

Algorithm of functions of subscriber access devices of a special purpose category data network simulator, to be implemented on specially developed hardware-software devices

Algorithms for performing the functions of the subscriber access section of the simulator of an integrated data network from several private (isolated) networks with high requirements for information security, reliability and other characteristics are proposed. Domestic development of such networks for various government departments is relevant and is carried out at the Department of Information Security of the Moscow State Technical University N. Bauman in the scientific and practical terms of creating a data network simulator in the framework of the educational laboratory stand. The purpose of the proposed algorithms is to use them for the work of students in creating a hardware-software simulator of such an integrated network.

УДК 621.392

Алгоритм формирования маршрутизации от источника в имитаторе сети ПД категории специального назначения

Бельфер Р.А.[6], Макаров И.М.[7], Никулина Т.П.[8]

Настоящая научно-практическая работа в рамках учебного лабораторного стенда является продолжением создания имитатора сети ПД специального назначения с высокими требованиями надежности, информационной безопасности и других показателей. Зарубежными и отечественными специалистами отмечаются недостатки обеспечения надежности и безопасности механизма маршрутизации в каждом узле коммутации, используемого в находящейся в эксплуатации сети ПД общеканальной сигнализации ОКС№7. В настоящей работе кратко изложен алгоритм, мало используемый в сетях связи общего пользования, механизма маршрутизации от источника, с учетом особенностей построения сети ПД категории специального назначения.

***Ключевые слова**: информационная безопасность (Information Security), надежность (reliability), сеть передачи данных (data transmission network), маршрутизация (routing)*

Введение

На кафедре "Информационная безопасность" МГТУ им. Н.Э. Баумана ведется научно-практическая работа по созданию учебного лабораторного стенда (УЛС) имитатора сети передачи данных (ПД) на основе виртуальных каналов. Сеть ПД основана на базе виртуальных каналов с установлением коммутируемого виртуального канала (КВК). Цель этих работ – получение знаний и опыта для создания отечественных сетей ПД категории специального назначения, к которым предъявляются высокие требования по надежности, информационной безопасности и другим характеристикам. В [1-3] и других работах по имитатору сети ПД на приведенной на рис.1 гипотетической конфигурации имитатора сети ПД приводятся основные положения по обеспечению этих требований. Для этого передача одного и того же сообщения в установленном соединении между оконечными пунктами производится одновременно по нескольким раздельным путям маршрутизации. Каждый путь маршрутизации включает три центра коммутации пакетов (ЦКП). К двум граничным ЦКП в каждом пути маршрутизации ЦКП 1.1 (адрес 11), ЦКП 3.1 (адрес 31), и ЦКП 1.2 (адрес 12), ЦКП 3.2 (адрес 32), подключены оконечные пункты, а ЦКП 2.1 (адрес 21), и ЦКП 2.2 (адрес 22), являются транзитными. Один или несколько из приведенных на рисунке оконечных пунктов (*a*,*b*,...,*c*) и (*d*,*e*,...,*f*) подключены к определенной частной изолированной сети. Несколько таких частных сетей обслуживают одно из ведомств (например, ОПК или МВД), образуя единую сеть ПД. Эти частные сети единой сети ПД специального назначения не являются виртуальными частными сетями, так как они не построены на основе сетей связи общего пользования (ССОП).

[6] Бельвер Рувим Абрамович, доцент, кандидат технических наук, МГТУ им. Н.Э. Баумана, Москва, a.belfer@yandex.ru,
[7] Макаров Илья Михайлович, МГТУ им. Н.Э. Баумана, Москва, ipost.mim@gmail.com
[8] Никулина Татьяна Павловна, МГТУ им. Н.Э. Баумана, Москва, tan.p.nikulina@gmail.com

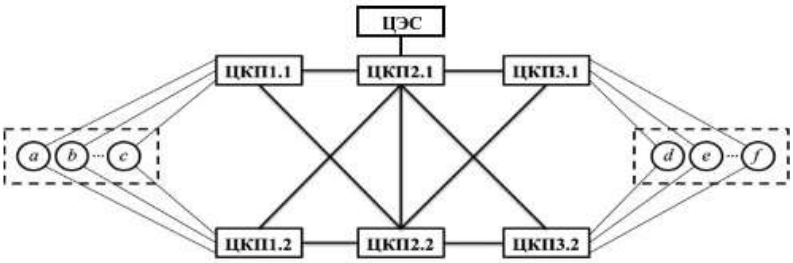


Рис.1. Конфигурация имитатора сети ПД с четырьмя путями маршрутизации

В этих работах предлагается использовать технологию маршрутизации от источника (принудительной маршрутизации) с указанием списка (цепочки) маршрутов в граничном узле абонентского доступа оконечного пункта источника установления соединения. Из известных нам сетей связи общего пользования сети асинхронного режима передачи АТМ (Asynchronous Transfer Mode) используют такую маршрутизацию [4].

Причина выбора такой технологии объясняется тем, что принятая технология маршрутизация в каждом узле коммутации в сетях связи общего пользования ССОП по причине сложности явилась причиной низкой надежности и информационной безопасности (на примере эксплуатации общеканальной сигнализации ОКС№7 [5-9]).

Для формирования маршрутов в граничном маршрутизаторе в [6] предлагается использовать приведенный на рис.1 центр эксплуатации сети (ЦЭС).

В настоящей работе предлагается алгоритм формирования защищенной цепочки маршрутизации для частного случая – исправности всех каналов имитатора сети ПД. Этот алгоритм основан на данных в ЦЭС о состоянии всех каналов связи сети ПД (исправное, т.е. активное или неисправное, т.е. неактивное). Канал связи переводится из неактивного в активное по команде с ЦЭС, а сообщения ККС выполняют функцию проверки его исправности. Канал связи переводится в неактивное состояние по результатам передач сообщений ККС. ЦКП, подключенный к этому каналу, сообщает о его неисправности передачей специального сообщения в ЦЭС. Эти данные ЦЭС получает от каналов сети ПД по результатам непрерывного контроля передаваемых сообщений пакетов данных, а в промежутках между ними сообщений контроля качества канала связи (ККС) специально выбранного формата.

Аппаратные средства имитатора сети ПД, разработанные выпускниками кафедры предыдущих лет, подлежат модернизации. В существующем учебном лабораторном стенде для имитации ЦКП и оконечных пунктов абонентского доступа используются микрокомпьютеры Raspberry Pi модели A+, которые передают по сети Wi-fi данные на один главный ПК. В настоящей реализации используется печатная плата Arduino, которая позволяет расширить имитацию сети ПД категории специального назначения в рамках учебного лабораторного стенда.

Алгоритм контроля качества каналов имитатора сети ПД

При имитации сети ПД одним компьютером алгоритм контроля качества каналов имитатора сети ПД включает выполнение следующих программ под управлением диспетчера программ. Составить во всех граничных ЦКП и транзитном ЦКП 2.2 очереди свободных блоков для приема сообщений контроля качества канала связи ККС – О1121, О1221, О3121, О3221, О2212, О1122, О1222, О3122, О3222. Установить начальные адреса характеристик этих очередей. В названии указанных очередей принята адресация канала приема сообщений. В адресации канала первые две цифры означают ЦКП-приема этого сообщения, а вторые – адрес ЦКП-отправителя.

В ЦЭС установлено состояние каждого канала имитатора сети ПД (активное или не активное).

Производится формирование очередей сообщений контроля качества канала связи ККС на передачу из ЦКП 2.1 – О2111, О2112, О2131, О2132, О2122, из ЦКП 2.2 – О2211,

О2212, О2231, О2232. . В адресации канала первые две цифры означают ЦКП-отправителя сообщения, а вторые – адрес ЦКП-приема. Формат ККС включат поля – тип сообщения, физический адрес канала, контрольно-проверочную комбинацию КПК по модулю 2, номер сообщения.

Передача N сообщений ККС в очереди свободных блоков О1121, О1221, О3121, О3221, О2212, О1122, О1222, О3122, О3222. (п.3).

Прием сообщений ККС в очереди О1121, О1221, О3121, О3221, О2212, О1122, О1222, О3122, О3222. (п.3). Проверка по КПК каждого принятого сообщения ККС. Если суммарное число принятых искаженными ККС превышает критерий, канал в анализируемой очереди фиксируется искаженным и выводится из эксплуатации с переводом в не активное состояние. При переводе канала из не активного состояния в активное состояние необходимо с помощью сообщений контроля качества канала проверить его исправность. Результаты проверки необходимо сообщить в ЦЭС из ЦКП, к которому подключен этот канал.

Алгоритм формирования цепочек путей маршрутов в граничном узле имитатора сети ПД

Запрос и формирование в ЦЭС цепочки путей маршрутизации

Для получения цепочки каждого пути маршрутизации в граничном маршрутизаторе имитатора сети ПД абонентского доступа с оконечным пунктом источника установления КВК при установлении соединения с этого маршрутизатора формируется сообщение “Запрос цепочки маршрутизации” (ЗЦМ). Такими маршрутизаторами в имитаторе сети ПД могут быть ЦКП с физическими адресами 11, 12, 31, 32. Формат сообщений ЗЦМ включает следующие поля: тип сообщения, физический адрес оконечного пункта источника сообщения запроса вызова ЗВ на установление соединения, физический адрес оконечного пункта назначения сообщения ЗВ на установление соединения, пути маршрутизации сообщений ЗЦМ в ЦЭС. Для надежности сообщения ЗЦМ передаются в ЦЭМ по нескольким путям маршрутизации. В ЦЭС при получении ЗЦМ на основании данных о состоянии каналов связи формируются цепочки маршрутизации всех путей маршрутизации для устанавливаемого соединения. При отказе из ЦЭС в граничный маршрутизатор передается соответствующее сообщение.

Передача из ЦЭС цепочек путей маршрутизации

В случае получения сообщения ЗЦМ для установления смешанного соединения (между оконечными пунктами разных частных сетей) в ЦЭС проводится проверка допустимости становления КВК между предлагаемыми оконечными пунктами. При допустимости соединения из ЦЭС в адрес запрашиваемого граничного ЦКП передаются сообщения – цепочки маршрутизации (ЦМ) всех путей маршрутизации КВК. Формат ЦМ включает следующие поля: тип сообщения; адрес граничного ЦКП абонентского доступа, запрашивающего в ЗЦМ цепочки физических адресов каждого из путей маршрутизации устанавливаемого КВК; цепочки маршрутизации всех путей КВК между указанными в ЗЦМ оконечными пунктами; пути маршрутизации сообщений ЦМ в граничный ЦКП, отправлявший запрос в ЗЦМ. Указанный формат сообщения ЦМ соответствует установлению КВК между оконечными пунктами одной и той же частной сети. В случае установления смешанного соединения (между оконечными пунктами разных частных сетей) в формат ЦМ включено дополнительное поле, указывающее на ЦКП, в котором на ЦКП 1.1, в котором обслуживаются пути обеих частных сетей устанавливаемого КВК. Это позволяет производить в этом ЦКП переключение КВК с одной частной сети на другую. Тип сообщения ЦМ отличается от КВК одной частной сети. Для надежности сообщения ЦМ передаются в ЦЭМ по нескольким путям маршрутизации. Если по истечении тайм-аута ответ ЦМ от ЦЭМ не получен граничный ЦКП повторно передает в ЦЭМ сообщение запроса ЗЦМ.

Все приведенные сообщения по установлению цепочек маршрутизации между граничным ЦКП и ЦЭС (ЗЦМ, ЦМ, отказ в установлении КВК) и сообщения между ЦКП и ЦЭС по коррекции состояния каналов должны подлежать канальному

шифрованию/дешифрации на каждом участке между смежными устройствами имитатора сети.

Выводы

Разработан для имитатора сети ПД категории специального назначения алгоритм формирования механизма маршрутизации от источника, что позволит решить сложную задачу построения объединенной сети ПД, включающей частные изолированные сети разных ведомств. В соответствии с ФЗ «О связи» эти сети предназначены для “обеспечения нужд государственного управления, обороны страны, безопасности государства и обеспечения правопорядка”.

Настоящая работа преподавателей и студентов кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана является продолжением создания аппаратно-программного имитатора такой сети ПД.

Литература

1. Матвеев В.А., Бельфер Р.А., Кравцов А.В. Анализ технологий построения сети передачи данных с высокими требованиями по информационной безопасности, н

а 2. Матвеев В.А., Басараб М.А, Бельфер Р.А., Кравцов А.В., Мерзляков Д.И. Алгоритм функционирования УЛС защищенной сети ПД на базе виртуальных каналов с в

ысокими требованиями к качеству обслуживания // Электросвязь. – 2017. – № 8. – С. 57–62.

н 3. Басараб М.А., Бельфер Р.А., Глинская Е.В., Кравцов А.В. Алгоритм ПО у

установления коммутируемого виртуального канала на абонентском доступе имитатора сети ПД с учетом обеспечения информационной безопасности // Первая миля. – 2017. – № 8. – С.64–69.

и 4. Дикер Палтуш Г. Сети АТМ корпорации Cisco. М.: Вильямс, 2004. 880 с.

5. Rufa G. Developments in Telecommunications. With a Focus on SS7 Network R

eliability //Springer, 2009. – 277 с.

6. Sengar, D. Wijesekera. S.Jajodia. Authentication and Integrity in telecommunication S

ignaling Network. Engineering of Computer-Based Systems,12th IEEE International C

onference and Workshops, pp. 163 – 170.

д 7. Yucun Yang1, Weiwei He 2, Suili Feng1. Security Analysis and Amendment of 3G C

ore Network Based on MTPsec, IEEE Pacific-Asia Workshop on Computational Intelligence a

nd Industrial Application, 2008, pp. 519-523.

ж 8. Бельфер Р.А., Горшков Ю.Г., Даннави М.Н. Последствия нарушений к

маршрутизации общеканальной сигнализации на функционирование сетей связи общего п

ользования, Вестник МГТУ им. Н.Э. Баумана сер. «Приборостроение», 2009 №3, С. 95-100.

9. Бельфер Р.А., Басараб М.А., Кравцов А.В., Алгоритмы коррекции таблицы маршрутизации в имитаторе сети ПД с обеспечением высокой надежности и безопасности, Электросвязь №6, 2018, С.63-66.

// Электросвязь. – 2017. – № 5. – С. 46–49.

Algorithm for generating routing from a source in a special purpose category PD network simulator

This scientific and practical work in the framework of the educational laboratory stand is a continuation of the creation of a simulator of a special-purpose data transmission network with high requirements for reliability, information security and other indicators. Foreign and domestic experts have noted the shortcomings in ensuring the reliability and safety of the routing mechanism at each switching node used in the common channel signaling data transmission SS7 in operation. This paper outlines the algorithm that is little used in public communication networks for a source-based routing mechanism and taking into account the peculiarities of building a special-purpose data transmission network.

УДК 004.056:336.7

Подход к управлению защитой информации в системах электронного банкинга

Бердюгин А.А.[9]

Актуальность темы исследования обусловлена недостатками качества управления информационной безопасностью в системах электронного банкинга. Приведена статистика количества DDoS-атак на банки и рассмотрена схема проведения DDoS-атак. Решена задача вероятностного анализа для определения закономерности компьютерных атак в рамках управления банковским операционным риском. Подчёркнута и обоснована необходимость использования десятипальцевого метода печати на клавиатуре для создания эффекта «лежачего полицейского» и оптимизации информационной безопасности. Применены анализ, синтез, методы аналогии и теории вероятностей.

Ключевые слова: информационная безопасность, банк, DDoS-атака, десятипальцевый метод печати

Постановка задачи

Банковский операционный риск – это вероятность возникновения убытков, причинами которых стали ненадёжность внутренних процедур управления рисками банка, халатность сотрудников, отказ автоматизированных систем либо воздействия внешних событий на функционирование банка (террористические акты, техногенные катастрофы и т.п.) [1-3]. Причиной расширения профиля операционного риска стало развитие систем электронного банкинга (СЭБ).

Не только финансовый, но и технический характер этих рисков требует использования различных методов анализа для оценки ожидаемых потерь от реализации операционного риска.

Активизация кибератак на СЭБ

Кибератаки на машины, банкоматы и кассовые аппараты нельзя отнести к числу техногенных катастроф, но они берут начало в опасной зоне. Причиной операционного риска может стать техногенная катастрофа. Но рассматривая операционный риск с точки зрения системного подхода, можно отнести этот риск как к банковским рискам, так и к техногенным рискам при недостаточной надёжности СЭБ. Надёжность в системе «Человек – Машина» (СЧМ), чем и являются СЭБ, – это показатель истинности (безошибочности) решения задачи, стоящей перед СЧМ. По статистическим данным она рассчитывается следующим образом:

$$P_{СЧМ} = 1 - \frac{m_{ОРЗ}}{N} \qquad (1)$$

где $m_{ОРЗ}$ – количество задач, решённых ошибочно, среди общего количества решаемых задач N [4-6].

В 2017-2018 годах возросло количество DDoS-атак на банки (90%), online-игры (142%), организации в сфере страхования (195%), букмекерские конторы (143%) и online-кассы (836%). В среднем в день по всему миру:

[9] Бердюгин Александр Александрович, Финансовый университет при Правительстве РФ, Москва, a40546b@gmail.com

- в 2016 было реализовано 100 кибератак DDoS;
- в 2017 году произошло 180 DDoS-атак;
- в 2018 году осуществлено 255 DDoS-атак[10].

Стандартная схема проведения DDoS-атаки изображена на рисунке 1.

Рис. 1. Стандартная схема реализации DDoS-атаки

Реализация DDoS-атак требует создания специализированных заражённых сетей троянских proxy-серверов, которые получают от злоумышленника экземпляр «мусорной» информации и адрес целевого ресурса. Затем через сервер-посредник ретранслируется команда на переполнение целевого сервера [4, 7].

Совершенствование информационной безопасности СЭБ

Компьютерная криминалистика (форензика) может использовать вероятностный анализ для определения закономерности кибератак. Пусть на банк «АВС» производятся крупные DDoS-атаки в среднем один раз в год. Стало известно, что на банк «АВС» произведены две независимые DDoS-атаки с интервалом в две минуты.

Обозначим через A реализацию первой DDoS-атаки, B – вторая DDoS-атака через две минуты после первой. Вероятность совместного наступления этих событий, в соответствии с теоремой умножения вероятностей $p(AB) = p(A) \cdot p(B \mid A)$, где $p(B \mid A)$ – условная вероятность второй DDoS-атаки при условии, что первая DDoS-атака произошла. Очевидно, что $p(A) < 1$. Отсюда следует, что $p(AB) < p(B \mid A)$.

Вычислим условную вероятность $p(B \mid A)$ с предположением, что распределение времени между DDoS-атаками это распределение является показательным.

Пусть время между двумя DDoS-атаками распределено по показательному закону. По условию интенсивность реализации DDoS-атак $\lambda = 1$ раз в год. Переведём интенсивность DDoS-атак на СЭБ и время между атаками в одну и ту же единицу времени – часы:

[10] Подробнее. В 2018 году число DDoS-атак на online-кассы возросло на 836%. URL: https://www.securitylab.ru/news/496859.php (дата обращения 8 декабря 2018 года).

$$\lambda = \frac{1}{365 \cdot 24} \text{ в час и } t = \frac{2}{60} \text{ час} \quad (2)$$

Вычислим произведение λt:

$$\lambda t = \frac{2}{365 \cdot 24 \cdot 60} \approx 3{,}8 \cdot 10^{-6} \quad (3)$$

Формула для вычисления условной вероятности реализации второй DDoS-атаки при условии, что за две минуты до неё была первая DDoS-атака, имеет вид:

$$p(B \mid A) = 1 - e^{-\lambda t} \quad (4)$$

Для показательной функции справедливо разложение в степенной ряд, ограниченное двумя членами разложения:

$$e^{-\lambda t} \approx 1 - \lambda t \quad (5)$$

Вычислим условную вероятность:

$$p(B \mid A) = \lambda t = 3{,}8 \cdot 10^{-6} \quad (6)$$

Поэтому вероятность совместного наступления двух событий может быть оценена неравенством:

$$p(AB) < 3{,}8 \cdot 10^{-6} \quad (7)$$

Таким образом, вероятность $p(AB) < 3{,}8 \cdot 10^{-6}$ близка к нулю. Поэтому событие AB следует признать практически невозможным. Тот факт, что это событие произошло, с точки зрения теории вероятностей означает: практически достоверно можно утверждать, что реализация двух DDoS-атак произошла не случайно[11] [8].

Нематематическим методом СМИБ, имеющим отношение к компьютерной грамотности пользователя объекта КИИ, является десятипальцевый метод печати на клавиатуре. Десятипальцевый метод печати требует разнородного распределения внимания на пальцах рук, что вызывает некоторые неудобства. Это выводит нас из зоны комфорта и, подобно «лежачему полицейскому», затрудняет неосознанное движение вперёд [9, 10].

Таким образом, десятипальцевый метод печати на клавиатуре предохраняет пользователей и менеджеров объекта КИИ от ошибок в информационной среде посредством совершенствования его моторики и способствует развитию СМИБ.

Выводы

Компьютерные атаки значительно расширяют профили типичных банковских рисков, а также могут нанести серьёзный урон бесперебойному функционированию СЭБ.

В статье решена задача вероятностного анализа совместной реализации DDoS-атак и рекомендован десятипальцевый метод печати на клавиатуре для совершенствования компьютерной грамотности пользователя объекта КИИ.

Достоверность научных решений подтверждается применением апробированных математических методов, опытом автора и других специалистов, предшествующими смежными исследованиями [4, 8, 11-13].

Литература

1. Probabilistic Modeling in System Engineering / By ed. A. Kostogryzov. – London: IntechOpen, 2018. 278 p.

2. Козьминых С.И. Математическое моделирование обеспечения комплексной

[11] Задача имеет реальные корни. 24 августа 2004 года произошли теракты в самолётах Ту-154 и Ту-134. Вылетев из аэропорта «Домодедово», лайнеры упали с разницей в три минуты. URL: https://ria.ru/20090824/182146689.html (дата обращения 8 декабря 2018 года).

безопасности объектов информатизации кредитно-финансовой сферы // Вопросы кибербезопасности. 2018. № 1 (25). С. 54–63.

3. Марков А.С. Модели оценки и планирования испытаний программных средств по требованиям безопасности информации//Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. 2011. № SPEC. С. 90-103.

4. Бердюгин А.А. Способ управления операционными рисками финансовой организации // Защита информации. Инсайд. 2018. № 2 (80). С. 78-81.

5. Ревенков П.В. Операционный риск в условиях возрастания кибератак на банки // Банковское дело. 2018. № 3. С. 56–60.

6. Тимошенков С.П. Надёжность технических систем и техногенный риск: учебник и практикум для бакалавриата и магистратуры / С.П. Тимошенков, Б.М. Симонов, В.Н. Горошко. М.: Издательство Юрайт, 2017. 502 с.

7. Julian Jang-Jaccard, Surya Nepal. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, Volume 80, Issue 5, August 2014, Pages 973–993. URL: https://doi.org/10.1016/j.jcss.2014.02.005.

8. Revenkov P.V., Berdyugin A.A. Human factor as a cause of risks in electronic banking services. CEUR Workshop Proceedings conference proceedings. 2017, pp. 122-126.

9. Хаммер Майкл, Лиза Хершман. Быстрее, лучше, дешевле: Девять методов реинжиниринга бизнес-процессов. М.: Альпина Паблишер, 2017. 352 с.

10. Клирфилд Крис, Тилчик Андраш. Неуязвимость. Отчего системы дают сбой и как с этим бороться. М.: Азбука-Аттикус, КоЛибри. 2018. 368 с.

11. Бердюгин А.А. Управление риском нарушения информационной безопасности в условиях электронного банкинга // Вопросы кибербезопасности. 2018. № 1 (25). С. 28-38.

12. Ревенков П.В., Бердюгин А.А. Расширение профиля операционного риска в банках при возрастании DDoS-угроз // Вопросы кибербезопасности. 2017. № 3 (21). С. 16-23.

13. Шеремет И.А. Направления подготовки специалистов по противодействию киберугрозам в кредитно-финансовой сфере // Вопросы кибербезопасности. 2016. № 5 (18). С. 3-7.

Научный руководитель: Ревенков Павел Владимирович, доктор экономических наук, профессор кафедры «Информационная безопасность», Финансовый университет при Правительстве РФ, Москва, email: pavel.revenkov@mail.ru.

Approach to Information Protection Managing in Electronic Banking Systems

Berdyugin A.A.[12]

Relevance of this research topic is due to the lack of quality management of information security in e-banking systems. The statistics of the number of DDoS-attacks on banks is given and the scheme of DDoS-attacks is considered. The probabilistic analysis problem to determine the pattern of computer attacks within the framework of banking operational risk management was solved. The necessity of using method of typing with ten-fingers on keyboard to create the effect of "speed bump" and optimize information security is emphasized and justified. Analysis, synthesis, methods of analogy and probability theory are applied.

Keywords: information security, bank, DDoS-attack, typing with ten-fingers method

[12] Berdyugin Alexander Alexandrovich, postgraduate student of the Department «Information Security», Financial University under the Government of the Russian Federation, Moscow. a40546b@gmail.com

УДК 681.3.067. **ББК 32.973.**

Психологические аспекты информационной безопасности

Валерий Васильевич Бондарев, кандидат военных наук, доцент Московского государственного технического университета им. Н. Э. Баумана.
bondarevvv@mail.ru

Рассматриваются вопросы практического психологического взаимодействия и сотрудничества в процессе защиты информации, приемы установления и поддержания психологического контакта, приемы социальной инженерии, теория конфликта, субъекты обеспечения информационной безопасности и их взаимодействие.
Ключевые слова: психология; информационная безопасность; инсайдер; нарушитель; защита информации; социальная инженерия; организационно-психологические меры защиты информации; мотивация.

Введение.

Почему пользователи записывают пароль на клочке бумаги и хранят его под клавиатурой или в ящике стола? Почему они не соблюдают правила ИБ? Почему руководство организации иногда очень сложно мотивировать потратить даже скромную сумму на ИБ? Почему с регуляторами/проверяющими/аудиторами сложно найти общий язык? Почему пользователи выбирают нестойкие пароли? Почему мы недооцениваем одни риски/угрозы и преувеличиваем другие?
Дать ответы на все эти вопросы может новое, ещё не до конца сформировавшееся направление в «классической» ИБ, которому и названия ещё нет. Обычно применяют такие термины, как «организационно-психологические аспекты ИБ», «информационно-психологическое направление в безопасности» и прочее.
Кроме того, есть и множество других направлений, в которых может помочь опытные профессионалы-психологи:

- понимание мотивации злоумышленников/нарушителей и поиск методов противодействия им;
- прогнозирование действий внутренних нарушителей;
- доведения до всех заинтересованных сторон (особенно руководства) актуальности ИБ;
- повышение осведомлённости в вопросах ИБ;
- формирование эффективной команды ИБ;
- эффективная работа с конечными пользователями, в частности, понимание действий пользователей.

Нужно отметить, что проблема информационно – психологических аспектов ИБ лежит в среде междисциплинарного взаимодействия: права, психологии, информационных технологий и «классической» ИБ.
Направления деятельности психологов в области ИБ: совершенствование практики подбора кадров, обращая особое внимание на выявление потенциальных инсайдеров; противодействие социальной инженерии; взаимодействие службы/администратора информационной безопасности с конечными пользователями; взаимодействие службы/администратора информационной безопасности с руководством организации.
Рассмотрим эти направления более подробно.

Совершенствование практики подбора кадров, обращая особое внимание на выявление потенциальных инсайдеров.

Сразу же необходимо отметить, что предлагаемая попытка выявить потенциальную склонность работника к инсайду не является чем-то из ряда вон выходящим. Подобные подходы практикуются и в других «родственных» областях. К примеру, глубоко обоснованная методика психологической диагностики профессиональной пригодности для работы в правоохранительной системе начала применяться более 15 лет назад в Российской Федерации. Одним из основных документов, регламентирующих психологическое тестирование в правовой практике России, является «Руководство по профессиональному психологическому отбору кандидатов на службу в органы прокуратуры Российской Федерации». В этом руководстве выделено пять факторов профессиональной пригодности, включающих соответствующие им комплексы профессионально важных качеств (ПВК): требуемый уровень социальной (профессиональной адаптации); достаточная нервно-психическая (эмоциональная) устойчивость; высокий уровень интеллектуального развития, познавательная активность; коммуникативная активность и компетентность; адекватные организаторские способности.
Но подбор кадров/выявление инсайдеров с учётом аспектов нарушений ИБ имеет свои особенности. Основные усилия необходимо сосредоточить на разработке модели нарушителя.
Конечно, данная модель нарушителя имеет слишком уж описательный характер, да и отталкиваться от профессии/возраста/пола и прочих «социально-демографических» характеристик работника, подозревая его на этом основании в принадлежности к инсайдерам, не стоит, так как это не слишком-то приблизит нас к требуемому результату. Поэтому для систематизации «всех и вся», выявления инсайдеров т отсеивания «подозрительных» соискателей можно и необходимо использовать различный инструменты. Например, опросник MBTI, основанного на идеях Карла Густава Юнга. Описывать применение этого опросника не будем. Суть: люди с одним психотипом, который выявлен при тестировании, могут оказаться более склонными к инсайду, чем с другим. Косвенным подтверждением этой мысли могут служить результаты исследования Эрика Шоу и Харли Стока «Индикаторы поведенческих рисков для выявления инсайдерских краж интеллектуальной собственности», в котором, в частности, описаны ключевые модели поведения, присущие инсайдерам, виновным в краже интеллектуальной собственности. Другими словами, для каждого психотипа существуют как достаточно полные описания, так и ключевые характеристики. Чем в большей степени человек им соответствует, тем ярче у него выражен тот или иной психотип. Но даже краткий перечень характеристик позволяет делать выводы о том, на что может оказаться способен человек.

Социальная инженерия
Самое эффективное, для чего применяется социальная инженерия, - это добыча информации.
Основным способом защиты от методов социальной инженерии является обучение сотрудников. Причём это обучение должно вестись с учётом рекомендаций психологов, учитывающих психотип обучаемого. Все работники компании должны быть предупреждены об опасности раскрытия персональной информации и конфиденциальной информации компании, а также о способах предотвращения утечки данных. Кроме того, у каждого сотрудника компании, в зависимости от подразделения и должности, должны быть инструкции о том, как

и на какие темы можно общаться с собеседником, какую информацию можно предоставлять для службы технической поддержки, как и что должен сообщить сотрудник компании для получения той или иной информации от другого сотрудника.

Взаимодействие администратора безопасности с конечными пользователями
Сотрудники организации являются самой массовой категорией нарушителей в силу их многочисленности, наличия у них санкционированного доступа на территорию, в помещения и к ресурсам системы, разнообразия мотивов совершения разного рода небезопасных действий. Причём подавляющее большинство нарушений со стороны сотрудников носит неумышленный характер. Однако, ущерб, который они при этом наносят организации, весьма значителен. Именно поэтому борьба с ошибками пользователей и обслуживающего персонала АС является одним из основных направлений работ по обеспечению безопасности.
Взаимодействие администратора безопасности с руководством организации
Какие конкретно формы и методы работы выбрать со своим руководителем, зависит от характера и темперамента этого руководителя. А характер и темперамент определяют его стиль, метод, тип руководства. Данный вопрос детально рассмотрен в работах американских психологов Р. Блэйк и Д.Моутон, в которых для определения типа менеджера разработана матрица типов руководителей. Подробности широко освещены в литературе и доступны для практического применения.

Кто же будет заниматься всем этим?
Вкратце алгоритм работы может быть примерно таким. HR-служба «прогоняет» сотрудника по определённому набору тестов. Информация передаётся в службу обеспечения ИБ. Зная, к какому типу принадлежит сотрудник, специалист в сфере обеспечения ИБ определяет его потенциальную склонность к инсайду (должны учитываться не только ключевые характеристики психотипа, но и другие переменные: выраженность предпочтений, склонность к риску, уровень социального интеллекта). Конечно, это примерный алгоритм. Как его реализовать – зависит от масштаба организации, предметной области, которой он функционирует, критичности ресурсов и ещё множества факторов.

Как использовать полученные результаты, например, результаты тестирования сотрудника? Здесь все достаточно просто. Если ваш работник – обладатель ярко выраженного психологического (соционического) типа, входящего в «группу риска», то за ним лучше всего «приглядывать». Другой пример – администратор безопасности с учётом типа руководителя организует общение с ним по вопросам обеспечения ИБ.

Что же касается достоверности результатов, здесь тоже нет сложностей. Описанный подход вряд ли способен полностью заменить профессиональный опыт руководителя, оценки экспертов, результаты применения других методов исследования личности. Но зато такие тесты могут компенсировать отсутствие достаточного профессионального опыта у вышеназванных лиц, оказать помощь в ситуации отсутствия экспертов и невозможности применить другие методы.

Выводы

Основной целью деятельности психологов совместно HR-службой, сотрудниками службы ИБ, юристами, «автоматизаторами» и т.д. - создание гармоничной среды, способствующей развитию сотрудников и всей организации в целом, что предполагает:

- улучшение психологического климата организации и повышение «боевого духа ее сотрудников», в том числе фокусирование усилий на защиту информации;
- совершенствование практики подбора кадров, обращая особое внимание на выявление потенциальных инсайдеров;
- оказание поддержки сотрудникам в развитии их способностей, в том числе таких, как запоминание паролей));
- сплочение коллектива в единую команду, стремящуюся парировать/нейтрализовать все угрозы безопасности по отношению к организации;
- устранение конфликтов, в первую очередь между пользователями и сотрудниками ИБ, между сотрудниками ИБ и сотрудниками ИТ;
- снижение текучести кадров, связанную с нарушениями режима ИБ;
- создание атмосферы доверия между сотрудниками ИБ и пользователями, добиваться, чтобы эти категории были союзниками, а не противниками по поддержанию режима ИБ;
- проведение разумной политики поощрения и наказания в организации, в том числе создания баланса между административным принуждением и сознательным выполнением регламентов ИБ;
- консультирование руководителей по психологическим аспектам деятельности организации в области ИБ;
- обучение руководителей и сотрудников психологическим технологиям взаимодействия и методам психологической защиты;

ЛИТЕРАТУРА

1. Бондарев В.В. Функционально-системный подход в подготовке специалиста в области информационной безопасности// Сборник трудов конференции. НУК ИУ МГТУ им. Н.Э. Баумана. М.: 2017.
2. Бондарев В.В. Учебное пособие. Введение в информационную безопасность автоматизированных систем//Москва. Издательство МГТУ им. Н.Э.Баумана. 2016 – 236 с.
3. ГОСТ Р ИСО/МЭК 27002 2012 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» (утвержден и введён в действие приказом Федерального агентства по техническому регулированию и метрологии от 24 сентября 2012 года №423-ст). Дата введения: 01.01.2014.
4. «О профессиональном психологическом отборе кандидатов на службу в органы прокуратуры Российской Федерации и обучение в государственные образовательные организации». Приказ Генеральной прокуратуры РФ от 15 сентября 2014 года № 493.

V.V.BONDAREV, P.H.D., Associated Professor

PSYCHOLOGICAL ASPECTS OF INFORMATION SECURITY

Keywords: psychology; Information Security; insider; the intruder; protection of information; social engineering; organizational and psychological measures to protect information; motivation; psychological monitoring; automated system; administrator; end user; psycho.

bondarevvv@mail.ru
964-707-72-28

УДК 004.056 : 519.832.2

Алгоритм поиска седловой точки в смешанных стратегиях на основе модификации метода Брауна-Робинсона для решения задачи выбора защищаемых объектов

Быков А.Ю.[13], **Крыгин И.А.** [14], **Гришунин М.В.** [15]

Представлена игровая постановка задачи выбора объектов для защиты и для нападения двух игроков – защитника и нападающего с учетом их ограниченных ресурсов. Постановка задачи является антагонистической игрой с конечными стратегиями, каждый игрок должен решить свою задачу булевого программирования при фиксированном решении другого игрока. Игра может быть сведена к матричной игре большой размерности. Для поиска седловой точки в смешанных стратегиях может быть применен метод Брауна-Робинсона, но он требует явного построения матрицы игры. Предложена модификация этого метода без явного построения матрицы игры, на начальных шагах алгоритма решается задача булева программирования для каждого игрока, на последующих шагах для снижения вычислительной трудоемкости используются результаты решения задач, полученные на начальных шагах. Представлен пример решения задачи.

Ключевые слова: информационная безопасность, теория игр, матричная игра, дискретная оптимизация

Введение

При решении различных задач защиты информации часто используется подход на основе теории игр. Как правило, рассматриваются два игрока: сторона защиты и сторона нападения [1-6]. Рассмотрим задачу выбора объектов для защиты и выбора объектов для атаки. Игра является игрой с нулевой суммой. Задача может быть сведена к матричной игре большой размерности. Предложен алгоритм, позволяющий находить седловую точку в смешанных стратегиях, на основе модификации метода Брауна-Робинсона без построения матрицы в явном виде, так как построение матрицы может требовать значительных вычислительных ресурсов. Некоторые похожие примеры подобных игровых задач представлены в [7-9].

1. Постановка задачи выбора игроками объектов для защиты и атаки

1.1. Исходные данные

1. $Z = \{z_1, z_2, \ldots, z_m\}$ – множество защищаемых объектов, $M = \{1,2,\ldots,m\}$ – множество индексов этих объектов.
2. $R = \{r_1, r_2, \ldots, r_l\}$ – множество ограниченных ресурсов стороны защиты, $L = \{1,2,\ldots,l\}$ – множество индексов этих ресурсов.
3. $N = \{n_1, n_2, \ldots, n_s\}$ – множество ограниченных ресурсов стороны нападения, $S = \{1,2,\ldots,s\}$ – множество индексов этих ресурсов.

[13] Быков Александр Юрьевич, доцент, кандидат технических наук, МГТУ им. Н.Э. Баумана, Москва, abykov@bmstu.ru

[14] Крыгин Иван Александрович, МГТУ им. Н.Э. Баумана, Москва, krygin.ia@gmail.com

[15] Гришунин Максим Вадимович, МГТУ им. Н.Э. Баумана, Москва, grishunin-mv@ya.ru

Параметры элементов множеств и отношений между ними

1. $w_i \geq 0,\ \forall\ i \in M$ – средний ущерб при нарушении безопасности *i*-го объекта.
2. $p_{np\,i} \in [0,1], \forall i \in M$ – вероятность предотвращения атаки на *i*-ый объект при его защите.
3. $a_{ki} \geq 0, \forall k \in L, i \in M$ – значение *k*-го ограниченного ресурса, используемого для обеспечения защиты *i*-го объекта.
4. $b_k \geq 0, \forall k \in L$ – максимальное значение *k*-го ограниченного ресурса.
5. $c_{ki} \geq 0, \forall k \in S, i \in M$ – значение *k*-го ограниченного ресурса стороны нападения, используемого для атаки на *i*-ый объект.
6. $d_k \geq 0, \forall k \in S$ – максимальное значение *k*-го ограниченного ресурса стороны нападения.

1.2. Искомые параметры

Введем переменную $x_i \in \{0,1\}, \forall i \in M$, $x_i = 1$, если *i*-ый объект защищается, $x_i = 0$ – в противном случае. Переменные образуют вектор $X = [x_1, x_2, ..., x_m]^T$. Введем переменную $y_i \in \{0,1\}, \forall i \in M$, $y_i = 1$, если *i*-ый объект подвергается атаке, $y_i = 0$ – в противном случае. Переменные образуют вектор $Y = [y_1, y_2, ..., y_m]^T$.

1.3. Показатели игроков

Для игры с нулевой суммой показатели качества двух игроков определяются ущербом стороны защиты. Средний ущерб:

$$U(X,Y) = U_{max}(Y) - U_{np}(X,Y) = \sum_{i \in M} w_i y_i - \sum_{i \in M} p_{pr\,i} w_i x_i y_i, \quad (1)$$

где: $U_{max}(Y) = \sum_{i \in M} w_i y_i$ – максимальный ущерб, который может быть при отсутствии защиты, $U_{np}(X,Y) = \sum_{i \in M} p_{pr\,i} w_i\, x_i y_i$ – предотвращенный ущерб.

Сторона защиты желает этот показатель минимизировать, а сторона нападения максимизировать.

1.4. Ограничения

Система ограничений на ресурсы защитника:

$$\Delta_{don}^{(X)}: \left\{ \sum_{i \in M} a_{ki} x_i \leq b_k, \forall k \in L. \right. \quad (2)$$

Система ограничений на ресурсы нападающего:

$$\Delta_{don}^{(Y)}: \left\{ \sum_{i \in M} c_{ki} y_i \leq d_k, \forall k \in S. \right. \quad (3)$$

Каждый из игроков решает задачу линейного булевого программирования при фиксированном решении другого игрока.

2. Модифицированный алгоритм на основе метода Брауна-Робинсона

Можно построить платежную матрицу игры в явном виде. Для этого необходимо перебрать все допустимые решения с максимальным числом единиц защитника и нападающего. Пусть решения защитника в матрице задают столбцы,

а решения нападающего задают строки. Элементами матрицы являются значения показателя (1) в условных единицах. Если размерности векторов X и Y равны 5, возможный вариант матрицы (табл.1).

Таблица 1.

Возможный вариант представления матрицы игры

Решения нападающего	**Решения защитника**					
	$[1,1,0,0,0]$	$[1,0,1,0,0]$	$[1,0,0,0,1]$	$[0,1,1,0,0]$	$[0,1,0,0,1]$	$[0,0,0,1,1]$
$[1,0,0,0,1]$	1660	1660	593	3190	2120	2120
$[0,1,0,0,0]$	385	3740	3740	385	385	3740
$[0,0,1,1,0]$	5940	2990	5940	2990	5940	4730
$[0,0,0,1,1]$	3330	3330	2260	3330	2260	1060

В модификации алгоритма не будем строить матрицу игры в явном виде. На каждом из шагов алгоритма будем последовательно решать оптимизационные задачи для защитника и нападающего. Для расчета суммарного выигрыша или проигрыша введем вещественные вектора размерности m: $X_{сум}, Y_{сум}$. Для расчета среднего решения для игроков введем вещественные вектора размерности m: $X_{сред}, Y_{сред}$. Решения задач сохраняются в списках решений игроков для последующего расчета частот появления этих решений.

Шаг 0. Полагаем $X_{сум} = [0,0,...,0]^T$, $Y_{сум} = [0,0,...,0]^T$, $X_{сред} = [0,0,...,0]^T$, $Y_{сред} = [1,1,...,1]^T$, $k_x = 0$, $k_y = 0$; где k_x – число полученных решений защитником, k_y – число полученных решений нападающим. $Y_{сред}$ – будем считать начальным решением нападающего. Создаем два решений списка: защитника и нападающего, изначально эти списки пустые. В списках хранятся найденные решения игроков, для каждого решения задан счетчик, содержащий значение числа повторений решения.

Шаг i-ый ($i = 1,3,5,...$, нечетный шаг). Решаем оптимизационную задачу защитника методом булевого программирования [10], находим оптимальный вектор $X^{(i)}$ и значение показателя $F_з^{(i)} = U\left(X^{(i)}, Y_{сред}\right)$, полагаем $k_x = k_x + 1$. Если найденное решение находится в списке решений защитника, счетчик для этого решения увеличивается на 1. Если решения нет в списке, помещаем его в список, значение счетчика для этого решения равно 1. $X_{сум} = X_{сум} + X^{(i)}$, $X_{сред} = X_{сум} / k_x$.

Шаг $(i+1)$-ый (четный шаг). Решаем оптимизационную задачу нападающего, находим оптимальный вектор $Y^{(i)}$ и значение показателя $F_н^{(i)} = U\left(X_{сред}, Y^{(i)}\right)$, полагаем $k_y = k_y + 1$. Если найденное решение находится в списке решений нападающего, счетчик для этого решения увеличивается на 1. Если решения нет в списке, помещаем его в список, значение счетчика для этого решения равно 1. $Y_{сум} = Y_{сум} + Y^{(i)}$, $Y_{сред} = Y_{сум} / k_y$. Проверяем критерий остановки: если $\left|F_з^{(i)} - F_н^{(i)}\right| < \xi$, то переходим к заключительному шагу, в противном случае, полагаем $i = i + 2$ и переходим к нечетному шагу.

Шаг заключительный. Для каждого из решений, находящихся в списках защитника и нападающего, определяем частоты их появлений, для этого значение

счетчика решения делим на k_x – для защитника и на k_y – для нападающего.

Основной недостаток предложенного алгоритма в том, что на каждом шаге требуется решать оптимизационные задачи, это требует существенных вычислительных ресурсов. Модифицируем алгоритм. В случае если получено N решений, которые уже есть в списках защитника и нападающего (на N шагах не получено новых решений), то оптимизационную задачу не решаем, а ищем оптимальное решение в существующем списке решений, размерность которого относительно невелика методом перебора.

3. Пример решения задачи

Пусть задано 8 объектов защиты, например, узлов сети. Значения ущерба и вероятности защиты объектов (табл.2).

Таблица 2.

Значение ущерба и вероятностей защиты объектов

Номер объекта	1	2	3	4	5	6	7	8
Значения w_i, в у.е.	4000	10000	3000	9000	5000	9500	10000	8000
Значения $p_{пр\,i}$	0.80	0.99	0.70	0.95	0.85	0.90	0.50	0.92

У защитника и нападающего по 4 вида ресурсов, примеры параметров ограничений для защитника и нападающего (табл.3).

Таблица 3.

Параметры системы ограничений на ресурсы защитника и нападающего

Параметры ограничений защитника									
№ ограничения	**Значения коэффициентов в левых частях ограничений для защитника, a_{ki}**								**Значения b_k**
1	100	1000	200	900	400	500	1200	1100	3000
2	0.03	0.30	0.05	0.15	0.30	0.30	0.35	0.10	0.70
3	0.05	0.20	0.20	0.25	0.30	0.10	0.33	0.35	0.60
4	0.01	0.05	0.02	0.05	0.02	0.01	0.01	0.01	0.20
Параметры ограничений нападающего									
№ ограничения	**Значения коэффициентов в левых частях ограничений для нападающего, c_{ki}**								**Значения d_k**
1	50	600	60	500	100	120	1000	550	1500
2	0.02	0.20	0.05	0.25	0.35	0.30	0.30	0.15	0.80
3	0.02	0.30	0.30	0.35	0.40	0.15	0.35	0.30	0.80
4	0.15	0.10	0.20	0.05	0.20	0.10	0.10	0.10	0.50

Результаты решения задачи предложенным алгоритмом представлены в (табл.4). При этом для критерия остановки использовалось достижение 0.01 % относительной погрешности в оценке значения показателя качества.

Таблица 4.

Результаты решения задачи предложенным алгоритмом

№ п/п	**Решение**	**Оценка вероятности**
	Решения для защитника X (достигнутое значение показателя 15031.326)	
1	1 1 1 0 0 1 0 0	0.472
2	0 0 0 1 0 0 1 0	0.000
3	1 0 1 1 0 1 0 0	0.349
4	1 0 0 0 0 1 0 1	0.000

5	1 1 0 0 0 0 1 0	0.008
6	1 0 0 0 0 1 1 0	0.146
7	1 1 0 1 0 0 0 0	0.025
Решения для нападающего Y (достигнутое значение показателя 15032.822)		
1	0 0 0 1 0 0 1 0	0.317
2	1 1 0 0 0 1 0 1	0.318
3	0 0 0 1 0 1 0 1	0.051
4	1 0 0 0 1 0 1 0	0.313

Решения с оценками вероятности менее 0.01 можно исключить, тогда остаются по 4 решения у защитника и нападающего. Решение задачи точным алгоритмом на основе сведения к задаче линейного программирования продемонстрировало подобные результаты. Размер исходной матрицы игры для примера составил 23 × 16.

Выводы

Исследована игровая задача выбора объектов (или активов) для защиты защитником и выбора объектов (активов) для атак нападающим, задачу можно свести к матричной игре большой размерности. Разработан модифицированный алгоритм поиска решения игры в смешанных стратегиях на основе идей алгоритма Брауна-Робинсона без построения матрицы игры в явном виде, что экономит вычислительные ресурсы.

Для снижения вычислительной сложности алгоритма предлагается решать оптимизационные задачи на начальных шагах алгоритма, на последующих шагах используются результаты, полученные ранее.

Достоверность полученных решений подтверждается их проверкой решением задачи точным методом, основанном на сведении игры к решению задачи линейного программирования.

Литература

1. Савченко С. О., Капчук Н. В.. Алгоритм построения модели нарушителя в системе информационной безопасности с применением теории игр // Динамика систем, механизмов и машин. 2017. Т. 5. № 4. С. 84-89. DOI: 10.25206/2310-9793-2017-5-4-84-89

2. Фёдоров С.Ю., Хализев В.Н. Модель выбора набора средств интегрированных систем безопасности на основе позиционной игры // Научные труды Кубанского государственного технологического университета. 2018. № 3. С. 58-65.

3. Zhen Ni, Qianmu Li, Gang Liu. Game-Model-Based Network Security Risk Control. Computer. 2018. Vol. 51. Iss. 4. P. 28-38. DOI: 10.1109/MC.2018.2141032

4. Hao Wu, Wei Wang. A Game Theory Based Collaborative Security Detection Method for Internet of Things Systems. IEEE Transactions on Information Forensics and Security. 2018. Vol.13. Iss. 6. P. 1432 – 1445. DOI: 10.1109/TIFS.2018.2790382

5. Hao Hu, Yuling Liu, Hongqi Zhang, Ruixuan Pan. Optimal Network Defense Strategy Selection Based on Incomplete Information Evolutionary Game. IEEE Access. 2018. Vol. 6 P. 29806 – 29821. DOI: 10.1109/ACCESS.2018.2841885

6. Mauro Barni, Benedetta Tondi. Adversarial Source Identification Game With Corrupted Training. IEEE Transactions on Information Theory. 2018. Vol. 64. Iss. 5. P. 3894 – 3915. DOI: 10.1109/TIT.2018.2806742

7. Быков А. Ю., Алтухов Н. О., Сосенко А. С. Задача выбора средств защиты информации в автоматизированных системах на основе модели антагонистической

игры // Инженерный вестник МГТУ им. Н.Э. Баумана. Электрон. журн. 2014. № 4. Режим доступа: http://engbul.bmstu.ru/doc/708106.html

8. Быков А. Ю., Шматова Е.С. Алгоритмы распределения ресурсов для защиты информации между объектами информационной системы на основе игровой модели и принципа равной защищенности объектов // Наука и образование: научное издание. 2015. № 9. DOI: 10.7463/0915.0812283.

9. Быков А.Ю., Крыгин И.А., Муллин А.Р. Алгоритм распределения ресурсов системы защиты между активами мобильного устройства на основе игры с нулевой суммой и принципа равной защищенности // Вестник МГТУ им. Н.Э. Баумана. Приборостроение. 2018. № 2. С. 48- 68. DOI: 10.18698/0236-3933-2018-2-48-68

10. Басараб М.А., Вельц С.В. Методы оптимизации и исследование операций в области информационной безопасности. М.: МГТУ им. Н.Э. Баумана, 2015. 64 с. Режим доступа: http://ebooks.bmstu.press/catalog/117/book967.html

The algorithm of saddle point search in mixed strategies based on Brown–Robinson method modification to solve problem of assets to protect selection

Bykov A.Yu. [16]**, Krygin I.A.** [17]**, Grishunin M.V.** [18]

Abstract. In this article the game formulation of assets to protect and assets to attack selection is presented. There are two players in this game – defender and attacker, and both have limited counting resources. It's a zero-sum game with finite strategies, each player must solve his own boolean programming task with fixed opponent solution. This game may be come down to high dimension matrix game. The Brown-Robinson algorithm may be applied to find the saddle point in mixed strategies, but it requires explicit game matrix creation. A modification of this method without explicit without explicit matrix creation is suggested. On initial stage of algorithm, a boolean programming task is solved for each player. On next stages the results of previous computations is used. An example of problem solution is presented.

Keywords: information security, game theory, matrix game, discrete optimization

[16]Aleksandr Bykov, Associated Professor, Ph.D., Bauman Moscow State Technical University, Moscow, abykov@bmstu.ru

[17]Ivan Krygin, Bauman Moscow State Technical University, Moscow, krygin.ia@gmail.com

[18]Maksim Grishunin, Bauman Moscow State Technical University, Moscow, grishunin-mv@ya.ru

УДК, 004.912

Современные ручные шифры и их использование в учебных курсах по криптографии на примере шифра Elsiefour

Варфоломеев А.А.[19]

Аннотация

Рассматриваются современные ручные шифры (hand cipher, pencil and paper cipher) на примере шифра ElsieFour. Дается автоматная модель данного шифра. Предлагаются модификации функции перехода состояний и функции выхода, повышающие стойкость и эффективность реализации. Данные модификации позволяют индивидуализировать задания для групп студентов по изучению алгоритмов шифрования и по разработке методов их анализа. Дается обобщение данного шифра, упрощающее процесс ручного шифрования.

Ключевые слова:

Ручные шифры, шифрующие автоматы, стойкость, криптография.

Введение.

Обычно в курсах по криптографии основное внимание уделяется современным алгоритмам шифрования и стандартам на их основе, таким как GOST, AES и прочим [1-3]. Для них легко можно найти в Интернете и программные реализации и контрольные примеры. Их использование предполагает наличие вычислительной техники и соответствующего программного обеспечения. Что в некоторых ситуациях может отсутствовать. Другие аргументы для разработки так называемых ручных шифров приводятся в работах их создателей.

Все исторические шифры (шифр Цезаря, квадрат Полибия, шифр Вижинера, …) предполагают наличие только карандаша (пера) и бумаги, а иногда некоторых подсобных средств. Описание исторических шифров широко известно даже для старших школьников и интерес к ним небольшой. Стойкость их тоже известна.

В настоящее время периодически появляются описания ручных шифров, отличающихся от исторических шифров повышенной стойкостью и удобством процессов зашифрования и расшифрования. Как правило они используют некоторые доступные или легко воспроизводимые подручные средства типа колоды игральных карт, таблиц. Примерами таких ручных шифров могут являться шифр Solitaire [4, 5], шифр Merdek [6], рассматриваемый здесь ElsieFour [7] и другие [8]. Эти шифры менее известны, чем исторические, а их изучение может помочь в изучении криптографии.

Описание шифра. Автоматная модель.

Шифр ElsieFour предложен в 2017 году в работе [7]. Здесь же можно найти его подробное описание и контрольные примеры. В основе лежит использование 6 x 6 таблицы (матрицы), элементы которой являются знаками английских букв и символов # _ 2 3 4 5 6 7 8 9 a b c d e f g h i j k l m n o p q r s t u v w x y z, пронумерованных целыми числами от 0 до 35. Ключ – начальный вид таблицы. Далее вид таблицы изменяется при шифровании каждого знака открытого текста: циклически сдвигается вправо одна строка и циклически сдвигается вниз один столбец.

Inputs: State matrix S; indexes i, j; a sequence of plaintext characters, P

[19] Варфоломеев Александр Алексеевич, канд. физ.-мат. н, доцент, МГТУ им. Н.Э. Баумана

Output: A sequence of ciphertext characters, C.

Algorithm: For each plaintext character P:

1. r ← row of S in which P appears ($0 \le r \le 5$)
2. c ← column of S in which P appears ($0 \le c \le 5$)
3. x ← (r + (S[i][j] / 6)) mod 6
4. y ← (c + (S[i][j] mod 6)) mod 6
5. C ← S[x][y]; output C
6. Right-rotate row r of S
7. Down-rotate column y of S
8. i ← (i + (C / 6)) mod 6
9. j ← (j + (C mod 6)) mod 6

The “Right-rotate row r” subroutine is:

10. (S[r][0], S[r][1], S[r][2], S[r][3], S[r][4], S[r][5]) ← (S[r][5], S[r][0], S[r][1], S[r][2], S[r][3], S[r][4])
11. c ← (c + 1) mod 6
12. If x = r: y ← (y + 1) mod 6
13. If i = r: j ← (j + 1) mod 6

The “Down-rotate column y” subroutine is:

14. (S[0][y], S[1][y], S[2][y], S[3][y], S[4][y], S[5][y]) ← (S[5][y], S[0][y], S[1][y], S[2][y], S[3][y], S[4][y])
15. x ← (x + 1) mod 6
16. If c = y: r ← (r + 1) mod 6
17. If j = y: i ← (i + 1) mod 6

Строки из [7, 5-6 стр.] пронумерованы для удобства ссылок.

Шифрующий автомат определяется множеством знаков входного алфавита (открытого текста), множеством знаков выходного алфавита (шифрованного текста), множеством внутренних состояний, функцией перехода состояний и функцией выхода. Внутренне состояние автомата в момент времени t это значение 6x6 матрицы {S_t [k][l]}, (k,l из интервала [0,5]) и двух ячеек памяти i(t) и j(t), принимающих значения от 0 до 5. Каждый элемент матрицы является знаком входного алфавита и встречается в матрице один раз. Начальное состояние матрицы – ключ. Число ключей равно 36!.

Функция выхода определяется приведенными выше шагами 1-5.

1. r(t) ← row of {S_t [k][l]} in which P(t) appears ($0 \le r \le 5$)
2. c(t) ← column of {S_t [k][l]} in which P appears ($0 \le c \le 5$)
3. x (t)← (r(t) + (S_t [i(t)][(j(t)] / 6)) mod 6
4. y(t) ← (c(t) + (S_t [i(t)][j(t)] mod 6)) mod 6
5. C(t) ← S_t [x(t)][y(t)]; output C.

Функция перехода состояний определяется сложными шагами 6-7 и 8-9.

Матрица {S_t [k][l]} переходит в матрицу {S_(t+1) [k][l]} после шагов 6 и 7, точнее 10 и 14 (Шаги 11-13 и 15-17, входящие в 6 и 7 не влияют на состояние матрицы).

Сложнее с получением i(t+1) и j(t+1). Если бы не было шагов 11-13 и 15-17, то выполнялись бы соотношения

8. i(t+1) ← (i(t) + (C(t) / 6)) mod 6
9. j(t+1)← (j(t) + (C(t) mod 6)) mod 6.

Однако шаги 11-13 и 15-17 могут изменить эти соотношения в случае

выполнения условий

11. c(t) ← (c(t) + 1) mod 6
12. If x(t) = r(t): y(t) ← (y(t) + 1) mod 6
13. If i(t) = r(t): j(t) ← (j(t) + 1) mod 6

и

15. x(t) ← (x(t) + 1) mod 6
16. If c(t) = y(t): r (t)← (r(t) + 1) mod 6
17. If j(t) = y(t): i(t) ← (i(t) + 1) mod 6

В этом случае i(t+1) и j(t+1) могут измениться на 1. Функция перехода состояний является реверсивной и при расшифровании производятся циклические сдвиги строки и столбца, а далее учитывается изменение ячеек i(t) и j(t).

Модернизация алгоритма шифрования.

Модернизаций – изменений алгоритма можно предложить множество. Например, с более сильным перемешиванием состояния при переходе к зашифрованию следующей буквы открытого текста. Но следует обратить внимание на шаги 11-13 и 15-17 алгоритма. Шаги 15-17 получены автоматически из шагов 11-13 заменой c и x, r и y, i и j. Шаг 11 влияет на шаг 16, но в результате изменяется значение r, которое обновляется далее не зависимо от этих шагов. Шаг 15 тоже не влияет на процесс. Он влиял бы, если бы шел до шага 12. Значение i меняется только от шага 13 (вероятность 1/6), значение j только от шага 17 (вероятность 1/6).

Если, например, поменять шаг 12 на 12` вида: If x = r: i ← (i + 1) mod 6, то на i будет влиять как шаг 13, так и шаг 12`. Аналогично с заменой шага 16 на 16` вида: If c = y: j ← (j + 1) mod 6, на j будет влиять как шаг 17, так и шаг 16`. Вариантов много, все требуют отдельного рассмотрения.

Обобщение алгоритма шифрования.

При практическом использовании шифра ElsieFour обращает на себя внимание размер таблицы, при котором возникают ошибки при сдвиге больших строк и столбцов. Размер матрицы 6 на 6 можно сделать параметром и уменьшать его до разумных пределов или увеличивать, по аналогии с обобщениями шифра Solitaire в работе [5]. Таблица 5 на 5 более удобна при ручном шифровании, а число различных ключей равен 25! = 15,5 10^24 (log (25!) = 83,68). А вариант шифра с таблицей 4 на 4 дает размер ключа в 44 бита (log 16!), подходящий для безлицензионного использования. У оригинального шифра ElsieFour размер ключа равен 138 битам.

Существенным является изменение размера алфавитов открытого и шифрованного текстов. Но это можно сделать простыми способами кодирования текстов в нужных алфавитах.

Вывод.

Современные ручные шифры обеспечивают достаточно высокую стойкость по сравнению с многими историческими ручными шифрами. Они являются важным источником для составления домашних заданий и курсовых проектов для студентов по курсу криптографии.

Созданный в 2017 году шифр ElsieFour требует модификации функции перехода состояний шифрующего автомата. Возможное обобщение алгоритма шифра на другие модули позволит повысить его эксплуатационные свойства или криптографическую стойкость.

Литература

1. Varfolomeev A.A. About some perspective training cryptography disciplines. In: В сборнике: CEUR Workshop Proceedings conference proceedings. 2017. V. 2081. P. 135-138.

2. Варфоломеев А.А. О некоторых перспективных учебных дисциплинах по криптографии // В сборнике: Безопасные информационные технологии Сборник трудов Восьмой всероссийской научно-технической конференции. НУК «Информатика и системы управления». Под. ред. М.А.Басараба. 2017. С. 98-101.

3. Шеремет И.А. Направления подготовки специалистов по противодействию киберугрозам в кредитно-финансовой сфере // Вопросы кибербезопасности. 2016. № 5 (18). С. 3-7 DOI: 10.21681/2311-3456-2016-5-3-7

4. Schneier B. The Solitaire Encryption Algorithm. 1999.

5. Варфоломеев А.А. Пудовкина М.А., О цикловой структуре алгоритма поточного шифрования Solitare фирмы Counterpane. Безопасность информационных технологий (БИТ), № 4, М.: МИФИ, 1999, с. 93 – 99.

6. Crowley P. Mirdek: a card cipher inspired by “Solitaire.” January 13, 2000. http://www.ciphergoth.org/crypto/mirdek/, retrieved February 2, 2015.

7. ElsieFour: A Low-Tech Authenticated Encryption Algorithm For Human-to-Human Communication. ePrintArchive. 2017-339.

8. Kallick B. Handycipher: a Low-tech, Randomized, Symmetric-key Cryptosystem. 2014.

Modern pancil and paper ciphers and their use in educational courses on cryptography on the example of Elsiefour cipher

Varfolomeev A.A., Ph.D.

Abstract.

We consider modern hand ciphers (hand cipher, pencil and paper cipher) on the example of the ElsieFour cipher. An automaton model of this cipher is given. Modifications of the state transition function and exit function are proposed, which increase the security and efficiency of the implementation. These modifications make it possible to individualize tasks for groups of students to study encryption algorithms and to develop methods for analyzing them. A generalization of this cipher is given, which simplifies the process of manual encryption.

Keywords: hand cipher, pencil and paper cipher, security, cryptography.

УДК 629.7.017.1

Специфика конструирования бортовой аппаратуры модульной авионики с учетом требований информационной безопасности

Глинская Е.В., Чичварин Н.В.[20]

В материалах публикации представлены результаты теоретико – экспериментальных исследований особенностей конструкций интегральной модульной авионики (ИМА). Проблематика работы заключается в поисках обеспечения конструктивных элементов ИМА защитой от вредоносного воздействия стороннего электромагнитного излучения. При этом учитываются различные аспекты электромагнитной совместимости (ЭМС) основных компонент и узлов бортовой радиоэлектронной аппаратуры и вычислительных средств летательного аппарата (ЛА). Показано, что для расчета защищенности элементов конструкции полезно строить математическую модель конструкции и узлов ЛА. При этом воздействие электромагнитного излучения необходимо моделировать на основе уравнений Максвелла, и их следствий а не путем применения приближенных полуэмпирических формул. Решение уравнений Максвелла осуществляется за счет применения численного метода конечных разностей. В работе показана возможность применения модели электромагнитного излучения на основе положений скалярной теории дифракции. Принятие проектных решений необходимо ориентировать на создание интеллектуально емкой и быстро модифицируемой технологии создания авиационного электронного оборудования, существенно снижающей издержки на разработку, производство, эксплуатацию и обслуживание оборудования за счет конструктивно-аппаратных (миниатюризация и избыточность) и программно-алгоритмических (локализация отказов и реконфигурация комплекса в реальном времени) решений.

Ключевые слова: авионика, бортовая аппаратура, безопасность, информация, конструкция, летательный аппарат, проектирование.

Введение

Анализ обзоров доступной литературы показывает, что проблема безопасности полетов нарастает [1-6]. По мнению специалистов, в условиях повышения уровня автоматизации перспективных авиационных двигателей, бортового оборудования, систем и агрегатов летальных аппаратов, возрастания сложности бортовых информационных систем существенное значение приобретает проблема защиты автоматизированных систем авиационной техники от угроз информационной безопасности. Источниками подобных угроз являются:

беспроводные информационно-телекоммуникационные устройства пассажиров, находящиеся на борту ЛА во время полета,

информационные атаки внешних злоумышленников по беспроводным каналам передачи данных, обеспечивающим доступ к бортовой вычислительной сети,

помехи, случайно, либо умышленно поставленные с помощью средств радиоэлектронной борьбы (РЭБ),

наводки от внутренних бортовых источников электромагнитного излучения.

[20] Волосатова Тамара Михайловна, **к**андидат технических наук, доцент кафедры «САПР» МГТУ им. Н. Э. Баумана», Москва, e-mail tamaravol@gmail.com.
Чичварин Николай Викторович, кандидат технических наук, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, Москва, e-mail genrih.gertz@gmail.com.

Анализ доступных источников показывает также, что переход к ИМА позволил перейти от идеи «система — одна функция» к мультифункциональной структуре — «много функций в одном». Технически проще решить такую проблему, если разделить аппаратные и программные платформы, т.е. сделать их независимыми от вычислительного ядра. Практически интеграция функций, которые ранее воспринимались как интеграция систем, сводится в новом поколении КБО к созданию БД функций и сигналов, а также коммуникатора функций на уровне программного обеспечения.

Потребность снизить стоимость авиационных комплектующих за счет расширения числа производителей и эксплуатационную эффективность за счет более мелкого, чем блок, сменяемого в эксплуатации элемента объективно привела в новом поколении комплекса бортового оборудования (КБО) к модульности аппаратного и программного обеспечений.

К основным унифицированным комплектующим следует отнести: базовую несущую конструкцию крейта, процессорный модуль общего назначения, модуль сетевого коммутатора, модуль концентратора сигналов, модуль оптического/электрического конвертора, модуль электропитания, индикаторы с графическими процессорами и индикационные панели. В качестве аппаратных компонентов, входящих в состав комплектующих вычислительного ядра, определены: базовая несущая конструкция сменного модуля, мезонины — графического контроллера, массовой памяти и ввода/вывода. Внедрение концепции ИМА в перспективных объектах авиационной техники предполагает разделение функциональных компонентов авионики на три иерархических уровня:

нижний уровень - унифицированные конструктивно-функциональные модули различного назначения, имеющие собственные вычислительные средства в компактном стандартизованном исполнении;

средний уровень - мультипроцессорные вычислительные системы, создаваемые из модулей нижнего уровня, конструктивно выполненные

в стандартизованном корпусе;

верхний уровень - бортовая локальная вычислительная сеть, интегрирующая вычислительные средства систем среднего уровня на основе центрального сетевого интерфейса высокой пропускной способности.

Любое изменение как аппаратной, так и программной части изделия, требует значительных затрат на повторное прохождение процесса сертификации.

Высокий уровень развития микроэлектронных технологий, широкое распространение программируемых логических интегральных схем (ПЛИС) и специализированных интегральных схем (Application Specific Integrated Circuit - ASIC) позволяют проектировать перспективные устройства на базе полностью аппаратных средств без применения программного обеспечения (ПО). Очевидно, что разработка и особенно конструирование подобных объектов проектирования требует новых подходов.

Цель исследований и решаемые задачи при подготовке рукописи

Целью исследований, основные результаты которых является разработка принципов конструирования аппаратно-программных средств с учетом требований обеспечения информационной безопасности. Для достижения поставленной цели последовательно решались следующие задачи:

выбор, либо разработка иерархии проектирования радиоэлектронных бортовых объектов ИМА,

постановка задачи конструирования с учетом требований обеспечения информационной безопасности,

рассмотрение методов и средств конструирования.

Основные результаты аналитического обзора

Как показывают результаты дополнительного анализа доступной литературы [4,7,8,9,10], наиболее актуальными источниками помех радиоэлектронной аппаратуре и вычислительным средствам ЛА являются:

беспроводные информационно-телекоммуникационные устройства пассажиров, находящиеся на борту ЛА во время полета;

атаки внешних злоумышленников по беспроводным радиоканалам каналам передачи данных, обеспечивающим доступ к бортовой вычислительной сети.

Помехи, поставленные с помощью средств радиоэлектронной борьбы (РЭБ) в случае попадания самолета в область ограниченного конфликта.

Участившиеся локальные и региональные конфликты, в которых применяются современное высокоточное оружие и средства РЭБ, угрожают почти напрямую полетам гражданских ЛА, находящихся в полете даже на значительном удалении от зоны боевых действий. Количественный рост и усложнение бортовой аппаратуры требуют более тщательного учета вопросов электромагнитной совместимости (ЭМС). Все это требует разработки новых методов проектирования комплекса бортового оборудования (КБО). В соответствии с современным блочно-иерархическим подходом к проектированию в работе введено описание структуры объектов ИМА, включающее пять уровней (см. Рис.1): архитектурный, функционально-логический, системотехнический, схемотехнический, физический [7]. Физический уровень соответствует этапу конструирования.

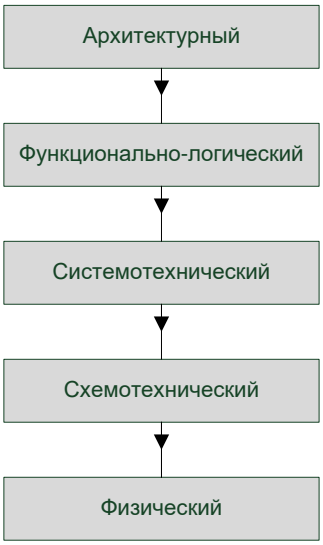


Рис.1. Иерархическая схема структуры аппаратно – программных средств аппаратуры ИМА

Для каждого из данных уровней необходимо рассматривать круг требующих решения задач, определять набор реализуемых на нем функций, производить анализ надежности и полноты обеспечения поставленных целей. Функционал архитектурного уровня соответствует степени детализации объекта проектирования, не требующей учета:

физического носителя сигнала,

логического носителя сигнала,

внутренней структуры подсистем передачи сообщений. На данном уровне иерархической структуры рассматриваются модели топологий объекта проектирования, правила и условия их построения.

Модели функционально-логического уровня строятся для решения задач согласования подсистем, входящих в состав объекта проектирования. В перечень задач, решаемых на данном уровне, входит контроль качества обработки сообщений, а также их защита от внешних помех. Например, к числу подобных помех относят методику криптоанализа с подменой авторизованных участников соединения. Однако, как известно, безупречных методов обеспечения защиты данных от несанкционированного использования не существует. Стоимость вскрытия защиты определяется лишь требуемыми для этого затратами вычислительных мощностей и других ценных ресурсов. В дополнение к несовершенству тех или иных методов обеспечения информационной безопасности, ситуация с возможностью несанкционированного доступа усугубляется неточностью соблюдения требований стандартов беспроводной связи в свете обеспечиваемой ими защиты данных или откровенными ошибками в построении защиты обмена данными.

Системотехнический уровень соответствует степени детализации в приближении моделей «черный ящик» или «серый ящик». Подсистемы данного уровня выполняют функции кодирования логических сигналов для их передачи физическим носителем в канале беспроводного соединения. На схемотехническом уровне в модельном представлении объекта проектирования учитывается физическая природа носителей сигнала совместно с характером преобразования в отдельных моделях типа «черный ящик».

На физическом уровне иерархической структуры выполняются работы по проектированию электромагнитной совместимости устройств, входящих в беспроводное соединение. Также на данном уровне рассматриваются аспекты взаимодействия устройств и помех в форме физических сигналов.

Методы рабочего проектирования (конструирования) КБО ИМА

Анлиз доступных публикаций показывает, что такие угрозы, как естественные или наведенные помехи бортовым средствам связи и навигации ЛА следует учитывать на системотехническом уровне проектирования. Угрозы, обусловленные нарушением ЭМС либо воздействием средств РЭБ при пролете ЛА мимо зон локальных военных конфликтов следует учитывать при разработке конструкции, т.е. на этапе рабочего проектирования. Рассмотрим несколько характерных примеров. По данным американской стороны, «русские войска с помощью самолётного многофункционального комплекса „Хибины“ способны оглушить и ослепить войска и вооружение НАТО, в том числе спутники в космосе, в зоне радиусом 300 км». Как следствие, радиокоммуникациям альянса требуются особые усилия и многократное дублирование сигналов для преодоления этих невидимых атак.

На авиабазу «Хмеймим» недавно прилетели два самолёта Ил-20 радиоэлектронной разведки и РЭБ, которые могут кружить по 12 часов над огромной территорией в любое время дня и ночи. Затем в Сирии был замечен наземный мобильный комплекс «Красуха-4», способный генерировать широкополосные помехи для средств радиосвязи на дальностях до 300 км. Есть сведения, что в Сирию также был переброшен комплекс «Борисоглебск-2», считающийся лучшим в своем классе. В прессе говорят, что крылатые ракеты Трампа сбивала и новейшая станция активных помех «Рычаг-АВ», которая может устанавливаться, как на вертолетах Ми-8, так и на наземной технике или на маломерных судах. Дело в том, что данная система РЭБ имеет свою «библиотеку» военных объектов, самообучаемое программное оборудование, которое, анализируя оружие потенциального врага, автоматически подбирает режим излучения для нейтрализации цели.. По имеющей у американцев статистике, наши РЭБ способны вдвое улучшить возможности российских ПВО. Судя по количеству не долетевших до цели «Томагавков», эксперты армии США не ошиблись. То, что в свое время Обама не нанес удар крылатыми ракетами по войскам Асада, говорит не столько о «слабости» 44 президента, сколько о его осведомленности. Именно по этой причине он также не решился ввести беспилотную зону. В то же время «учитывая напряженную кампанию угроз Соединенных Штатов против Сирии и России, Москва воздержится, чтобы заявить открыто о своей победе и уж тем более, не раскроет «слабые места американских ракет».

Опубликован материал, согласно которому Россия применила в Сирии новейшую аппаратуру радиоэлектронной борьбы и которая якобы внешним воздействием отключила приборы наведения большинства «Томагавков». Создать помехи приборы наведения «Томагавков» с помощью систем РЭБ невозможно. Эти системы способны «забить» помехами радиоприемные устройства ракеты, например, приемник GPS. Но на борту крылатых ракет расположено несколько дублирующих и дополняющих друг друга систем, которые обеспечивают высокоточный выход на цель.
Во-первых, это инерциальная система наведения, основанная на гироскопах я являющаяся полностью автономной, и на которую никакие помехи не действуют. Но у нее низкая точность наведения - за час полета "набегает" ошибка около 800 м и поэтому ее надо корректировать, используя более точные навигационные системы. Для наведения крылатых ракет на цель используются еще две системы позволяющие осуществлять точный выход на цель. Это корреляционная система Tercom и оптическая система DSMAC. Им можно противодействовать только «разрушив» бортовую радиоэлектронику в частности, электромагнитной засветкой средствами РЭБ. Таким образом, появление гражданской авиации даже на значительном удалении от районов местных конфликтов

Уравнения Максвелла в изотропных и однородных средах без дисперсии [14]:

$\boldsymbol{rot}(\overrightarrow{\boldsymbol{H}}) = \frac{\partial \vec{E}}{\partial t}\varepsilon_0$ (1)	$\boldsymbol{rot}(\overrightarrow{\boldsymbol{E}}) = -\frac{\partial \vec{H}}{\partial t}\mu_0$ (2)
$\mathrm{Div}(\overrightarrow{\boldsymbol{E}}) = 0$ (3)	$\mathrm{Div}(\overrightarrow{\boldsymbol{H}}) = 0$ (4)

$D=\varepsilon_0\varepsilon E$, (5)
$B=\mu_0\mu H$, (6)
$j=\gamma E$, закон Ома (7)

где ε0 и μ0 — соответственно электрическая и магнитная постоянные, ε и μ — соответственно диэлектрическая и магнитная проницаемости, γ — удельная проводимость вещества, E – вектор электрического поля, H - вектор магнитного поля, B – вектор магнитной индукции, D - вектор электрической индукции.

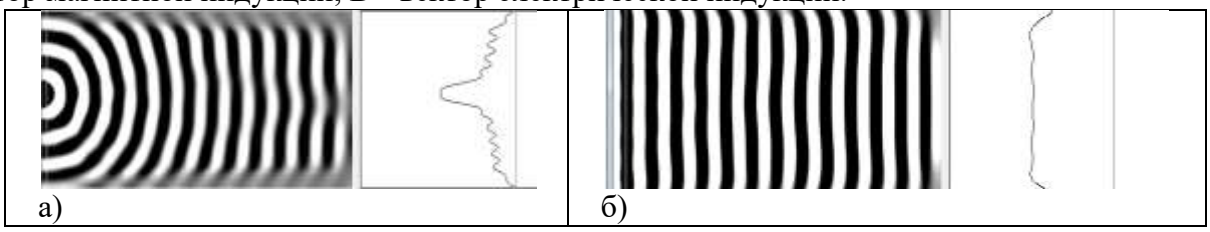


Рис. 2. Решение уравнений Максвелла для случаев прохождения свободного слоя пространства излучением со сферическим а) и плоским б) волновыми фронтами.

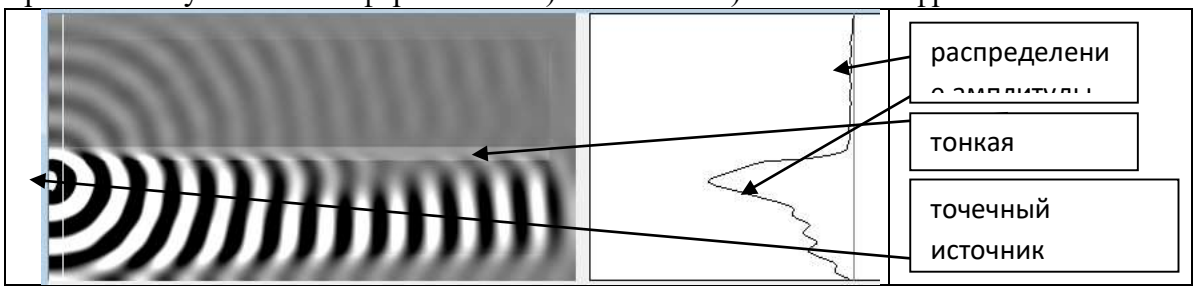


Рис. 3 Решение уравнений Максвелла для случая прохождения излучения через металлическую пластину.

Уравнения Максвелла представляют собой точную модель, применимую для макроописания электромагнитного излучения. Однако применимость их во многих практических случаях весьма ограничена. Для оценки пропускания экранов бортовой аппаратуры зачастую невозможно узнать значения ε0, ε и μ0, μ - требуется сложный эксперимент. Рассмотрим возможность более простого подхода.

Продифференцировав уравнение (1) по времени и заменив в полученном уравнении $\frac{\partial \vec{H}}{\partial t}$ из уравнения (2), получим:

. –

$$\frac{1}{\mu_0}\boldsymbol{rotrot}(\overrightarrow{\boldsymbol{E}}) = \varepsilon_0 \frac{\partial^2 \vec{\boldsymbol{H}}}{\partial t^2} \qquad (8)$$

Пользуясь формулой векторного анализа: $\boldsymbol{rotrot}(\overrightarrow{\boldsymbol{E}}) = \text{graddiv}(\overrightarrow{\boldsymbol{E}}) - \overrightarrow{\Delta \boldsymbol{E}}$ и принимая во внимание уравнение (3), получим:

. $$\overrightarrow{\Delta \boldsymbol{E}} - \frac{1}{c^2}\frac{\partial^2 \overrightarrow{\boldsymbol{E}}}{\partial t^2} = 0 \qquad (9)$$

Аналогичным образом находим, что вектор $\vec{\boldsymbol{H}}$ удовлетворяет волновому уравнению:

$$\overrightarrow{\Delta \boldsymbol{H}} - \frac{1}{c^2}\frac{\partial^2 \overrightarrow{\boldsymbol{H}}}{\partial t^2} =$$

0 (10)

где $c = \frac{1}{\sqrt{\varepsilon_0 \mu_0}}$ – скорость волны.

В рамках скалярной теории дифракции принято [15], что в любой точке Q(x, y, z) однородной среды в областях, свободных от токов и зарядов (в частности, отсутствуют источники излучения), вещественная функция u(Q, t) , которая описывает электромагнитное возмущение, удовлетворяет скалярному однородному волновому уравнению, формально аналогичному (9) и (10) [15]:

$$\Delta u - \frac{1}{v^2}\frac{\partial^2 u}{\partial t^2} = 0 \qquad (11)$$

где $\Delta = \partial^2/\partial x^2 + \partial^2/\partial y^2 + \partial^2/\partial z^2$ – оператор Лапласа;

$v = c/n$ – скорость света в среде;

$c = 299776 \pm 4$ км/с – скорость света в вакууме;

n – показатель преломления.

в скалярной теории дифракции [15] принимается, что U(Q,t) представляет собой одну из двух взаимно перпендикулярных декартовых компонент Ex(Q,t) и Ex(Q,t) электрического поля, колеблющихся в плоскости, перпендикулярной направлению распространения волны. Хотя скалярная теория не позволяет учесть явление поляризации и тонкие эффекты дифракции, для инженерных приложений, в частности при модельном представлении реальных электромагнитных волн, проходящих диэлектрики и металлы, такое допущение дает удовлетворительные результаты. Но даже при описанных допущениях решить волновое уравнение удается для небольшого числа частных случаев. Одним из таких решений является модель, которая строится на представлении суперпозиции плоских и сферических волн. Амплитуду однородной плоской монохроматической волны можно представить в виде:

$U(Q,t) = A(Q)\exp(-2\pi j v_t\, t), A(Q) = a\exp\left(2\pi j\overrightarrow{k_n}\ \vec{r}\ \right) = a\exp(2\pi j\overrightarrow{v_n}\ \vec{r}\ )$, где $\overrightarrow{v_n}$ - вектор пространственной частоты, $\vec{r}$ - радиус – вектор точки с координатами y, z. Любое решение волнового уравнения вида: $U(Q,t) = s\,[(\vec{r}\ \vec{e}, t)]$ представляет собой плоскую волну, так как в каждый момент времени t_0 величина U(Q,t) постоянна во всех точках плоскости, задаваемой векторным уравнением в виде скалярного произведения:

$\vec{r}\ \vec{e} = d = const$

где $\vec{r}(x, y, z)$ – радиус-вектор точки;

$\vec{e}(\cos\alpha, \cos\beta, \cos\gamma)$ – единичный вектор нормали к плоскости, координаты которого определяются направляющими косинусами (рис.).

$k_n = 2\pi/\lambda_n; \quad \lambda = v/\nu_t = vT$ – длина волны в среде с показателем преломления n.

Иначе говоря, плоская волна, фаза которой постоянна во всех точках некоторой плоскости, имеет плоский волновой фронт.

Скалярное комплексное выражение для электрического поля сферической расходящейся монохроматической волны получается в результате замены t на t – r/v , так что с учетом однородности A(Q) = a /r можно записать:

$$U_{pcx}(Q,t) = \frac{a}{r}\exp[-i2\pi\nu_t(t - \frac{r}{v})] = \frac{a}{r}\exp(i\frac{2\pi}{\nu_n}r)\exp(-i2\pi\nu_t t)$$

Откуда комплексная амплитуда однородной сферической расходящейся монохроматической волны:

$$A_{pcx}(Q) = (a/r)\exp(ik_n r) = (a/r)\exp(i2\pi\nu_n r)$$

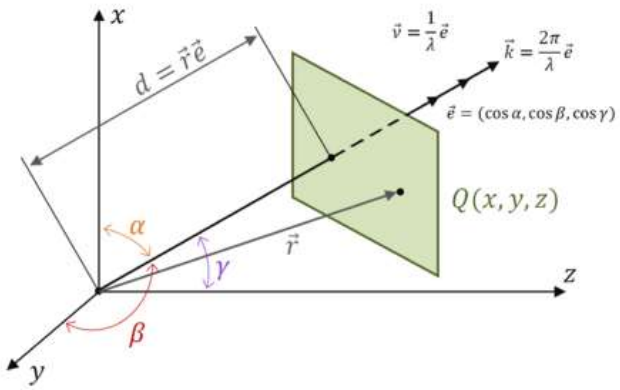


Рис.4. Трехмерная геометрическая модель, идентифицирующая процесс распространения однородной плоской волны в пространстве

Так как общее выражение для сферической волны, сходящейся к началу координат, имеет вид:

$$U_{сх}(Q,t) = s(r+vt)/r,$$

то комплексно сопряженная амплитуда:

$$A_{сх}(Q) = A_{рсх}(Q) = (a/r)\exp(ik_n r) = (a/r)\exp(-i2\pi\nu_n r)$$

соответствует однородной сферической сходящейся монохроматической волне.

Для расчета пропускания сплошных корпусов бортовой РЭА вышеприведенные выражения достаточно, точны. Остается привести выражения для интенсивности излучения. Для расчета пропускания в сетчатых и композитных структурах необходимо учитывать дифракцию излучения. Далее, как и прежде будем иметь в виду очень короткие волны, близкие СВЧ диапазону. Конструкции экранов электромагнитного излучения (ЭМИ) классифицированы на Рис.5 [13]. Многие из них выполнены из металлизированной сетки. Её пропускание следует рассчитывать с учетом дифракции.

Рис. 5. Классификация конструкций экранов электромагнитного излучения

Проанализируем дифракцию световой волны на транспаранте с амплитудным пропусканием:

$$t(x,y) = t_0 - t_1\cos(2\pi\eta y)$$

При $t_0 \geqslant t_1 > 0$ непосредственно за транспарантом

$$U(x,y,0) = A_0 t(x,y) = A_0 t_0 + 0.5 A_0 t_1 \exp(2\pi i \eta y) + 0.5 A_0 t_1 \exp(-2\pi i \eta y)$$

Первый член данного выражения описывает плоскую волну, распространяющуюся вдоль оси z, как и падающая волна, второй и третий члены - плоские волны, направления распространения которых с осью z составляют углы φ_1 и φ_2, причем $\varphi_1 = -\varphi_2 = \arcsin(\lambda\eta)$. Таким образом, в результате дифракции часть падающей на транспарант световой волны отклоняется от первоначального направления распространения.

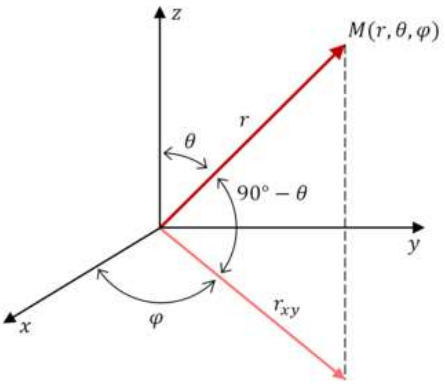


Рис. 6. Связь между координатами сферической и прямоугольной систем координат

Амплитудное пропускание двумерной дифракционной решетки в общем случае описывается комплексной периодической функцией двух переменных x и y. Однако его также легко представить в виде суммы простейших синусоидальных функций путем разложения в ряд Фурье:

$$t(x,y) = \sum_{n=-\infty}^{\infty} \sum_{m=-\infty}^{\infty} t_{nm} \exp(-i2\pi\xi_n x) \exp(-i2\pi\eta_m y)$$

Дифрагированная на таком транспаранте световая волна представляет собой суперпозицию бесконечного числа плоских волн с амплитудами, пропорциональными соответствующим коэффициентам разложения t_{nm} и направлениями распространения, определяемыми $\cos\alpha_n = \lambda\xi_n$ и $\cos\beta_m = \lambda\eta_m$. Следовательно, суммарная амплитуда дифрагированных волн в плоскости $z = d$

$$U(x,y,d) = A_0 \sum_{n=-\infty}^{\infty} \sum_{m=-\infty}^{\infty} t_{nm} t_{nm} \exp[-ikd(1-\lambda^2\xi_n^2-\lambda^2\eta_m^2)^{1/2}] \times \exp(-i2\pi\xi x) \exp(-i2\pi\eta y) d\xi d\eta$$

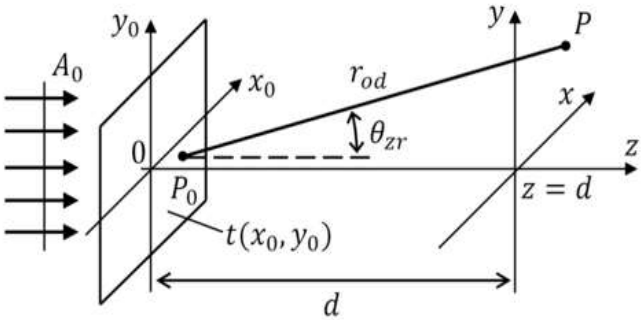


Рис.7. К решению задачи дифракции с помощью интеграла Френеля-Кирхгофа

В общем случае амплитудное пропускание дифрагирующего объекта является комплексной непериодической функцией двух переменных x и y, поэтому t (x, y)

заменяют интегралом Фурье. Комплексную амплитуду дифрагированной волны в плоскости z = d при этом также выражают с помощью интеграла

$$U(x,y,d) = A_1 \iint_{-\infty}^{\infty} T(\xi,\acute{\eta}) \exp\left[-jkd\sqrt{(1-\lambda^2\xi^2-\lambda^2\acute{\eta}^2}\right] \exp(-2\,\pi jx\xi) \exp(-2\pi jy\acute{\eta})\, d\acute{\eta}d\xi \qquad (5')$$

где $T(\xi,\eta)$ - преобразование Фурье от $t(x,y)$, причем интегрирование, по существу, производят в области, удовлетворяющей неравенству $\xi^2+\eta^2 \leqslant 1/\lambda^2$ (вне этой области волны быстро затухают при удалении от транспаранта).

Если:

$$|x-x_0| \ll z,\ |y-y_0| \ll z,$$

то можно полагать, что $\cos\theta_{zr} \approx 1$ с ошибкой менее 5%, если угол $\theta_{zr} < 18^\circ$. и, поскольку

$$r_{O_z} = z\sqrt{1+[(x-x_0)/z]^2-[(y-y_0)/z]^2} \approx z,$$

и $(x-x_0)^2/z^2 \approx 0,\ (y-y_0)^2/z^2 \approx 0$ согласно, то учитывая первые два члена данного разложения для аппроксимации квадратного корня, примем

$$r_{O_z} \approx z\left[1+\frac{(x-x_0)^2}{2z^2}+\frac{(y-y_0)^2}{2z^2}\right] = z+\frac{(x-x_0)^2}{2z}+\frac{(y-y_0)^2}{2z}$$

Тогда интеграл Френеля-Кирхгофа можно записать в следующем упрощенном виде:

$$U(x,y,z) = \frac{ik}{2\pi z}e^{-ikz}\int\int_{-\infty}^{\infty} U_0(x_0,y_0)\exp\left\{-\frac{ik}{2z}[(x-x_0)^+(y-y_0)\right\} dxdy$$

Интегральное преобразование вида

$$\Phi(\xi) = \int_{-\infty}^{\infty} f(x)\exp\left[-\frac{i}{2}(\xi-x)^2\right]dx,$$

есть преобразование Френеля. Приближение Френеля справедливо в зоне:

$$\sqrt[3]{\frac{(a+\rho)^4}{\lambda}} \leqslant z \leqslant \frac{l_{\min}^4}{\lambda^3}$$

где a - максимальный радиус раскрыва;

ρ - максимальный радиус области наблюдения в плоскости а именно

$$\frac{\lambda_0^2+y_0^2}{\lambda} \ll z$$

Если можно принять, что $\exp[-\frac{ik}{2z}(x_0^2+y_0^2)] \approx 1.$ то дифракционная формула еще более упроститься:

$$U(x,y,z) = \frac{ik}{2\pi z} e^{-ikz} \int\int_{-\infty}^{\infty} U_0(x_0,y_0) \exp\left\{-\frac{ik}{2z}[(x-x_0)^+(y-y_0)\right\} dxdy$$

Полученное приближение имеет основной множитель в виде интеграла, являющегося преобразованием Фурье распределения комплексных амплитуд $U_0(x_0,y_0)$ излучения, дифрагировавшего на экране. Существенность приведенной методики можно проиллюстрировать следующими примерами. На Рис. 8 – 10 приведены графики, характеризующие эффективность сетчатых экранов [13]:

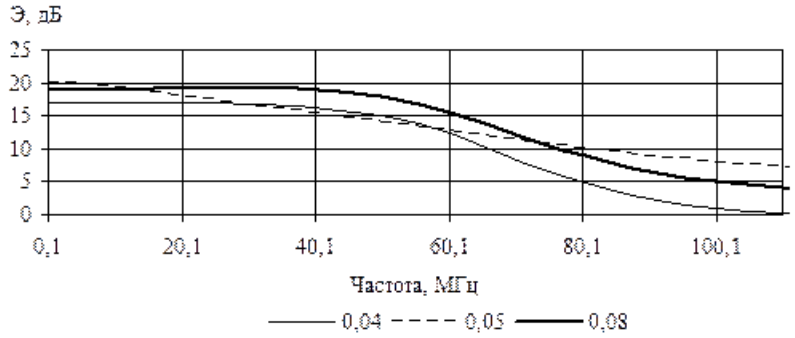


Рис. 8. Частотная зависимость эффективности экранирования для сетчатых экранов ЭМИ с различным диаметром микропровода.

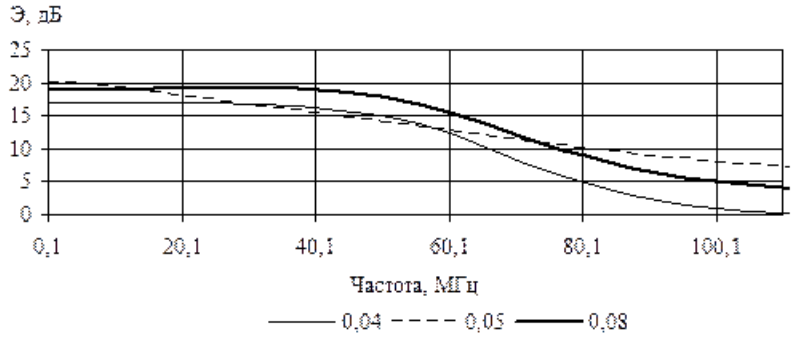


Рис. 9. Частотная зависимость эффективности экранирования для сетчатых экранов ЭМИ с различным диаметром микропровода

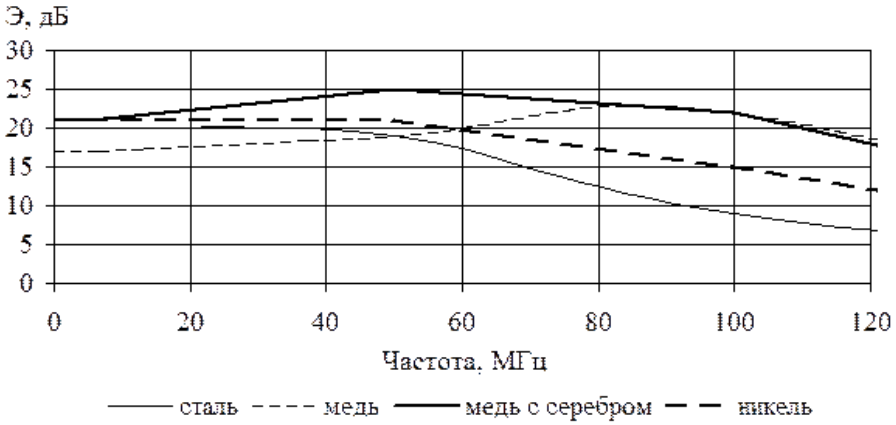


Рис. 10. Частотная зависимость эффективности экранирования для сетчатых экранов ЭМИ с микропроводом из различных материалов

Большим значением коэффициента отражения обладают экраны ЭМИ, конструктивно выполненные в виде четвертьволнового поглотителя, в котором радиопоглощающий материал (РПМ) находится на некотором расстоянии от отражающей ЭМВ поверхности. Поглощение достигает максимального значения на частоте, соответствующей длине волны, четверть которой равна расстоянию между верхней поверхностью поглощающего материала и отражающей поверхностью, а также на всех ее высших нечетных гармониках (рис. 11).

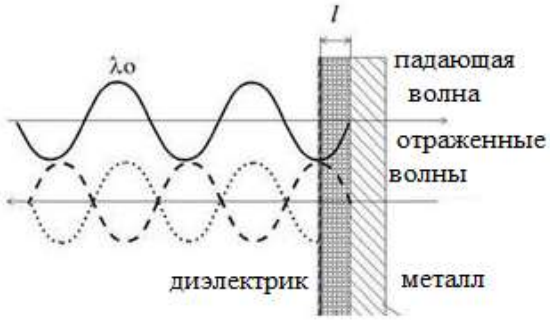


Рис. 11. Схема взаимодействия с ЭМИ четвертьволнового экрана

Конструкции четвертьволновых экранов ЭМИ широко используются в технике и их расчет возможно и необходимо вести по методикам, рассмотренным выше и опирающимся на скалярную теорию дифракции [14, 15]. Они являются высокоэффективными с точки зрения подавления ЭМВ, но в узкой полосе частот, что обусловлено конструктивными их особенностями и представляется главным их недостатком. Одной из важнейших задач, решаемых при создании РПМ, является уменьшение массы конструкции, что достигается путем использования порошкообразных материалов, в том числе магнитных. Размер частиц и магнитная проницаемость порошкообразных материалов применяемых в конструкциях экранов ЭМИ, определяют их рабочий диапазон частот. Недостатком таких материалов, как и четвертьволновых РПМ, является их узкодиапазонность, а при использовании магнитных порошкообразных материалов – высокая стоимость. Использование магнитных материалов в виде порошков, в том числе специальной формы, позволяет создавать эффективные экраны ЭМИ с граничной частотой до 10 ГГц, однако массовое практическое использование сдерживается их высокой стоимостью, обусловленной сложным технологическим процессом изготовления и дорогостоящим сырьем. Формирование геометрических неоднородностей на поверхности экрана ЭМИ (пирамидальной, клиновидной формы) (рис. 4.10) позволяет обеспечить широкодиапазонность характеристик отражения. Взаимодействие с ЭМВ в подобных конструкциях обусловлено не только параметрами материала, из которого она изготовлена, но и сложной формой волноведущей поверхности (рис. 4.11). В таких конструкциях падающая ЭМВ преобразуется в поверхностную волну и по мере ее переотражения от неоднородностей поверхности ее энергия уменьшается.

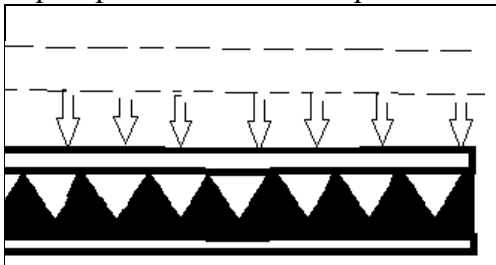


Рисунок , а)

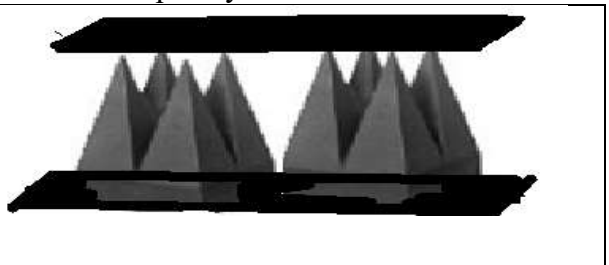
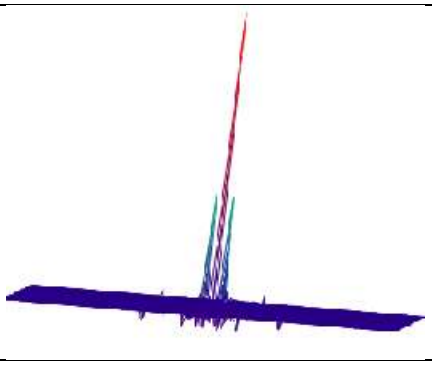


Рисунок , б)

	
Рисунок , а)	Рисунок , б)

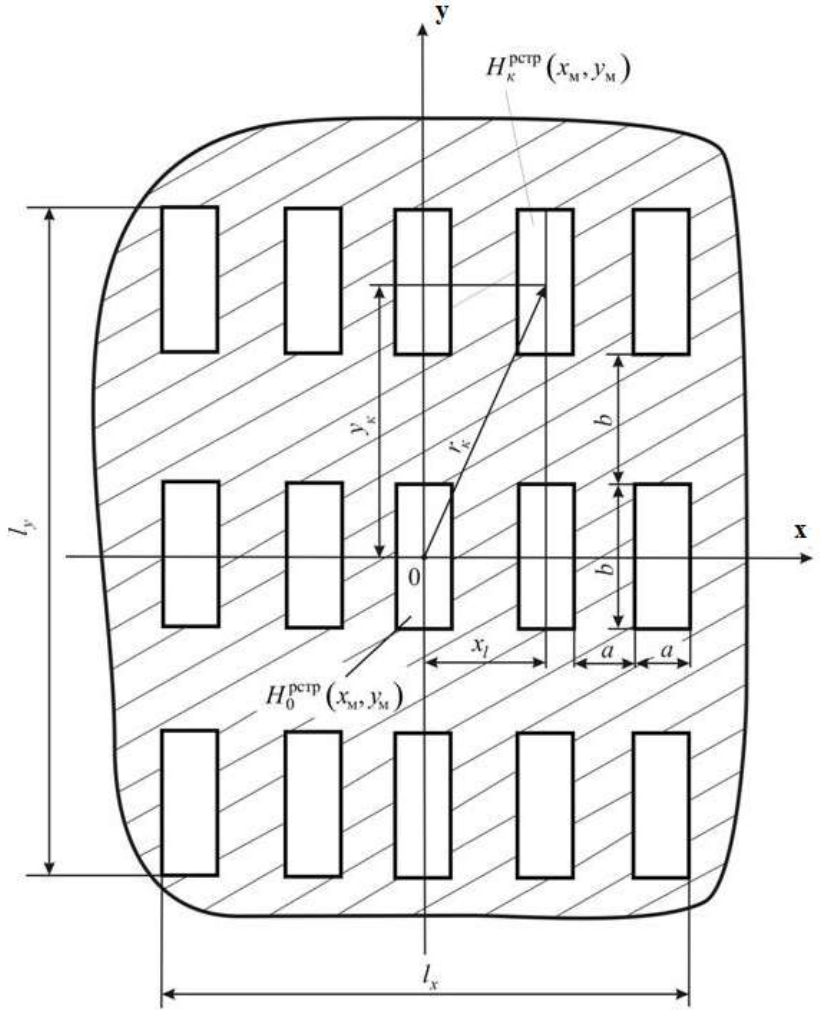


Рисунок .

$$U(v_{x,}v_y) = U_0 F\left\{\left[rect\left(\frac{x_p}{a}\right)(*)\frac{1}{2a}comb\left(\frac{x_p}{2a}\right)\right]rect\left(\frac{x_p}{l_x}\right)\right\}\cdot$$

$$F\{\left[rect\left(\frac{y_p}{b}\right) * \frac{1}{2b}comb\left(\frac{y_p}{2b}\right)\right]\cdot rect\left(\frac{y_p}{l_y}\right)\} =$$

$$= U_0\left(\frac{l_x l_y}{4}\right)\sum_{k=-\infty}^{\infty} sinc\left(\frac{\pi k}{2}\right)sinc[\pi l_y(v_y - \frac{k}{2a})]sinc\left(\frac{\pi n}{2}\right)sinc[\pi l_y\left(v_y - \frac{n}{2b}\right)]$$

В любом практическом случае при проведении конструкторских расчетов в конце концов необходимо оперировать интенсивностью ЭМИ. В этих расчетах используются доступные характеристики вещества экранов – коэффициенты отражения и пропускания. Из теории Максвелла известно, что объемная плотность электрической энергии ω, Дж/м3,

Заключение

В статье предлагается применять блочно – иерархический подход к проектированию и нисходящая технология разработки аппаратуры комплекса бортового оборудования интегральной модульной авионики. Приводятся уровни проектирования. Показано, что действие умышленных и случайных помех средствам связи и навигации самолетоа следует учитывать при проектировании бортовых РЭА и ВС на верхних иерархических уровнях вплоть до системотехнического, а действие мощных внешних и внутренних внеканальных засветок учитывать на уровне рабочего проектирования (конструирования).

Проведенные исследования позволяют сделать следующие основные выводы:

Источники вероятных внешних и существующих электромагнитных засветок на борту гражданских самолетов характеризуются высокой и сверхвысокой частотами

особенности внешних и внутренних источников электромагнитного излучения на борту гражданского самолета требуют применения специальной методики расчета пропускания экранов конструкций.

необходимо и возможно применять методики расчета при конструировании бортовой РЭА и ВС, построенные на основе скалярной теории дифракции.

.

Литература

1. [Электронный ресурс]., www.aviasafety.ru/crash-stat, (дата обращения 25.05.2018).

2. Информационная безопасность [Электронный ресурс]., Android*, Блог компании «Apps4All», (дата обращения - 25.05.2018).

3. Ефанов В.Н. Открытые архитектуры в концепции авионики пятого поколения // Бодрунов С.Д. - Мир авионики. – 2004. – № 5. – С. 20–28.

4. Е.В. Книга, Принципы организации вычислительных систем перспективных летательных аппаратов/[Электронный ресурс]., elektropribor.spb.ru› **(**дата обращения *15.06.2018).*

5. Матвеев В.А., Бельфер Р.А., Глинская Е.В. Угрозы и методы защиты в сборных сенсорных узлах летающих сенсорных сетей // Вопросы кибербезопасности. 2015. № 5 (13). С. 26-31.

6. Чичварин Н.В. Экспертные компоненты САПР. – М.: Машиностроение, 1991. – 240 с.: ил.

7. Евгенов А.В. Направления развития интегрированных комплексов бортового оборудования самолетов гражданской авиации. / Авиакосмическое приборостроение. – 2003. – № 3. – С. 48–53.

8. Платформа интегрированной модульной авионики. Патент на полезную модель RU №108868 U1 / Богданов А.В., Васильев Г.А., Виноградов П.С., Егоров К.А., Зайченко А.Н., Ковернинский И.В., Петухов В.И., Романов А.Н., Смирнов Е.В., Уткин Б.В., Федосов Е.А., Шукало А.В. Бюл. №27, 27.09.2011.

9. Бортовая центральная вычислительная система [Электронный ресурс]. URL: http://www.rpkb.ru/lines-of-business/electronic direction/on-board-computers/onboard-central-computer-system/index.php?sphrase id=3710 (дата обращения 01.06.2018).

10. Буравлев А., Чельдиев М., Барыбин А., Костенко В., Тумакин Д., Петров Г. Масштабируемые мультипроцессорные вычислительные системы высокой производительности // Современные технологии автоматизации. 2009. № 3. С. 72-82.

11. Федосов Е.А., Косъянчук В.В., Сельвесюк Н.И. Интегрированная модульная авионика // Радиоэлектронные технологии №1 (2015). с. 66 - 72

12. Глинская Е.В., Чичварин Н.В. Моделирование угроз информационной безопасности бортовых вычислительных средств самолета. / Вестник МГТУ им. Н.Э. Баумана, сер. «Приборостроение», - 2016 - №6. с.85 -97.

13. Конструкции экранов электромагнитного излучения/, [Электронный ресурс]. helpiks.org›5-8074.html, *(*дата обращения *15.06.2018).*

14. Ландау, Л. Д., Лифшиц, Е. М. Теория поля. — М.: Физматлит, 2001. — 534 с. — («Теоретическая физика», том II). — ISBN 5-9221-0056-4.

15. Борн М., Вольф Э. Основы оптики: Пер. с англ. под ред. Г. П. Мотулевич. М.: Наука, 1970. 855 с.

Specificity of designing on-board equipment of modular avionics taking into account information security requirements.

Glinskaya E.V, Chichvarin N.V.

The publication presents the results of theoretical and experimental studies of the features of integrated modular avionics (IMA) designs. The problematic of the work consists in the search for the provision of IMA structural elements with protection against harmful effects of external electromagnetic radiation. At the same time, various aspects of electromagnetic compatibility (EMC) of the main components and assemblies of onboard radioelectronic equipment and computer facilities of an aircraft (LA) are taken into account. It is shown that it is useful to build a mathematical model for the design and components of aircraft for calculating the security of structural elements. In this case, the effect of electromagnetic radiation must be modeled on the basis of Maxwell's equations, and not by using approximate semi-empirical formulas. The Maxwell equations are solved by applying the numerical finite difference method. The adoption of design solutions should be oriented towards the creation of an intellectually capacious and rapidly modifiable technology for the creation of aviation electronic equipment, which substantially reduces the costs for the development, production, operation and maintenance of equipment through hardware and software (miniaturization and redundancy) and software-algorithmic (localization of failures and reconfiguration of the complex in real time) solutions.

Key words: avionics, onboard equipment, safety, information, design, aircraft.

УДК 629.7.017.1

Способы моделирования аппаратуры модульной авионики в условиях вредоносных воздействий

Волосатова Т.М.[1], Чичварин Н.В.[2]

Рассматриваются результаты исследований и анализа способов моделирования угроз информационной безопасности (ИБ) комплексов связи и навигации самолета, проведенных с целью построения формализованной модели угроз комплексу бортового оборудования (КБО). Основное внимание уделено ИБ бортовой аппаратуры связи и навигации летательного аппарата (ЛА). Учтено, что в условиях повышения уровня автоматизации бортового оборудования, систем и агрегатов летальных аппаратов, возрастания сложности бортовых информационных систем существенное значение приобретает проблема защиты радиоэлектронной аппаратуры (РЭА) от угроз информационной безопасности. Исследования проведены на основе анализа современной интегральной авионики (ИМА).

Ключевые слова: *авионика, безопасность, вычислительные средства, информация, модель, навигация, самолет, угрозы.*

Введение

Анализ обзоров доступной литературы показывает, что проблема безопасности полетов нарастает [1-6].

Особенно актуальна задача разработка методов моделирования угроз информационной безопасности каналов связи и навигации интегральной модульной авионики на имитационных стендах, поскольку построить теоретические модели угроз ИБ КБО ЛА далеко не всегда возможно.

Цель исследований и решённые задачи.

Основными задачами исследований явились:

анализ источников атак на средства связи и навигации ЛА,

анализ характера и последствий атак на ЛА,

Как показывают результаты анализа доступной литературы, источниками угроз являются:

беспроводные информационно-телекоммуникационные устройства пассажиров, находящиеся на борту ЛА во время полета;

атаки внешних злоумышленников по беспроводным радиоканалам каналам передачи данных, обеспечивающим доступ к бортовой вычислительной сети.

Помехи, случайно, либо умышленно поставленные с помощью средств радиоэлектронной борьбы (РЭБ)

Участившиеся локальные и региональные конфликты, в которых применяются современное высокоточное оружие и средства РЭБ, угрожают почти напрямую полетам гражданских ЛА, находящихся в полете даже на значительном удалении от зоны боевых действий.

1Волосатова Тамара Михайловна, кандидат технических наук, доцент кафедры «САПР» МГТУ им. Н. Э. Баумана», Москва, e-mail tamaravol@gmail.com.

2Чичварин Николай Викторович, кандидат технических наук, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, Москва, e-mail genrih.gertz@gmail.com.

. Целью исследований, основные результаты которых изложены в настоящей публикации является разработка математической модели помех управлению полёта самолёта, применимой для стендов исследования информационной безопасности самолета.

Анализ бортовых средств связи и навигации самолетов.

Анализ доступных источников показал, что для приемников радиосигналов, обеспечивающих связь с самолетом, используется приемники, выполненные по схеме супергетеродина (Рис.2)

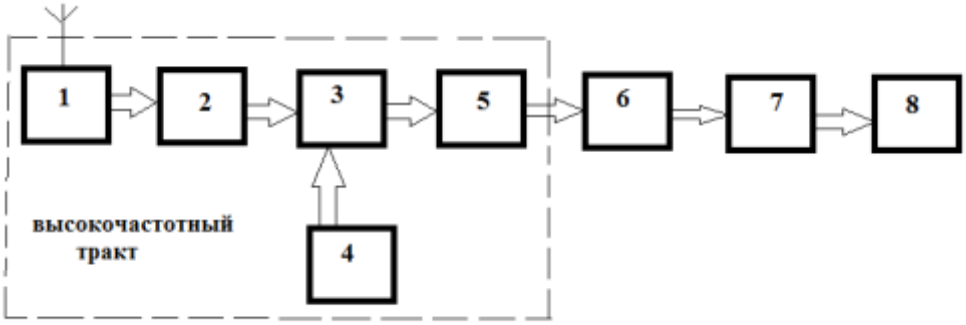


Рис. 2. Структурная схема типичного супергетеродинного приемника. 1 – преселектор (ПР), 2 -– усилитель высокой частоты (УВЧ), 4 – гетеродин (Гт), 3 - смеситель (С), 5 - усилитель промежуточной частоты (УПЧ), 6 – детектор (Д), 7 - усилитель низкой частоты УНЧ, 8 – регистратор (Р).

Для приема/передачи данных в GPS отведено три диапазона частот: L1 (1563-1587 МГц), L2 (1217-1237 МГц) и L5 (1164-1188 МГц). Приемные ВЧ тракты для каждого из диапазонов принципиально друг от друга не отличаются. Далее рассматривается прием сигнала в диапазоне частот L1. Структурная схема типового супергетеродинного приемника GPS/ГЛОНАС изображена на рис. 3.

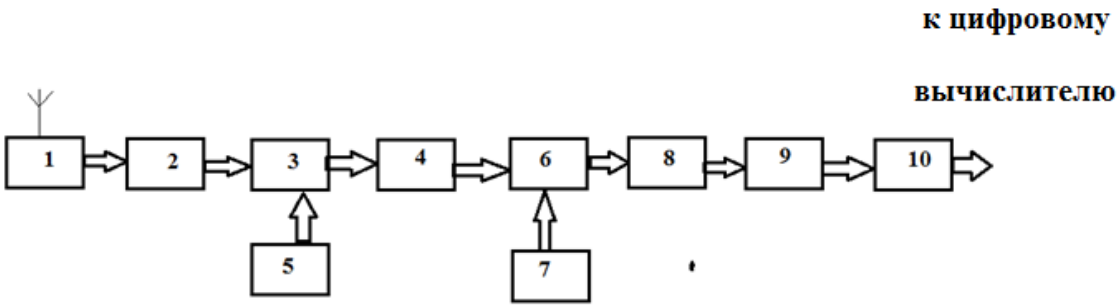


Рис.3. Структурная схема приемника GPS. 1 - малошумящий усилитель преселектора (МПШУ), 2 первый полосовой фильтр (ПФ1), 2 - второй полосовой фильтр (ПФ2), 3 – первый смеситель (СМ), 4 – второй смеситель (СМ), 5 - первый гетеродин (Гет1), 7 - второй гетеродин (Гет2), 8 - фильтр низких частот (ФНЧ), 9 – усилитель (У), 10 – аналогово–цифровой преобразователь (АЦП).

Входной сигнал из антенного блока поступает на малошумящий усилитель (МШУ). После МШУ, на полосовом фильтре (ПФ1) происходит высокочастотная фильтрация сигнала. Первый ПФ должен быть настроен на среднюю частоту принимаемого диапазона, и обеспечивать достаточное ослабление по зеркальному каналу приема. Первая промежуточная частота (ПЧ) составляет 102 МГц, а центральная частота диапазона L1 - 1575 МГц. Соответственно, первый ПФ должен обеспечивать достаточное ослабление на частотах 1670 МГц и выше. После фильтрации сигнал подвергается первому преобразованию частоты, в результате чего спектр сигнала переносится на частоту 102 МГц (первая ПЧ). После преобразования частоты производится повторная фильтрация с помощью ПФ2. Центральная частота ПФ2 составляет 102 МГц, а его полоса пропускания - не более 20 МГц.

Во многих приемниках сигналов GPS/ГЛОНАС сигнал подвергается второму преобразованию частоты, после которого он переносится на вторую промежуточную частоту 10 МГц.. После второго преобразования частоты, и последующих операциях фильтрации и усиления, сигнал поступает на АЦП и далее на цифровой вычислитель. Как известно, спектр частот подавляющего числа источников помех распределен по закону $\frac{1}{v}$, где v – частота. Перенос несущей частоты в дальний частотный диапазон как раз обеспечивает уход от наиболее опасных вредоносных воздействий. Немаловажную роль в обеспечении безопасности полета ЛА играют системы посадки по глиссаде. К ним относятся, в частности, маркерные системы. Функциональная схема типичного маркерного приемника приведена на рис. 4. Анализ показывает, что и в этом случае приемник выполнен по супергетеродинной схеме. Для предупреждения перегрузки УПЧ охвачен традиционной системой АРУ. Таким образом, при моделировании необходимо учесть нелинейность. сигнала; 11 – звуковой сигнал; 12 – сигнальные индикаторы.

Рассмотрим математическую модель высокочастотного блока супергетеродина, которая, как показал проведенный анализ, является его основной отличительной частью. Модель преселектора можно представить колебательным звеном с передаточной функцией:

$$W(p) = \frac{1}{Tp^2+T\varepsilon p+1},$$

а в случае применения преобразования Фурье:

$$W(v_t) = \frac{1}{-Tv_t{}^2+Tj\varepsilon v_t+1},$$

Тогда спектр выходного сигнала $\tilde{u}'(v_t)$ связан со спектром входного сигнала $\tilde{u}(v_t)$ выражением:

$$\tilde{u}'(v_t) = \tilde{u}(v_t)W(v_t)$$

Также можно моделировать и усилитель промежуточной частоты. Модель смесителя моделируется операцией умножения:

$$U_{вых}(t) = U_{вх}(t)U_г(t)$$

где: $U_{вх}(t)$ - входной сигнал, снимаемый с преселектора,

$U_г(t)$ - сигнал гетеродина.

Сигналы $U_{вх}(t)$ и $U_г(t)$ моделируются периодическими функциями и представимы рядами Фурье:

$$U_{вх}(t) = U_0 + \sum_{n=1}^{\infty}\left(U_{вх_n}\cos\frac{n\pi t}{T} + U_{вх_n}\sin\frac{n\pi t}{T}\right)$$

$$U_г(t) = U_0 + \sum_{n=1}^{\infty}\left(U_{г_n}\cos\frac{n\pi t}{T} + U_{г_n}\sin\frac{n\pi t}{T}\right)$$

Рассмотрим одно из произведений гармоник сигналов $U_{вх}(t)$ и $U_г(t)$:

$$U_{вх_k}\cos\frac{k\pi t}{T}U_{г_l}\cos\frac{l\pi t}{T} = 0.5(U_{г_k}U_{вх_k}][\cos(\frac{k\pi t+l\pi t}{T}) + \cos(\frac{k\pi t-l\pi t}{T})]$$

При формировании модели шумов, воздействующих на бортовые средства радиосвязи и навигации самолета следует ориентироваться именно на указанную схему обработки принятой смеси сигнал + шум в имитационной модели. Рассмотрим модели сигналов и спектров. Графики моделей АМ сигнала и модуля спектра представлены на Рис7. и Рис.8 соответственно. Модели получены в среде MathCAD, и поэтому легко переносятся в среду MatLab/Simulink, которые в свою очередь, сопрягаются с LabView.

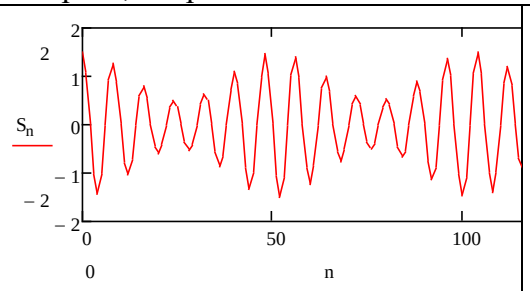


Рис.7. Осциллограмма АМ сигнала

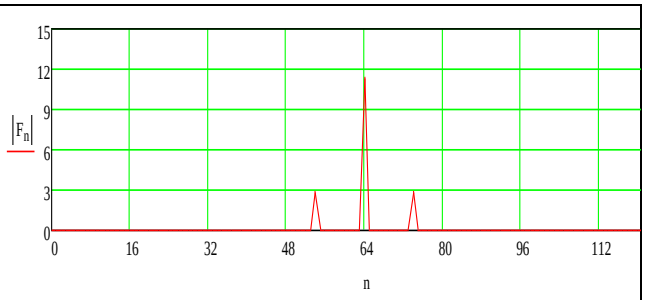


Рис.8.Модуль спектра АМ сигнала

Модель аддитивной смеси модулированного по амплитуде сигнала и шума (случайного процесса).

$$U_{АМШ}(t) = U_0\{1 + mU_{ог}(t)\}\cos(2\pi v_n t) + c(t) \qquad (1)$$

где: Uor(t) – сигнал огибающей, m – индекс глубины модуляции, vn – несущая частота, c(t) – реализация случайного процесса.

Модель аддитивной смеси частотно –модулированного сигнала и шума.

$$U_{чм}(t) = U_0\cos\{2\pi[v_н + m\Delta v_н U_{ог}(t)]t\} + C(t) \qquad (2)$$

где: Uor(t) – сигнал огибающей, m – индекс глубины модуляции, vn – несущая частота, Δvn – девиация несущей частоты, c(t) – реализация случайного процесса.

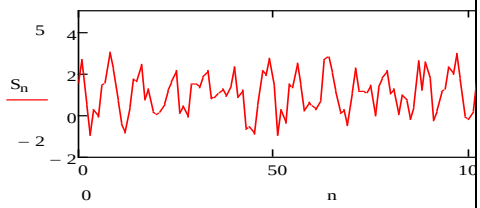


Рис.9. Осциллограмма АМ сигнала с гауссовским шумом

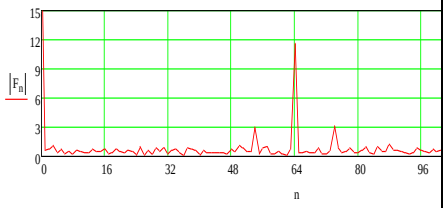


Рис.10. Модуль спектра АМ сигнала с гауссовским шумом

В станциях помех линиям радиосвязи с сигналами с аналоговой модуляцией зачастую формируется помеха в виде несущей, модулированной по частоте полосовым шумом с девиацией частоты.

$$U_{чмш}(t_j) = U_0\cos\{2\pi v_н v_н t_j + \sum_{k=0}^{N-1} m_{fk}\sin(2\pi f_{ok}t_j + \varphi_k)\} \qquad (3)$$

$$m_{fk} = a\frac{Um_{ok}+dU_k}{v_{ok}} \qquad (4)$$

где: U0 — амплитуда несущего колебания; vn — частота несущего колебания; vok , φk — частота и фазовый сдвиг k-ой гармоники сигнала огибающей; Nг — количество моделируемых гармонических составляющих в сигнале огибающей; Umk , dUk — амплитуды гармонических составляющих сообщения и их девиации, mk — парциальные коэффициенты амплитудной модуляции, вычисляемые по формуле:

$$m_k = a\frac{Um_k + dU_k}{U_0} \qquad (5)$$

$$U_{AM}(t_j) = U_0\{1 + \sum_{k=0}^{N-1} m_k(Um_k + dU_k)\cos[2\pi(v_{ok} + dv_k)t_j]\}\cos(2\pi v_n t_j) \qquad (6)$$

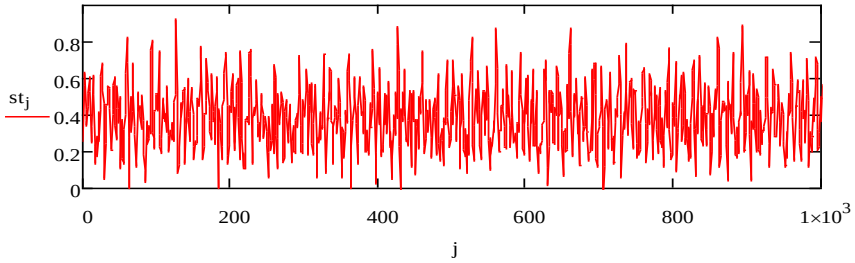


Рис.11. Осциллограмма модели частотно-модулированной шумовой помехи.

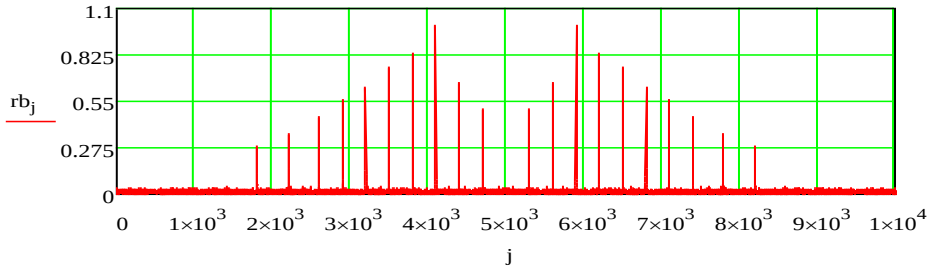


Рис.12. Модуль спектра частотно-модулированной шумовой помехи

Рассмотренные модели помех обладают заданной степенью адекватности и в равной степени применимы как для аналитического моделирования, так и с использованием аппаратно-программных средств LabView.

Заключение.

Проведенные исследования позволили сделать следующие выводы:

концепция ИМА существенно меняет подход к построению стендов проверки бортового оборудования на всех стадиях жизненного цикла;

предложены модульные модели помех средствам связи и управления перспективными гражданскими самолетами;

проведен учет влияния радиопомех в подсистемах связи и навигации самолета в стендах ИМА.

Полученные результаты позволяют адекватно моделировать воздействие вредоносного излучения на бортового оборудования связи и навигации ЛА, построенного по стандартным схемам ИМА.

Литература

1. Глинская Е.В., Чичварин Н.В. Моделирование угроз информационной безопасности бортовых вычислительных средств самолета. / Вестник МГТУ им. Н.Э. Баумана, сер. «Приборостроение», - 2016 - №6. с.85 -97.
2. Интернет – ресурс: www.aviasafety.ru/crash-stat, последний доступ – *20.04.2018*.

3. Интернет-ресурс: Информационная безопасность*, Android*, Блог компании «Apps4All», Последний доступ - 25.12.2016.
4. Интернет - ресурс: *Документы ИКАО* - Библиотека - Авиационный портал Airspot, *airspot.ru/library/dokumenty-ikao, последний доступ – 20.04.2018*
5. Богданов А.В. и др. Платформа интегрированной модульной авионики.- Патент на полезную модель №108868 U1 RU, МПК G06F 9/00, №2011121962/08. Заявл. 01.06.2011. Опубл. 27.09.2011.
6. Матвеев В.А., Бельфер Р.А., Глинская Е.В. Угрозы и методы защиты в сборных сенсорных узлах летающих сенсорных сетей // Вопросы кибербезопасности. 2015. № 5 (13). С. 26-31.
7. Интернет-ресурс: Маркерный канал, StudFiles.net›preview/3213119/, *последний доступ – 20.04.2018*
8. Герлих Х. Модульная система авионики самолета. - Патент №2413655 C2 RU, МПК B64C 19/00. №2008123940/11. Заявл. 16.11.2006. Опубл. 10.03.2011. Бюл. №7.
9. Джанджгава Г.И. Авионика пятого поколения: новые задачи – новая структура./ Евгенов А.В. Направления развития интегрированных комплексов бортового оборудования самолетов гражданской авиации. / Авиакосмическое приборостроение. – 2003. – № 3. – С. 48–53.
10. Ефанов В.Н. Открытые архитектуры в концепции авионики пятого поколения // Бодрунов С.Д. - Мир авионики. – 2004. – № 5. – С. 20–28.
11. Чичварин И.Н. Структурное моделирование угроз информационной безопасности систем автоматизированного проектирования / Вестник МГТУ. Серия Приборостроение – 2013, - №3. - С.58-75

Ways to protect modular avionics equipment from harmful effects

Volosatova T.M., Chichvarin N.V.

The results of research and analysis of methods for modeling threats to information security (IS) of communication systems and navigation of the aircraft, conducted in order to build a formalized model of threats to the on-board equipment complex are considered. The main attention is paid to the onboard equipment of communication and navigation equipment of the aircraft. It has been taken into account that in the conditions of increasing the level of automation of onboard equipment, systems and components of lethal apparatus, and the increasing complexity of onboard information systems, the problem of protecting electronic equipment (REA) from information security threats becomes essential. Research conducted on the basis of the analysis of modern integrated avionics (IMA).

Keywords: avionics, safety, computing facilities, information, model, navigation, aircraft, threats.

Literature

УДК 343.1:343.14:343:98

Средства криминалистического исследования фонограмм

Горшков Ю.Г.[21]

Выполнен анализ принципов построения средств криминалистического исследования фонограмм на основе преобразования Фурье. Изложена методология частотно-временного анализа речевого сигнала с использованием вейвлет-технологии. Приводится структура аппаратно-программного комплекса криминалистического исследования фонограмм на основе многоуровневого вейвлет-анализа «Эксперт МВА». Проведено сравнение частотно-временных характеристик сонограмм звуков речи, полученных с использованием преобразования Фурье и многоуровневого вейвлет-преобразования. Представлены примеры построения вейвлет-сонограмм с высоким частотно-временным разрешением.

Ключевые слова: *фонограмма, криминалистическое исследование, многоуровневый вейвлет-анализ*

Введение. Вопросы создания инструментальных средств анализа и методов криминалистического исследования аудиозаписей (фонограмм), их эффективного применения в практике экспертов-фоноскопистов за последние годы относятся к наиболее важным [1-8]. Особое значение при разработке новых методов исследования фонограмм придается решению задач, связанных с созданием надежной технологии обнаружения признаков их монтажа. Широкое распространение звуковых редакторов, доступных программ обработки и монтажа аудиозаписей привели к ситуации, когда фальсификация вещественных доказательств, в качестве которых могут быть фонограммы речи, является даже для непрофессионала относительно простой задачей. В то же время вопросы обнаружения признаков монтажа фонограмм, как правило, всегда относились к трудно разрешимым.

Комплексы криминалистического исследования фонограмм на основе преобразования Фурье. В настоящее время исследования, проводимые при анализе звуков речи, основываются на спектральной модели для стационарного сигнала. К недостаткам данной модели следует отнести отсутствие характеристик для основных шумовых составляющих в произносимых согласных и это при том, что в большинстве языков основная речевая информация передается согласными звуками. Практически во всех комплексах криминалистического исследования фонограмм реализованы алгоритмы идентификации личности по голосу с использованием исключительно характеристик гласных звуков. Разработанная специалистами ООО «Центр Речевых Технологий» методика криминалистической идентификации дикторов с использованием комплекса исследования фонограмм «Икар Лаб» является развитием известной методики идентификации дикторов «Диалект». Включает в себя на этапе инструментального анализа сравнение статистик основного тона голоса и формант, формантное «выравнивание», экспертное сравнение формант ударных гласных. В последние годы широкое применение находят комплексы «Justiphone» и «OTExpert». Принятие решения при идентификации личности по голосу в перечисленных средствах основывается на оценке спектральных характеристик гласных звуков, полученных на основе преобразования Фурье.

1 Горшков Юрий Георгиевич, к.т.н., доцент, МГТУ им. Н.Э. Баумана, Москва, y.gorshkov@npo-echelon.ru

Комплекс криминалистического исследования фонограмм с использованием многоуровневого вейвлет-анализа «Эксперт МВА». Специалистами ГК «НПО «Эшелон» и кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана созданы программно-аппаратные средства комплекса «Эксперт МВА» с использованием технологии многоуровневого вейвлет-анализа или высокоточной обработки речевых акустических сигналов аудиозаписей «речевой микроскоп» [4-7]. Назначение «Эксперт МВА» - криминалистическое исследование фонограмм, включающее определение подлинности аудиозаписей и идентификацию диктора. На рис. 1. представлена структура комплекса «Эксперт МВА».

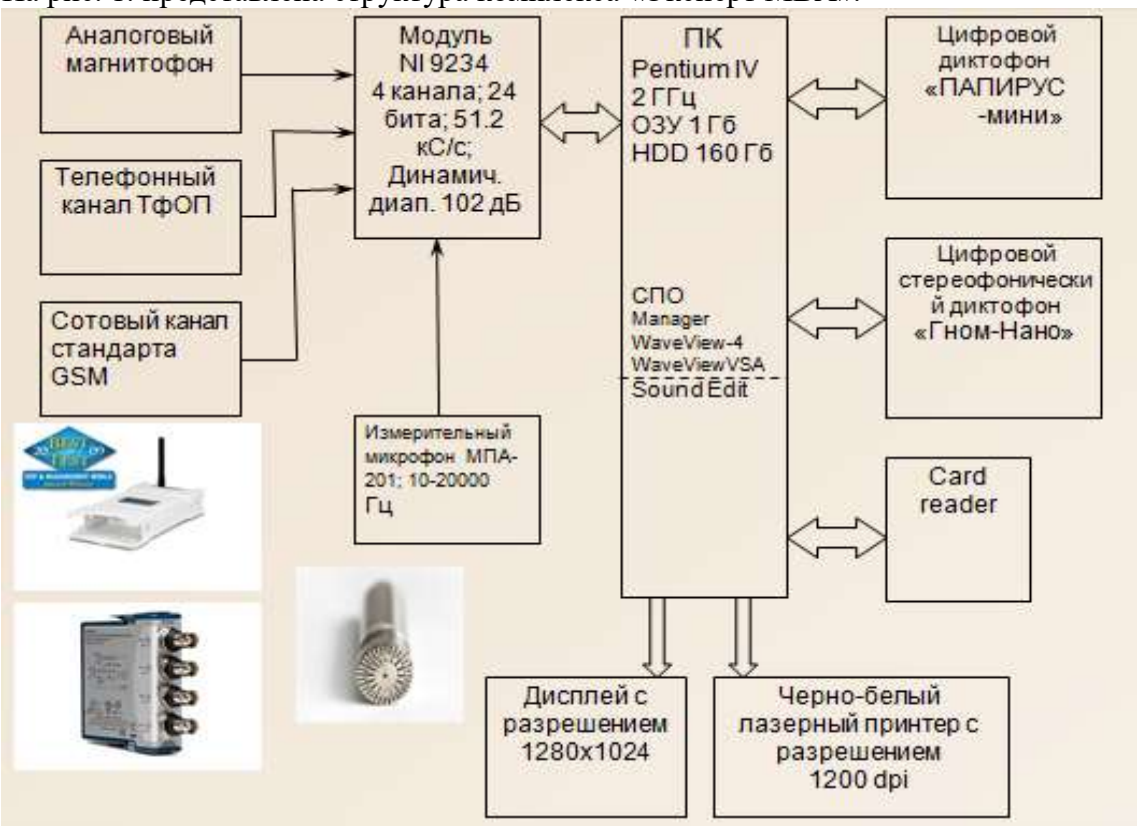


Рис. 1. Структура комплекса «Эксперт МВА»

Технические характеристики комплекса «ЭКСПЕРТ МВА»:

- 4-х канальный ввод звуковых сигналов с использованием модуля NI 9234, National Instruments (USA), 24 бита, 51.2 кС/с, динамический диапазон 102 дБ;
- голосовой ввод на базе измерительного микрофона МПА-201, AKG (Австрия), полоса частот: 10 Гц - 20 кГц;
- специальное программное обеспечение анализа сигналов «Manager», «WaveView-4», «WaveView VSA», «Sound Edit», диапазон обрабатываемых сигналов: 1 Гц - 10 кГц;
- защищенный индивидуальный профиль пользователя с записями (алгоритм шифрования AES), хранение записей пользователя в одном зашифрованном файле.

С использованием средств «Эксперт МВА» разработана новая методика инструментального исследования акустических сигналов аудиозаписей. Отличие данной методики от распространенных, построенных на основе Фурье-анализа,

заключается в том, что в ней применяется технология цифровой обработки речевых сигналов нового поколения - многоуровневый вейвлет-анализ (МВА).

Задачи, решаемые комплексом «Эксперт МВА» при проведении фоноскопической экспертизы:

1. Определение подлинности аудиозаписи.
2. Оценка эмоционального состояния говорящего.
3. Идентификация дикторов на основе построение высокоточных «звуковых портретов» гласных и согласных звуков.
4. Документирование акустической обстановки окружения.
5. Заключение о качестве аудиозаписи и соответствии характеристик, используемых средств регистрации предъявляемым требованиям.

Отличительные особенности комплекса криминалистического исследования фонограмм «Эксперт МВА»:

- получение частотно-временных параметров не только гласных, но и согласных звуков;
- обработка низкочастотных биомедицинских сигналов (10-30 Гц) говорящего;
- выделение сигналов фона сети питания 50 Гц малого уровня (до -60 дБ).

Выводы

Комплекс криминалистического исследования фонограмм с использованием многоуровневого вейвлет-анализа «Эксперт МВА» относится к средствам фоноскопической экспертизы нового поколения. Неоднократно применялся в судебной практике. Успешно демонстрировался на мероприятиях:

1. Международная научно-практическая конференция «СПЕЦ-криминалистическая техника». ФКУ «НПО «Специальная техника и связь» Министерства внутренних дел Российской Федерации 28 февраля 2017 года.
2. X Международный салон средств обеспечения безопасности «Комплексная безопасность 2017», 6-9 июня. Спасательный центр МЧС России. Ногинск.
3. Международный военно-технический форум «Армия-2018». 21-26 августа, КВЦ «Патриот», Московская область, г. Кубинка.

Литература

1. Горшков Ю.Г. Криминалистическое исследование фонограмм. Методические указания к лабораторным работам. МГТУ им. Н.Э. Баумана. 2017. 32 с.

2. Горшков Ю.Г. Обработка речевых и акустических биомедицинских сигналов на основе вейвлетов / Научное издание. М.: Радиотехника. 2017. 240 с.

3. Галяшина Е. И. К вопросу о достоверности криминалистической идентификации личности по цифровым фонограммам устной речи // Известия Тульского государственного университета. Экономические и юридические науки. 2016. Том 3, № 2. С. 19-25.

4. Горшков Ю.Г. Многоуровневый вейвлет-анализ акустических сигналов при решении задач фоноскопической экспертизы / «Информатизация и информационная безопасность правоохранительных органов»: Материалы XX Международной научной конференции. 2011. Москва. С. 379-387.

5. Горшков Ю. Г. Применение комплекса «ЭКСПЕРТ МВА» при криминалистическом исследовании фонограмм // Материалы XXIII Всероссийской научной конференции «Информатизация и информационная безопасность правоохранительных органов», 28 мая 2014 г. Москва. С. 212-217.

6. Горшков Ю. Г. Визуализация многоуровневого вейвлет-анализа фонограмм // Электронный журнал «Научная визуализация». Национальный Исследовательский Ядерный Университет «МИФИ». 2015. № 2. Том 7, квартал 2. С. 96-111.

7. Горшков Ю. Г., Каиндин А. М., Марков А. С., Цирлов В. Л. Система определения подлинности фонограмм. Патент на полезную модель RUS 150244. 30.12.2013. Заявка № 2013158829/08. Бюл. № 4.

8. Горшков Ю.Г. Тестирование средств засекречивания речи//Вопросы кибербезопасности. 2015. № 2 (10). С. 26-30.

PHONOGRAM FORENSIC INVESTIGATION TOOLS

Y.G. Gorshkov[1]

The principles of the construction of systems studies of phonogram forensic investigation tools based on the Fourier transform are analyzed. Methodology of the time-frequency analysis of the voice signal using the wavelet technology is presented. The paper provides the structure of a multilevel wavelet analysis based hardware software complex for forensic investigation of phonograms «Expert MBA». It compares the time-frequency characteristics of sonograms of speech sounds based on the Fourier transform and a multilevel wavelet transform. It provides examples to build wavelet sonograms with a high time-frequency resolution.

Keywords: *phonogram, forensic investigation, multilevel wavelet analysis*

1 Yuri Gorshkov, Ph.D., Bauman MSTU, Moscow, y.gorshkov@npo-echelon.ru

УДК 004.056

Методы применения машинного обучения для первичного анализа внутреннего программного обеспечения

Давыдов В.Н., студент, МГТУ им. Н.Э. Баумана, Москва, vovdavydo@yandex.ru

В результате данной исследовательской работы были разработаны и апробированы методы применения машинного обучения для первичного встроенного программного обеспечения, которые включают в себя методы определения типа данных, адресов начала функций и определение заимствованных функций в исследуемом файле. Для решения первых двух описанных задач была использована рекурентная нейронная сеть, а для решения третьей задачи был использован метод k-ближайших соседей (kNN) для выявления наиболее вероятной функции из базы библиотек. Описанные методы были реализованы на языке программирования Python и апробированы на тестовой выборке данных.

Ключевые слова: анализ двоичных файлов, нейронная сеть, машинное обучение, обратная разработка.

Введение

В настоящее время количество электронных устройств очень быстро растет. Исследователям для решения различных целей зачастую требуется изучение внутреннего программного обеспечения (ВПО) без доступа к исходным кодам программного обеспечения, в том числе и для определения и поиска НДВ во встроенном программном обеспечении. Это достаточно трудоемкая задача, что делает процесс исследования дорогостоящим и длительным, так как она не может быть полностью автоматизирована. Однако, в процессе обратной разработки можно выделить типовые этапы, которые могут быть частично или полностью автоматизированы, в том числе и при помощи использования различных технологий машинного обучения. Подобная автоматизация способна существенно сократить необходимое время для проведения анализа встроенного программного обеспечения устройства, что приведет к снижению себестоимости проведения исследования.

Выделение этапов задач для автоматизации

Процесс исследования ВПО устройства практически всегда начинается с извлечения образа ПЗУ из устройства и получения дизассемблированного кода. Обычно это делается при помощи дизассемблеров. В рассмотренном примере в качестве дизассемблера будет использована программа IDA Pro, так как она отличается от других дизассемблеров достаточно широкими возможностями и возможностью разработки плагинов (скриптов) на языке Python. При загрузке полученного образа в дизассемблер необходимо указать процессорную архитектуру целевой платформы, которая может быть недоступна по разным причинам (нет документации на процессорное устройство, отсутствующая маркировка на чипе, отсутствие устройства и т.д.). В подобных случаях приходится перебирать все возможные архитектуры и различные порядки байт и убеждаться в корректности подбора процессорной архитектуры, что занимает достаточно большой промежуток времени при относительно большом образе ПЗУ. При загрузке также следует правильно указать адрес размещения образа ПЗУ, который также может быть заранее неизвестен по вышеперечисленным причинам. Кроме того, в случае, если в устройстве есть загрузчик нулевого уровня, который осуществляет размещение данных из ПЗУ в определенные места адресного пространства, то адрес загрузки будет неизвестен даже при наличии документации на процессорное устройство.

После определения процессорной архитектуры необходимо получить адреса старта всех функций и прочих ресурсов (изображений, архивов, строк, таблиц и т.д.) с классификацией блоков данных на различные типы.

При дальнейшем анализе ВПО следует учесть тот факт, что большая часть кода заимствуется при помощи использования различных библиотек с открытым исходным кодом [1]. В случае, если распознать функции из открытых библиотек в ВПО, то дальнейший анализ будет существенно проще и быстрее, так как зачастую НДВ связано с различными интерфейсами передачи данных, которые, как правило, реализованы в стандартных библиотеках. Кроме того, в случае, если в процессе анализа существует возможность установить версию или время сборки ВПО, существует возможность определить наличие опубликованных уязвимостей в используемых библиотеках при помощи использования базы уязвимостей.

Описание алгоритма работы

На первом этапе алгоритма необходимо определить тип данных, которые находятся в ПЗУ. Стоит учесть тот факт, что в ПЗУ могут находится различные типы данных, например, исполняемый код определенной архитектуры, строки, сжатые данные и т.д. На выходе первый этап алгоритма должен выдать информацию о том, какого типа данные находятся в том или ином месте программы. Для реализации этого этапа была применена рекуррентная нейронная сеть [2]. Этот выбор был обусловлен тем, что архитектура этой нейронной сети способна обрабатывать «цепочки» информации [3, 4], которые, в нашем случае, представляют байты, полученные их ПЗУ. Пример визуализированных выходных данных приведены на рисунке 1.

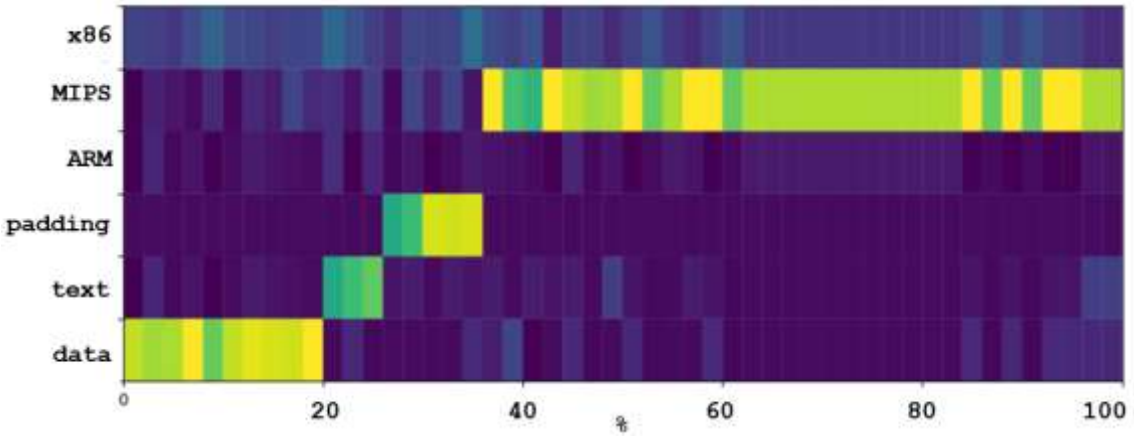


Рис.1. Пример выходных визуализированных данных после первого этапа

В приведенном примере видно, что система определила, что первые 20% тестового файла занимают неопределенные данные, после которых находится текст, далее находится отступ (пространство, которое зачастую забито определенными константами), далее находится исполняемый код для платформы MIPS.

Далее, для определенной выше архитектуры при помощи рекуррентной нейронной сети (LSTM [5]) определяются адреса начала функций. После этого этапа создается список адресов начала функций.

Далее, используя данные, полученные на первых двух этапах, следует произвести загрузку двоичного файла в программу IDA Pro.

После создание базы ВПО в дизассемблере IDA Pro следует начать поиск заимствованного кода [6]. Для этого был получен комплекс параметров («Features»), по которым будет производиться поиск заимствованных функций из

открытых библиотек:

- размер буфера в стеке для функции;
- количество арифметических инструкций;
- количество логических инструкций;
- количество инструкций записи в память;
- количество инструкций чтения из памяти;
- общее количество инструкций;
- общее количество блоков;
- количество безусловных переходов;
- количество условных переходов;
- количество внутренних вызовов функций;
- значения констант, используемых в функции;
- количество входных параметров.

На основании параметров, вычисленных при помощи программы IDA Pro, в пространстве, базисом которого являются вышеперечисленные параметры, строятся точки, которые отождествляются с определенными функциями для каждой «эталонной» библиотеки. Далее, при поиске заимствованного кода, вычисляется координата исследуемой функции в этом пространстве и при помощи метода поиска k-ближайших соседей (kNN) [7] выполняется поиск ближайшей функции. В случае, если расстояние до ближайшей функции превышает максимально допустимое, то считается, что функция не найдена, и она остается нераспознанной.

В результате, после анализа всех функций, будут определены все заимствованные функции.

Стоит отметить, что необходимо определить коэффициенты в векторе ошибок для каждого составляющего базиса – это может быть сделано при помощи метода градиентного спуска, минимизируя функцию общей ошибки на обучающих данных.

Выводы

В результате данной исследовательской работы были проанализированы и апробированы различные методы и подходы использования машинного обучения для первичного анализа двоичных файлов. Было выделено три этапа в процессе проведения анализа внутреннего программного обеспечения: определение типа данных и целевой процессорной архитектуры для кода; для блока кода определение адресов начала функций; поиск функций, которые были взяты из открытых библиотек, добавленных в разрабатываемую систему. Первые два этапа используют технологию рекуррентных нейронных сетей, а третий этап использует метод k-ближайших соседей для поиска наиболее подходящей функции в базе с эталонными функциями.

В процессе обучения удалось получить точность определения типа данных и целевой процессорной архитектуры в 95%. Получение списка адресов начал функций происходит с точностью 97%, при чем баланс был намеренно сдвинут в сторону ошибки второго рода, так как в задаче определения функций предпочтительнее не создать функцию, там, где она действительно есть, нежели чем создать несуществующую функцию, что может ввести исследователя в заблуждение.

Данные методы способны существенно ускорить процесс исследования встроенного программного обеспечения, решая достаточно трудоемкие, но

однотипные задачи первичного анализа двоичных файлов.

Литература

1. Воробьев К.А., Климина Д.А. Поиск заимствованных фрагментов в исходном программном коде // Актуальные вопросы науки и техники 2017 С. 62-64.
2. Будыльский Д. В. GRU и LSTM: Современные рекуррентные нейронные сети // Общество с ограниченной ответственностью "Издательство Молодой ученый" 2015 С. 51-54.
3. Куликов Г.С., Грачев Н.С., Кудинов В.А. Анализ тональности текста с помощью рекуррентных нейронных сетей // Научный альманах 2016 С. 401-404.
4. Сбоев А. Г., Воронина И. Е., Гудовских Д. В., Селиванов А. А. Продвинутые нейросетевые модели для решения задачи определения тональности // Вестник воронежского государственного университета. Серия: Системный анализ и информационные технологии 2016 С. 178-183
5. Будыльский Д. В. GRU и LSTM: Современные рекуррентные нейронные сети // Общество с ограниченной ответственностью "Издательство Молодой ученый" 2015 С. 51-54.
6. Юмаганов А.С., Мясников В.В. Поиск похожих последовательностей кода в исполняемых файлах на основе структурного анализа функций // Сборник трудов ИТНТ-2018. Самарский национальный исследовательский университет имени академика С.П. Королева. 2018 С. 2429-2436.
7. Щелконогов А.Н. Аспекты решения задачи классификации на основе алгоритма KNN-алгоритма // Прикладные исследования и технологии ART2018 2018 С. 176-178.

Научный руководитель: Басараб Михаил Алексеевич, доктор технических наук, профессор, МГТУ им. Н.Э. Баумана, basarab.iu8@gmail.com

METHODS OF APPLICATION OF MACHINE LEARNING FOR PRIMARY ANALYSIS OF FIRMWARE.

Davydov V.N., student, Bauman Moscow State University, Moscow, vovdavydo@yandex.ru

As a result of this research, methods of applying machine learning for primary firmware were developed and tested, which include methods for determining the type of input data, addresses of the beginning of functions and determining borrowed functions in the file. To solve the first two problems described, a recurrent neural network was used, and to solve the third problem, the k-nearest neighbors (kNN) method was used to identify the most probable function from the library base. The described methods were implemented in the Python programming language and tested on a test data sample.

Key words: binary analysis, neural network, machine learning, reverse engineering.

УДК 004.056

Выявление аномальной активности пользователей интернет-ресурсов

Давыдов В.Н.[22]

В результате данной исследовательской работы была разработана и апробирована комплексная система для выявления аномальной активности пользователей интернет-ресурсов на примере социальной сети «Instagram». Разработанная система классифицирует запросы пользователей к защищаемому интернет-ресурсу и выдает вероятность принадлежности обрабатываемого запроса к легитимному запросу или аномальному. Обучающие данные для обоих классов были сгенерированы в процессе данной исследовательской работы. Решение о принадлежности запроса к определенному классу выносится на основании двух независимых модулей системы.

Ключевые слова: бот, аномальная активность, интернет-ресурс, машинное обучение.

Введение

В настоящее время в сети "Интернет" существует множество сервисов, которые представляют услуги различной направленности - доступа к файлам (файлообменники, системы контроля версий и прочее), медийные (новостные ресурсы, видео, аудио и фото-хостинги), социальные (мессенджеры, социальные сети и прочее). Перечисленные выше ресурсы пользуются большой популярностью. Некоторые из этих ресурсов ежедневно обслуживают многомиллионную аудиторию. Например, ресурс Facebook ежедневно посещает 720 млн уникальных пользователей. Ежемесячно Instagram использует - 700 млн пользователей, VK - 97 млн пользователей, YouTube – порядка 1 млрд пользователей.

Подобная популярность делает эти ресурсы крайне заманчивыми и для злоумышленников, которые пытаются использовать эту популярность для получения своей выгоды в обход пользовательскому соглашению. Кроме того, злоумышленники могут осуществлять действия, для намеренного причинению вреда сервису - расходование ресурсов сервиса (загрузку ненужных данных большого объема, слишком частое использование сложных запросов и прочее), занятия множества имен и(или) идентификаторов и так далее.

Для недопущения подобных ситуаций, которые могут нарушить работу сервиса или сделать его менее привлекательным для пользователей, вводятся различные системы для выявления и предотвращения аномальной активности пользователей [1].

Использование стандартных механизмов для ограничения действий ботов (например, CAPTCHA) далеко не всегда является хорошим решением, так как при слишком частом использовании ее в интернет-ресурсе, она делает его менее привлекательным для пользователя. Кроме того, в наше время существуют различные решения [2, 3] для обхода подобных систем.

Получение обучающих данных

Для получения обучающих данных обоих классов необходимо было получить трафик обмена данными между клиентом социальной сети «Instagram» и сервером. Обучающие данные, относящиеся к классу «легитимные действия» были получены при помощи использования связки прокси-сервер Fiddler и эмулятор смартфона на

[22] Давыдов Владимир Никитич, студент, МГТУ им. Н.Э. Баумана, Москва, vovdavydo@yandex.ru

операционной системе Android Nox. После настройки эмулятора и прокси-сервера для захвата трафика, производилось использование официального приложения сервиса «Instagram». Полученные данные были сохранены в формате JSON [4] и поданы на вход обучающей системы. Данные, относящиеся к классу «аномальные действия» также были получены при помощи использования прокси-сервера, но в качестве клиента были использованы боты, работающие по различным алгоритмам и выполняющие различные задания – сбор данных, раскрутка своего аккаунта, раскрутка другого ресурса, регистрация новых пользователей. Полученные пакеты были также сохранены в формате JSON.

Описание алгоритма работы

Разработанный алгоритм содержит в себе две системы для выявления аномальной активности.

Первая система представляет из себя фильтр невозможных запросов. Для некоторых запросов (постановка комментария, осуществление подписки или постановка лайка) сопровождается рядом предшествующих запросов. Эти запросы не обязательно выполнять для совершения вышеописанных действий, но в случае, если запросы формируются лицензионным приложением, последовательность запросов будет строго соблюдена (рис. 1).

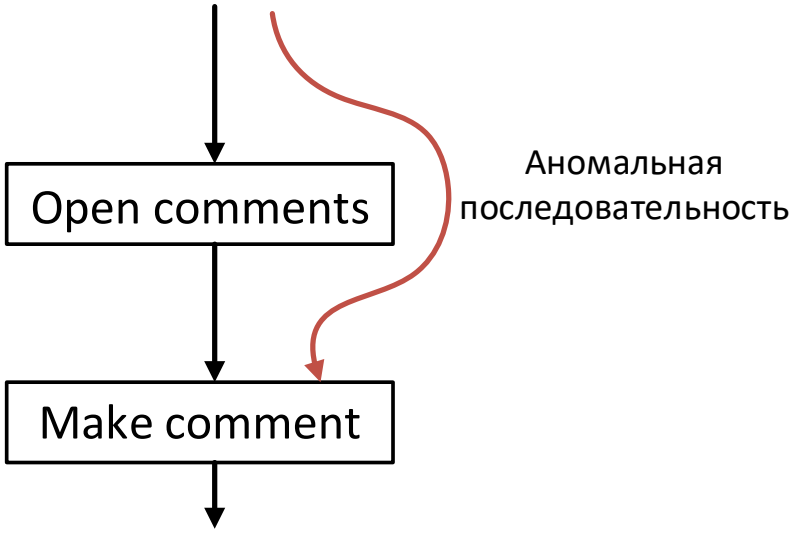


Рис.1. Пример аномальной последовательности запросов

Для того, чтобы оставить комментарий под записью в сети «Instagram» лицензионное приложение в начале отправляет запрос на получения списка уже размещенных комментариев. После этого запроса возможна отправка запроса на размещение нового комментария. Запрос на размещение комментария без запроса на открытие списка комментариев не возможен при работе лицензионного приложения. Стоит отметить, что API многих интернет-ресурсов, как открытое, так и закрытое все же обрабатывает подобные запросы.

В случае, если была выявлена подобная аномальная цепочка запросов, система принимает решение о том, что действие аномальное.

Вторая система представляет из себя классификатор [5, 6], который решает, к какому классу (легитимному или аномальному), отнести текущего пользователя. Классификация происходит на основе анализа характеристики текущего объекта по различным критериям, подробное описание которых будет приведено ниже.

Обработка данных

Рассмотрим более подробно структурную схему работы системы (рис. 2).

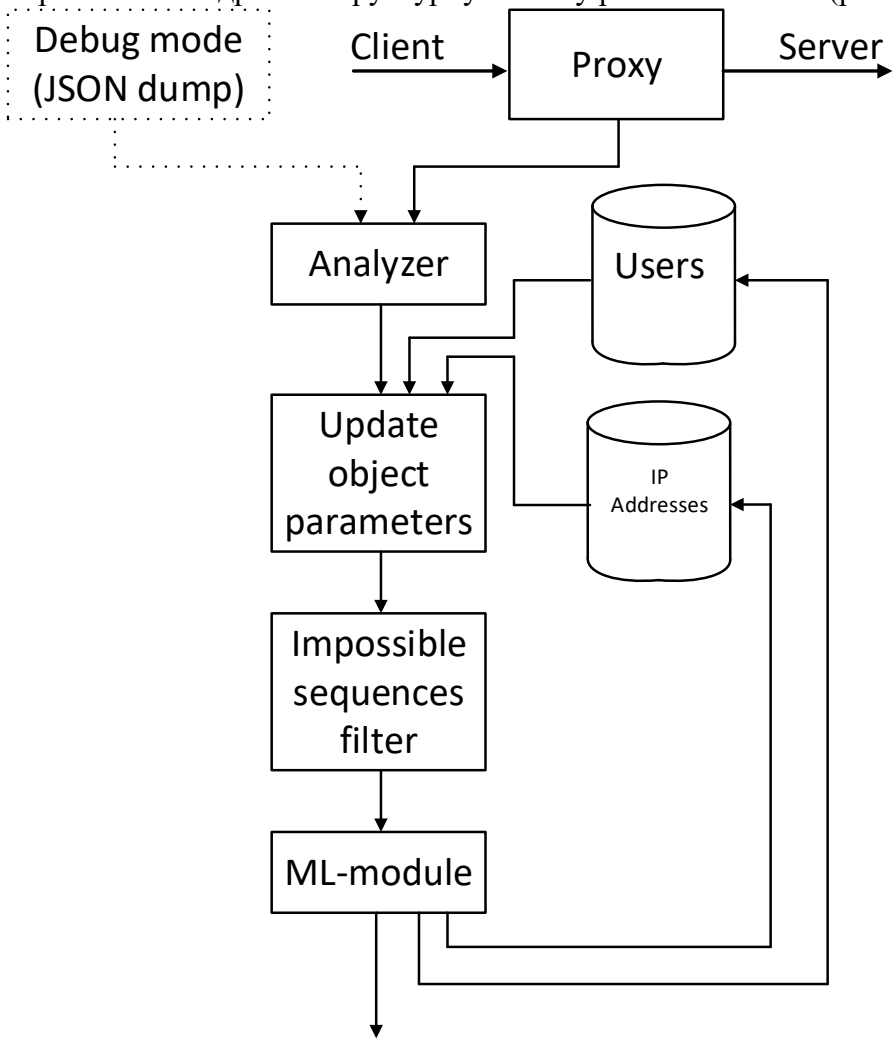


Рис.2. Структурная схема работы системы выявления аномальной активности пользователей

Система последовательно обрабатывает каждый входящий пакет. На основе каждого пакета обновляется характеристика конкретного пользователя или, в случае, если пользователь на этот момент не установлен (в момент регистрации или попытке входа), IP-адреса клиента.

Характеристика специфична для каждого ресурса. В рамках данной работы были составлены следующие характеристики для каждой сущности. Для сущности «пользователь» это:

- среднесуточное время онлайн, $T_{average\text{-}online}$;
- количество подписок, $N_{subscription}$;
- количество подписчиков, $N_{subscriber}$;
- количество лайков за последние сутки, $N_{likes\text{-}last\text{-}day}$;
- среднесуточное количество лайков, $N_{likes\text{-}average}$;
- количество комментариев за последние сутки, $N_{comments\text{-}last\text{-}day}$;
- среднесуточное количество комментариев, $N_{comments\text{-}average}$;

- количество подписок за сутки, $N_{subscription\text{-}last\text{-}day}$;
- среднесуточное количество подписок за последние сутки, $N_{subscription\text{-}average}$;
- текущий уровень доверия, TL.

Для сущности «IP-адрес» это:

- среднесуточное количество входов, $N_{logins\text{-}\ average}$;
- среднесуточное количество неуспешных входов, $N_{fail\text{-}logins}$;
- количество входов за последние сутки, $N_{logins\text{-}last\text{-}day}$;
- среднесуточное количество регистраций, $N_{register\text{-}\ average}$;
- количество регистраций за последние сутки, $N_{register\text{-}last\text{-}day}$;
- принадлежность к списку открытых прокси, PRX;
- текущий уровень доверия, TL.

Далее происходит обработка первым фильтром – фильтром невозможных запросов.

После обработки данных первым фильтром происходит обработка обновленной характеристики пользователя вторым модулем. После получения результатов от обоих компонентов системы, происходит обновления уровня доверия к текущему объекту.

Выводы

В результате данной исследовательской работы была разработана система, которая смогла идентифицировать 75% пользователей, от которых исходит аномальная активность в рамках данного исследования. Текущий бот-фильтр сервиса «Instagram» смог определить лишь 25% от того же трафика. При этом процент ложных срабатываний составлял 5% от всех пользователей, от которых исходил легитимный трафик.

Стоит отметить, что при применении этой системы в реальном интернет-ресурсе в характеристику могут входить другие параметры, которые повышают уровень доверия к конкретному пользователю, например, авторизация при помощи привязки аккаунта к номеру телефона или подтверждению того, что этот аккаунт не является ботом, а принадлежит популярной персоне. Например, в процессе исследования активности различных пользователей в интернет-ресурсе «Instagram», было обнаружено, что среднесуточная активность аккаунтов знаменитостей может быть практически круглосуточной, в то время, среднесуточная активность среднестатистического пользователя составляла 1,5 часа в день. При использовании разработанного классификатора, аккаунты со столь высокой активностью могут быть отнесены к классу «аномальные», хотя в действительности, они являются легитимными.

Литература

1. Сачков И.К., Назаров А.Н. автоматизация противодействия бот-атакам // T-COMM: ТЕЛЕКОММУНИКАЦИИ И ТРАНСПОРТ. том: 8, номер: 6, 2014. С. 5-9.

2. Жданов О.Н. распознавание современных CAPTCHA // научный вестник воронежского государственного архитектурно-строительного университета. Серия: студент и наука. 2014. № 6 (10). С. 221-224.

3. Гуськова А.М. исследование эффективности применения captcha как средства защиты сайтов // современные тенденции развития науки и технологий 2015. № 5-2. С. 12-17.

4. Шмидт И.А. выбор оптимальной json-модели для хранения результатов испытаний // фундаментальные исследования изд. Издательский Дом "Академия Естествознания" 2016. № 11-3. С. 620-625.

5. Ботабеков М.А. development of programs for recognition of human emotional state // news of science and education т.2, 2017. № 9. С. 15-23.

6. БотабекоВ М.А, Рашитулы А. применение методов машинного обучения для выявления

бот-трафика среди запросов к веб-приложению // СБОРНИК СТУДЕНЧЕСКИХ НАУЧНЫХ РАБОТ ФАКУЛЬТЕТА КОМПЬЮТЕРНЫХ НАУК ВГУ МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» т.2, 2017. С. 119-123.

Научный руководитель: Басараб Михаил Алексеевич, доктор технических наук, профессор, МГТУ им. Н.Э. Баумана, basarab.iu8@gmail.com

THE ARTICLE TITLE

Davydov V.N.[23]

As a result of this research, a complex system was developed and tested to detect abnormal activity of users of Internet resources using the example of the social network "Instagram". The developed system classifies user requests to the protected Internet resource and gives the probability of belonging to the processed request to the legitimate request or anomalous. Training data for both classes were generated during this research work. The decision on whether the request belongs to a particular class is made on the basis of two independent modules of the system.

Key words: bot, abnormal activity, Internet resource, machine learning.

[23] Vladimir Davydov, student, Bauman Moscow State University, Moscow, vovdavydo@yandex.ru

УДК 004.056

Передача скрытых сообщений с использованием протоколов без гарантированной доставки пакетов.

Демченко И.А.[24]

Объектом исследования является сетевая стеганография. Цель исследования — рассмотрение возможности передачи секретных сообщений при помощи протоколов без гарантированной доставки пакетов. В результате исследования было выявлено, что подобные протоколы можно использовать в стеганографии, но для этого требуется предварительное тестирование канала связи. Кроме этого скрываемую информацию необходимо подвергать помехоустойчивому кодированию каскадным кодом, основанным на блочных кодах. Вместо стегоключа необходимо использовать флаги, указывающие на те пакеты, которые содержат в себе скрытые сообщения.

Ключевые слова: стеганография, пакеты, флаг, помехоустойчивое кодирование

Введение. Сетевая стеганография – вид стеганографии, в котором в качестве носителя секретной информации используют сетевые протоколы эталонной модели Open System Interconnection (OSI). Сетевую стеганографию можно представить в виде ряда методов модификации данных в заголовках сетевых протоколов и в полях полезной нагрузки пакетов. К сетевой стеганографии также относят изменение структуры передачи пакетов и гибридные методы в том или ином сетевом протоколе (иногда нескольких сразу) [1].

Возможность использования протокола без гарантированной доставки пакетов в стеганографии. Сетевая стеганография зачастую реализуется при использовании протоколов, гарантирующих доставку пакетов (например, TCP). Но многие популярные типы потокового контента в сети Интернет, такие, как видеотрансляции в прямом эфире, интернет-радио, IP-телефония, часто используют протоколы без гарантированной доставки. Большой объем данных, передающихся с использованием таких протоколов, делает привлекательной идею использовать подобные протоколы для передачи скрытых сообщений. Примером такого протокола может служить UDP.

Передача скрытых сообщений через подобные протоколы может быть сопряжена со следующими проблемами:

1 Возможная потеря пакетов при передаче.
2 Нарушенный порядок получения пакетов.

Для оценки возможных потерь пакетов при передаче был проведен эксперимент.

В эксперименте генерируются последовательности UDP-пакетов, которые передаются из узла А в узел Б. В узле Б принимаемые пакеты подсчитываются, и программа формирует статистику, какой процент пакетов был успешно принят. Для уменьшения элемента случайности последовательность каждой длины подается несколько раз. По результатам эксперимента (табл.1) в последовательности длиной 1000 и больше пакетов наблюдается большой разброс значений процентов принятия пакетов. Такая ситуация не позволяет без дополнительных условий использовать данный протокол для стеганографии.

[24] Демченко Иван Александрович — студент кафедры «Информационная безопасность», МГТУ им. Н. Э. Баумана, Москва, Российская Федерация, demchenko.ivan96@gmail.com.

Таблица 1

Результаты теста. Процент успешного принятия пакетов на маршрутах

Кол-во отправ. пакетов	10	100	1 000	10 000	100 000	1 000 000
Владыкино-Вешняки	100%	100%	63%	19%	10%	9%
Кунцево-Вешняки	100%	100%	100%	65%	37%	37%
Измайлово-Вешняки	100%	100%	100%	98%	99%	99%
Раменское-Вешняки	100%	100%	97%	97%	97%	96%

К потере пакетов могло привести воздействие разнообразных дестабилизирующих факторов на сети связи, а также активизация систем обнаружения вторжения (IDS) провайдеров.

Рассмотрим введение задержки между пакетами. Это сильно влияет на скорость, так как количество генерируемых пакетов может достигать нескольких десятков тысяч. Проведем подобные тесты для последовательностей пакетов, при передаче которых была введена задержка между пакетами в 1 мс. По результатам эксперимента (табл. 2) процент успешно принятых пакетов стабилизировался и стал равен 98-100% даже при передаче последовательностей до 1 000 000 пакетов. Данные цифры уже дают повод говорить, что при некоторых условиях передача стегосообщений по протоколам передачи без гарантированной доставки пакетов возможны, но требуют предварительного тестирования канала связи.

Таблица 2

Результаты теста. Процент успешного принятия пакетов на маршрутах при задержке в 1 мс

Кол-во отправ. пакетов	10	100	1 000	10 000	100 000	1 000 000
Владыкино-Вешняки	100%	99%	99%	98%	98%	99%
Кунцево-Вешняки	100%	100%	100%	99%	99%	99%
Измайлово-Вешняки	100%	100%	100%	99%	98%	99%
Раменское-Вешняки	100%	100%	99%	98%	99%	99%

Проблема использования стегоключа. Допустимое протоколами данного типа нарушение порядка пакетов делает невозможным использование стегоключа, указывающего на порядковый номер пакета, из которого следует извлекать информацию. Разработан алгоритм на основе идеи флагов. В каждом пакете, в котором скрыта часть стегосообщения, выделяется некоторое количество бит под флаг — N. Выбор параметра N можно производить, уже отталкиваясь от конкретного алгоритма встраивания. Приложение, принимающее скрываемое сообщение, будет сканировать входящие пакеты на наличие флага в заранее определенном месте и при нахождении его считывать биты скрываемого сообщения.

В каждом следующем пакете, содержащем скрываемое сообщение, число флага будет увеличиваться на единицу, до достижения максимально возможного исходя из его разрядности (2^N–1), затем после максимального числа будет вновь передаваться число «0» и процесс увеличения числа на единицу будет повторен.

Необходимо искать сразу несколько последовательных флагов, на случай, если один или несколько последовательных пакетов будет потеряно. При нахождении флага, отличающегося от предыдущего более чем на единицу, следует количество бит, которое должно было находиться в потерянных пакетах, считать равным нулю. При потере количества пакетов, превышающих возможность

исправления корректирующим кодом, следует отправить отправителю сигнал об ошибке передачи и месте скрываемого сообщения, где произошел обрыв приема.

Помехоустойчивое кодирование. Помехоустойчивое кодирование необходимо по следующим причинам:

1 Возможные ошибки при передаче пакета, повлекшие за собой ошибки в поле данных пакета.
2 Ошибочные считывания данных скрытых сообщений из пакетов, не содержащих их, из-за ошибочного детектирования флагов.
3 Потеря пакетов, содержащих в себе скрытое сообщение.

Классификация помехоустойчивых кодов насчитывает более сотни различных наименований [2, 3], однако зачастую в этой предметной области различают всего три основных направления: это блоковые коды, непрерывные (или сверточные) коды и турбокоды (каскадные коды).

Блоковые коды, как правило, хорошо справляются с редкими, но большими пачками ошибок; их эффективность при частых, но небольших ошибках (например, в канале с аддитивным белым гауссовским шумом), менее высока. Сверточные коды эффективно работают в канале с белым шумом, но плохо справляются с пакетами ошибок. Более того, если декодер ошибается, на его выходе всегда возникает пакет ошибок [4].

Исследования последних лет показали много общего между блоковыми и сверточными кодами. В ряде работ свойства этих кодов объединяются, но новой информации о свойствах кодов это объединение не дает [5-10]. Сверточный код может быть представлен как систематический.

Преимущества разных способов кодирования можно объединить, применив каскадное кодирование. При этом информация сначала кодируется одним кодом, а затем другим, в результате получается код-произведение.

Возвращаясь к задаче данной работы, отметим, что при ошибочном детектировании флага в считанной информации может быть как одиночная ошибка, так и пакет ошибок. При потере пакета с флагом, мы получим сразу пакет ошибок. Поскольку с пакетами ошибок лучше справляются блоковые коды, то и выбираемый алгоритм каскадного кодирования должен основываться на блоковых кодах.

Выводы. Проведенный эксперимент показал, что передача скрытых сообщений с помощью протоколов без гарантированной доставки пакетов возможна, но имеет ряд ограничений. Для передачи требуется предварительное тестирование канала связи и настраивание параметров передачи стегосообщений.

Вместо традиционных форматов стегоключа предложен алгоритм встраивания в пакеты со скрытыми сообщениями флагов.

При передаче скрываемого сообщения с использованием исследуемого типа протоколов существует необходимость применения помехоустойчивого каскадного кодирования блочными кодами.

Литература

1 Бзовская А.Д. Сетевая стеганография как способ защиты информации, передаваемой по открытым каналам связи // Альманах мировой науки 2016. № 10-1(13) С. 55-57. URL: http://scjour.ru/docs/amn.2016.10.01.pdf
2 Математика. Большой энциклопедический словарь / Гл. ред. Прохоров Ю.В. 3-е изд.– М.: Большая Российская энциклопедия, 1998. – 848 с.
3 Прокис, Джон. Цифровая связь / Джон. Прокис; пер. с англ.; под редакцией Д. Д. Кловского.– М.: Радио и связь, 2000. – 800 с.
4 Помехозащищенное кодирование. Коды Хэмминга: Методические указания к лабораторной работе / М.В. Долгоруков, В.В.Беспалько, О. Е. Александров. Екатеринбург:

кафедра молекулярной физики УГТУ-УПИ, 2008. 34 с.
5 Банкет В. Л. Цифровые методы в спутниковой связи / В. Л. Банкет, В. М. Дорофеев. – М.: Радио и связь, 1988. – 240 с.
6 Велдон, И. Дж. Циклические коды, задаваемые разностными множествами / И. Дж. Велдон // Некоторые вопросы теории кодирования. – М., 1970. – С.9–21.
7 Возенкрафт, Дж. Последовательное декодирование / Дж. Возенкрафт и Рейффен. М.: Иностр. лит-ра, 1963.– 152 с.
8 Злотник, Б. М. Помехоустойчивые коды в системах связи / Б. М. Злотник // Статистическая теория связи. – М.: Радио и связь, Вып. 31, 1989. – 232 с.
9 Зяблов, В. В. Метод обнаружения ошибочного декодирования с использованием списков / В. В. Зяблов, М. А. Цветков // Информационные процессы. – 2004. – Т .4. № 2. – С. 188–201.
10 Viterbo E. and Boutros J. A universal lattice code decoder for fading channels, IEEE Trans. On Inform. Theory, vol. 45, pp. 1639–1642, July 1999.

Научный руководитель: Зайцева Анастасия Владленовна, кандидат технических наук, доцент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация, zav@bmstu.ru.

Transmission of hidden messages using protocols with no guaranteed packet delivery

Demchenko I.A.[25]

The object of research is network steganography. The objective of the present study was to determine the possibility of transmitting secret messages using protocols without guaranteed packet delivery. The study has shown that such protocols can be used in steganography, however, preliminary testing of the communication channel is required. Besides, secret messages must be encoded with error-correcting concatenated codes based on block codes. Instead of a stego key, special flags must be used to indicate packets that contain hidden messages.

Keywords: steganography, packets, flag, error-correction coding.

[25]Demchenko Ivan Aleksandrovich. — student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation., demchenko.ivan96@gmail.com

УДК 004.056.55, 004.056.55

Клеточные автоматы в криптографии

Жоголев Г.Д.[26]

В настоящей статье рассматривается применимость теории клеточных автоматов в криптографии. Обозреваются публикации, исследующие методы получения приложимых в криптографии свойств клеточных автоматов. Также обозреваются статьи, в которых строятся криптографические модели, основанные на клеточных автоматах, рассматривается применение клеточных автоматов к построению криптографических алгоритмов.

Ключевые слова: однородные структуры, генератор псевдослучайных последовательностей, вычислимость, граф Рамануджана, лавинный эффект, бент-функции.

Введение

Клеточные автоматы находят широкое применение в криптографии [1-4]. Клеточный автомат определяется следующим образом [5]: некоторое пространство с ортонормированным базисом разобьем целочисленными координатными прямыми на ячейки. Сопоставим каждой ячейке упорядоченное множество ячеек, которые будут считаться соседними с ней, множество будет составляться по одинаковому правилу для всех ячеек. Сопоставим каждой ячейке множество значений (состояний), которые она может принимать, множество значений также одинаково для всех ячеек. Одинаковым для всех ячеек будет и правило изменения состояния ячейки. Для этой модели время будет течь дискретными шагами. Каждый такт ячейка, исходя из состояний ее соседей, будет вычислять свое значение для следующего такта работы системы. Таким образом для данной модели характерны следующие свойства:

Дискретность течения времени.

Локальность действия правила преобразования значения ячейки.

Однородность модели. Для всех ячеек действуют одинаковые законы в независимости от их расположения.

Несмотря на кажущуюся простоту модели, зачастую поведение клеточных автоматов зачастую оказывается сложным и способным моделировать поведение различных физических систем [5, 6]. Клеточные автоматы находят свое применение и в теории параллельных вычислений. Также многие ученые обращали свое внимание на самовоспроизводящееся поведение клеточных автоматов, в том числе [7, 8].

Некоторые свойства клеточных автоматов

В зависимости от исходных состояний и функций перехода, клеточные автоматы могут обладать различными свойствами. Как отметил Стивен Вольфрам [9-11], для клеточных автоматов может быть определена мера их сложности, изменяющаяся, которая позволяет судить об их поведении на временном промежутке. Сложность некоторых автоматов растет линейно или квадратично, рост сложности других может не поддаваться вычислению. Последнее позволяет предположить, что вычислить конечное поведение таких автоматов не представляется возможным за конечное число шагов. Исходя из чего многие возможные задачи, такие как «проблема остановки» или задача о восстановлении предыдущего состояния обобщенного клеточного автомата, рассмотренная в статье [12] могут быть сведены к NP-полным задачам, что, как и статистическое

[26] Жоголев Глеб Денисович, студент, МГТУ им. Н.Э. Баумана, г. Москва,zhogolevg@mail.ru

поведение клеточных автоматов [10], предоставляет возможности для применения их в криптографии.

Некоторые результаты в криптографии

Клеточные автоматы могут применяться в криптографии как часть системы криптографического преобразования или представлять каждый шаг своего развития как раунд преобразования. Во втором случае для расшифрования сообщения необходима обратимость клеточного автомата.

Иллюстрацией первого случая может служить генератор псевдослучайных последовательностей, разработанный Сухининым [13]. Где применяются статистические свойства клеточного автомата. Генератор случайных чисел построен в соответствии со следующими требованиями:

Выходные последовательности должны иметь большой период.

Статистические свойства выходных последовательностей не отличаются от статистических свойств случайных двоичных последовательностей.

Быстродействие алгоритмов должно быть высоким.

Генератор представляет собой два клеточных автомата размером 37x11 ячеек. Выбранные размеры обеспечивают высокую скорость работы генератора и уменьшают вероятность возникновения пространственных периодов в клеточных автоматах. Выходная последовательность получается из суммируемых по модулю два значений ячеек подрешетки автомата размера 32x8. Выбор для формирования выходной последовательности только части ячеек автоматов усложняет восстановление состояния клеточного автомата по выходной последовательности, для этих же целей служит операция побитового сложения по модулю два выходов двух автоматов. Стоит отметить, что автоматы действуют по разным правилам преобразования и имеют различное, специально подобранное, начальное заполнение.

Для обеспечения минимальной длины периода значение ячейки, максимально удаленной от ячеек, выбранных для формирования выходной последовательности клеточного автомата, складывается по модулю два с выходным значением регистра сдвига с линейными обратными связями. При этом минимальная длина периода T_G может быть оценена сверху как:

$$T_G < 2^{M_G} = 2^{M_{C_1}+M_{C_2}+M_R} \quad (1)$$

Здесь M_G – общее количество ячеек в генераторе, M_{C_1} количество ячеек в первом клеточном автомате, M_{C_2} количество ячеек во втором клеточном автомате, а M_R количество ячеек в регистре сдвига.

Нижняя граница T_G зависит от периода регистра сдвига с линейными обратными связями и может быть оценена как:

$$2^{M_R} - 1 \leq T_G \quad (2)$$

Оценка справедлива при условии примитивности характеристического многочлена регистра сдвига с линейными обратными связями.

Второй случай может быть представлен моделью симметричного блочного шифра, построенного на клеточном автомате [14]. Для блочного преобразования используется обратимый клеточный автомат, обладающий рассеивающими и перемешивающими свойствами. Размеры, размерность решетки, алфавит внутренних состояний, окрестность и шаблон соседства фиксированы. Обратимое правило развития клеточного автомата задается секретным ключом шифрования, в связи с чем вводится отображение K:

$$K: \{0,1\}^q \to T \quad (3)$$

Здесь q битовая длина ключа, T множество допустимых локальных функций перехода клеточного автомата. Для данной модели выделяется подмножество локальных функций перехода $\hat{T}$ множества T , обладающих свойствами перемешивания и рассеивания. И отображение K приобретает вид:

$$K: \{0,1\}^q \to \hat{T} \quad (4)$$

Одной из задач конструирования криптосистем обратимых клеточных автоматов будет поиск правил, позволяющих определить принадлежность локальной функции преобразования к множеству $\hat{T}$.

В связи с рассмотренными выше моделями криптографических устройств возникает вопрос обеспечения криптографических свойств клеточных автоматов, рассмотренный П.Г. Ключаревым для обобщенных автоматов в статье [15]. В этой статье П.Г. Ключарев строит семейство функций, удовлетворяющее условиям как можно большей нелинейности, равновесности. Семейство функции строится на основе конкатенаций бент-функций, построенных методом Ротхауса.

Бент-функция по методу Ротхауса строится:

$$\beta(x_1, y_1, \dots, x_k, y_k) = \bigoplus_{i=1}^{k} x_i y_i \oplus s(x_1, \dots, x_k) \quad (5)$$

Здесь $s(x_1, \dots, x_k)$ произвольная булева функция, $\beta(x_1, y_1, \dots, x_k, y_k)$ бент-функция. Далее строятся функции:

$$g_1(u, x_1, x_2, \dots, x_{2k}) = (1 \oplus u)\beta_1(x_1, \dots, x_{2k}) \oplus u\beta_2(x_1, \dots, x_{2k}) \quad (6)$$

$$g_2(v, u, x_1, x_2, \dots, x_{2k}) = (1 \oplus v)((1 \oplus u)\beta_1(x_1, \dots, x_{2k}) \oplus u\beta_2(x_1, \dots, x_{2k})) \oplus v((1 \oplus u)\beta_3(x_1, \dots, x_{2k}) \oplus u\beta_4(x_1, \dots, x_{2k})) \quad (7)$$

Функции g_i являются равновесными и применяются как локальные функции связи однородного клеточного автомата. Свойства таких функций (6), (7) позволяют получить равномерную выходную последовательность однородного обобщенного клеточного автомата, добиться большого периода клеточного автомата и оценить снизу этот период.

Получив семейство функций g_i естественно попробовать применить их для построения генератора псевдослучайных последовательностей, что сделано в работе [16]. Важным для применения в криптографии свойством клеточных автоматов является лавинный эффект способность динамической системы существенно изменять выходную последовательность при небольших изменениях входных данных. В работе [16] предложено для получения хороших свойств лавинного эффекта использовать для построения клеточного автомата граф Рамануджана.

Такие свойства графа Рамануджана, как диаметр графа D и некоторые другие, позволяют получить хорошие лавинные свойства.

Для графа Рамануджана размера n, степени k диаметр D удовлетворяет:

$$D = 2\log_{k-1} n + O(1) \quad (8)$$

Это соотношение показывает, что диаметр графа Рамануджана всего в два раза больше следующей нижней оценки диаметра регулярного графа:

$$D \geq \log_{k-1} n + 1 - \log_{k-1} k \quad (9)$$

Это обеспечивает хорошие лавинные свойства клеточного автомата.

Еще одним примером полезности свойств клеточных автоматов является хэш-функция на основе итераций обобщенного клеточного автомата, рассмотренная в работе [4]. Каждые несколько тактов работы клеточного автомата к его заполнению подмешивается очередной блок хэшируемого сообщения, после чего, через определенное количество шагов снимается выходное значение. Вычисление хэш-функции происходит по следующему алгоритму:

Этап абсорбирования:

$$(x_i, y_i) = F_{t_i}(x_{i-1} \oplus M_i, y_{i-1}) \quad (10)$$

Этап дополнительного перемешивания:

$$(h_1, z_1) = F_{t_2}(x_q, y_q) \quad (11)$$

Этап снятия значения

$$\left(h_{j+1}, z_{j+1}\right) = F_{t_3}\left(h_j, z_j\right) \quad (12)$$

Здесь M_i блок шифруемого сообщения, $F_t: \{0,1\}^N \to \{0,1\}^N$ функция перехода клеточного автомата, аргументом которой является начальное заполнение клеточного автомата, а значением заполнение клеточного автомата через t шагов.

Вывод

Рассмотрены способы построения генераторов псевдослучайных последовательностей, статистические свойства которых не отличаются от статистических свойств случайных двоичных последовательностей. Отмечена возможность моделирования свойств клеточных автоматов для получения свойств, применимых в криптографии. Рассмотрены алгоритмы шифрования, основанные на клеточных автоматах.

Литература

1. Жуков А.Е. Клеточные автоматы в криптографии. Часть 1. // Вопросы кибербезопасности. 2017. № 3 (21). С. 70-76. DOI: 10.21681/2311-3456-2017-3-70-76.
2. Жуков А.Е. Клеточные автоматы в криптографии. Часть 2 // Вопросы кибербезопасности. 2017. № 4 (22). С. 47-66. DOI: 10.21681/2311-3456-2017-4-47-66.
3. Зотов Я.А. Использование клеточных автоматов в симметричной криптосистеме // Вопросы кибербезопасности. 2015. № 3 (11). С. 43-45.
4. Ключарёв П.Г. Метод построения криптографических хэш-функций на основе итераций обобщенного клеточного автомата // Вопросы кибербезопасности. 2017. № 1 (19). С. 45-50. DOI: 10.21681/2311-3456-2017-1-45-50.
5. Кудрявцев В.Б., Подколзин А.С., Болотов А.А. Основы теории однородных структур. - М.: Наука. Гл.ред. физ.-мат.лит., 1990. – 296 с. ISBN 5-02-01426602.
6. Тоффоли Т., Марголус Н. Машины клеточных автоматов: Пер. с англ. М.: Мир, 1991. 280 с.
7. Дж. Фон. Нейман. Теория самовоспроизводящихся автоматов. Пер. с англ. М.: Мир, 1971. 326 с.
8. Banks, E. R., 1971, "Information processing and transmission in cellular automata," // MIT Project MAC report No. TR-81.
9. Wolfram S. Cryptography with Cellular Automata // Lecture Notes in Computer Science, vol. 218, 1986. Pp. 429–432.
10. Wolfram, S. (1983): Statistical mechanics of cellular automata. // Review of Modern Physics, 55, 601–644
11. Wolfram S. Random Sequence Generation by Cellular Automata // Advances in Applied Mathematics, vol. 7, 1986. Pp. 429–432.
12. Ключарев П.Г. NP-трудность задачи о восстановлении предыдущего состояния обобщенного клеточного автомата. // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. 2012.-№ 1. С. 11.
13. Сухинин Б.М. Разработка генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов // Наука и образование, № 9, 2010. С. 34–41.

14. Евсютин О.О., Шелупанов А.А. Приложения клеточных автоматов в области информационной безопасности и обработки данных //Доклады ТУСУРа, 2012, № 1(25), часть 2, с. 119 - 125.
15. Ключарёв П.Г. Обеспечение криптографических свойств клеточных автоматов. // Математика и математическое моделирование. 2012; №3. С. 13.
16. Ключарёв П. Г. Клеточные автоматы, основанные на графах Рамануджана, в задачах генерации псевдослучайных последовательностей // Машиностроение и компьютерные технологии. 2011. №10. С. 22.

Научный руководитель Петр Георгиевич Ключарев, доцент кафедры «Информационная Безопасность» МГТУ им. Баумана, кандидат технических наук, pgkl@yandex.ru

Cellular automata in cryptography

Zhogolev G. D.[27]

This article examines the applicability of the theory of cellular automata in cryptography. Publications investigating methods for obtaining cellular automaton properties applicable to cryptography are considered. It also reviews articles that build cryptographic models based on cellular automata, discusses the use of cellular automata to constructing cryptographic algorithms.

Keywords: homogeneous structures, pseudo-random sequence generator, computability, Ramanujan graph, avalanche effect, bent-functions.

[27] Zhogolev Gleb Denisovich, student, BMSTU, Moscow, zhogolevg@mail.ru

УДК 004.056.55

Автоматизация дифференциального криптоанализа по ошибкам вычислений применительно к поточным аппаратно-реализуемым шифрам

Климцов В.Е.[28], Чиликов А.А.[29]

Аннотация. Мы предлагаем возможную структуру программного обеспечения, позволяющего автоматизировать процесс оценки стойкости поточных криптоалгоритмов к fault-атакам. На примере анализа алгоритма Grain-128 просматриваются этапы, программная реализация которых позволит существенно сократить время работы криптоаналитика. Добавив к этому возможность строить различные модели криптосистем и визуальное представления генерируемой информации, получаем проект универсального ПО для автоматизации fault-анализа. Методы, которые позволят интерпретировать принципы, использованные в ходе работы с алгоритмом Grain-128, для большой группы поточных шифров на данный момент в полной мере не определены. Но, безусловно, в основу лягут таблицы распределения сбоев и решение систем линейных уравнений.

Ключевые слова: eSTREAM, Grain-128, fault-атаки, криптоанализ.

Введение

Любой криптоалгоритм, реализованный в программном или же аппаратном исполнении, выполняется на определенном физическом устройстве, которое так или иначе взаимодействует с окружающей его средой. Такое взаимодействие можно измерить, а в некоторых случаях и намеренно спровоцировать, с целью получения информации, которая может быть полезна при проведении криптоанализа данного алгоритма. Такая информация называется информацией, полученной по сторонним каналам, а атаки, использующие ее, соответственно – атаки по сторонним каналам[1].

Одним из видов такого воздействия являются fault-атаки, в рамках которых в криптосистему намеренно вносятся сбои для получения дополнительной информации[2]. В настоящее время они считаются одними из самых эффективных атак как на поточные, так и на блочные шифры, несмотря на то, что их успешное проведение зависит не только от структуры алгоритма, но и от того, на каком устройстве он реализуется.

Данный тип анализа весьма интересен по отношению к поточным аппаратно-реализуемым шифрам. Подобный класс алгоритмов направлен на сохранения стойкости в условиях использования недорогой и малопроизводительной элементной базы[3]. Зачастую в ней не реализованы аппаратные механизмы защиты от внесения сбоев, ведь их использование ведет к увеличению конечной стоимости.

Анализ стойкости шифров является трудоемким процессом, ввиду того, что для каждого шифра используется индивидуальный подход. Однако при этом подавляющее большинство поточных криптоалгоритмов имеют похожую

[28] Климцов Владимир Евгеньевич, аспирант кафедры ИУ-8 МГТУ им. Н.Э. Баумана, Москва, sentlabs@bk.ru

[29] Чиликов Алексей Анатольевич, кандидат физико-математических наук, доцент кафедры ИУ-8 МГТУ им. Н.Э. Баумана, Москва, chilikov@passware.com

структуру. Возникает вопрос, возможно ли автоматизировать их анализ для конкретной модели сбоев.

eSTREAM

После взлома всех 6 поточных шифров, предложенных в проекте NESIIE, Европейский союз организовал новый проект по выявлению поточных шифров, пригодных для широкого применения, который получил название eSTREAM. Результатом проекта, в категории шифров предназначенных для аппаратной реализации, стали Trivium, Grain и MIKEY.

Trivium

Trivium – синхронный поточный шифр, который может генерировать вплоть до 2^{64} бит ключевого потока на основе 80-битного секретного ключа (Key) и 80-битного вектора инициализации (IV)[4]. Как и в большинстве проточных шифров этот процесс делится на две стадии – инициализация и непосредственно генерация гаммы.

Изначальное состояние Trivium представляет собой 3 сдвиговых регистра суммарной длины в 288 бит. Каждый такт происходит изменение битов в регистрах сдвига путём нелинейной комбинации прямой и обратной связи.

Grain-128

В основе шифра лежат три основных блока: регистр сдвига с линейной обратной связью (далее – LFSR), регистр сдвига с нелинейной обратной функцией связи (далее – NFSR) и выходная функция[5]. Выходная функция определена как нелинейная комбинация значений определенных ячеек обоих регистров, каждый из которых имеет длину 128.

Так же как и в Trivium здесь присутствует стадия инициализации. В Grain используются 128-битный ключ и 96-битный вектор инициализации. Все ячейки NFSR заполняются битами ключа, а IV помещается в LFSR с нулевой ячейки, оставшиеся заполняются единицами. После чего шифр отрабатывает 256 тактов, не подавая ключевой поток на выход, вместо этого каждый бит гаммы складывается с функциями обратной связи как LFSR, так и NFSR.

Mikey 2.0

Третьим поточным шифром, предназначенным для аппаратной реализации, которому удалось удовлетворить все требования eSTREAM стал MIKEY 2.0 (Matual Irregural Clocking KEYstream generator)[6].

Так же как и Trivium в MIKEY используется 80-битный ключ, а длина вектора инициализации может варьироваться от нуля до восьмидесяти бит включительно. В отличие от 2-х предыдущих шифров MIKEY состоит всего из двух частей − регистров R и S, каждый из которых имеет длину 100 бит. В целом R можно считать линейным регистром, а S – нелинейным.

Анализ Grain-128

Из всех представленных на eSTREAM шифров, наибольший интерес представляет Grain-128, ввиду того, что имеет самую простую структуру, наибольшую длину гаммы, генерируемой с одной пары (Key,IV), возможность увеличения скорости работы и регулярное тактирование. Так же в описании алгоритма авторы подчеркивают, что fault-атаки на данный момент являются одними из наиболее успешных подходов к анализу современных поточных шифров.

Классический метод проведения fault-атак на LFSR-based шифры был описан Хоком и Шамиром[7]. Он состоит из следующих этапов:

1) Внесение ошибки и генерация гаммы.

2) Прогнозирование природы ошибки.

3) Проверка предположения, в случае, если оно было не верным, составляется новый прогноз.

4) Повтор шагов 1-3 $O(j)$ раз, где j – количество входных параметров фильтрующей функции.

5) Решение системы линейных уравнений.

Эти 5 пунктов можно объединить в 2:

- анализ возможности локализации ошибок;
- анализ возможности восстановления секретной информации.

Для Grain-128 результатами этих двух этапов будут алгоритмы A и B, позволяющие однозначно определить ячейку, в которую попал сбой, и восстановить значения регистров после этапа инициализации соответственно. Эти методы основаны на свойствах функции, генерирующей ключевой поток, а именно на вероятности изменения ее выхода, при инверсии одного из входов.

По разнице в гамме криптосистем со сбоем и без можно построить таблицы распределения ошибок, по которым можно выделить уникальные сигнатуры, позволяющие определить ячейку регистра в которую изначально попал сбой. Таким образом конструируется алгоритм A.

Для алгоритма B используется похожий принцип, однако по разнице в гамме строится система линейных уравнений над изначальными значениями регистров. Получив по 128 линейно независимых уравнений для каждого регистра, алгоритм заканчивает работу.

Далее, решив систему и просчитав этап инициализации в обратном порядке, получаем ключ и вектор инициализации[8].

Автоматизация процесса при помощи ПО

Пример дифференциального криптоанализа по ошибкам вычислений Grain-128 показывает, что процесс оценки стойкости шифра включает в себя множество трудоемких операций, автоматизация которых может значительно снизить временные затраты на анализ алгоритма. На данный момент большинство публикаций на эту тему посвящено блочным шифрам[9,10]. Однако на примере анализа Grain-128 можно предложить состав программного обеспечения для поточных алгоритмов.

Для начала необходим программный модуль, позволяющий аналитику проектировать модели шифров и работать с ними. Он будет являться основной для программного обеспечения автоматизация анализа.

Следующий модуль будет отвечать за локализацию ошибок. В его основе должен лежать алгоритм, позволяющий однозначно определить в какую ячейку памяти попал сбой. Например, приведенный выше метод построения таблиц распределения ошибок для последующего определения уникального признака изменения выходного потока для каждой из областей памяти.

Далее идет модуль, автоматизирующий анализ возможности получения секретной информации шифра. Подобрать общий алгоритм, который позволит программному обеспечению ответить на данный вопрос – возможно невыполнимая задача. Однако, как упоминалось выше, практически для всех поточных шифров данный этап сводится к построению и решению системы линейных уравнений, что так же можно автоматизировать.

Так как оценить стойкость шифра в полностью автоматическом режиме практически невозможно, последний модуль должен отвечать за предоставление

аналитику информации, генерируемой программным обеспечением в простом и понятном формате.

Заключение

Представленные на eSTREAM в секции аппаратно-реализуемых шифры имеют схожую структуру. Это делает возможным построение обобщенных алгоритмов в ходе анализа их стойкости к fault-атакам. Например, использование таблиц распределения сбоев для выделения уникальных признаков, позволяющих однозначно определить позицию внесенной ошибки. Кроме того практически для любого криптоалгоритма необходимо строить и решать системы линейных уравнений, анализировать свойства функций усложнения и различия между генерируемыми ключевыми потоками в системах со сбоем и без соответственно.

Автоматизация этих операций существенно сократит временные затраты криптоаналитика и позволит ему начинать работу уже имея некоторый набор исходной информации, а в некоторых случаях сразу определить стоек шифр или же нет, например, в случае если локализовать ошибку невозможно.

Список использованных источников

1. Introduction to Side-Channel Attacks [Электронный ресурс]. – Режим доступа: https://www.springer.com/cda/content/document/cda_downloaddocument/9780387718279-c1.pdf, свободный – (18.03.2018).
2. On the importance of Checking Cryptographic Protocols for Faults [Электронный ресурс]. – Режим доступа: https://link.springer.com/content/pdf/10.1007%2F3-540-69053-0_4.pdf, свободный – (18.03.2018).
3. Comparison of the Hardware Implementation of Stream Ciphers [Электронный ресурс]. – Режим доступа: http://iajit.org/PDF/vol.2,no.4/2-Galanis.pdf, свободный – (18.03.2018).
4. Trivium Specifications [Электронный ресурс]. – Режим доступа: http://www.ecrypt.eu.org/stream/p3ciphers/trivium/trivium_p3.pdf, свободный – (12.03.2018).
5. A Stream Cipher Proposal: Grain-128 [Электронный ресурс]. – Режим доступа: http://www.ecrypt.eu.org/stream/p3ciphers/grain/Grain128_p3.pdf, свободный – (13.03.2018).
6. The stream cipher MICKEY 2.0 [Электронный ресурс]. – Режим доступа: http://www.ecrypt.eu.org/stream/p3ciphers/mickey/mickey_p3.pdf, свободный – (14.03.2018).
7. Fault Analysis of Stream Ciphers [Электронный ресурс]. – Режим доступа: https://link.springer.com/content/pdf/10.1007%2F978-3-540-28632-5_18.pdf, свободный – (16.03.2018).
8. Fault Analysis of Grain-128 [Электронный ресурс]. – Режим доступа: https://www.math.u-bordeaux.fr/~gcastagn/publi/HOST09_FAGrain.pdf, свободный – (16.03.2018).
9. Differential Fault Analysis Automation [Электронный ресурс]. – Режим доступа: https://eprint.iacr.org/2017/673.pdf, свободный – (16.03.2018).
10. Fault Attacks Made Easy: Differential Fault Analysis Automation on Assembly Code [Электронный ресурс]. – Режим доступа: https://eprint.iacr.org/2017/829.pdf, свободный – (16.03.2018).

Automation of Differential Fault Analysis of Stream Hardware Aimed Ciphers

Klimtsov V.E.[30], Chilikov A.A.[31]

Abstract. We propose a software to automatically estimate the resistance of stream ciphers against fault attacks. For Grain-128 we recognize some “critical” phases of analysis. When these phases are fully or partialy programmed time costs of analysis is reduced. If we append components to construct of cipher models and to and visualize an information which is generated, we can obtain the universal software for automation of fault analysis. We can't sate methods of Grain-128 principles adoptation to wide group of stream ciphers right now. But these methods definitely are based on fault distribution tables and solving systems of linear equations.

Keywords: eSTREAM, Grain-128, fault attacks, cryptanalysis.

[30] Klimtsov Vladimir, PhD student of IU8 Department of BMSTU, Moscow, sentlabs@bk.ru
[31] Chilikov Alexey, PhD in Physico-mathematical sciences , Associate Professor of IU8 Department of BMSTU, Moscow, chilikov@passware.com

УДК 004.056.55

О производительности и статистических свойствах некоторых криптографических алгоритмов, основанных на обобщенных клеточных автоматах

Ключарёв П.Г. [32]

В работе кратко описаны результаты статистического тестирования псевдослучайных функций, основанных на обобщенных клеточных автоматах. В качестве графов этих автоматов использованы различные графы Рамануджана (в том числе, графы Пайзера, графы $Y^{p,q}$ Любоцкого-Филипса-Сарнака и случайные графы Рамануджана). При достаточном числе шагов автомата эти функции проходили все статистические тесты, а существенных различий между статистическими свойствами таких функций, использующих графы Рамануджана из разных семейств, не наблюдалось. Кроме того, кратко описаны результаты тестирования производительности реализованных на программируемых логических интегральных схемах (ПЛИС) криптографических хэш-функций, основанных на обобщенных клеточных автоматах и на конструкции, аналогичной криптографической губке (Sponge). Их производительность на порядок превышает производительность функции Keccak (SHA-3) при реализации на ПЛИС.

Ключевые слова: обобщенные клеточные автоматы, криптоалгоритм, статистический тест, ПЛИС.

Введение

Криптографические алгоритмы находят широчайшее применение в задачах обеспечения информационной безопасности. Одно из основных предъявляемых к любым криптоалгоритмам требований – криптостойкость. Кроме того, в связи с постоянным повышением требований к пропускной способности систем передачи информации, криптоалгоритмы должны демонстрировать высокую производительность.

Ранее автором были предложены методы построения симметричных шифров и криптографических хэш-функций на основе обобщенных клеточных автоматов (в ряде работ, в том числе в работах [1,2]). Такие криптоалгоритмы показывают высокую скорость работы при аппаратной реализации, что позволяет эффективно их применять для различных целей (в том числе, [3,4]). В настоящей работе приведены некоторые результаты, связанные со статистическим тестированием и тестированием производительности некоторых криптоалгоритмов, основанных на обобщенных клеточных автоматах.

Обобщенные клеточные автоматы и основанные на них криптоалгоритмы

Однородный обобщенный клеточный автомат – это ориентированный граф (в данной работе мы используем термин «граф», допуская петли и кратные ребра), каждой вершине v_i которого соответствует булева переменная (будем называть ее ячейкой) m_i. Для каждой вершины, входящие в неё ребра некоторым образом пронумерованы числами $1,\ldots,d$. Кроме того, задана локальная функция связи – булева функция $f(x_1,\ldots,x_d)$. Автомат работает по шагам. На шаге с номером t вычисляются новые значения ячеек:

$$m_i(t) = f(m_{\eta(i,1)}(t-1), m_{\eta(i,2)}(t-1),\ldots, m_{\eta(i,d)}(t-1)),$$

[32] Ключарёв Петр Георгиевич, к.т.н., доцент, МГТУ им. Н.Э. Баумана, Москва, pk.iu8@yandex.ru

где $\eta(i, j)$ – номер вершины, из которой выходит ребро, входящее в вершину i и имеющее номер j. Заполнением обобщенного клеточного автомата $M(t)$ на шаге t будем называть набор значений ячеек $(m_1(t), m_2(t), \ldots, m_N(t))$. Начальным заполнением будем называть заполнение перед первым шагом. Здесь мы рассматриваем только обобщенные клеточные автоматы, в графах которых для любого ребра (u,v) присутствует ребро (v,u). Такие графы можно рассматривать как неориентированные, если каждую такую пару ориентированных ребер заменить на неориентированное ребро $\{u,v\}$.

Ранее автором были предложены методы создания криптографических алгоритмов, основанных на обобщенных клеточных автоматах. Среди них – методы создания блочных шифров [1] и криптографических хэш-функций [2]. Они основаны на псевдослучайной функции, базирующейся на обобщенных клеточных автоматах [5], которая представляет собой конструкцию, которую можно неформально описать следующим образом. Функция принимает на вход два аргумента: ключ и входной блок. Обобщенный клеточный автомат получает начальное заполнение, состоящее из входного блока, ключа и специальной константы. Далее совершается определенное число шагов обобщенного клеточного автомата и из получившегося его заполнения выбираются определенные биты, из которых и формируется выходное значение функции. Такая функция задается рядом параметров, в числе которых граф обобщенного клеточного автомата, локальная функция связи, число шагов, константа и др. Отметим, что термин «псевдослучайные функции» понимается в данной работе в слабом смысле, т.е., неформально говоря, это такие функции, которые нельзя отличить от случайных посредством определенного набора статистических тестов.

О статистическом тестировании

Было проведено статистическое тестирование, которое показало, что псевдослучайная функция, основанная на обобщенных клеточных автоматах, успешно проходит статистические тесты при достаточном числе шагов. При этом тестировались различные варианты этой функции, отличающиеся графом обобщенного клеточного автомата – использовались графы Рамануджана из семейства Пайзера [6] (графы из этого семейства основаны на изогениях между суперсингулярными эллиптическими кривыми), семейства $Y^{p,q}$ Любоцкого-Филипса-Сарнака (LPS-Y) [7], а также случайные регулярные графы, для которых произведена проверка на то, что они являются графами Рамануджана (такие графы обсуждаются, например, в работе [8]). Тестирование проводилось посредством методики, созданной на основе методики статистического тестирования блочных шифров, описанной в [9]. В качестве набора статистических тестов использовался набор тестов NIST Statistical Test Suite (NIST STS) [10]. Для успешного прохождения тестов, в зависимости от числа ячеек обобщенного клеточного автомата (выбиралось около 20 графов из каждого семейства с числом вершин в диапазоне от 200 до 4100), требовалось от 3 до 6 шагов клеточного автомата для тестов сцепления блоков и корреляции выхода и входа, а для тестов на лавинный эффект в большинстве случаев требовалось от 7 до 9 шагов. При этом существенных отличий между результатами статистических тестов псевдослучайных функций, основанных на обобщенных клеточных автоматах с графами из разных семейств, не наблюдалось.

Эти результаты подтверждают статистические свойства ряда предложенных автором криптографических алгоритмов, основанных на рассматриваемых псевдослучайных функциях.

Также было проведено статистическое тестирование блочных шифров, основанных на обобщенных клеточных автоматах (тестировались шифры с четырьмя раундами, длиной блока 128 бит и длиной ключа 128 бит). Тестирование показало, что при достаточном числе шагов эти шифры проходят все статистические тесты.

О реализации на ПЛИС клеточно-автоматной хэш-функции, основанной на конструкции, аналогичной криптографической губке.

Программируемая логическая интегральная схема (ПЛИС) – это цифровая интегральная микросхема, логика работы которой задается посредством программирования. Описание реализуемых ею схем осуществляется на специализированном языке (в данной случае применяется язык VHDL). Для компиляции VHDL-файла и моделирования использовались САПР Altera Quartus II и Altera ModelSim.

Хэш-функция, предложенная в работе [2], основана на обобщенных клеточных автоматах и создана на основе концепции криптографической губки. Эта хэш-функция была реализована на ПЛИС. При этом производительность на ПЛИС Altera Stratix V при некоторых параметрах превышала 100 Гбит/с, что на порядок превышает производительность хэш-функции Keccak (SHA-3). Кроме того, была показана достаточно низкая ресурсоемкость (в зависимости от параметров – от нескольких тысяч LE).

Выводы

Таким образом, результаты проведенных исследований подтвердили гипотезу о хороших статистических свойствах псевдослучайных функций, основанных на обобщенных клеточных автоматах. Учитывая, что на этих функциях основаны некоторые криптоалгоритмы, предложенные автором, эти результаты также в определенном смысле подтверждают их статистические свойства. Кроме того, клеточно-автоматная хэш-функция на основе конструкции, аналогичной криптографической губке (Sponge), показала высокую производительность при аппаратной реализации.

В заключении, автор благодарит Е.Л. Зорина за предоставление вычислительных мощностей для проведения статистического тестирования.

Работа выполнена при поддержке РФФИ (проект №16-07-00542).

Литература

1. Ключарёв П. Г. Блочные шифры, основанные на обобщённых клеточных автоматах // Наука и образование. Научное издание МГТУ им. Н.Э. Баумана. - 2012. - № 12. С. 361-374

2. Ключарёв П. Г. Метод построения криптографических хэш-функций на основе итераций обобщенного клеточного автомата // Вопросы кибербезопасности, 2017, №1 (19), С.45-50.

3. Быков А.Ю., Панфилов Ф.А., Зенькович С.А. Модель и методы многокритериального выбора классов защищенности для объектов распределенной информационной системы и размещения баз данных по объектам // Вопросы кибербезопасности, 2016, №2 (15), С.9-20.

4. Быков А.Ю., Панфилов Ф.А., Ховрина А.В. Алгоритм выбора классов защищенности для объектов распределенной информационной системы и размещения данных по объектам на основе приведения оптимизационной задачи к задаче теории игр с непротивоположными интересами // Блочные шифры, основанные на обобщённых клеточных автоматах // Наука и образование. Научное издание МГТУ им. Н.Э. Баумана. - 2016. - № 1. С. 90-107.

5. Ключарёв П. Г. Построение псевдослучайных функций на основе обобщённых клеточных автоматов // Наука и образование. Электронное научно-техническое издание. - 2012. - № 10.

6. Pizer A.K. Ramanujan graphs and Hecke operators // Bull. Amer. Math. Soc. 1990. V.23.

7. Sarnak P. Some Applications of Modular Forms. Cambridge University Press, 1990.

8. Ключарёв П.Г. Построение случайных графов, предназначенных для применения в криптографических алгоритмах, основанных на обобщенных клеточных автоматах. // Математика и математическое моделирование. – 2017. – №3. С 77-90.

9. Randomness testing of the advanced encryption standard finalist candidates: Rep. / DTIC Document ; Executor: J. Soto, L. Bassham, 2000.

10. Rukhin A., Soto J., Nechvatal J. et al. NIST Special Publication 800-22 revision 1a. - 2010.

On performance and statistical properties of some cryptographic algorithms based on generalized cellular automata

Klyucharev P.G. [33]

The paper briefly describes the results of statistical testing of pseudorandom functions based on generalized cellular automata. Various Ramanujan graphs are used as graphs of these automata (in particular, Pizer graphs, $Y^{p,q}$ LPS graphs and random Ramanujan graphs). These functions with sufficient number of steps of automata have successfully passed all statistical tests, and no significant differences are found between the statistical properties of such functions, based on graphs from different families. In addition, results of performance testing of FPGA implementation of cryptographic hash functions, based on generalized cellular automata, with the construction similar to a cryptographic sponge, are briefly described. Their performance exceeds the performance of FPGA implementation of Keccak (SHA-3).

Keywords: generalized cellular automata, cryptographic algorithm, statistical test, FPGA.

[33] Peter Klyucharev, Ph.D., Associate Professor, Bauman Moscow State Technical University, Moscow, pk.iu8@yandex.ru

УДК 621.391

Стеганографический метод идентификации авторского права на аудиофайл

Ковынёв Н.В.[34]

В последние годы распространение носителей с записью музыкальных произведений осуществляется только через специализированные магазины. Таким образом, ответственность за распространение контрафактной продукции несет и руководство магазина. Поэтому руководство магазина должно быть убеждено в отсутствии контрафактной продукции в товаре. Для этого применим самый простой способ – занесение меток (цифровых водяных знаков (ЦВЗ) в аудиофайл. Однако стеганографические методы сокрытия данных не являются криптоустойчивыми. Это объясняется тем, что число методов стеганографии конечно и определить тот или иной метод можно простым перебором. Следует отметить, что проблема защиты от контрафактного копирования музыкальных произведений переплетается с проблемой плагиата: достаточно провести аранжировку музыкального произведения с помощью звукового редактора (soundeditor) и доказать факт распространения контрафактной продукции или плагиата становится невозможно.

Ключевые слова: *алгоритм, данные, сокрытие, криптография, стеганография, контрафакт, кодирование, цифровой водяной знак.*

Введение

Целью исследований является разработка защиты накопителей от несанкционированного копирования. Решались следующие задачи:

- аналитический обзор известных технических решений,
- анализ известных стегоалгоритмов, применяемых для внедрения идентификационных меток в аудиофайл,
- разработка комбинированных алгоритмов для внедрения идентификационных меток в аудиофайл,

Цель стеганографии – безопасный обмен данными совершенно незаметным образом, который отрицает сам факт наличия секретных сообщений. Если метод стеганографии вызывает у кого-то подозрения, то такой метод признается неудачным.

Модель аудио стеганографии состоит из носителя (аудио файл), сообщения и пароля. Под носителем понимается файл, который скрывает или будет скрывать секретную информацию. Стеганографическая модель изображена на рис.1. Сообщение – данные, которые отправитель хочет оставить в тайне. В качестве передаваемого сообщения могут выступать простой текст, изображение, аудио и другие типы файлов. Пароль символизирует ключ, зная который, получатель сможет гарантированно декодировать сообщение из файла. Файл-носитель с конфиденциальной информацией называется стегофайлом.

[34] Ковынёв Николай Витальевич, аспирант, МГТУ им. Н.Э. Баумана, Москва, n.kovynyov@gmail.com

Рис. 1. Стеганографическая модель

Процесс сокрытия информации состоит из следующих двух шагов:

- Идентификация избыточных битов в файле-носителе. Избыточные биты - биты, которые могут быть модифицированы без порчи качества или нарушения целостности файла-носителя.
- Избыточные биты в файле-носителе заменяются битами секретной информации.

Базовые подходы в аудиостеганографии

1. Метод LSB.

Самый распространённый метод - LSB (Least Significant Bit, наименьший значащий бит) алгоритм, который заменяет наименьший значащий бит в нескольких байтах файла-носителя, чтобы скрыть последовательность байтов, содержащих скрытые данные [2-11].

2. Четное кодирование.

Четное кодирование один из самых надежных способов аудио стеганографии. Данный метод разбивает сигнал на отдельные части и встраивает каждый бит секретного сообщения в четный бит. Если четный бит в выбранной области не подлежит кодированию в секретный бит, то процесс инвертирует младший бит одной из выборки данной области. На рис.2 представлена процедура такого кодирования.

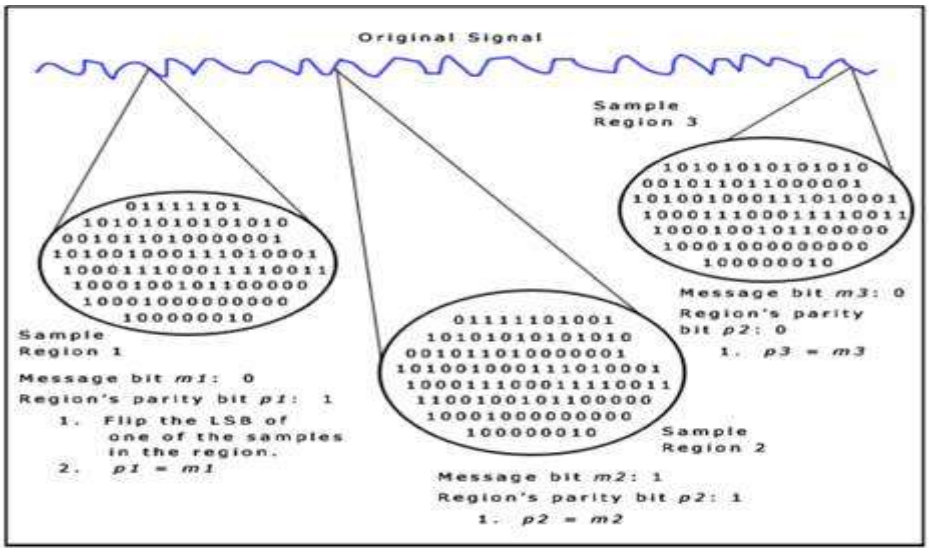


Рис. 2. Четное кодирование

3. Фазовое кодирование.

Данный метод работает путем замены фазы исходного звукового сегмента на опорную фазу, которая представляет собой секретную информацию. Остальные сегменты фазы корректируются для сохранения определенной фазы между сегментами. Тогда происходит резкое изменение фазового соотношения между каждой частотной составляющей, шумы становятся заметными. Однако, если фазу модифицировать не сильно, то человеческое ухо не распознает каких-либо изменений.

Секретное сообщение встраивается только в фазу первого сегмента:

$$\text{Новая фаза} = \begin{cases} \pi/2 & \text{если бит сообщения} = 0 \\ -\pi/2 & \text{если бит сообщения} = 1 \end{cases}$$

- Используя новую фазу первого сегмента создается новая матрицы фаз и разницы между ними;
- Звуковой сигнал восстанавливается путем применения обратного дискретного преобразования Фурье с использованием новой матрицы и исходной матрицы величин, после чего звуковые сегменты сцепляются.

Получатель должен знать длину сегмента, чтобы извлечь секретное сообщение из звукового файла. После чего он с помощью дискретного преобразования Фурье может извлечь секретную информацию.

Метод расширенного спектра. Метод расширенного спектра пытается передать секретные сведения по спектру частот звукового сигнала. Данный метод распространяет секретную информацию по спектру частот звукового файла, используя код, который не зависит от фактического сигнала.

Эхо – метод. Данный метод встраивает секретную информацию в звуковой файл, вводя эхо в дискретный сигнал. Главные преимущества эхо-метода – это высокая скорость передачи данных, а также повышенная устойчивость по сравнению с другими методами.

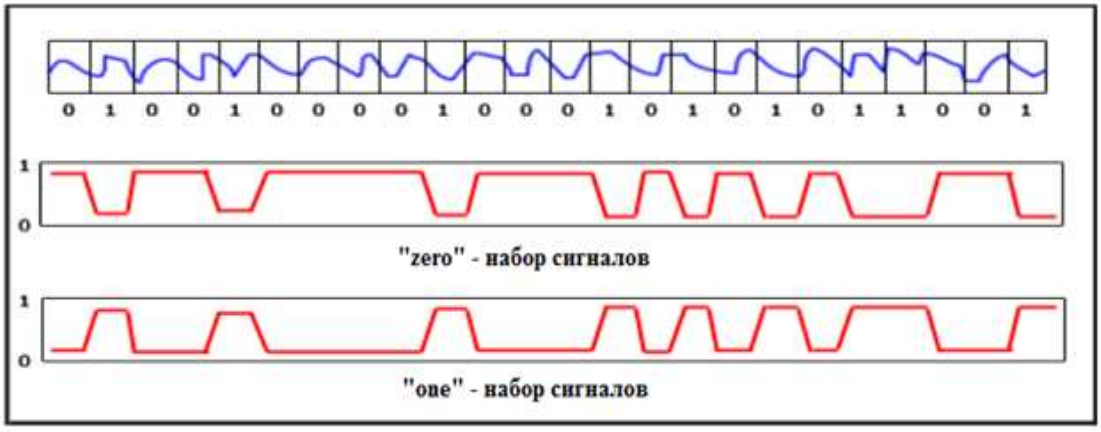


Рис. 3. Пример работы эхо-метода

Основные недостатки использования таких методов как эхо, расширенного спектра и четности кодирования заключаются в том, что они вносят шум в аудиофайл, который может быть довольно различимым для человеческого уха, а также надежность данных методов вызывает вопросы.

Фазовое кодирование имеет основной недостаток, заключающийся в низкой скорости передачи данных из-за того, что секретное сообщение кодируется только на первом сегменте сигнала. Следовательно, этот метод используется только тогда, когда передается небольшое количество данных.

Среди выше предложенных методов стеганографии метод наименьшего значащего бита или LSB является самым простым методом для встраивания секретной информации.

Возможные способы решения

Для решения поставленной задачи требуется не только обеспечить конфиденциальность сообщения, но еще и скрыть сам факт его наличия, получения, либо сам факт несанкционированного применения бытовой регистрирующей аппаратуры.

Метод реализуется следующим образом:

Формируется цифровая Фурье – голограмма документа, математическая модель которой имеет вид :

$$h(x,y) = \left[\left|w(x,y)\right|\exp\{j\Phi(x,y)\} + \exp\{j(xM+yN)\}\right]^2 = \left|w(x,y)\right|^2 + \\ + \left|w(x,y)\right|\cos\left[xM+yN+\Phi(x,y)\right] + 1. \qquad (1)$$

где: $w(x,y) = \left|w(x,y)\right|\exp(j\Phi(x,y))$ - преобразование Фурье изображения документа W(u,v) в плоскости записи голограммы, $\exp\{j(xM+yN)\}$ - опорная когерентная волна $\exp\{j(xM+yN)\}$, где M и N – пространственные частоты, соответствующие углам падения волны по нормали к плоскости регистрации голограммы.

Первый член в выражении (1) характеризует дополнительную засветку голограммы пучком света от объекта и не содержит фазовой характеристики и не несет никакой информации о восстановленном изображении. Следовательно, получаем:

$$h(x,y) = A_0 + \left|w(x,y)\right|\cos\left[xM+yN+\Phi(x,y)\right], \qquad (2)$$

Где: постоянная составляющая A_0 – максимальное значение w(x,y) = w(0,0). Значения *M* и *N* используются при восстановлении и представляют собой ключи шифрованному сообщению.

Восстановление Фурье – голограммы производится по алгоритму, обратному алгоритму формирования. Преобразование Фурье от полученной функции голограммы h(x,y) будет состоять из суммы двух изображений водяного знака W(u,v), смещенных относительно начала осей координат на величины несущих частот M и N:

$$\Im\{h(x,y)\} = \tilde{W}(u,v) = W(u-M, v-N) + W(-u-M, -v-N) + A(u,v), \qquad (3)$$

Где: $\Im$ - оператор Фурье-преобразования, *A(u,v)* – автокорреляционная функция. Автокорреляция *A(u,v)* располагается в начале координат и подавляется как в цифровой голографии, так и в оптической. Второе изображение *W(-u-M,-v-N)* является зеркальным отображением *W(u-M,v-N)* относительно центра осей координат. При использовании Фурье-голограммы используется ее свойство избыточности, что позволяет использовать для последующего встраивания только часть массива, содержащего отсчеты цифровой голограммы.

Полученную цифровую голограмму можно заносить в пустой аудиоконтейнер любым известным методом. Неизвестность факта занесения в

файл именно голограммы, а также неизвестность фазы опорного пучка восстанавливающего излучения позволяет обеспечить высокую криптоустойчивость метода. На Рис.4. приведено изображения-контейнеры со встроенной косинусной и Фурье голограммами. Справа приведено восстановленное изображение, полученное из искаженного контейнера (фотография) со стего.

Следует признать, что если аудиоконтейнер известен, то внедренное стего легко выделить с применением программы WinHex. На Рис.5. приведен пример сравнения пустого контейнера и контейнера со стего. Черным выделены байты с внедренным сообщением.

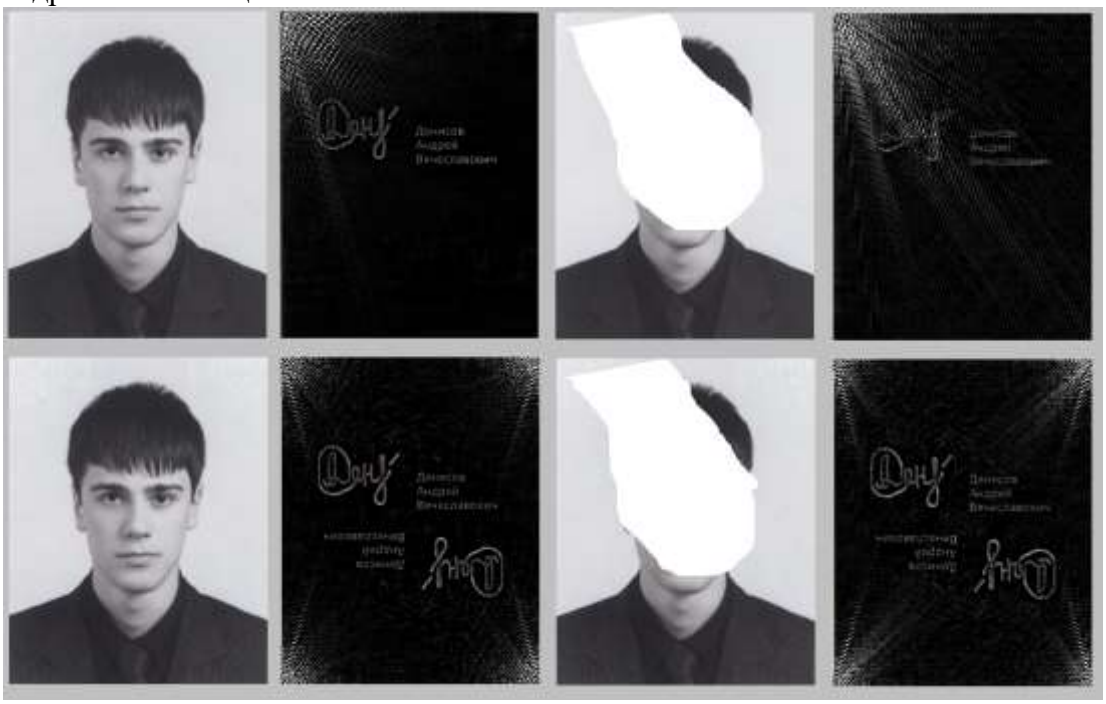
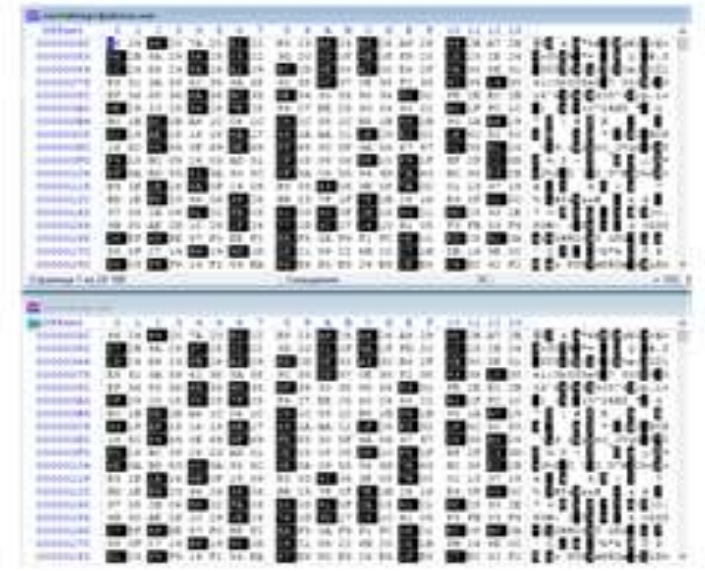


Рис.4. Изображение-контейнер со встроенной косинусной и Фурье голограммами. Справа – удалена часть области в контейнере со стего



..

Рис.5. Пример реализации атаки с помощью ПО WinHex на аудиоконтейнер со стегосообщением при известном пустом контейнере

Анализ доступных публикаций показал, что одной из распространенных технологий защиты от копирования, является создание особо определяемых дискет. Их особенность заключается в том, что на дискете создается специально организованная метка, которая используется как признак ее дистрибутивности. Для создания метки можно применить программные и аппаратные, а также их комбинирование стеганографические средства. К одному из таких средств можно отнести метод сокрытия голографической метки в аудиофайле. В работе [3] показан способ сокрытия Фурье – голограмм текстов в изображениях. К аппаратным методам иожно отнести метод, использующий аналоговый Фурье – процессор (Рис.6). Метод сокрытия голографической метки в аудиофайле описан в публикации впервые.

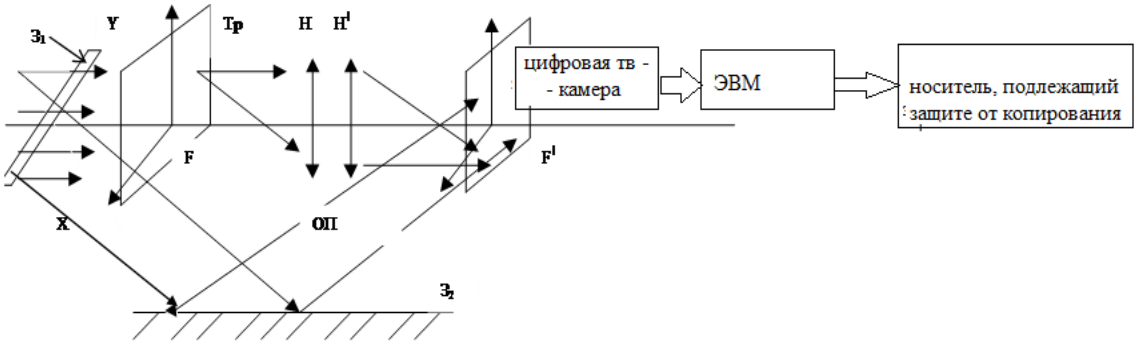


Рис.6. Процессор для формирования аналоговой Фурье – голограммы. $З_1$ – полупрозрачный зеркальный делитель, Тр – транспарант с изображением метки, ОП – опорный пучок, H_1, H_2 – главные плоскости Фурье –объектива, F' – задняя фокальная плоскость – плоскость голограммы.

Вывод

Исследования, результаты которых изложены в настоящей публикации, позволяют утверждать следующее:

- проведен обзор технических решений
- проведен аналитический обзор алгоритмов цифровой стеганографии с позиций применимости для решения поставленной задачи.
- предложен способ защиты носителя музыкального произведения от несанкционрованного копирования.
- Проведена попытка разработки комбинированных алгоритмов для внедрения идентификационных меток в аудиофайл

Литература

1. Бирюков А. Стеганография: реализация и предотвращение // Системный администратор. 2015. №4 (149). С. 24-27

2. Бабина О.И. Лингвистическая стеганография: современные подходы. Часть 1 // Вестник южно-уральского государственного университета. 2015. №3 том 12. С. 27-33

3. Еськова С.П., Коварда В.В. Контрафактная и фальсифицированная продукция: понятия, сущность, отличительные особенности // Молодой ученый. 2016. №20. С. 36-308.

4. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. Солон — пресс. 2009. 265 С.

5. Пахоруков А.С., Попов А.А. Стеганография. Скрытие стего в изображении // Сборник трудов конференции Наука. Технологии. Инновации. 2016. С. 184-186

6. Волосатова Т.М., Чичварин Н.В. Исследование и разработка алгоритма защиты проектно документации в CAD/CAM/CAE от несанкционированного доступа// Инженерный журнал: наука и инновации. Электронное издание. Раздел: Информационные технологии. 2014. №2(26). DOI: 10.18698/2308-6033-2014-2-1201.

7. Глинская Е.В., Чичварин Н.В. Информационная безопасность открытых каналов передачи проектной документации, продуцируемой в САПР // Вопросы кибербезопасности. 2014. № 4 (7). С. 11-22.

8. Al-Shatanawi, O.M. A new image steganography based on denoising methods in wavelet domain./O. M. Al-Shatanawi, N. N. Emam//International Journal of Network Security & Its Applications (IJNSA). -2015. -No.2: Vol.7. -С. 18-25.

9. Волосатова Т.М., Чичварин Н.В. Метод сокрытия данных в стереофонических аудиофайлах // Инженерный вестник. 2015. №9. http://engbul.bmstu.ru/doc/792392.html (дата обращения : 12.11.2018)

10. Красов А.В., Штеренберг С.И. Методика выбора контейнера для скрытого вложения информации. 4-я Международная научно-практическая конференция «Научные аспекты инновационных исследований», «Аспект», Самара. 2014. -С. 6

11. Кочергина М.А., Первова Н.В. Стеганография. Метод замены наименее значащего бита. Сборник научных трудов / под редакцией Калмыкова Б.М. - Чебоксары: Чувашский государственный университет имени И.Н. Ульянова. 2014. С. 86-89

Научный руководитель: Медведев Николай Викторович, доцент, к.т.н., доцент кафедры «Информационная безопасность» (ИУ-8) МГТУ им. Н.Э. Баумана, medvedevnick54@yandex.ru.

Steganographic method for identifying copyright on an audio file

Kovynyov N.V.[35]

In recent years, the distribution of carriers with the recording of musical works is carried out only through specialized stores. Thus, the management of the store is responsible for the distribution of counterfeit products. Therefore, the store management must be convinced of the absence of counterfeit products in the product. To do this, the easiest way is to record tags (digital watermarks (DWs) in an audio file.) However, steganographic methods of data concealment are not crypto-resistant, because the number of steganography methods is finite and it is possible to determine one method or another by simple search.

***Key words**: algorithm, data, concealment, cryptography, steganography, counterfeiting, coding, digital watermark.*

[35] Nikolai Kovynyov, postgraduate student , Bauman Moscow State Technical University, Moscow, n.kovynyov@gmail.com

УДК

Сжатие биометрических сигналов с помощью дискретного косинусного преобразования и дискретного преобразования Чебышева

Кондрашев И.В.[36]

На примере электрокардиографического (ЭКГ) сигнала рассмотрено сравнение двух методов, используемых при компрессии биомедицинских данных. Эти методы используют дискретное преобразование Чебышева (ДПЧ), основанное на ортогональных полиномах и дискретное косинусное преобразование (ДКП), часто используемое при компрессии ЭКГ. При частоте дискретизации 500 Гц экспериментальные результаты показывают, что восстановленные сигналы, обработанные с использованием ДКП, имеют более низкую погрешность, чем при использовании ДПЧ, при одной и той же степени сжатия. Для оценки сигналов использовались метрики MSE и SNR.

Ключевые слова: сжатие, компрессия, электрокардиограмма, дискретное преобразование Чебышева, дискретное косинусное преобразование.

Введение

В современной медицине, особенно в контексте развития телемедицины, необходимо хранить и передавать большое количество медицинских данных о пациентах. Одним из таких примеров является электрокардиограмма (ЭКГ), которая представляет собой электрические волны, производимые сердечной деятельностью человека. Огромное количество записей ЭКГ, регистрируемых каждый год, требуют больших объемов памяти для хранения. Так как каждая база данных, хранящая у себя огромное количество записей, имеет свой лимит, и скорость передачи этих данных ограничена, то необходимо уменьшать размер данных файлов. Решить проблему можно с помощью компрессии, целью которой является достижение высокой степени сжатия при сохранении соответствующей диагностической информации в восстановленном сигнале.

Принципы сжатия биомедицинских сигналов

Процессы сжатия, независимо от того, работают ли они на аудио, видео, изображениях или других форматах файлов, подразделяются на два основных типа: сжатие без потерь и с потерями. В методах сжатия без потерь исходные данные могут быть точно восстановлены из их сжатой формы, в то время как при сжатии с потерями можно получить только приближенную оценку исходных данных.

Сжатие без потерь обычно применяется для сжатия текста, в то время как компрессия с потерями используется в случае изображений и звука, где небольшая потеря разрешения часто не обнаруживается или, по крайней мере, приемлема. Примечательно, что под термином «потеря», подразумеваются не случайно потерянные данные, а частотные составляющие, которые могут являться шумом. Таким образом, при сжатии данного типа важно выяснить, полностью ли поддерживается или «улучшается» после сжатия аутентичный смысл сигнала.

Сжатие биомедицинского сигнала требует глубокого изучения его свойств, для обеспечения, как успешного сжатия, так и точного представления диагностики сигнала [1-3]. С этой целью биоакустическое сжатие данных следует обрабатывать иначе, чем сжатие изображений или речевых данных. Это связано с тем, что свойство человеческого глаза или уха выступает в качестве сглаживающего фильтра, позволяя допустить определенную степень искажения данных, но, при этом, существенные области должны быть сохранены с максимально возможной

[36] Кондрашев Иван Владимирович, магистрант, МГТУ им. Н.Э. Баумана, Москва, beenv12@gmail.com

морфологической точностью для четкого представления диагностической информации.

Сжатие сигнала

Процесс сжатия на примерах дискретного косинусного преобразования (ДКП) [4] и дискретного преобразования Чебышева (ДПЧ) [5,6] проходит следующим образом. К сигналу с частотой дискретизацией равной 500 Гц (рис. 1), взятому на интернет-портале PhysioNet [7], применяются данные преобразования. Часть полученных коэффициентов (рис. 2-3), которая была ниже установленного порога, обнуляется (пороговое сжатие или *thresholding*). Затем с помощью обратных преобразований сигнал заново восстанавливается из оставшихся коэффициентов. На рис. 4 показаны восстановленные сигналы при сжатии 10:1 (обнуление 90% коэффициентов), а на рис. 5 продемонстрированы сигналы при сжатии 10:2 (обнуление 80% коэффициентов).

Рис. 1. Исходная ЭКГ

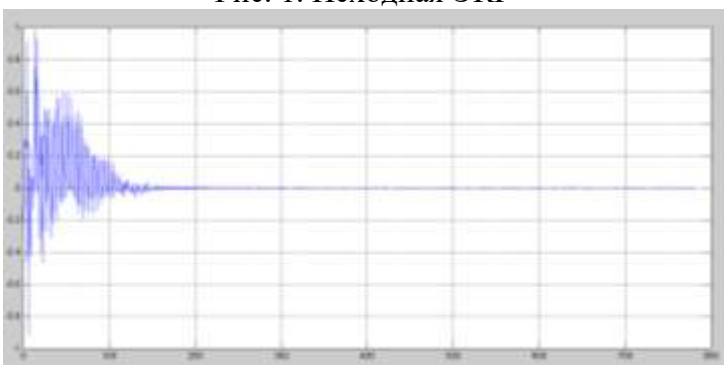
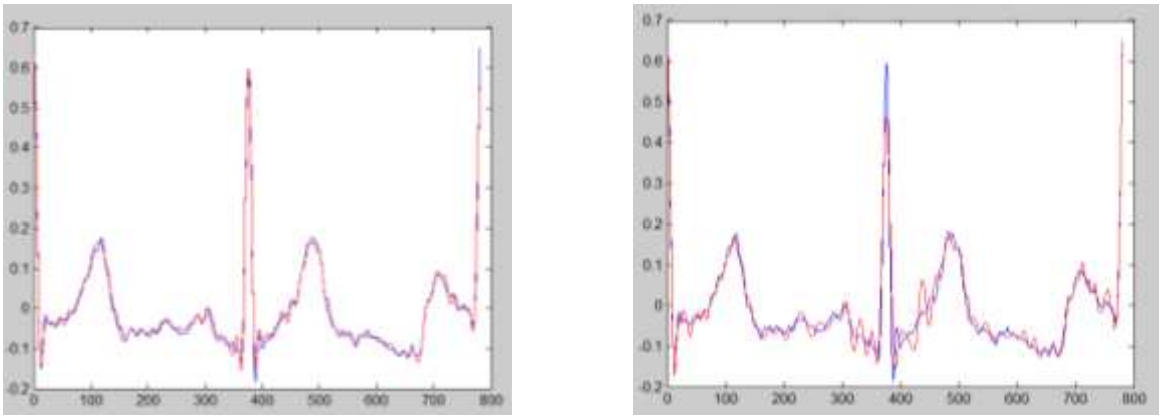


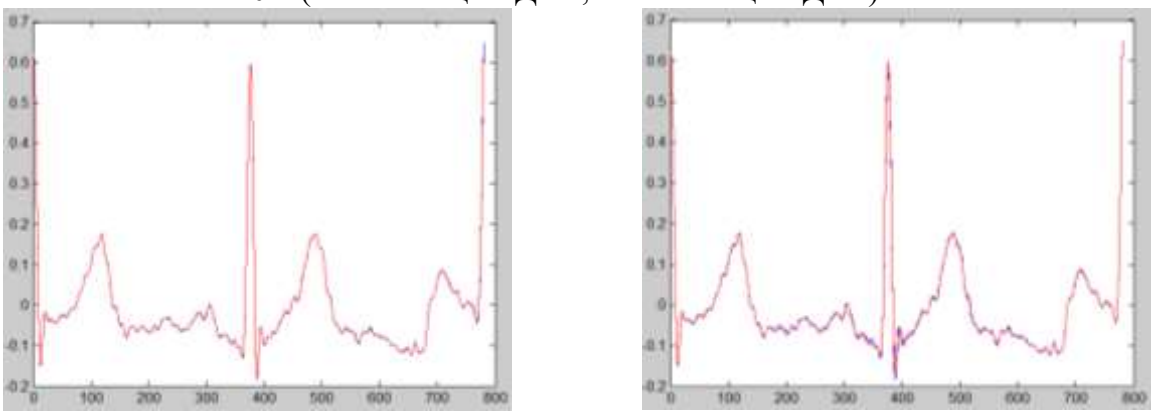
Рис. 2. Коэффициенты ДКП

Рис. 3. Коэффициенты ДПЧ



а) б)

Рис. 4. Исходный ЭКГ сигнал (синий) и сжатый ЭКГ сигнал (красный) при сжатии 10:1 (а - с помощью ДКП, б - с помощью ДПЧ)



а) б)

Рис. 5. Исходный ЭКГ сигнал (синий) и сжатый ЭКГ сигнал (красный) при сжатии 10:2 (а - с помощью ДКП, б - с помощью ДПЧ)

Для оценки сигналов используются величины среднеквадратичного отклонения (*MSE*) (рис. 6) и отношение сигнал-шум (*SNR*) (рис. 7):

$$MSE = \frac{1}{N}\sum_{i=1}^{N}\left(S(i) - \hat{S}(i)\right)^2, \quad (1)$$

$$SNR = \frac{\sum\left(S(i)\right)^2}{\sum\left(S(i) - \hat{S}(i)\right)^2}. \quad (2)$$

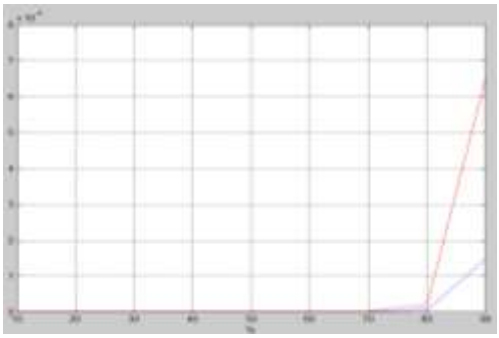
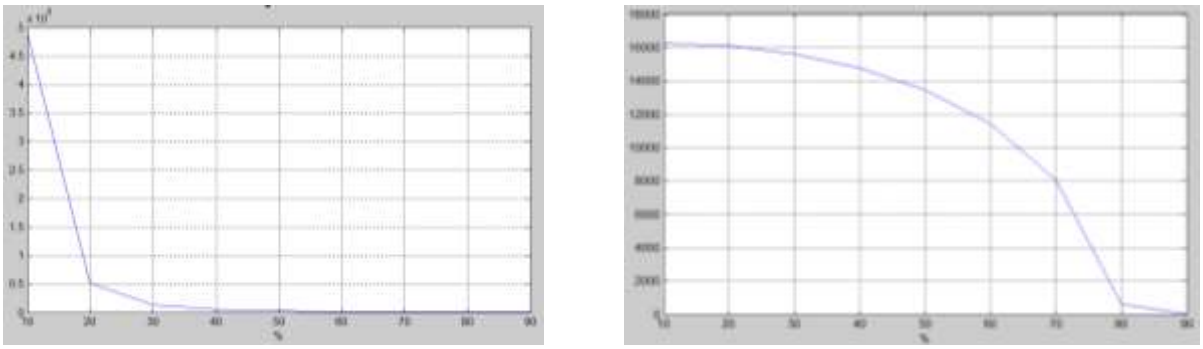


Рис. 6. График ошибки MSE от процентов обнуленных коэффициентов (синий - ДКП, красный - ДПЧ)



а) б)

Рис. 7. График ошибки SNR от процентов обнуленных коэффициентов (а - при сжатии с помощью ДКП, б - при сжатии с помощью ДПЧ)

Экспериментальные результаты показали, что при обнулении первых 90% коэффициентов (сжатие 10:1) сигнал теряет свою исходную форму, особенно при использовании ДПЧ, что является не допустимым при сжатии биомедицинских сигналов. При обнулении первых 80% сигнал повторяет свою форму с небольшими ошибками, что по меркам человеческого глаза является допустимым. Что касается самих методов, ДКП показало себя намного лучше, в силу того, что величина *MSE* меньше, а отношение сигнал-шум на два порядка выше, чем у ДПЧ.

Заключение

Необходимость хранения все больших объемов цифровых биометрических данных в течение более долгого срока требует исследования новых подходов к решению проблемы ограничения памяти с помощью методов сжатия сигналов. В случае с биомедицинскими данными требуется проводить более тщательный анализ самого процесса, т.к. сжатие может привести к искажению диагностической информации, а также потере уникальных биометрических свойств сигнала конкретного пациента.

В результате проведенного эксперимента с помощью двух дискретных преобразований — ДКП и ДЧП, часто используемых в биомедицинской практике, было осуществлено сжатие сигналов ЭКГ. Были рассмотрены разные степени сжатия. На основе полученных оценок *MSE* и *SNR* сделаны выводы, что лучшее качество процесса сжатия достигается при ДКП сигнала с коэффициентом сжатия 10:2.

Литература

1. R.M. Rangayyan, Biomedical Signal Analysis: A Case-Study Approach, A Treatise on Electricity and Magnetism, 1nd ed. New York: John Wiley & Sons, Inc., 2002. Рангаян Р.М. Анализ биомедицинских сигналов. Практический подход / Пер. с англ. под ред. А.П. Немирко.- М.: ФИЗМАТЛИТ, 2007.-440 с.

2. Leontios J. Hadjileontiadis, Biosignals and compression standarts, M-Health: Emerging Mobile Health Systems, pp. 277-292, 2006.

3. S. M. S. JALALEDDINE, C. G. HUTCHENS, R. D. STATTAN, W. A. COBERLY, ECG Data Compression Techniques-A Unified Approach, IEEE Transactions on Biomedical Engineering, Vol. 37, NO. 4, April 1990 pp. 329-343.

4. Belina J. Allen, V.A., ECG data compression using the discrete cosine transform (DCT), Oct. 1992, pp. 687–690, Computers in Cardiology 1992.

5. R. Chaturvedi and Y. Yadav, Analysis of ECG signal by Polynomial Approximation, International Journal on Recent and Innovation Trends in Computing and Communication, May 2014, 2 (5), pp. 1029-1033.

6. D. Tchiotsop and S. Ionita, ECG Data Communication Using Chebyshev Polynomial Compression Methods, University of Pitesti, Romania, 2010.

7. Интернет-портал PhysioNet - [Электронный ресурс]. URL: https://www.physionet.org; (дата обращения: 29.08.2018).

Научный руководитель: Басараб Михаил Алексеевич, доктор физико-математических наук, профессор, заведующий кафедрой «Информационная безопасность» (ИУ-8) МГТУ им. Н.Э. Баумана, basarab.iu8@gmail.com

Compression of ECG signals using discrete cosine transform and discrete Chebyshev transform

Kondrashev I.V.[37]

Two techniques used in ECG (electrocardiogram) compression are compared. These two techniques use DCT (discrete cosine transform), one of the most common transformations in ECG compression and DChT (discrete Chebyshev transform), based on orthogonal polynomials. With sampling rate of 500 Hz, the experimental results show that the reconstructed signals obtained using DCT have a lower error than when using a DChT. The error between the original signals and the reconstructed signals is measured using MSE metrics and the signal quality is estimated with SNR value.

Key words: compression, ECG, discrete Chebyshev transform, discrete cosine transform.

[37] Kondrashev Ivan, Bauman Moscow State Technical University, Moscow, beenv12@gmail.com

УДК

Математическая постановка задачи распределения вычислительных ресурсов между средствами защиты информации на основе дискретно-непрерыной игры

Крыгин И. А.[38]

Аннотация

В работе рассмотрена задача распределения ограниченных вычислительных ресурсов автоматизированной системы между средствами защиты информации. Для её решения предложено использование методов теории игр, и была описана соответствующая игра. Сформулированы условия дискретно-непрерывной игры. В такой игре сторона защиты выбирает конкретные средства защиты, множество элементов выбора дискретно. В то же время, из-за неполной информации об атакующей стороне можно считать, что атакующая сторона осуществляет свой выбор с вероятностной неопределенностью, множество элементов выбора для нее непрерывно.

Ключевые слова: ограничения, дискретно-непрерывная игра, задача распределения вычислительных ресурсов, средства защиты информации

Введение

При разработке и проектировании автоматизированных систем часто ставится задача выбора программно-аппаратных средств различного назначения. Эффективное решение такой задачи для автоматизированных систем с ограниченными вычислительными ресурсами имеет особое значение.

В последнее десятилетие ноутбуки, смартфоны, «умные часы» и другие виды мобильных устройств получили значительное распространение и стали неотъемлемой частью жизни обычного человека. Они используются для подключения к Интернету, следят за состоянием здоровья, помогают совершать покупки, и это приводит к тому, что они являются хранилищами чувствительной информации, конфиденциальность, целостность и доступность которой необходимо обеспечивать.

Мобильные устройства подвержены не свойственным стационарным компьютерам угрозам информационной безопасности, таким как потеря, кража, угрозам, связанным с подключением к беспроводным сетям. С другой стороны, мобильность накладывает значительные ограничения на вычислительные способности таких устройств, и это необходимо учитывать при проектировании систем информационной безопасности.

Решение многих задач обеспечения информационной безопасности прямыми методами вычислительно сложное и становится неэффективным при большой размерности входных данных. Использование таких математических инструментов, как теория игр, может в некоторых случаях сделать поиск оптимального решения более эффективным [1-4].

В [5] авторы рассматривают алгоритмы распределения ресурсов для защиты информации между объектами информационной системы на основе игровой модели.

[38] Крыгин И. А., аспирант, МГТУ им. Н.Э. Баумана, ИУ8 «Информационная Безопасность»

В [6] рассмотрен алгоритм выбора классов защищенности объектов распределенной информационной системы и размещения данных по объектам с использованием теории игр.

В [7] рассмотрены алгоритмы распределения ресурсов системы защиты между активами мобильного устройства на основе игры с нулевой суммой.

Для мобильных устройств вопрос распределения ограниченных вычислительных ресурсов между средствами защиты информации является особенно актуальным. Ниже сформулирована математическая постановка задачи распределения вычислительных ресурсов между средствами защиты информации на основе дискретно-непрерывной игры.

Задача распределения вычислительных ресурсов между средствами защиты информации

Рассмотрим информационную систему, которой доступно множество средств защиты информации, и которая имеет ограничения на ресурсы (например CPU, RAM, HDD). Система подвергается нападению множеством атак. Атакующая сторона также имеет ограничения на ресурсы. Атаки могут быть выбраны случайным образом.

Параметры стороны защиты заданы следующими множествами:

- $R = \{r_1, r_2, \dots, r_n\}$ – множество ресурсов;
- $N = \{1, 2, \dots, n\}$ – множество индексов ресурсов защиты;
- $L = \{l_i | i \in N\}$ – количество ресурса $r_i \in R$;
- $S = \{s_1, s_2, \dots, s_k\}$ – множество средств защиты;
- $K = \{1, 2, \dots, k\}$ – множество индексов средств защиты;
- $A = \{a_{i,j}, i \in N, j \in K\}$ – требования к средству защиты S_j по ресурсу R_i.

Выбор средств защиты определяется вектором:

$$X = [x_1, x_2, \dots, x_k]$$

где $x_i \in \{0,1\}$ – определяет, выбрано ли средство защиты s_k

Условие удовлетворения системы требованиям к ресурсам представляется неравенством:

$$\sum_{j \in K} a_{i,j}\, x_j \le l_i, \forall i \in N \qquad (1)$$

Цель защиты - обеспечение информационной безопасности активов путем выбора набора средств защиты. Необходимо учитывать, что вычислительные ресурсы мобильного устройства ограничены, и это может повлиять на конечное решение.

Аналогично для нападения.

Параметры стороны нападения заданы следующими множествами:

- $Z = \{z_1, z_2, \dots, z_f\}$ - множество ресурсов нападения;
- $F = \{1, 2, \dots, f\}$ - множество индексов ресурсов нападения;
- $D = \{d_i | i \in F\}$ – количество ресурса $z_i \in Z$;
- $E = \{e_1, e_2, \dots, e_g\}$ - множество атак;
- $G = \{1, 2, \dots, g\}$ - множество индексов атак;
- $B = \{b_{i,j} | i \in F, \forall\, j \in G\}$ – требования проведения атаки E_j по ресурсу Z_i.

Выбор атаки определяется вектором:

$$Y = [y_1, y_2, \dots, y_g]$$

где $y_i \in [0,1]$ – вероятность выбора атаки e_g

Условие реализуемости атак по ресурсам представляется неравенством:

$$\sum_{j \in G} b_{i,j} y_i < d_{i_i}, \forall i \in F \quad (2)$$

Цель нападения – нарушить свойства безопасности автоматизированной системы.

Также следует определить следующие множества:

- $P = \{p_{i,j} \in [0,1], i \in K, j \in G\}$ – вероятность отражения атаки E_j средством защиты S_i;
- $O = \{o_g, g \in G\}$ - проигрыш защиты от успешной реализации атаки e_g;
- $U = \{u_g, g \in G\}$ – выигрыш нападения от успешной реализации атаки e_g;

Выбор атаки нападения может зависеть от его представления о выборе набора средств защиты. Справедливо и то, что средства защиты следует выбирать с учетом вероятных атак противника.

Показатель качества защиты $t: X, Y, P, O \to \mathbb{R}$ при условии (1) – математическое ожидание «проигрыша» при реализации атаки. Цель защиты – минимизировать этот показатель.

Показатель качества нападения $m: X, Y, P, U \to \mathbb{R}$ при условии (2) – математическое ожидание «выигрыша» при реализации атаки. Цель нападения – максимизировать этот показатель.

Рассмотрим несколько вариантов начальных условий, решения при которых следует рассмотреть.

По соотношению «выигрыша и «проигрыша» сторон:

- «выигрыш» одной стороны равен «проигрышу» другой ($u_g = o_g, g \in G$);
- «выигрыш» одной стороны не равен «проигрышу» другой ($u_g \neq o_g, g \in G$).

Выбор средств защиты не может быть выполнен в смешанных стратегиях, так как это является частью конфигурации информационной системы, выбор средства защиты осуществляется в чистых стратегиях, выбор атаки осуществляется в смешанных стратегиях.

Таким образом необходимо найти такие X, Y, что математические ожидание

$$t = \sum_{e \in E} \left(1 - \max_{i \in K} \{x_i p_{i,e}\}\right) y_g \cdot o_g \to min$$

$$m = \sum_{e \in E} \left(1 - \max_{i \in K} \{x_i p_{i,e}\}\right) y_g \cdot u_g \to max$$

при ограничениях (1) и (2).

Выводы

В других подобных исследованиях было показано (8-14), что использование методов теории игр для нахождения решения при больших размерностях входных данных может быть эффективнее, чем поиск решения первоначальной задачи «прямыми» методами. Таким образом, дальнейшие исследования в этой области являются обоснованными и могут принести положительные результаты, которые будут использованы для решения сформулированной задачи.

Литература

1. Быков А.Ю., Панфилов Ф.А., Зенькович С.А. Модель и методы многокритериального выбора классов защищенности для объектов распределенной информационной системы и размещения баз данных по объектам // Вопросы кибербезопасности. 2016. № 2 (15). С. 9-20.

2. Калашников А.О. Пример использования теоретико-игрового подхода в задачах обеспечения кибербезопасности информационных систем // Вопросы кибербезопасности. 2014. № 1 (2). С. 49-54.

3. Чесноков В.О. Применение алгоритма выделения сообществ в информационном противоборстве в социальных сетях // Вопросы кибербезопасности. 2017. № 1 (19). С. 37-44.

4. Шматова Е.С. Выбор стратегии ложной информационный системы на основе модели теории игр // Вопросы кибербезопасности. 2015. № 5 (13). С. 36-40.

5. Быков А. Ю., Шматова Е.С. Алгоритмы распределения ресурсов для защиты информации между объектами информационной системы на основе игровой модели и принципа равной защищенности объектов // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2015. № 9. DOI: 10.7463/0915.0812283.

6. Быков А. Ю., Панфилов Ф. А., Ховрина А. В. Алгоритм выбора классов защищенности для объектов распределенной информационной системы и размещения данных по объектам на основе приведения оптимизационной задачи к задаче теории игр с непротивоположными интересами // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2016. № 1. DOI: 10.7463/0116.0830972.

7. Быков А.Ю., Крыгин И.А., Муллин А.Р. Алгоритмы распределения ресурсов системы защиты между активами мобильного устройства на основе игры с нулевой суммой и принципа равной защищенности // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. 2018. № 2 (119). С. 48-68. DOI: 10.18698/0236-3933-2018-2-48-68

8. Li L., Shamma J. Efficient computation of discounted asymmetric information zero-sum stochastic games // 54th IEEE Conf. on Decision and Control (CDC). 2015. P. 4531–4536. DOI: 10.1109/CDC.2015.7402927

9. Xiannuan Liang, Yang Xiao. Game Theory for Network Security // IEEE Communications Surveys & Tutorials. 2013. Vol. 15, iss. 1. P. 472 – 486. DOI: 10.1109/SURV.2012.062612.00056.

10. Yanwei Wang, Yu F.R., Tang H., Minyi Huang. A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks // IEEE Transactions on Wireless Communications. 2014. Vol. 13, no. 3. P. 1616 – 1627. DOI: 10.1109/TWC.2013.122313.131118.

11. Koppel A., Jakubiec F.Y., Ribeiro A. A saddle point algorithm for networked online convex optimization // IEEE Transactions on Signal Processing. 2015. Vol. 63. No. 19. P. 5149–5164. DOI: 10.1109/TSP.2015.2449255

12. Schottle P., Bohme R. Game theory and adaptive steganography // IEEE Transactions on Information Forensics and Security. 2016. Vol. 11. No. 4. P. 760–773. DOI: 10.1109/TIFS.2015.2509941

13. Paramasivan B., Prakash M., Kaliappan M. Development of a secure routing protocol using game theory model in mobile ad hoc networks // Journal of Communications and Networks. 2015. Vol. 17. No. 1. P. 75–83. DOI: 10.1109/JCN.2015.000012

14. Shah S.V., Chaitanya A.K., Sharma V. Resource allocation in fading multiple access wiretap channel via game theoretic learning // 2016 Information Theory and Applications Workshop (ITA). 2016. P. 1–7. DOI: 10.1109/ITA.2016.7888137

Научный руководитель: Быков А.Ю.[39]

[39] Быков А.Ю., к.т.н., доцент, МГТУ им. Н.Э. Баумана, ИУ8 «Информационная Безопасность»

The mathematical formulation of problem of counting resources distribution between security tools based on discrete-continuous game

Krygin I.A.[40]

Abstract. In this article it is considered the problem of counting resources distribution between security tools. It is suggested using game theory techniques to solve it, and the corresponding game is described. The discrete-continuous game conditions are formulated. In this game defense side choose specific security tools, the set of selection items is discrete. In the same time, due to out of information, it should be considered attacker to choose attacks with probabilistic uncertainty, the set of selection items is continuous.

Keywords: limitations, discrete-continuous game, problem of counting resources distribution, security tools

[40] Krygin I.A. — post-graduate student, Department of Information Security, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, str. 1, Moscow, 105005 Russian Federation).

УДК 004.056.55

Новые арифметические операции конечного коммутативного кольца и их использование в криптографии

Лебедев А. Н.[41]

Рассматривается класс обобщенных арифметических операций конечного коммутативного кольца, параметризуемых элементами группы подстановок на нем. Среди множества таких подстановок выделяются классы легко реализуемых, с их помощью вводятся новые арифметические операции на конечном кольце вычетов по модулю целого числа. При помощи новых арифметических операций строятся обобщенные протоколы Диффи-Хеллмана со строгой аутентификацией сторон.

Ключевые слова: конечное поле, конечное коммутативное кольцо, новые арифметические операции, криптография, эллиптические кривые, протокол Диффи-Хеллмана, аутентификация.

Введение. Оригинальный протокол Диффи-Хеллмана формирования общего секрета (ключа) парой пользователей сети выглядит следующим образом [3]:
стороны умеют вычислять однонаправленные функции $f(x)$, $g(x, y)$,
стороны независимо выбирают случайные элементы x, y множества X, вычисляют значения функции $f(x)$, $f(y)$ и обмениваются ими по любому доступному им (открытому) каналу

$$f(x) \leftrightarrow f(y),$$

а затем вычисляют общий секрет по формулам

$$K = g(x, f(y)) = g(f(x), y).$$

Основными примерами таких пар функций $f(x)$, $g(x, y)$, являются:

- дискретная экспонента по модулю простого числа p:
  $f(x) = a^x \pmod p$, $g(x, f(y)) = f(y)^x \pmod p$.

В этом случае общий секрет вычисляется по формуле
$K = g(x, f(y)) = f(y)^x \pmod p = g(y, f(x)) = f(x)^y \pmod p = a^{(x*y)} \pmod p$
и представляется элементом мультипликативной группы $Z^*(p)$ поля $Z(p)$. Такой протокол обозначается DH [2, 5, 7].

- вычисление кратной точки эллиптической кривой над полем $Z(p)$
  $E(a, b, p) = \{(x, y) | x, y \in Z(p), y^2 = x^3 + a*x + b\}$.

Пусть $P \in E(a, b, p)$, - точка эллиптической кривой, функции f и g определяются как

$$f(x) = x*P, \text{ и } g(x, f(y)) = x*(y*P),$$

а общий секрет вычисляется по формуле

$$K = g(x, f(y)) = x*(y*P) = g(y, f(x)) = y*(x*P).$$

Он представляется элементом (или только его первой координатой) циклической подгруппы $<P>$ группы точек эллиптической кривой $E(a, b, p)$ над полем $Z(p)$, порожденной точкой P, где порядок группы $|<P>| = q$ – также большое простое число. Такой протокол обычно обозначается ECDH [1, 3, 4, 5].

Главным недостатком протокола Диффи-Хеллмана (DH) и его модификации для эллиптических кривых (ECDH), является отсутствие взаимного подтверждения подлинности сторон [3, 5] (их взаимной аутентификации). Поэтому были предложены протоколы с аутентификацией сторон [2, 4, 6, 7, 8, 9, 10, 11, 12].

Мы предлагаем новый метод формирования общего секрета парой пользователей, обобщающий известные варианты протокола Диффи-Хеллмана с

[41] Лебедев Анатолий Николаевич, к.ф.-м.н., с.н.с., доцент МГТУ им. Н.Э. Баумана, Москва, lan@lancrypto.com, lebedevan@bmstu.ru

аутентификацией сторон. Метод строится на основе введения новых арифметических операций в кольце вычетов $Z(p-1)$ для функций

$$f(x) = a^{x} \pmod p, \text{ и } g(x, f(y)) = f(y)^{x} \pmod p, \quad (1)$$

и общего секрета

$$K = g(x, f(y)) = f(y)^{x} \pmod p = g(y, f(x)) = f(x)^{y} \pmod p = a^{(x*y)} \pmod p, \quad (2)$$

а также для новых арифметических операций в поле вычетов Z(q) как множестве всех кратностей точки $P \in E(a, b, p)$, для которой $|<P>| = q$, [5], то есть функции f и g определяются как

$$f(x) = x*P, \text{ и } g(x, f(y)) = x*(y*P), \quad (3)$$

а общий секрет пары пользователей вычисляется по формуле

$$K = g(x, f(y)) = x*(y*P) = g(y, f(x)) = y*(x*P). \quad (4)$$

Параметризация арифметики. Для описания предлагаемого метода мы рассмотрим более общую алгебраическую задачу. Пусть $R = <R, +, *>$ - конечное коммутативное кольцо с единицей и $n = |R|$, пусть $\alpha, \mu, \sigma \in S(n)$ – некоторые подстановки на множестве R [1]. Определим новые арифметические операции на множестве R следующим образом:

$$x \oplus y = \sigma^{-1}(\alpha(\sigma(x) + \sigma(y))), \quad (5)$$

$$x \otimes y = \sigma^{-1}(\mu(\sigma(x)*\sigma(y))), \quad (6)$$

где символами сложения (+) и умножения (*) обозначены заданные по определению операции кольца $R = <R, +, *>$, [1]. Тогда справедлива

Теорема 1. *Введенные выше операции сложения* $x \oplus y = \sigma^{-1}(\alpha(\sigma(x) + \sigma(y)))$ *и умножения* $x \otimes y = \sigma^{-1}(\mu(\sigma(x)*\sigma(y)))$ *на множестве R удовлетворяют всем аксиомам коммутативного кольца, изоморфного кольцу* $<R, +, *>$ *тогда и только тогда, когда подстановка* μ *есть умножение на некоторый обратимый элемент кольца R, т. е.* $m \in R^*$, *а подстановка* $\alpha = id$ *тождественная*.

Легко вычислимые подстановки. Кроме алгебраических требований к новым операциям сложения и умножения в кольце R, для практических применений важно, чтобы подстановки $\sigma^{-1}, \alpha, \mu, \sigma$, которые параметризуют введенные новые операции, были легко вычислимы. Самым простым из этих классов представляется класс сдвигов, то есть подстановок вида

$$\alpha(x) = x + d$$

где d - некоторый элемент кольца $Z(n)$. Для удобства дальнейшего изложения мы будем представлять элемент d кольца $Z(n)$ в виде $k*m^{-1} = k/m$ с некоторым элементом k кольца и элементом m группы $Z^*(n)$. Тогда можно утверждать, что справедлива следующее

Утверждение 2. *Если на множестве {0, 1, . . ., n-1} операции сложения и умножения заданы по формулам*

$$x \oplus y = (x + k/m) + (y + k/m) – k/m,$$

$$x \otimes y = m*(x + k/m)*(y + k/m) – k/m,$$

для произвольного k и m обратимого относительно операции умножения по модулю n, *то относительно этих новых операций также выполняются все аксиомы кольца Z(n).*

Обобщенные протоколы с аутентификацией сторон. Рассмотрим теперь возможность использования описанных выше новых арифметических операций в кольце вычетов $Z(n)$ и, в частности, в конечном простом поле $Z(q)$ для построения новых протоколов формирования общего секрета с аутентификацией сторон по сравнению с известными [2, 4, 6, 7, 9, 10, 11, 12].

Протокол ADH

1. Пользователи умеют вычислять дискретные функции
   $f(x) = a^{\wedge}x$, $g(x, f(y)) = g(y, f(x)) = a^{\wedge}(x \otimes y)$
   в мультипликативной циклической группе $G = <a>$ порядка q
2. Стороны независимо генерируют случайные целые числа $1 < x, y < q$
3. Вычисляют значения функции $f(x)$, $f(y)$ и обмениваются ими по любому каналу
4. $$f(x) \leftrightarrow f(y),$$
5. Зная общие параметры аутентификации - пару чисел (k, m), вычисляют общий секрет по формулам
   $$K = g(x, f(y)) = g(y, f(x)) = a^{\wedge}(x \otimes y).$$

Протокол AECDH

1. Пользователи умеют вычислять дискретные функции
   $f(x) = x*P$, $g(x, f(y)) = = g(y, f(x)) = (x \otimes y)*P$
   в аддитивной циклической группе $<P>$ порядка q
   точки P некоторой эллиптической кривой
   $E(a, b, p) = \{(x, y) | x, y \in Z(p), y^2 = x^3 + a*x + b\}$ над полем $Z(p)$.
2. Стороны независимо генерируют случайные целые числа $1 < x, y < q$.
3. Вычисляют значения $f(x)$, $f(y)$.
4. Обмениваются ими по открытому каналу,
5. $$f(x) \leftrightarrow f(y),$$
6. Зная общие параметры аутентификации - пару чисел (k, m), вычисляют общий секрет по формулам
   $$K = g(x, f(y)) = g(y, f(x)) = (x \otimes y)*P.$$

Вывод. Предложенные новые арифметические операции позволяют значительно расширить класс протоколов, обобщающих протокол Диффи-Хеллмана и не снижающих стойкости.

Литература

1. Курош А. Г. Теория групп. - М.: Наука. 1967.
2. Blake-Wilson S., Menezes A. Authenticated Diffie-Hellman Key Agreement Protocols // Lecture Notes in Computer Sci. – 1999. - Vol. 1556. – P. 339-361.
3. Diffie W., Hellman M. E. New Directions in Cryptography // IEEE Trans. Inform. Theory. – 1976. – Vol. IT-22. no. 6. – P. 644-654.
4. Diffie W., van Oorschot P., Wiener M. Authentication and Authenticated Key Exchange // Designs, Codes and Cryptography. – 1992. – Vol. 2. no. 2 – P. 107–125.
5. Koblitz N. Elliptic curve cryptosystems // Math. of Computations. – 1987. – Vol. 48. no. 177. – P. 203-209.
6. Lucy G., Lakshmi K., Kumar A. Authenticated Key Exchange Protocols for Parallel Network File System // International Journal of Innovative Technologies. – 2016. - Vol. 4. no. 8. – P. 1487 – 1491.
7. Matsumoto T., Takashima Y., Imai H. On Seeking Smart Public Key Distribution Systems // Trans. IECE of Japan. – 1986. - Vol. E69. no. 2. – P. 99-106.
8. Montgomery P. "Modular Multiplication Without Trial Division" // Mathematics of Computation. - 1985. - vol. 44. no. 170, pp. 519–521.
9. Popescu C. A Secure Authenticated Key Agreement Protocol // Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference. – 2004. – Vol. 2. – P. 783-786.
10. Unger N., Goldberg I. Improved Strongly Deniable Authenticated Key Exchanges for Secure Messaging // Proceedings on Privacy Enhancing Technologies. – 2018. – Vol. 1. - P. 21–66.
11. Wang Z., Hu H. Efficient KEA-Style Lattice-Based Authenticated Key Exchange // IACR Cryptology ePrint Archive. – 2018. - Report 2018/690.
12. Chatterjee S., Koblitz N., Menezes A., Sarkar P. Another Look at Tightness II: Practical Issues in Cryptography // IACR Cryptology ePrint Archive. – 2016. – Report 2016/360.

A New Arithmetic in A Finite Commutative Ring and its Use in Cryptography

Lebedev A.N.[42]

Abstract. In this paper we introduce a new class of arithmetic operations in a finite commutative ring. The elements of this class are parametrized by substitutions on the ring. Among all the substitutions we highlight a class of easy implementable ones and use them to construct new arithmetic operations in a finite integer modulo residues ring. These operations are used to design some extended authenticated Diffie-Hellman cryptographic protocols.

Keywords: finite field, finite commutative ring, new arithmetic operations, cryptography, elliptic curves, Diffie-Hellman protocol, authentication.

[42] Anatoly Nikolayevich Lebedev, Ph.D., senior scientist, associate professor of Moscow State Technical University. N.E. Bauman, Moscow, lan@lancrypto.com, lebedevan@bmstu.ru

УДК 004.056.2

Способ многофакторной аутентификации электронных документов с визуализацией и использованием дополнительного канала

Лебедев А. Н.[43]

Предлагается новый способ обеспечения целостности электронных данных путем их заверения электронной подписью, реализуемой на аппаратном токене, только после их дополнительной визуальной проверки отправителем на экране смартфона и явно выраженного подтверждения их целостности. Предлагаемый метод аутентификации данных позволяет повысить степень защиты данных от необнаруженного их изменения и гарантировать их целостность при подтверждении правильности электронной подписи отправителя под блоком данных. Использование электронной подписи для аутентификации данных обеспечивает неотказуемость владельца закрытого ключа подписи.

Ключевые слова: электронная подпись, визуализация данных, аутентификация, протокол WiFi, протокол Bluetooth, мессенджер, протокол TLS.

Введение. Оригинальные алгоритмы и протоколы подтверждения аутентичности электронных сообщений или отдельных блоков данных при помощи технологии электронной подписи не затрагивали вопросов, связанных с возможностью несанкционированного изменения данных уже после показа их пользователю на экране компьютера непосредственно «на пути» в программу вычисления электронной подписи.

Однако, при широком распространении этой технологии, прежде всего, в рамках систем так называемого дистанционного банковского обслуживания (ДБО) хакерами были предложены относительно несложные вредоносные программы, которые позволяли выполнить изменение электронного платежного документа непосредственно после его демонстрации на экране компьютера, но до его заверения электронной подписью. Наиболее известная из таких программ получила название Silent Banker [1].

Радикальным методом защиты от такого рода атаки является категорический запрет пользователю компьютера, на котором выполняется заверение электронных документов с помощью электронной подписи, выходить в интернет и даже подключать к нему непроверенные USB-накопители. Однако практика показывает, что столь строгие запреты, как правило, не выполняются. Особенно это относится к подключению непроверенных USB-накопителей, как показал известный инцидент с вирусом Stuxnet [2]. А это приводит к значительным финансовым и имиджевым потерям для организации-пользователя.

Значительным шагом в сторону повышения надежности защиты данных от несанкционированного и необнаруживаемого изменения стал переход основной массы пользователей на использование для выполнения ЭП на специальном аппаратном модуле (токене), который позволяет выполнять все действия, связанные с использованием закрытого ключа ЭП непосредственно в защищенной памяти токена, не позволяя его извлечь из защищенной памяти устройства.

Однако это ни в коей мере не решило проблему подмены подписываемых данных уже после их показа на экране компьютера при передаче в токен для хэширования и вычисления ЭП. В качестве паллиативной защитной меры

[43] Лебедев Анатолий Николаевич, к.ф.-м.н., с.н.с., доцент МГТУ им. Н.Э. Баумана, Москва, lan@lancrypto.com, lebedevan@bmstu.ru

разработчики стали предлагать подключать к компьютеру специализированные простые устройства для визуализации данных непосредственно перед их отправкой в токен на подписание ЭП. Такие устройства, называемые «Антифрод-терминалами» [3], PIN-pad [4], и др. также не являются радикальными решениями, а выглядят, скорее, как своеобразные «костыли» для поддержки работоспособности технологии ЭП.

Другой подход, который предлагается на рынке, состоит в том, чтобы все закрытые ключи создания ЭП всех пользователей были собраны на одном защищенном сервере формирования ЭП, и при необходимости пользователи, обращаясь на него и проходя процедуру аутентификации, направляли на сервер свои электронные документы на подписание [4].

С точки зрения надежности и юридической чистоты такого варианта ЭП она не выдерживает критики: при наличии нежелательного для себя электронного документа, подписанного его ключом, пользователь всегда может заявить, что его закрытый ключ находился в распоряжении администратора сервера и поэтому он не несет за подписанные им электронные документы ответственности. При грамотно построенной защите в суде или арбитраже он вполне может выиграть такой спор.

Предлагаемый способ аутентификации электронных документов. Мы предполагаем, что пользователь располагает компьютером с подключаемым к нему через USB-порт аппаратным токеном, реализующим алгоритм вычисления ЭП, а также обладающим дополнительным микроконтроллером, который позволяет токену осуществлять обмен данными по протоколу Bluetooth со смартфоном пользователя или по протоколу WiFi через посредство компьютера, к которому он подсоединен, передавая на смартфон электронный документ или его существенные части, а также получая со смартфона подтверждение на выполнение вычисления ЭП под конкретным документом (блоком данных). В этом случае способ действия сторон в процессе аутентификации данных выглядит следующим образом

1. Пользователь подключает токен к компьютеру, оформляет на компьютере электронный документ и отправляет его на подписание в токен.
2. Токен обрабатывает документ в защищенной памяти и отправляет его (или отдельные его существенные части) по протоколу Bluetooth на смартфон пользователя.
3. Пользователь визуально проверяет правильность содержимого электронного документа на экране смартфона и при его правильности отправляет сигнал по протоколу Bluetooth токену на вычисление ЭП.
4. Получив подтверждение пользователя со смартфона, токен вычисляет ЭП.

Другой вариант предлагаемого способа многофакторной аутентификации электронных данных выглядит следующим образом

1. Пользователь подключает токен к компьютеру, оформляет на смартфоне электронный документ и отправляет его на подписание в компьютер, к которому подсоединен токен. При этом используются протоколы защищенного интернет-соединения, реализуемые широко распространенными месенджерами
2. Токен, получив документ через WiFi, обрабатывает документ в защищенной памяти и отправляет его (или отдельные его существенные части) по протоколу WiFi на смартфон пользователя.

3. Пользователь проверяет содержимое электронного документа на экране смартфона и при его правильности отправляет сигнал по протоколу WiFi токену на вычисление ЭП.
4. Получив подтверждение пользователя со смартфона, токен вычисляет ЭП.

Выводы. Предлагаемый способ многофакторной аутентификации электронных сообщений и отдельных блоков данных позволяет значительно повысить надежность защиты обрабатываемых данных от несанкционированных изменений при помощи технологии электронной подписи, а также защититься от атак путем подмены подписываемого электронного документа непосредственно перед его подписанием в памяти токена.

Литература

1. Symantec // https://www.symantec.com/security-center/writeup/2007-121718-1009-99
2. Вирус Блокада // https://habr.com/post/159053/
3. Аладдин Р.Д. // https://www.aladdin-rd.ru/
4. Актив // https://www.aktiv-company.ru/
5. КриптоПро // http://www.cryptopro.ru/
6. Chatterjee S., Koblitz N., Menezes A., Sarkar P. Another Look at Tightness II: Practical Issues in Cryptography // IACR Cryptology ePrint Archive. – 2016. – Report 2016/360.

Method for Multifactor Authentication of Electronic Documents with Visualization by an Additional Channel

Anatoly N. Lebedev[44]

Abstract. A new method to protect a digital document integrity is presented. The method is based upon a digital signature procedure implementation only after additional confirmation of the document integrity by an user smart phone. This method provides us with much higher security level with respect to any attack based upon an electronic document forgery just before signing it. The method uses some features of the well known communication protocols WiFi and Bluetooth.

Keywords: digital (electronic) signature, data visualization, authentication, WiFi protocol, Bluetooth protocol, messenger, TLS.

[44] Anatoly Nikolayevich Lebedev, Ph.D., senior scientist, associate professor of Moscow State Technical University. N.E. Bauman, Moscow, lan@lancrypto.com, lebedevan@bmstu.ru

УДК 004.056.5

Повышение стойкости стеганографических алгоритмов при использовании фрактальных ключей

Магомедова Д.И.[45]

Данная работа посвящена повышению качества стеганографических методов внедрения секретной информации в неподвижные изображения. Предложено использование дополнительных секретных ключей в виде сгенерированных фрактальных множеств Жюлиа. Предложенный метод позволяет улучшить качество извлеченных данных в условиях компрессии, а также увеличить стойкость к несанкционированному доступу.

Ключевые слова: *множество Жюлиа, алгоритм Дармстердтера-Делейгла, пространственная область, секретный ключ, фрактальный анализ*

Введение

Стеганографические методы скрытия секретных данных нашли свое применение во многих областях науки. Они используются для защиты авторских прав, скрытой передачи данных, скрытой аннотации документов и в других целях [1].

Существует более 700 различных стеганографических алгоритмов, большая часть из которых предназначена для работы с неподвижными изображениями. Такой выбор обусловлен несколькими факторами. Во-первых, особенности различных форматов изображения позволяют скрыть большие объёмы секретных данных. Во-вторых, при использовании изображений в качестве контейнеров можно достичь наиболее незаметного скрытия для человеческих органов чувств.

Однако данная методика имеет ряд недостатков. Усовершенствование методов компрессии изображений приводит к искажению встроенных данных. К тому же для получения секретной информации злоумышленнику в большинстве случаев необходимо знать только алгоритм встраивания.

Фрактальные ключи

Понятия фрактал и фрактальная геометрия, появившиеся в конце 70-х, с середины 80-х прочно вошли в обиход математиков и программистов. Слово фрактал образовано от латинского fractus и в переводе означает состоящий из фрагментов. Оно было предложено Бенуа Мандельбротом в 1975 году для обозначения нерегулярных, но самоподобных структур. Одним из основных свойств фракталов является самоподобие. В самом простом случае небольшая часть фрактала содержит информацию обо всем фрактале.

С математической точки зрения фрактал можно определить как объект, хаусдорфова размерность которого больше топологической и является дробной. Различаются натуральные фракталы – те, которые можно встретить в природе (облака, деревья, береговые линии) и алгебраические, которые строят на основе алгебраических формул [2].

В качестве фрактальных ключей в данной работе использовалось множество Жюлиа. Генерация производилась с использованием алгоритма времени убегания.

Алгоритм времени убегания определяет местоположение каждого пикселя на

[45] Магомедова Дженнет Исламутдиновна, аспирант, Московский технический университет связи и информатики, Москва, jimagomedova@gmail.com

карте возможных состояний системы и присваивает ему цвет. Принимая местоположение пикселя в качестве начальных условий, алгоритм выполняет итерацию системы до тех пор, пока не произойдет одна из двух возможностей. Если очевидно, что итерации не приводят к аттрактору, границу которого мы хотим осветить, то начальные условия не принадлежат этому аттрактору, а соответствующему пикселю присваивается цвет, основанный на том, сколько итераций, потребовались для определения непринадлежности аттрактору [3].

Алгоритм основан на использовании комплексных отображений, сопоставляющих одному комплексному числу $z_n = x_n + iy_n$ другое комплексное число $z_{n+1} = x_{n+1} + iy_{n+1}$ по итерационному правилу $z_{n+1} = f(z_n)$, где$f(z)$ – некоторая нелинейная функция, z,n – номер итерации. Используется квадратичный комплексный полином $f(z) = z^2 + c$, где $c=x+iy$ начальная точка на комплексной плоскости.

Пошагово алгоритм можно описать следующим образом:

1) Ввод начальных значений. Прежде чем перейти к формированию фрактального множества необходимо задать некоторые начальные условия, а именно:
- максимальное количество итераций *k*;
- размерность прямоугольника *l*x*l*, в пределах которого будет построено множество;
- координаты центра прямоугольника c_x,c_y;
- размер изображения, которое будет содержать фрактал *m*x*m*.
2) Формирование прямоугольника *l*x*l*;
3) Попиксельное разделение сформированного прямоугольника;
4) Расчёт радиуса *R*;
5) Определение принадлежности точек множеству.

С использованием вышеприведенного алгоритма был сгенерирован секретный ключ со следующими параметрами: c = -0.76643+0.16471*i, l = 1.5, k = 30.

Встраивание секретных данных

Встраивание секретных данных производилось в два этапа. В первую очередь производилось добавление цифрового знака в сгенерированный фрактальный ключ методом замены наименее значимого бита (рис.1). Затем полученное изображение добавлялось в контейнер с использованием алгоритма Дармстердтера-Делейгла[4] (рис 2). Это алгоритм встраивания в пространственную область изображения, основанный на блочном делении. Каждый бит секретной информации встраивался в один блок синего канала исходного контейнера.

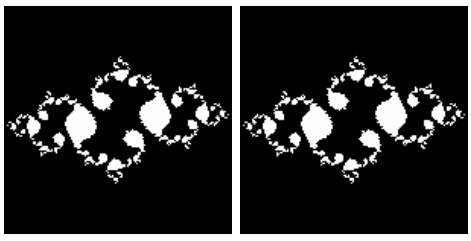


Рис.1. а) сгенерированный фрактальный ключ, б) ключ со встроенным ЦВЗ

Рис.2. а) незаполненный оригинальный контейнер; б) контейнер со встроенным секретным ключом

Извлечение секретных данных

Извлечение производилось по следующему алгоритму. В первую очередь из заполненного контейнера методом Дармстердтера-Делейгла извлекается секретный ключ (рис. 3). После получения ключа на приемной стороне генерируется фрактал с использованием заранее выбранных параметров. Цифровой водяной знак восстанавливается в процессе вычитания полученного ключа и сгенерированного фрактала (рис.4).

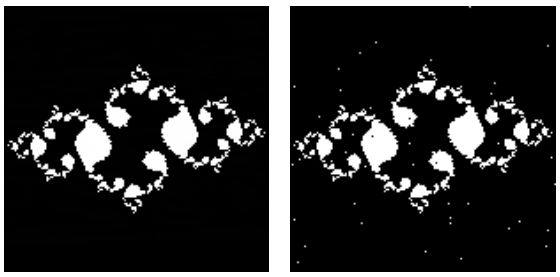


Рис 3. а) Созданное фрактальное изображение+ ЦВЗ. б)Извлеченное фрактальное изображение, содержащее ЦВЗ

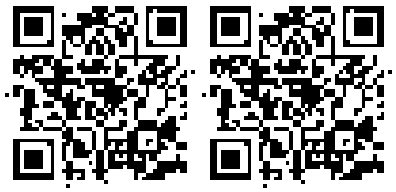


Рис.4. а) Исходный ЦВЗ б) Извлеченный из фрактального изображения цифровой водяной знак

В результате выполнения алгоритма был получен водяной знак очень высокого качества. Несмотря на то, что можно наблюдать небольшие искажения пикселей на извлеченном секретном ключе, полученный водяной знак полностью идентичен оригинальному. Нет никаких видимых искажений, возможно чтение информации из QR-кода.

Повышение стойкости алгоритма к несанкционированному доступу

Для оценки секретности разработанной системы была смоделирована ситуация, в которой злоумышленник завладел секретным ключом со встроенным ЦВЗ, а также ему известны некоторые параметры сгенерированного фрактала, а

именно размер прямоугольника *l*, максимальное число итераций *k* и размер изображения *m*. Единственным неизвестным параметром является начальная точка *c*. В качестве примера было сгенерировано четыре фрактала с различными значениями параметра *c* (рис. 5) и произведено извлечение водяного знака с использованием полученных изображений (рис. 6).

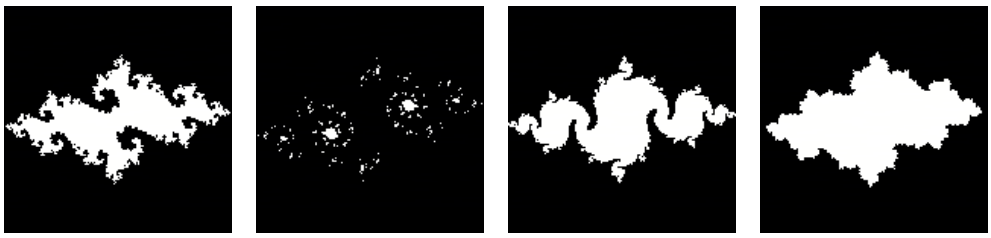


Рис. 5. Фрактальные изображения с различным значением с
а) -0.73949 + 0.16498**i*; б) -0.74549 + 0.37841**i*; в) -0.80939 + 0.12388**i*; г) -0.63949 +0.19098**i*.

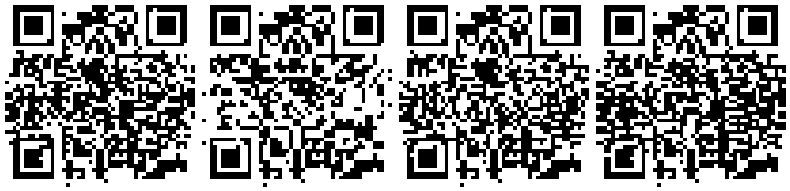


Рис. 6. Водяные знаки, полученные при извлечении с использованием фракталов, представленных на рис. 10.

Как видно из рисунков все изображения, полученные в результате эксперимента, настолько значительно отличаются от оригинального ЦВЗ, что извлечение информации из QR кода становится невозможным.

Выводы

В результате проведенных исследований показано, что использование фрактальных ключей улучшает качество внедрения и извлечения секретной информации в стеганографических системах. Благодаря использованию секретных ключей, удалось при извлечении секретной информации получить цифровой водяной знак высокого качества без видимых визуальных искажений и возможностью чтения информации из QR-кода.

Главным достоинством разработанной методики является высокая секретность встраивания. Злоумышленник не сможет сгенерировать секретный ключ без точного знания параметров, используемых при генерации фрактального ключа.

Литература

1..Шелухин О. И., Канаев С. Д. Стеганография. Алгоритмы и программная реализация. Под. редакцией проф. Шелухина О.И. – М.: Горячая линия – Телеком. 2017. – 616 с.

2. Шелухин О.И., Магомедова Д.И. Анализ методов измерения фрактальной размерности цветных и черно-белых изображений // Наукоемкие технологии в космических исследованиях Земли. 2017. Т.9. №6. С.6-16.

3.Sisson P. D. Fractal art using variations on escape time algorithms in the complex plane, Journal of Mathematics and the Arts, 2007, Volume 1, pp. 41-45.

4.Darmstaedter V., Delaigle J. F., Quisquater J.J., Macq B. Low cost spatial watermarking, In Computers and Graphics, August 1998, volume 4, pp. 417-423.

Научный консультант: Шелухин Олег Иванович, д.т.н., профессор, заведующий кафедрой «Информационная безопасность» Московского технического университета связи и информатики, sheluhin@mail.ru

Improving the resistance of the steganographic algorithm using fractal keys

Magomedova J.I.[46]

Abstract. This work is devoted to improving the quality of steganographic methods for the introduction of classified information in still images. The use of additional secret keys in the form of generated fractal Julia sets is proposed. The proposed method allows to improve the quality of extracted data under compression conditions, as well as to increase resistance to unauthorized access.

Keywords: Julia set, Darmsterdter-Deleigle algorithm, spatial domain, secret key, fractal analysis

[46] Magomedova Jennet, postgraduate student, Moscow Technical University of Communication and Informatics, Moscow, jimagomedova@gmail.com

УДК 004.056

Схема пост-квантовой агрегированной подписи на основе теории алгебраического кодирования

Макаров А.О.[47]

В данной статье представлена схема пост-квантовой последовательной агрегированной подписи на основе теории алгебраического кодирования — APCFS. Представленная конструкция является расширением существующей схемы электронной подписи Parallel-CFS для получения на её основе последовательной агрегированной подписи для произвольного числа подписантов, размеры которой не растут с увеличением их числа.

Ключевые слова: криптография на основе теории кодирования, схема электронной подписи CFS, агрегированная подпись, пост-квантовая криптография

Введение

Системам обеспечения безопасности часто приходится иметь дело с электронными подписями, выработанными различными пользователями для различных сообщений. Для уменьшения размеров итоговых подписей, как правило, используются так называемые схемы агрегированных подписей [1], позволяющих преобразовать различные индивидуальны электронные подписи в единую подпись, которая затем может быть использована для проверки любого из подписанных сообщений.

Большинство современных схем подписи (включая агрегированные) основываются на предположении о сложности задач факторизации больших чисел и нахождения дискретного логарифма. Однако, принимая во внимание возможность появления в ближайшем будущем квантового компьютера, способного на эффективное выполнение алгоритма Шора [2], наиболее остро встаёт задача разработки пост-квантовых схем подписи.

В данной статье представлено расширение существующей пост-квантовой схемы подписи Parallel-CFS, построенной на основе задач теории кодирования, для получения последовательной агрегированной подписи. Представленная схема является первой описанной агрегированной схемой подписи на основе задач теории кодирования.

Схема агрегированной электронной подписи APCFS

В данном разделе представлено формальное описание предлагаемой схемы пост-квантовой агрегированной подписи. В качестве основы для построения схемы используется параллельная схема CFS [3], к которой применяется принцип последовательной агрегации, аналогичный схеме MQSAS [4], а именно построения агрегированной подписи с использованием произвольной подстановки [5]. Схема получила название Агрегированной Параллельной Подписи CFS — APCFS.

Генерация ключей: Выбрать параметры m и t, $n = 2^m$, i, δ: $\binom{n}{n+\delta} > 2^{mt}$, и i криптографических хэш-функции $h_1, \ldots, h_i$. Пусть $\Gamma(g, S)$ двоичный код Гоппы, заданный полиномом $g \in \mathbb{F}_2^{2^m}$ степени t и поддержкой S, где S — перестановка элементов $\mathbb{F}_2^{2^m}$. Пусть H систематическая $mt \times n$ матрица проверки кода $\Gamma(g, S)$

[47] Макаров Артём Олегович, аспирант кафедры «Криптология и кибербезопасность», НИЯУ «МИФИ», Москва, zma.94@mail.ru

является открытым ключом, g и S образуют закрытый ключ.

Агрегированная подпись. Имея подпись σ_{n-1} сообщений $D_1, \ldots, D_{n-1}$, открытые ключи $H_1, \ldots, H_{n-1}$, получить агрегированную подпись для сообщений $D_1, \ldots, D_n$ (рис.1). Сначала производится проверка агрегированной подписи σ_{n-1}. В случае её верности для сообщения D вычисляются i хэш значений $h^{(n)} = h_1(D_n)||h_2(D_n)||\ldots||h_i(D_n)$, к которым побитно прибавляется подпись σ_{n-1}: $h_{\oplus}^{(n)} = h^{(n)} \oplus \sigma_{n-1} = h_{\oplus_1}^{(n)}||h_{\oplus_2}^{(n)}||\ldots||h_{\oplus_i}^{(n)}$. Если длина вектора σ_{n-1} меньше длины $h^{(n)}$, то σ_{n-1} дополняется с помощью дополнения PKCS#7. Затем используется алгоритм декодирования кодов Гоппы схемы CFS с полным декодированием для получения i ошибок $e_1^{(n)}, \ldots, e_i^{(n)}$ веса не более $t + \delta$, таких что $H \times e_i^T = h_{\oplus_i}^{(n)}$. Подписью является $\sigma = \sigma_n = \phi_{t+\delta}^{-1}\left(e_1^{(n)}\right)||\ldots||\phi_{t+\delta}^{-1}\left(e_i^{(n)}\right)$.

Агрегированная проверка подписи. Имея сообщения $D_1, \ldots, D_n$, агрегированную подпись $\sigma = \sigma_n = p_1^n||\ldots||p_i^n$, открытые ключи $H_1, \ldots, H_n$ для $k = n, \ldots, t$ последовательно вычисляются (рис.2):

$$h_{\oplus j}^k = H \times \phi_{t+\delta}\left(p_j^{(k)}\right), j = 1, .., i, \quad (1)$$

$$\sigma_{i-1} = unpad(h_{\oplus 1} \oplus h_1(D_k)||\ldots||h_{\oplus i} \oplus h_i(D_k)), \quad (2)$$

где $unpad$ операция удаления PKCS#7 дополнения. В конце производится проверка $\sigma_0 =? 0$.

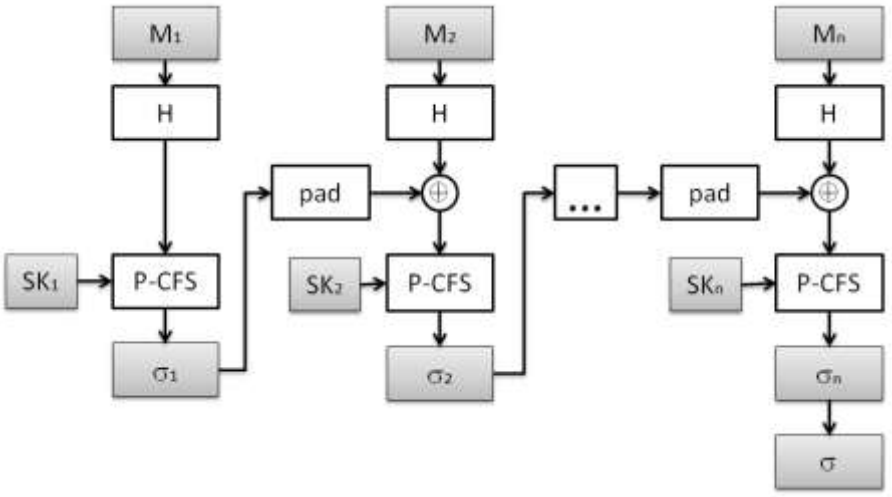


Рис.1. Схема получения агрегированной подписи APCFS

Для демонстрации корректности схемы без потери общности зафиксируем $i = 2$. При осуществлении проверки подписи, в случае если хотя бы одна подпись в цепочке будет неверна, итоговое значение σ_0 будет отлично от нуля, так как в случае неверной подписи $\sigma = p_1^{(j)}||p_2^{(j)}$ данная подпись не даст равенства $h_{\oplus 1}^{(j)} = H \times \phi_{t+\delta}\left(p_1^{(j)}\right), h_{\oplus 2}^{(j)} = H \times \phi_{t+\delta}\left(p_2^{(j)}\right)$, что впоследствии даст неверное значение $\sigma_{j-1} = p_1^{(j-1)}||p_2^{(j-1)}$. Таким образом, равенство $\sigma_0 = 0$ возможно только в случае верных подписей $\sigma_j, j = 1, .., n$.

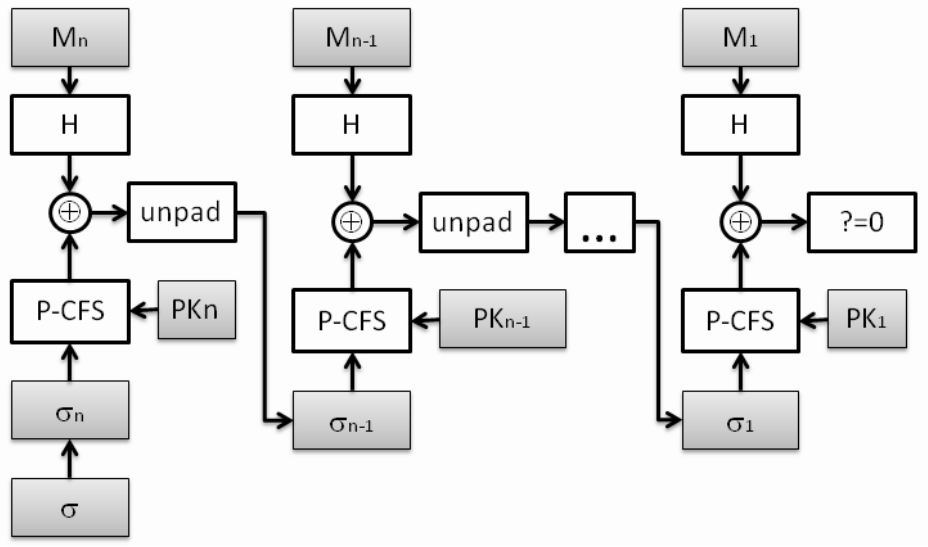


Рис.2. Схема проверки агрегированной подписи APCFS

При формировании каждой новой подписи каждым подписантом могут быть использованы техники сжатия подписи, описанные в [6]. Таким образом, каждая агрегированная подпись σ_j будет иметь меньший размер. При максимальном сжатии операция проверки усложняется на незначительное число матричных операций в матрице H, что не оказывает значительного влияния на скорость проверки подписи.

Параметры схемы APCFS

Предлагаемые параметры схемы подписи APCFS представлены в таблице 1. Заметим, что схема APCFS является оптимальной, и коэффициент сжатия не зависит от изменения параметров.

Производительность APCFS на одном ядре Intel Xeon W3670 3.20GHz составляет порядка одной подписи в секунду, что является приемлемым значением, при использовании в реальных системах [7].

Таблица 1.

Рекомендуемые параметры подписи Parallel-CFS

Параметры (m, t, δ, i)	Параметр стойкости	Размер открытого ключа	Размер подписи, бит	Число операция для осуществления подписи
(20,8,2,2)	75	20 MB	196	$2^{16,3}$
(20,8,2,3)	81	20 MB	294	$2^{16,9}$
(18,2,2,2)	76	5 MB	162	$2^{19,5}$
(18,2,2,3)	83	5 MB	288	2^{20}
(19,9,2,2)	80	10,7 MB	209	$2^{19,5}$
(19,9,2,3)	87	10,7 MB	309	2^{20}
(16,10,2,2)	75	1,2 MB	180	$2^{22,8}$
(16,10,2,3)	82	1,2 MB	270	$2^{23,4}$

В таблице 2 представлено сравнение подписи APCFS с агрегированной подписью MQSAS и подписью на основе RSA. На рисунке 3 представлено сравнение размеров подписей MQSAS и APCFS при различном числе подписантов.

Таблица 2.

Сравнение подписи APCFS с подписью MQSAS и RSA

Название схемы (параметры)	Параметр стойкости	Размер открытого ключа	Размер индивидуальной подписи	Размер агрегированной подписи (20 подписантов)
APCFS (16,10,2,3)	82,5	1,2 MB	270 бит	270 бит
APCFS (19,9,2,2)	80,5	10,7 MB	206 бит	206 бит
MQSAS (96,65,2,2,2)	80	55,7 kB	102 бит	254 бит
MQSAS (96,5,6,6,2)	80	55,7 kB	114 бит	570 бит
RSA (1024,17)	80	256 B	1024 бит	—

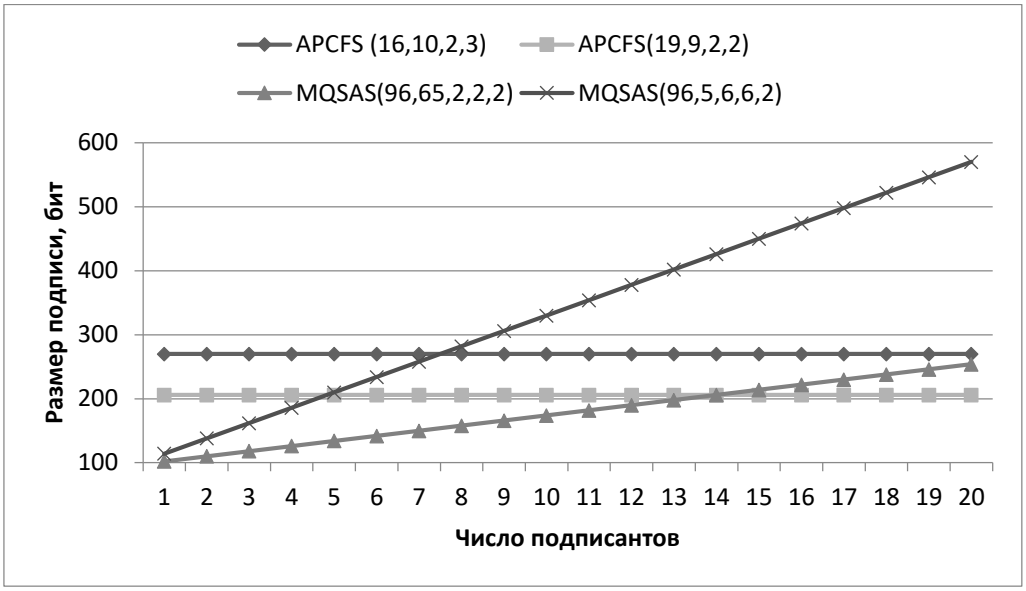


Рис.3. Сравнение размеров агрегированных подписей APCFS и MQSAS

Как видно из сравнения, схема APCFS обеспечивает такой же уровень стойкости, как и MQSAS, однако имеет меньший размер агрегированной подписи, при определённых параметрах. В то же время стоит отметить, что размер открытого ключа схемы APCFS значительно больше, чем в схеме MQSAS (на несколько порядков), что ограничивает применение данной схемы на встраиваемых устройствах, для которых большой размер ключей может стать критичным.

Выводы

В статье была описана первая схема агрегированной подписи на основе теории кодирования — APCFS. Представленная схема обладает малым размером подписи и высокой скоростью проверки, однако низкой скоростью подписи (порядка одной секунды) и имеет достаточно большой размер ключей. Параметр стойкости схемы составляет 80 бит.

Описанная схема, в отличии от других известных пост-квантовых схем, обладает полной агрегацией, т.е. не увеличивает свой размер с ростом числа подписантов и позволяет получить преимущество в размерах подписи уже при 8 подписантах по сравнению со схемой MQSAS.

Описанные в данной статье результаты могут быть использованы для реализации схемы пост-квантовой агрегированной подписи при переходе к пост-квантовым криптосистемам.

Литература

1. Boneh D. A Survey of Two Signature Aggregation Techniques / Dan Boneh, Craig Gentry, Ben Lynn, Hovav Shacham // CryptoBytes. – 2003. – Vol. 6, № 2.
2. Grover L. A fast quantum mechanical algorithm for database search // Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. – 1996. – pp. 212–219
3. Finiasz M. Parallel-CFS Strengthening the CFS McEliece-Based Signature Scheme / Matthieu Finiasz // Selected Areas in Cryptography - 17th International Workshop. – 2011. – pp. 159-170
4. Bansarkhani R. MQSAS - A Multivariate Sequential Aggregate Signature Scheme / Rachid El Bansarkhani, Mohamed Saied Emam Mohamed, Albrecht Petzoldt. // International Conference on Information Security. – 2016. – 19p
5. Lysyanskaya A. Sequential Aggregate Signatures from Trapdoor Permutations / Anna Lysyanskaya, Silvio Micali, Leonid Reyzin, Hovav Shacham. // EUROCRYPT 2004: Advances in Cryptology. – 2004. – pp. 74-90
6. Courtois N. How to achieve a McEliece-based digital signature scheme / N. Courtois, M. Finiasz, and N. Sendrier // Nicolas Courtois, Matthieu Finiasz, Nicolas Sendrier // Lecture Notes in Computer Science: ASIACRYPT 2001. – 2001. – pp. 157–174
7. Landais G. CFS Software Implementation / Gregory Landais, Nicolas Sendrier // Cryptology ePrint Archive. – 2012. – 15p

Научный руководитель: Варфоломеев Александр Алексеевич, к.физ.-мат.н., доцент, МГТУ им. Н. Э. Баумана, a.varfolomeev@mail.ru

APCFS – Post-Quantum Code Based Aggregate Signature Scheme

Makarov A.O.[48]

Abstract. This article presents code-based sequential aggregate signature scheme APCFS as extension of Parallel-CFS signature scheme. The proposed aggregation technique allows to achieve full signature aggregation, such that the size of aggregate signature is the same as the size of individual Parallel-CFS signature. By doing this we create the first code-based signature scheme of this kind.

Keywords: code based cryptography, CFS signature, aggregate signature, post-quantum cryptography

[48] Artyom Makarov, Department of Cryptology and Cybersecurity, NRNU MEPhI, Moscow, zma.94@mail.ru

УДК 004.02

Обзор методов защиты персональных данных пользователя в web-приложениях

Маркова И.А.[49]

Статья освещает основные методы защиты персональных данных в сфере web-технологий, раскрыты основные угрозы информационной безопасности, способы их реализации и меры по предотвращению утечек.

Ключевые слова: информационная безопасность, утечка персональных данных, методы защиты информации.

Введение

В связи с постоянным развитием технологий высокоскоростного доступа в Интернет важные компоненты любой отрасли перемещаются в среду web: электронная коммерция, порталы государственных услуг, социальные сети, электронная почта, новостные порталы, видеоконференции, персональные web-сайты.

Пока что ситуация с утечками данных, складывающаяся в 2016 году, не выглядит утешительной. Согласно опубликованным результатам всемирного Индекса критичности утечек данных (Breach Level Index, BLI), в первой половине 2016 года было публично зафиксировано 974 серьезных утечки данных, в результате которых было похищено или потеряно 554 миллиона записей данных. И какими бы плохими ни казались эти статистические данные, печальная правда заключается в том, что это всего лишь вершина айсберга [1].

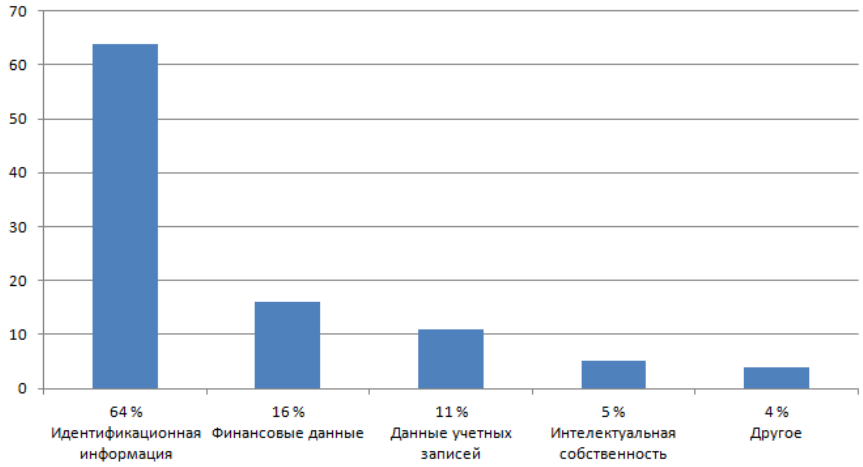


Рис.1. Виды взломов

Для построения указанных систем используются web-приложения, представляющие собой клиент-серверные приложения, в которых клиентами являются браузеры пользователей, а сервером – web-сервер. Логика web-приложения распределена между сервером и клиентом, хранение данных осуществляется в основном на сервере, обмен информацией происходит по сети. Большинство web-приложений являются распределенными и их можно представить в виде трех взаимодействующих уровней: клиент (web-браузер, отправляющий запрос), web-сервер, данные (БД, статистика).

[49] Маркова Ирина Александровна, аспирант, МГТУ им. Баумана, Москва, gurina.irina.94@gmail.com

В зависимости от области применения web-приложения в нем может обрабатываться информация различного уровня доступа и персональных данных пользователей, информация о банковских картах или идентификационные данные и пароли.

Анализ данных исследований, проведенных аналитическим центром PT Research, осуществляющих проведение тестов на проникновение и аудит информационной безопасности показывают, что уязвимости web-приложений являются одним из наиболее распространенных методов реализации злоумышленниками атак на web-приложения с целью завладения ценной информацией [2-4].

Таблица 1

Статистика угроз и их распределение по частоте реализации

№ п/п	Тип угрозы безопасности web-приложения	Доля угроз, %	Доля уязвимых web-приложений, %
1.	Межсайтовое кодирование (XSS-атаки)	19,23	27,27
2.	SQL-инъекции	17,65	49,35
3.	Неправильная конфигурация web-сервера	11,09	37,36
4.	Вредоносное программное обеспечение	12,44	37,66
5.	Подделка межсайтовых запросов (CSRF)	2	7,79
6.	Вызов исключительных ситуаций	11,54	20,78
7.	Прочее	26,05	50

В результате успешной реализации угроз происходит нарушение доступности, целостности и конфиденциальности информации, заражение вредоносным программным обеспечением, недоступность сервисов и прочие потери.

Типы угроз безопасности web-приложений

Межсайтовое кодирование (XSS-атаки)

Атакующая сторона внедряет в выдаваемую web-страницу вредоносный код, который запускает вредоносный сценарий на стороне пользователя. При посещении им зараженной страницы сценарий загружается в браузер пользователя и там запускается. Вредоносный код может быть вставлен в страницу как через уязвимость web-сервере, таки на компьютере пользователя.

SQL-инъекции

Представляет собой подделку определенного запроса к базе данных сайта. При помощи данной уязвимости можно заставить скрипт передавать серверу управление баз данных запрос, который нужен злоумышленнику, а не запрос, на который рассчитывал разработчик. Злоумышленник, используя SQL-инъекцию, может получить доступ к вашим персональным данным, паролям и другой информации которая может храниться на сервере.

Неправильная конфигурация web-сервера

Эта атака, которая использует уязвимости, получившиеся в результате ошибок администрирования web-сервера, приводит к раскрытию или изменению информации злоумышленником.

Вредоносное программное обеспечение

Представляет собой удавшуюся атаку на web-сервер, и как следствие, заражение компьютерным вирусом сервер, на котором развернут ресурс.

Подделка межсайтовых запросов (CSRF)

Атака направлена на имитирование запроса пользователя к стороннему web-приложению. Уязвимость широко распространена из-за особенностей

архитектуры многих web-приложений (многие web-приложения нечетко определяют, действительно ли запрос сформирован настоящим пользователем).

Вызов исключительных ситуаций

Эта атака, которая направлена на систематический вызов исключений и просмотр информации о них [5].

При обеспечении защиты web-приложений необходимо учитывать ряд особенностей их функционирования:

- web-приложения должны быть доступны для своих пользователей 24 часа в сутки 7 дней в неделю;
- web-приложения чаще всего имеют прямой доступ к базам данных пользователей и другой важной информации;
- узконаправленные web-приложения более восприимчивы к атакам, потому что не подвергаются длительному изучению и тестированию, чем более известные общедоступные аналоги;
- традиционные сетевые средства защиты информации не смогут отразить специализированные атаки на web-приложения, так как при помощи браузеров злоумышленник легко получит доступ к внутренним системам и серверам;
- ручное обнаружение и устранение уязвимостей web-приложений не является самым эффективным методом обеспечения безопасности web-приложения.

Для снижения рисков и предотвращения атак на web-приложения необходимо применять комплекс средств защиты информации.

Во-первых, обеспечение защиты необходимо осуществлять еще на стадии проектирования и разработки web-приложения путем создания безопасного кода и планирования рационального состава системы защиты.

Даже если программный код написан без ошибок и уязвимостей, необходима комплексная защита, учитывающая наличие баз данных приложений, web-сервера и прочих элементов ИТ-платформы. Это достигается за счет применения различных средств и методов защиты:

- недопущение ошибок в скриптах при разработке web-приложения;
- сканирование кода web-приложения на наличие уязвимостей;
- использование систем многофакторной аутентификации пользователей;
- применение антивирусного программного обеспечения;
- применение защищенных каналов связи и сетевых протоколов при установке соединения клиента с web-сервером и передачи данных между ними (VPN, HTTPS);
- применение обратных прокси-серверов и прикладных шлюзов на уровне web-сервера;
- применение локальных и сетевых систем обнаружения вторжений;
- применение специализированных межсетевых экранов уровня приложений, которые обладают встроенным функционалом предотвращения вторжений и обеспечивают защиту от целенаправленных сетевых атак [6,7].

Вывод

В данной статье рассмотрены основные типы угроз персональных данных в web-приложениях. Анализ статистики угроз информационной безопасности выявил наиболее уязвимые элементы web-приложений. Даны практические рекомендации по уменьшению рисков атак на web-приложения.

Все эти меры требуется выполнять в комплексе, поскольку защита по раздельности не принесет желаемого эффекта. Угрозы, как в отношении

определенного направления использования web-приложений, так и конкретных технологий меняются очень быстро, поэтому важно регулярно отслеживать статистику угроз web-технологий, анализировать выявленные инциденты и оценивать риски их выявления на систему защиты web-приложения.

Научный руководитель Быков Александр Юрьевич, к.т.н., доцент, МГТУ им. Баумана, Москва, abykov@bmstu.ru

Литература

1. Статистика уязвимостей web-приложений за 2016-2017 года. url: http://www.securitycripts.ru.

2. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2017. 992 с.

3. Ахмед Весам М.А. Защита информации в коммерческих web-приложениях \\ Перспективы развития информационных технологий. 2015. №1(24). С. 164-168.

4. Власенко А.В., Дзьобан П.И., Жук Р.В. Защита персональных данных при авторизации пользователя в распределенных информационных системах, построенных на основе web-технологий \\ Вестник Адыгейского государственного университета. 2017. №2 (201). С. 120-128.

5. Бирюков А.А. Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2012. 474 с.

6. Узденова Г.З., Крахотина Е.В., Свиридова А.В. \\ Инфокоммуникационные технологии в науке, производстве и образовании (ИНФОКОМ-6). 2014. №1. С. 302-305.

7. Мельников, В.П. Информационная безопасность и защита информации: учеб. пособие для студентов высших учебных заведений//В.П. Мельников. -М.: «Академия», 2008. -336 с.

Overview of methods of user's personal data protection in web-applications

Markova I. A.

The article highlights the main methods of personal data protection in the field of web-technologies, reveals the main threats to information security, ways of their implementation and measures to prevent leaks.

Keywords: information security, personal data leakage, methods of information protection.

УДК 004.02

Особенности обеспечения безопасности персональных данных при работе в информационных системах обработки персональных данных

Маркова И.А.[50]

Статья освещает основные вопросы защиты персональных данных в информационных системах обработки персональных данных, раскрывает основные понятия административно-правового, организационного методов и средств защиты информации.

Ключевые слова: информационная безопасность, законодательство РФ, выявление угроз безопасности, подсистемы обеспечения защиты информации.

Введение

Актуальность данной темы заключается в том, что все данные, используемые для работы в любой организации, при неправильном обращении могут стать мощным орудием в руках злоумышленников. Поэтому их защита играет важную роль в деятельности организации. Объектом исследования является определение оптимальных мер по обеспечению безопасности персональных данных в информационных системах обработки персональных данных.

Методы защиты персональных данных в информационных системах обработки персональных данных

По данным Identity Theft Resource Center (ITRC), в 2017 году было зафиксировано 1579 утечек данных, от которых пострадало примерно 179 миллионов записей. Получается, что за один календарный год число нарушений данных выросло на 44%. ITRC отслеживает пять отраслей, но категория «бизнес» уже третий год подряд имеет самые высокие показатели. Наиболее громким нарушением данных в прошлом году стал случай с Equifax – одним из трех основных агентств по кредитной отчетности. Жертвами стало порядка 147,9 миллионов человек, а потому объем скомпрометированных данных просто огромен. Украденная информация содержала имена, даты рождений, адреса и номера страховок. [1].

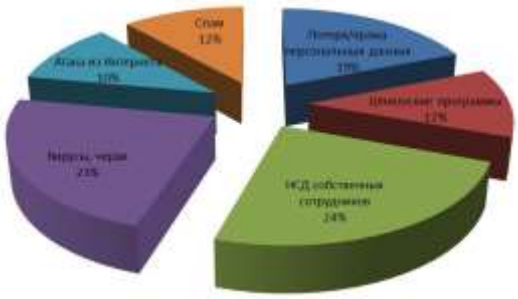


Рис.1. Актуальные угрозы информационной безопасности

Любая система защиты персональных данных состоит из трех важных составляющих: административно-правовых методов, организационных методов и средств защиты информации.

К административно-правовым методам защиты относят нормы действующего законодательства Российской Федерации в области персональных данных. Актуальность обеспечения безопасности персональных данных при их обработке в информационных системах регламентируется Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных» и Постановлением

[50] Маркова Ирина Александровна, аспирант, МГТУ им. Баумана, Москва, gurina.irina.94@gmail.com

Правительства Российской Федерации от 17 ноября 2007 года №781 «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» [2,3].

Данные документы направлены на решение следующих задач:

- предотвращение несанкционированного доступа к персональным данными и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- обеспечение возможности незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных.

С учетом возможного вреда, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности устанавливаются:

- уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;
- требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- требования к материальным носителям и технологиям хранения данных вне информационной системы персональных данных.

Решение вопросов обеспечения организационных методов защиты персональных данных должно предусматривать подготовку кадров, выделение необходимых финансовых и материальных средств, закупку и разработку программного и аппаратного обеспечения [4]. Безопасность персональных данных при их обработке в информационных системах персональных данных определяется следующими задачами:

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением сертифицированных средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационных систем обработки персональных данных;
- учетом машинных носителей персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- разграничение прав доступа к персональным данным, а так же обязательная регистрация и учет всех действий, совершаемых с персональными данными в информационных системах обработки персональных данных;

- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем обработки персональных данных.

В обязательном порядке разрабатываются следующие организационные положения:

- положение об организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах;

- должностные инструкции персоналу информационных систем обработки персональных данных в частности обеспечения безопасности персональных данных при их обработке;

- рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации.

Для осуществления мероприятий по защите персональных данных от несанкционированного доступа и неправомерных действий операторов и пользователей система защиты персональных данных может включать в себя:

- подсистему управления доступом, регистрации и учета;

- подсистему обеспечения целостности;

- подсистему обеспечения безопасности межсетевого взаимодействия информационных систем персональных данных;

- анализа защищенности;

- подсистему обнаружения вторжений;

- антивирусную защиту;

- подсистема криптографической защиты каналов связи [5,6].

Под подсистемой управления доступом, регистрации и учета понимаются утилиты и программные средства блокирования несанкционированного доступа, в которых реализуются функции диагностики (тестирование файловой системы), регистрации (ведение журнала событий), сигнализации (предупреждение о обнаружении фактов несанкционированного доступа или действий, нарушение штатного режима работы информационной системы персональных данных).

Подсистема обеспечения целостности реализована преимущественно штатными средствам операционных систем или СУБД.

Для осуществления функций разграничения доступа к информационным ресурсам применяется подсистема обеспечения безопасности межсетевого взаимодействия информационных систем персональных данных реализованная в межсетевом экранировании, которое реализуется программными или программно-аппаратными межсетевыми экранами. Подсистема анализа защищенности выполняет задачи по осуществлению контроля настроек защиты установленных операционных систем на рабочих станциях или серверах и позволяет произвести оценку возможности проведения атак на сетевое оборудование, контролирует безопасность установленного программного обеспечения. Для безопасной передачи данных в организации по открытым каналам связи или в несегментированной сети служить система криптографической защиты каналов связи.

Таким образом, в данной статье были рассмотрены основные методы защиты персональных данных в информационных системах обработки персональных данных, даны краткие характеристики каждого направления деятельности по обеспечению защиты.

Вывод

В данной статье рассмотрены основные методы защиты персональных данных в информационных системах обработки персональных данных. Представленная тема очень актуальна для многих организаций в связи с распространением работы с персональными данными, как сотрудников, так и клиентов. Предложенные методы защиты персональных данных соответствуют требованиям действующего законодательства РФ и рекомендованы к применению для операторов информационных систем.

В заключение хотелось бы отметить, что один какой-либо способ защиты не обеспечит должной защиты, необходимо комплексно защищать информационные системы обработки персональных данных. Как показывает практика, внедрение перечисленных систем защиты способно обеспечить недоступность персональных данных. Информационные технологии очень быстро развиваются, прогресс не споит на месте, поэтому необходимо пристально следить за развитием и своевременно совершенствовать свою систему защиты.

Литература

1. Статистика уязвимостей web-приложений за 2016-2017 года. url: http://www.securitycripts.ru.

2. Назаров И.Г., Язов Ю.К., Остроухова Е.С. Особенности организации обеспечения безопасности персональных данных при обработке в информационных системах персональных данных \\ Информационная безопасность. 2010. №1. С.71-76.

3. Шакалов М.С. Система защиты персональных данных при их обработке в информационной системе персональных данных \\ Педагогическое образование на Алтае.2014 №1 (2). С.453-454.

4. Бочкарева Т.О., Ковшиков В.А., Малеин А.С. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных \\ Актуальные проблемы деятельности подразделений УИС. 2015. №1. С. 70-72.

5. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2017. 992 с.

6. Бирюков А.А. Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2012. 474 с.

Научный руководитель: Быков Александр Юрьевич, к.т.н., доцент, МГТУ им. Баумана, Москва, abykov@bmstu.ru

Features of personal data security when working in information systems of personal data processing

Markova I. A.

The article highlights the main issues of personal data protection in information systems of personal data processing, reveals the basic concepts of administrative and legal, organizational methods and means of information protection.

Keywords: information security, legislation of the Russian Federation, identification of security threats, information security subsystem.

УДК 003.26.004.7.004.9

Выравнивание загрузки узлов компьютерной сети

Тезисы доклада Медведева Н.В.[51]

Балансировка загрузки узлов сети при обработке трафика высокоприоритетных сообщений в сети уменьшает его влияние на низкоприоритетный трафик. Увеличение интенсивности поступления высокоприоритетных сообщений на узел сети приводит к росту времени ожидания в очереди низкоприоритетных сообщений, поэтому возникает необходимость сбалансированного распределения по узлам показателя качества обслуживания, что важно для обеспечения защиты информации в сети.

Кроме того, необходимо предотвращение высокой загрузки на одни узлы, в то время как загрузка на другие узлы намного ниже. Загрузка на узел определяется как отношение величины полного потока через узел к его пропускной способности. Задача состоит в минимизации суммы стоимостей балансировки узлов, принадлежащих множеству маршрутов для каждого класса потока. Идея, лежащая в основе этой функции, заключается в том, чтобы «штрафовать» маршрутизацию потока через узел по мере увеличения его загрузки. На рисунке 1 представлена стоимостная функция балансировки для узла с единичной пропускной способностью.

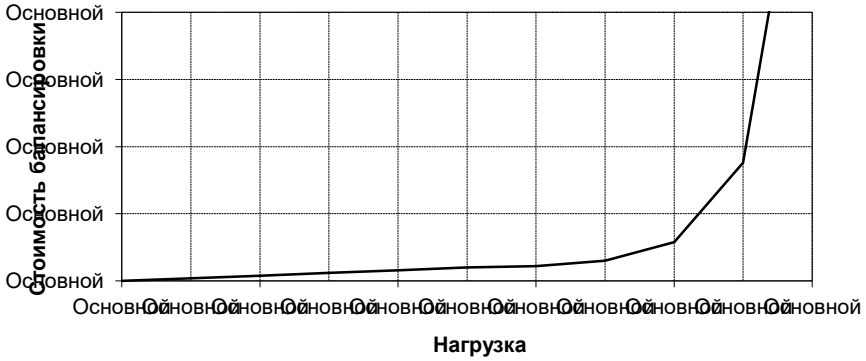


Рис. 1. - Пример функции стоимости балансировки

Пусть $\phi(\cdot)$ – стоимостная функция балансировки. Стоимость выравнивания загрузки $\phi(m)$ на узел m зависит от полного потока через него $f(m)$, создаваемого потоками всех классов, маршруты которых проходят через данный узел. Полный поток $f(m)$ через узел m определяется по следующей формуле:

$$f(m) = \sum_{k \in \mathrm{K}} \sum_{i=1}^{n_t^k} a_m^{k,i} f_i^k \qquad \forall m \in \mathrm{E}, \quad (1)$$

где

$$a_m^{k,i} = \begin{cases} 1, & \textit{если } i-\textit{ый маршрут используется для } k \textit{ потока, проходящего через ребро } m \\ 0, & \textit{в противном случае} \end{cases},$$

f_i^k - доля k-потока, маршрутизированного по i-маршруту из соответствующего множества маршрутов.

E - множество ветвей графа.

Полный поток, проходящий через узел m, должен удовлетворять ограничению $f(m) \le c(m), \ \forall m \in \mathrm{E}$, где $c(m)$ - пропускная способность узла m.

[51] Медведев Николай Викторович, к.т.н., доцент кафедры «Информационная безопасность»

Загрузка на узел m равна $\lambda(m) = \dfrac{f(m)}{c(m)}$ (2)

Стоимостная функция $\phi(\cdot)$ зависит от способа распределения потоков по маршрутам соответствующих классов. Пусть $\varphi_i^k = \dfrac{f_i^k}{f^k}$ – доля k-потока, маршрутизированного по i-пути. Тогда распределение k-потока по маршрутам множества R^k можно записать в виде вектора $\boldsymbol{\varphi}^k = \left(\varphi_1^k, \varphi_2^k, ..., \varphi_{n^k}^k\right)$, стоимость балансировки которого равна $\phi(\boldsymbol{\varphi}^k) \overset{not}{=} \phi^k$.

Пусть векторное пространство $\Omega^k = \left\{\boldsymbol{\varphi}^k : f_\bullet^k \le f^k,\ f_i^k \le \min\limits_{l \in r_i^k}\{c(l)\}\right\}$ – пространство возможных распределений k-потока по маршрутам, тогда $\phi(\Omega^k) = \left\{\phi(\boldsymbol{\varphi}^k) : \boldsymbol{\varphi}^k \in \Omega^k\right\}$ его образ под действием функции $\phi(\cdot)$. Определим теперь пространство совместного распределения потоков Ω как подпространство произведения пространств распределений отдельных потоков $\Omega^1 \times ... \times \Omega^K$, на котором выполняется условие: $\Omega = \{(\boldsymbol{\varphi}^1, ..., \boldsymbol{\varphi}^K) : \boldsymbol{\varphi}^i \in \Omega^i, i = \overline{1,K}, f(l) \le c(l)\}$. Соответственно, $\phi(\Omega) = \{\phi(\boldsymbol{\varphi}^1, ..., \boldsymbol{\varphi}^K) : (\boldsymbol{\varphi}^1, ..., \boldsymbol{\varphi}^K) \in \Omega\}$ – образ пространства Ω под действием стоимостной функции. Для простоты обозначим стоимость совместного распределения K потоков $\phi_{1...K} \coloneqq \phi(\boldsymbol{\varphi}^1, ..., \boldsymbol{\varphi}^K)$.

Задача выравнивания загрузки состоит в нахождении совместного распределения с минимальной стоимостью балансировки, то есть такого $\phi'_{1...K} \in \phi(\Omega)$, *что* $\phi'_{1...K} \le \phi_{1...K},\ \forall \phi_{1...K} \in \phi(\Omega)$. (3)

Вторая цель оптимизации модели достигается минимизацией суммы стоимостей балансировки всех узлов:

$$\min \sum_{m \in \mathsf{E}} \phi(m) \qquad (4)$$

Алгоритм 1. Нахождение минимальной стоимости балансировки $\phi'_{1...K}$.

Шаг 1. Задание исходных данных.

1.1. Множество классов $\mathsf{K} = \{k : k = (s,d),\ s,d \in \mathsf{V}_1, s \ne d\}$.

1.2. Пропускные способности узлов $c(l), l = \overline{1,E}$.

1.3. Потоки $f^k, k = \overline{1,K}$

1.4. Множество маршрутов $\tilde{\mathsf{R}}_T$.

1.5. $\phi(\Omega) = \varnothing$.

Шаг 2. Нахождение минимальной стоимости $\phi'_{1...K}$.

2.1. Построить пространство совместных распределений потоков Ω.

2.2. Выбрать $(\boldsymbol{\varphi}^1, ..., \boldsymbol{\varphi}^K) \in \Omega$.

2.3. Определить потоки на узлах $f(l), l = \overline{1,E}$ по формуле (2.3).

2.4. Вычислить стоимость балансировки $\phi(l)$ для каждого узлы по (2.5).

2.5. Найти стоимость $\phi_{1...K}$ совместного распределения, изменить множество $\phi(\Omega) = \phi(\Omega) \bigcup \{\phi_{1...K}\}$ и положить $\Omega = \Omega \setminus \{(\boldsymbol{\varphi}^1, ..., \boldsymbol{\varphi}^K)\}$.

2.6. Если $\Omega \ne \varnothing$, то вернуться к шагу 2.2.

2.7. Найти $\min_{\phi_{1...K} \in \phi(\Omega)} \{\phi_{1...K}\}$ и завершить работу алгоритма.

На примере графа сети, изображенного на рисунке 2, проиллюстрируем, как форма функции балансировки загрузки соотносится с ее чувствительностью к несбалансированно распределенной загрузке.

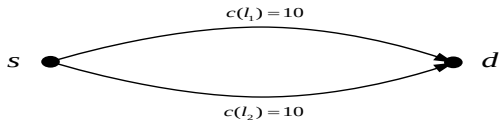


Рис. 2. - Пример графа сети для иллюстрации чувствительности функции балансировки загрузки к неравномерному распределению загрузки

Пусть величина (s,d)-потока равна 10, что с физической точки зрения соответствует интенсивность поступления запросов от узла s к узлу d равна 10 единиц/с. Для любой задачи маршрутизации может быть найдена оптимальная загрузка на узлы графа соответствующей сети. В данном случае оптимальным является равное распределение потока между двумя путями, и оптимальная загрузка равна 0,5. Чтобы показать влияние точной формы функции поиск оптимального решения задачи распределения потоков, сравним две разные функции: ϕ^a, определяемые по формуле (3). Определив функции ϕ^a можно показать, что существует несколько решений с минимальным значением стоимости балансировки, одно из которых не соответствуют оптимальному распределению загрузки. На рисунке 3 показано, что оптимальному значению загрузки на узел соответствует первая точка перелома функции.

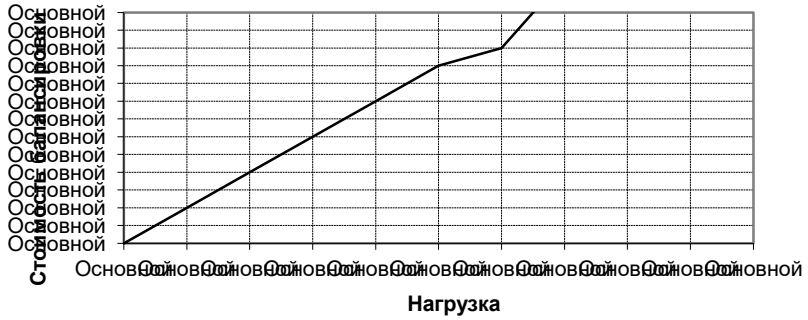


Рис. 3. - Оптимальное значение загрузки 0,5 соответствует первой точке перелома функции ϕ^a

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 . *Самуйлов К.Е.* Методы анализы и расчета сетей ОКС 7 – М.: Изд-во РУДН, 2002.

2 . *Кристофидес Н.* Теория графов. Алгоритмический подход. – М.: Мир, 1978.

3 . S.C. Erbas and C. Erbas. A multiobjective offline routing model for MPLS networks. Proc. Of the 18th International Teletraffic Congress (ITC-18), pages 471-480, Berlin, Germany, August-September 2003.

4 . Олифер В.Г., Олифер Н.А. Компьютерные сети: принципы, технологии, протоколы – СПб.:Питер, 2001.

УДК 003.26.004.7.004.9

Вероятностные характеристики обнаружения скрытых изображений

Медведев Н. В.[52], Глинская Е. В.[53]

В статье рассмотрены основы исследования файлов, подлежащих экспертизе, содержащих шифрованное изображение. Для защиты собственно информации разработано большое количество криптографических алгоритмов. Однако эти алгоритмы не позволяют скрыть от несанкционированного пользователя факт наличия зашифрованной информации.

Большинство информационных процессов связаны с решением проблемы выбора. Эта же проблема решается при поиске лучших в определенном смысле алгоритмов обработки изображений. Основные алгоритмы обнаружения скрытых изображений выносят решения типа: различаются сигналы или нет, изображение искажено или нет и т.п. Задача дешифровки формируется относительно изображения, вызывающего подозрение у экспертов на предмет присутствия скрытого изображения.

Ключевые слова: криптография, шифрованная информация, экспертиза.

Задачей шифрования и сокрытия информации является создание методов, аппаратуры и программного обеспечения, совокупность которых обеспечивала бы минимальную вероятность обнаружения шифрованной информации.

Согласно ТТЗ, изображения, регистрируемые ЦФА и подлежащие шифровке, должны быть обнаружены и идентифицированы в максимально возможный временной интервал [1]. В настоящей НИР исследования ведутся, исходя из классического правила криптографии:

Любая шифрованная информация может быть обнаружена и идентифицирована.

Основные определения:

В дальнейшем будем считать, что задача дешифровки формируется относительно изображения, вызывающего подозрение у экспертов на предмет присутствия скрытого изображения.

Изображение, подлежащее экспертизе, представляет собой реализацию случайного процесса Y, поскольку случай возникновения подозрения непредсказуем.

Вероятность присутствия шифрованной информации в реализации Y равна P(α/Y), где α – скрытое изображение.

Вероятность отсутствия шифрованной информации в реализации Y равна P(o/Y).

Перечисленные вероятности являются условными и апостериорными. Поскольку их можно определить только после экспертизы, и, кроме того, они соответствуют условию возникновения шифрованной информации в анализируемом изображении [2].

Таким образом, для определения P(α/Y) и P(o/Y) необходимо определить вероятность совместного появления двух событий.

$$P(AB)=P(A)*P(B/A)=P(B)* P(A/B), \quad (1)$$

где P(A) – вероятность появления одного из событий:

P(A) – вероятность возникновения подозрения о наличии шифрованной информации;

P(A) – вероятность существования (обнаружения) шифрованного изображения в объекте, предъявляемого экспертизе.

Далее считаем, что событие «А» заключается в том, что у эксперта возникло подозрение о том, что файл, подлежащий экспертизе, содержит шифрованное изображение.

В этом случае:

$$P(Y)*P(\alpha/Y)=P(\alpha)* P(\alpha/Y) \quad (2)$$

[52] Медведев Николай Викторович, ктн, доцент кафедры «Информационная безопасность»

[53] Глинская Елена Вячеславовна, старший преподаватель кафедры «Информационная безопасность»

Следовательно:

$P(\alpha/Y)=(P(\alpha)* P(\alpha/Y))/ P(Y)$ (3)

Если считать, что событие «В» заключается в отсутствии шифрованной информации, то:

$P(O/Y)=(P(o)* P(o/Y))/ P(Y)$ (4)

$P(\alpha)$ и $P(o)$ определяют априорные вероятности наличия и отсутствия шифрованного изображения в файле, предъявленном на экспертизу.

В задаче кодирования и расшифровки скрытых изображений оба из перечисленных выше случаев содержат полную группу событий, поэтому:

$P(\alpha)+P(o)= 1,$ (5)

а также $P(\alpha/Y)+P(o/Y)=1$ (6)

При такой постановке задачи можно воспользоваться основными выводами теории обнаружения [3].

Поэтому, далее вводим в рассмотрение критерий абсолютного отношения правдоподобия:

$L\alpha= P(\alpha/Y)/P(o/Y)= P(\alpha/Y)/(1-P(o/Y))= P(\alpha)/P(o)* P(\alpha/Y)/P(o/Y);$ (7)

На основании изложенного можно записать:

$P(\alpha/Y)= L\alpha/(1+L\alpha)$ (8)

Таким образом, можно считать, что $L\alpha$ определяет вероятность наличия шифрованной информации в реализации, предъявленной на экспертизу.

Если в результате экспертизы подозрительного файла было установлено, что

$L\alpha>1,$

то это означало бы:

$P(\alpha/Y)>0.5,$

и, следовательно:

$P(o/Y)=1-P(\alpha/Y)>0.5.$ (9)

Отсюда следует, что $P(\alpha/Y)>P(o/Y)$, то есть вероятность наличия шифрованного изображения в подозрительном файле выше вероятности его отсутствия.

Однако для определения $L\alpha$ необходимо не только определить величину:

$W= P(Y/\alpha)/P(Y/o),$ (10)

но узнать заранее значения $P(\alpha/Y)$ и $P(o/Y)$.Поскольку перечисленные вероятности являются априорными, для эксперта (экспертов) необходимо точно узнать обстоятельства, дающие основания для возникновения подозрений о наличии шифрованной информации.

В теории обнаружения величину W называют отношением правдоподобия. Для его вычисления необходимо, как отмечалось выше, чтобы априори были известны обстоятельства происхождения подозрительного файла.

Таким образом, можно считать, что решения экспертизы всегда сопровождаются ошибками. Программно-аппаратные средства, которыми располагает экспертиза, могут также вырабатывать ошибочные посылки, связанные с естественным несовершенством названных средств, т. е. наличием методических ошибок, носящих случайный характер. Кроме того, анализируемый экспертизой подозрительный файл может содержать вирусы, которые оказывают непредсказуемое воздействие на работу программно-аппаратных средств экспертизы.

ЛИТЕРАТУРА

1 Асанович В.Я., Маньшин Г.Г. Информационная безопасность. Анализ и прогноз информационного воздействия. М.: Амалфея, 2016 г. – 204 с.

2 Блэк У. Интернет. Протоколы безопасности. СПб.: Питер, 2015 г. – 288 с.

3 Вьейра Р. SQL Server 2000. Программирование. Часть 1, 2. М.: Бином. Лаборатория знаний. 2004 г.

PROBABILITY CHARACTERISTICS OF DETECTION OF HIDDEN IMAGES.

Medvedev N.V.[54], Glinskaya E.V.[55]

The article describes the basics of the study files to be examined, containing an encrypted image. To protect the information itself developed a large number of cryptographic algorithms. However, these algorithms do not allow hiding the presence of encrypted information from an unauthorized user. Most of the information processes are related to solving the problem of choice. The same problem is solved when searching for the best in some sense image processing algorithms. The main algorithms of the transforming elements of the IC make decisions of the type: whether the signals are different or not, the image is distorted or not, etc. The task of decoding is formed relative to the image, causing suspicion among experts for the presence of a latent image.

Keywords: cryptography, encrypted information, expertise.

[54] Nikolay Medvedev, Ph.D., Associate Professor, Department of Information Security
[55] Glinskaya Elena Vyacheslavovna, Senior Lecturer of the Department "Information Security"

УДК 004.056.

Методика тестирование программного обеспечения при ограниченном доступе к исходным текстам

Миронов С.В.[56]

В докладе рассмотрены проблемные вопросы структурного анализа исходных текстов программ. Для случая отсутствия исходных текстов рассмотрены возможности использования методов тестирования по принципу «черного ящика». Представлен результаты экспериментов. Показано, что в ряде случаев тестирование по принципу «черного ящика» может иметь место.

Ключевые слова: тестирование, черный ящик, программные закладки

Введение

К основным мероприятиям по оценке степени безопасности программного обеспечения относят обязательную сертификацию по требованиям безопасности информации [9]. Однако возможности сертификации ограничены как временными рамками, так и нормативно-правовыми и конструкторскими требованиями. Кроме того, сертификация программного обеспечения по требованиям безопасности должна производиться на соответствие Руководящего документа 1999 г. создания, в котором используются, как показала практика, не эффективные методы выявления программных закладок[57]. Еще одним существенным требованием, накладываемым Руководящим документом, является наличие исходных кодов на исследуемый программный продукт. Это требование весьма критично для разработчиков, т.к. образуется потенциальный канал утечки интеллектуальной собственности [4, 11, 13, 15]. Это также объясняет, почему зарубежные производители редко проводят сертификацию своих продуктов в нашей стране [4-6, 10].

Существуют методы анализа программных продуктов, которые не требуют наличия исходных текстов программ (например, [1-3, 7, 12]), к таким методам относят методы тестирования программного обеспечения. Данные методы широко применяются за рубежом [14], а в нашей стране еще не получили широкого распространения. Возникает вопрос, могут ли методы и средства тестирования программ без исходных кодов повысить эффективность проведения сертификационных испытаний программного обеспечения, а также определить, какие изменения в нормативных документах должны быть приведены для внедрения методов тестирования программ без исходных кодов в рамки сертификационных испытаний [8].

Методический подход к тестированию без исходных текстов

В случае тестирования методом черного ящика, т.е. без исходного кода, эффективность применения поведенческого тестирования зависит от полноты составления тестов. Данный вид тестирования заключается в проверке исполняемых модулей программ на соответствие документам разработчика и выявление уязвимостей и некорректностей при написании кода. При проведении тестирования можно использовать также методы структурного тестирования. Это достигается, например, путем применения операции дизассемблирования и

[56] Миронов Сергей Владимирович, Минфин России, Москва, smironovs@yandex.ru

[57] Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» 1999 г.

декомпиляции и затем статического анализа. К сожалению, нет 100% вероятности корректного перевода машинного кода в языки программирования высокого уровня, и она напрямую зависит от объема кода программы.

К основным методам тестирования черного ящика [1, 2, 12] относят:

тестирование функциональности на соответствие эксплуатационным документам;

стрессовое и нагрузочное тестирование;

тестирование граничных значений;

тестирование производительности;

тестирование совместимости с другими средствами;

тестирование входных параметров или рандомизированное тестирование;

тестирование работы с окружением;

тестирование подсистем безопасности.

В табл. 1 представлен анализ эффективности различных методов

Таблица 1.

Уязвимость	Методы тестирования белого ящика	Методы тестирования черного ящика	Эффективность
Логический бомбы	Сигнатурный анализ	Дизассемблирование с последующим сигнатурным анализом	Методы тестирования белого ящика эффективнее методов черного ящика
Хулиганский код	Сигнатурный и экспертный анализ	Дизассемблирование с последующим сигнатурным анализом и функциональное тестирование	Методы тестирования белого ящика эффективнее тестирования
Ошибки, возникающие в случае использования редко используемых входных данных	Экспертный анализ	Тестирование граничных значений и рандомизированное тестирование	Методы тестирования черного ящика эффективнее методов белого ящика
Недекларированные входные параметры	Экспертный анализ	Тестирование граничных значений и рандомизированное тестирование	Методы тестирования черного ящика эффективнее методов белого ящика
Некорректности кодирования	Экспертный анализ	Функциональное тестирование и экспертный анализ дизассемблированного кода	Примерно одинаковые
Уязвимости подсистем безопасности	Экспертный анализ	Стрессовое и нагрузочное тестирование, тестирование на безопасность	Методы тестирования черного ящика эффективнее методов белого ящика
Скрытые каналы	Экспертный анализ	Тестирование работы с окружением,	Методы тестирования черного ящика

		тестирование на безопасность	эффективнее методов белого ящика
Ошибки при работе с памятью	Экспертный анализ	Стрессовое и нагрузочное тестирование	Методы тестирования черного ящика эффективнее методов белого ящика
Переполнение буфера	Сигнатурный и экспертный анализ	Стрессовое и нагрузочное тестирование, функциональное тестирование	Методы тестирования черного ящика эффективнее методов белого ящика
Ошибки, связанные с отказом в обслуживании	Экспертный анализ	Стрессовое и нагрузочное тестирование, тестирование производительности	Методы тестирования черного ящика эффективнее методов белого ящика
Несанкционированная передача данных	Сигнатурный и экспертный анализ	Тестирование функциональности и тестирование работы с окружением	Методы тестирования черного ящика эффективнее методов белого ящика

Из сравнительной таблицы видно, что потенциал у тестирования программного обеспечения без исходных текстов достаточен для выявления большинства уязвимостей и по эффективности не уступает тестированию с исходными кодами.

Анализ трудоемкости проведения испытаний

Для сравнения методов сертификации и тестирования была использована тестовая программа (клиент IRC-службы) [11].

В результате сравнения использовались следующие средства:

1) Средства проведения тестирования методом белого ящика: UCA, АИСТ, Parasoft C++Test.

2) Средства проведения тестирования методом черного ящика: IBM Rational Purify, IBM Rational Robot, IDA-Pro, ZxSniffer, специализированные скрипты для рандомизированного тестирования.

В рамках проведения тестирования у средств тестирования методами белого ящика хорошо себя показал только сигнатурный анализ. Сигнатурный анализ показал места потенциально возможных операций, однако непосредственное выявление уязвимостей проводился экспертным методом. Время, необходимое для просмотра всего кода равнялось 40 часов. Испытание по данному виду уязвимости заканчивалось, если выявлены все уязвимости, либо делался вывод об очень большом времени необходимом для выявления дальнейших уязвимостей.

В результате получены данные, представленные в табл. 2.

Таблица 2.

Уязвимости	Выявлено методами белого ящика	Выявлено методами черного ящика	Затраченное время выявления методами белого ящика	Затраченное время выявления методами черного ящика
Логические бомбы	5	2	40 часов	150 часов
Хулиганский код	4	2	30 часов	200 часов
Ошибки, возникающие в случае использования	2	2	20 часов	4 часа

редко используемых входных данных				
Недекларированные входные параметры	3	3	20 часов	10 часов
Некорректности кодирования	2	1	30 часов	100 часов
Уязвимости подсистем безопасности	3	3	40 часов	20 часов
Скрытые каналы	1	0	40 часов	Не выявлено за 200 часов
Ошибки при работе с памятью	3	2	40 часов	80 часов
Переполнение буфера	2	2	40 часов	80 часов
Ошибки, связанные с отказом в обслуживании	1	1	40 часов	80 часов
Несанкционированная передача данных	2	2	30 часов	60 часов
ИТОГО:	28	21		

По результатам сравнительного анализа можно сделать вывод, что на представленных программных уязвимостях оба метода тестирования показали себя на достаточно высоком уровне. Следовательно, можно использовать методы тестирования без исходных кодов для выявления программных закладок определенных классов.

Краткие выводы

Сложившееся противоречие между природой реальных уязвимостей программного кода и нормативно-методической базой испытаний по требованиям безопасности и желанием разработчиков не предоставлять исходные тексты требует решения. Необходимо внедрение в испытания большого количества методов тестирования без исходных текстов, обладающие большим потенциалом и не чувствительные к исходным текстам программ. Проведения независимого тестирования программ по требованиям безопасности увеличит уверенность покупателей в приобретаемых продуктах.

Накопленный опыт сертификационных испытаний на отсутствие недекларированных возможностей и программных закладок, а также независимого тестирования программных продуктов позволяет наметить пути совершенствования нормативной базы, основанной на применении методов тестирования программ без исходных текстов.

Список используемой литературы

1. Бейзер Б. Тестирование черного ящика. Технологии функционального тестирования программного обеспечения систем - СПб.: Питер, 2004.

2. Котляров В.П., Коликова Т.В. Основы тестирования программного обеспечения - М.: Интернет-Университет Информационных технологий, 2006 – 285.

3. Марков А.С., Миронов С.В., Цирлов В.Л. Выбор сетевого сканера для анализа защищенности сети // Byte Россия. 2005. № 6 (82). С. 67-70.

4. Марков А.С., Миронов С.В., Цирлов В.Л. Выявление уязвимостей в программном коде//Открытые системы, №12, 2005. С.64-69.

5. Марков А.С., Миронов С.В., Цирлов В.Л. Выявление уязвимостей программного обеспечения в процессе сертификации // Информационное противодействие угрозам терроризма. 2006. № 7. С. 177-186.

6. Марков А.С., Миронов С.В., Цирлов В.Л. Выявление уязвимостей программного обеспечения в процессе сертификации // Известия ЮФУ. Технические науки. 2006. № 7 (62). С. 82-87.

7. Марков А.С., Миронов С.В., Цирлов В.Л. Опыт тестирования сетевых сканеров уязвимостей // Информационное противодействие угрозам терроризма. 2005. № 5. С. 109-122.

8. Марков А.С., Миронов С.В., Цирлов В.Л. Разработка политики безопасности организации в свете новейшей нормативной базы//Защита информации. Конфидент, 2004. -№2. -С. 20-28.

9. Марков А.С., Шеремет И.А. Теоретические аспекты сертификации средств защиты информации//Оборонный комплекс -научно-техническому прогрессу России. 2015. № 4 (128). С. 7-15.

10. Марков А.С., Щербина С.А. Испытания и контроль программных ресурсов//Information Security, 2003. -№ 6 -С. 25.

11. Миронов С.В. Подход к структурному анализу исходных кодов программного обеспечения. В сборнике: Безопасные информационные технологии Сборник трудов Восьмой всероссийской научно-технической конференции. НУК «Информатика и системы управления». Под. ред. М.А.Басараба. 2017. С. 308-310.

12. Рибер Г., Малмквист К., Щербаков А. Многоуровневый подход к оценке безопасности программных средств//Вопросы кибербезопасности. -2014. -№ 1. -С. 36-39.

13. Скворцов М.А., Петренко С.А. Анализ методик поиска уязвимостей в исходном коде. // В сборнике: Безопасные информационные технологии Сборник трудов Восьмой всероссийской научно-технической конференции. НУК «Информатика и системы управления». Под. ред. М.А.Басараба. 2017. С. 401-405.

14. Петренко А.А., Петренко С.А. НИОКР агентства DARPA в области кибербезопасности // Вопросы кибербезопасности. 2015. № 4 (12). С. 2-22.

15. Харжевская А.В., Ломако А.Г., Петренко С.А. Представление программ инвариантами подобия для контроля искажения вычислений//Вопросы кибербезопасности. 2017. № 2 (20). С. 9-20.

Software testing in the absence of source code

Mironov S.V.

The report addresses the issues of structural analysis of the source code of programs. For the case of the absence of source texts, the possibilities of using black-box testing methods were considered. Presents the results of experiments. It is shown that in some cases, testing by the principle of "black box" can take place.

Keywords: testing, black box, software bookmarks

УДК 004.056

Использование бинарной инструментации кода в динамическом анализе программного обеспечения

Островский А.С.[58], Малахов М.В.[59]

В статье рассмотрен метод инструментации исполняемого кода программ, в качестве одного из методов динамического анализа, применяемого при анализе программного обеспечения на предмет наличия уязвимостей и в задачах обратной инженерии. Указана практическая целесообразность применения данного метода на современном этапе развития информационных технологий. Дана классификация типов инструментации кода с указанием их основных особенностей. Перечислены и кратко охарактеризованы наиболее известные бинарные инструментаторы. Сделан вывод о необходимости создания нового инструмента бинарной инструментации кода, выработаны основные требования к нему.

Ключевые слова: поиск уязвимостей, инструменты анализа кода, анализ исполняемого кода.

Введение

При решении ряда задач, связанных с обеспечением информационной безопасности автоматизированных систем, возникает необходимость разработки безопасного программного обеспечения (ПО). Внедряемый в настоящее время ГОСТ Р 56939 [1] регламентирует обязательность выполнения динамического анализа такого ПО.

Динамический анализ основан на многократном запуске исследуемого ПО на исполнение. Поиск дефектов (уязвимостей и некритических ошибок) при динамическом анализе производится путем генерации выборки различных наборов входных данных, близкой к полной, передачи их на вход исследуемой программы и анализа информации об обработке программой этих данных. Однако в связи с существенным ростом возможностей вычислительных систем наблюдается значительное увеличение размерности наборов входных данных. При этом сложность динамического анализа растет экспоненциально. Одним из методов, используемых для снижения размерности наборов входных данных при динамическом анализе ПО, является метод инструментации кода [2,3].

Инструментация кода

Инструментация кода представляет собой частичное изменение программы, при котором она (или её часть, которую необходимо исследовать) сохраняет свою функциональность, при этом производит дополнительные действия, целью которых является извлечение информации о состоянии программы в ходе её исполнения [4].

В области обеспечения информационной безопасности инструментация кода широко применяется для решения задач [5]:

трассировки вызовов;

построения графов потока управления и потока данных;

определения условий возникновения уязвимостей;

обнаружения неизвестных уязвимостей;

фаззинга;

обнаружения shell-кодов;

[58] Островский Александр Сергеевич, кандидат технических наук, МГТУ им Н.Э. Баумана, Москва, aleksandr_ostrovsky@mail.ru

[59] Малахов Михаил Валерьевич, МГТУ им Н.Э. Баумана, Москва, misha.malaxow@yandex.ru

модификации ПО (внесения исправлений безопасности);

реверс-инжиниринга.

Уязвимости ПО могут появляться в самых различных вычислительных системах, в связи с этим инструментация кода должна быть инвариантна к используемой архитектуре исследуемой системы.

Таким образом, в связи с внедрением ГОСТ Р 56939, регламентирующего обязательность применения процедуры динамического анализа при разработке безопасного ПО, возникает необходимость использования инструментатора, позволяющего снизить размерность наборов входных данных при динамическом анализе ПО для различных архитектур вычислительных систем.

Классификация инструментаторов кода

Рассмотрим классификацию существующих инструментаторов, применяемых в задачах анализа исходного и исполняемого кода.

Инструментация исходного кода выполняется на уровне конструкций языка программирования. Этот метод предоставляет возможность проанализировать граф потока управления программы, обеспечить полное покрытие кода программы. К недостаткам инструментации исходного кода относится то, что для работы инструментатора требуется исходный код. Это, например, не позволяет анализировать работу подключаемых скомпилированных библиотек [6]. Указанный факт в значительной мере снижает область применения инструментаторов исходного кода. В связи с этим в статье в дальнейшем будет рассматриваться инструментация исполняемого кода.

Бинарная инструментация (инструментация исполняемого кода) представляет собой изменение машинного кода программы. Выделяют два вида бинарной инструментации кода: статическую и динамическую. Статическая бинарная инструментация представляет собой изменение машинного кода программы до начала её выполнения. Динамическая инструментация производится непосредственно во время выполнения программы [7].

В настоящее время статическая инструментация используется в таких средствах анализа, как EXE, KLEE и SAGE [3].

EXE представляет собой инструмент для поиска ошибок в программах, автоматически генерирующий входные данные, на которых возникает ошибка. Средство KLEE является измененным вариантом EXE, использующим язык промежуточного представления LLVM. Средство SAGE фокусируется на построении как можно более полного покрытия кода, в отличие от предыдущих решений не требует исходный код исследуемой программы.

Динамическая инструментация используется в таких средствах анализа, как Flayer и Catchconv [3].

Инструмент Flayer определяет выполнимость условных операторов в зависимости от входных данных программы. Средство Catchconv схоже по функционалу с Flayer, но лишено проблемы невоспроизводимости ошибок, внутри себя дополнительно использует решатель STP.

Ниже приведено краткое описание популярных статических и динамических бинарных инструментаторов.

Статические бинарные инструментаторы

BIRD [8] – инструмент бинарного анализа и инструментации. BIRD предоставляет пользователю две основных возможности: дизассемблирование двоичного файла и работа с ним или вставка пользовательских инструкций сразу в бинарный файл в указанные места. Код инструментатора оформляется в виде

динамической библиотеки, которая вызывается из исследуемого файла с помощью замены инструкций. На основе системы BIRD был разработан инструмент, осуществляющий внедрение модуля защиты от несанкционированного изменения кода во время выполнения. Инструментатор работает только на машинах с архитектурой x86 под управлением Windows.

PEBIL [9] – программа для инструментации ELF-файлов, запускаемых на ОС Linux. PEBIL внедряет вызовы инструментирующего кода в заранее указанные точки приложения. Имеет в себе инструменты для внедрения кода, позволяющего считать количество операций с плавающей запятой, количество обращений к памяти и моделировать число кэш-попаданий при работе исследуемого приложения.

Динамические бинарные инструментаторы

PIN [10] – фреймворк, позволяющий создавать инструменты для динамического анализа программ, разработан компанией Intel. PIN имеет возможности передавать в качестве входных параметров инструментирующему коду текущее содержимое регистров. Также имеет ограниченный доступ к символьной и отладочной информации. На сегодняшний день применяется не только для анализа компьютерной архитектуры, но и в качестве инструмента для тестирования свойств безопасности, эмуляции и анализа параллельных программ. Компания Intel встроила PIN во многие свои инструменты. Работает только на архитектурах IA32, IA64.

Valgrind [11] – среда для создания инструментов динамического анализа. Существующие инструменты на основе Valgrind могут автоматически определять множество ошибок управления памятью и потоками. В настоящий момент дистрибутив Valgrind включает в себя такие инструменты, как: детектор ошибок памяти; анализатор выполнения кода, собирающий данные об обращения в кэш и точках, где процессор неправильно предсказал ветвление; анализатор вызовов функций; анализатор выделения памяти в различных частях программы; анализатор кода на наличие различных ошибок синхронизации в многопоточном коде. Работает только на архитектурах IA32, IA64 и ARM.

Выводы

На данный момент существуют динамические и статические бинарные инструментаторы для архитектур IA-32, IA-64 и ARM, обладающие достаточно развитым и разнообразным функционалом.

С развитием интернета вещей возникает потребность исследовать другие архитектуры, при работе с которыми также возникает задача анализа бинарного файла с априорно неизвестным разбиением на секции кода и данных. Целью дальнейших исследований будет разработка статического бинарного инструментатора, способного при небольшой настройке инструментировать машинный код различных архитектур. Данный инструментатор должен быть интегрирован со средствами анализа машинного кода класса IDA Pro или Radare2.

Литература

1. Барабанов А.В., Марков А.С., Цирлов В.Л. 28 магических мер разработки безопасного программного обеспечения//Вопросы кибербезопасности. 2015. № 5 (13). С. 2-10.

2. Аветисян А.И., Белеванцев А.А., Чукляев И.И. Технологии статического и динамического анализа уязвимостей программного обеспечения // Вопросы кибербезопасности № 3(4), 2014, с. 20-28.

3. Вартанов С.П., Герасимов А.Ю. Динамический анализ программ с целью поиска ошибок и уязвимостей при помощи целенаправленной генерации входных данных // Труды Института

системного программирования РАН, том 26, вып. 1, 2014, с. 375-394. DOI: 10.15514/ISPRAS-2014-26(1)-15.

4. Вартанов С.П., Герасимов А.Ю. Применение динамического анализа для поиска дефектов в программах на языке Java // Труды Института системного программирования РАН, том 25, 2013, с. 9-28. DOI: 10.15514/ISPRAS-2013-25-1.

5. Diskin G. Binary instrumentation for security professionals // Paper presented at the conference Black Hat USA, Las Vegas, 2011.

6. Nethercote N. Dynamic binary analysis and instrumentation. // University of Cambridge, 2004, pp 1-170.

7. Ермаков М.К., Вартанов С.П. Применение статической бинарной инструментации с целью проведения динамического анализа программ для платформы ARM // Труды Института системного программирования РАН, том 27, вып. 1, 2015, с. 5-24. DOI: 10.15514/ISPRAS-2015-27(1)-1.

8. Nanda S., Li W., Lam L., Chiueh T. BIRD: Binary Interpretation using Runtime Disassembly // International Symposium on Code Generation and Optimization, 2006, pp 1-13. DOI: 10.1109/CGO.2006.6.

9. Laurenzano M., Tikir M., Carrington L., Snavely A. PEBIL: Efficient static binary instrumentation for Linux // IEEE International Symposium on Performance Analysis of Systems & Software (ISPASS), 2010, pp. 175-183. DOI:10.1109/ISPASS.2010.5452024.

10. Pin. Pin – a Dynamic Binary Instrumentation Tool // URL : https://software.intel.com/en-us/articles/pin-a-dynamic-binary-instrumentation-tool.

11. Valgrind. Instrumentation Framework for Building Dynamic Analysis Tools // URL : http://valgrind.org.

Using binary instrumentation of code in dynamic analysis of software

Ostrovsky A.S.[60], Malahov M.V.[61]

The article considers the method of instrumentation of the executable program code, as one of the methods of dynamic analysis used in the analysis of software for finding vulnerabilities and in reverse engineering tasks. The practical expediency of using the method at the present stage of information technologies development is revealed. A classification of the types of code instrumentation with an indication of their main features is resulted in this article. The most famous binary code instrumentation tools are listed and briefly characterized. The conclusion is that there is a need to create a new binary instrumentation tool for which the basic requirements were worked out.

Keywords: vulnerabilities scan, code analysis tools, analysis of executable code.

[60] Ostrovsky Alexander Sergeevich, candidate of technical sciences, Moscow State Technical University, aleksandr_ostrovsky@mail.ru

[61] Malahov Mihail Valerievich, Moscow State Technical University, misha.malaxow@yandex.ru

УДК 65.01

Анализ нормативной базы в области разработки безопасного программного обеспечения

Райкова Н.О.[62]

В данной статье представлено описание концепции системы менеджмента разработки безопасного программного обеспечения, основанная на требованиях международных и национальных стандартов в области информационной безопасности. Проведена оценка нормативной базы в области разработки безопасного программного обеспечения.

Ключевые слова: система менеджмента разработки безопасного программного обеспечения, безопасное программное обеспечение, уязвимость программного обеспечения.

Введение

С увеличением сложности информационных систем, возросли риски информационной безопасности, связанные с наличием уязвимостей программного обеспечения (ПО), установленного в информационных системах. [1] Долгое время в России отсутствовала нормативная база, регулирующая данную сферу деятельности. Однако существовал ряд международных стандартов и методологий, описывающих технические меры и механизмы разработки безопасного программного обеспечения, например, ISO 15408, ISO 27034-1, ISO TR 24772, Microsoft Security Development Life Cycle, Cisco Security Development Life Cycle, OpenSAMM, OWASP CLASP. Основным недостатком данных стандартов является отсутствие четкой структуры проведения оценки соответствия процессов разработки ПО требованиям к разработки безопасного программного обеспечения. Стоит отметить, что ранее данный недостаток предлагалось решать с помощью международного стандарта ISO 15408, используемого в рамках сертификации программного обеспечения. Но использование положений этого документа только во время разработки и дальнейшей оценки соответствия безопасности программного обеспечения недостаточно, так как отсутствует комплексное решение по элементам управления для разработки безопасного программного обеспечения и общей ориентированностью стандарта на программное обеспечение с функциями безопасности. Таким образом до недавнего времени предъявлялись требования только к оценке программного обеспечения, упуская при этом оценку процесса разработки [2].

Национальный стандарт ГОСТ Р 56939-2016

В 2016 году был утвержден национальный стандарт ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» (далее ГОСТ), который и определяет содержание и порядок выполнения работ по созданию программного обеспечения с использованием методов защищенного программирования. ГОСТ содержит базовый набор из 28 требований (рис. 1), которые необходимо реализовать на соответствующих этапах жизненного цикла программного обеспечения. В нем рассматриваются общие и технические меры к следующим процессам жизненного цикла программного обеспечения (далее ПО).

[62] Райкова Наталья Олеговна, аспирант кафедры ИУ8 МГТУ им. Н.Э. Баумана, Москва,
E-mail: natalya_raykova@mail.ru

Рис. 1. Структура представления ГОСТ

Однако все также остается не описанной сама система менеджмента разработки безопасного программного обеспечения (далее СМРБПО). В данной статье представим возможную концепцию СМРБПО, основываясь на требования международных и национальных стандартам в области информационной безопасности.

Концептуальные основы стандарта по безопасной разработке

1. Область применения

СМРБПО предназначена для организаций, которые занимаются разработкой ПО, независимо от их типа и масштаба.

2. Цели

Построение СМРБПО направлено на выбор соответствующих мер управления безопасностью процесса разработки ПО, предназначенных для предотвращения появлений и устранения уязвимостей ПО.

3. Самостоятельная единица или составная часть

На первый взгляд довольно хлопотно для организаций иметь сразу несколько систем менеджмента при организации своей деятельности. В то же время СМРБПО имеет множество точек соприкосновения с другими системами менеджмента – с системой менеджмента качества (СМК), с системой менеджмента информационной безопасности (СМИБ). [3, 4] Поэтому можно использовать СМРБПО возможно использовать не только отдельно, но и в качестве подсистемы СМИБ.

4. Процессный подход

СМРБПО должна использовать одинаковый подход для интеграции с другими системами менеджмента (СМК и СМИБ). Поэтому предполагается использование процессного подхода (рис. 2). [5]

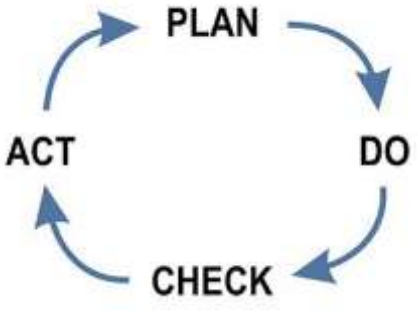


Рис.2. Цикл Деминга

5. Документация

Должна определять иерархию уровней документации в соответствии с ГОСТ Р ИСО/МЭК 27001, начиная от политики информационной безопасности до описания определенных процедур. [6] В соответствии с ГОСТ Р 56939-2016 в организации должно быть разработано руководство по разработке безопасного ПО.

6. Руководство и управление

Для любой системы менеджмента приверженность руководства является ключевым моментом. Поэтому должны быть четко определены задачи руководства по отношению к СМРБПО, например, обеспечение необходимыми ресурсами, контроль достижения запланированных целей, необходимое распределение ответственности и так далее. [7]

7. Повышение осведомленности

Должна быть определена периодичность обучения сотрудников организации с целью повышения осведомленности в области разработки безопасного ПО.

8. Планирование

СМРБПО должна определять требования безопасности (например, обеспечение конфиденциальности, реализация разграничения доступа, обеспечение идентификации и аутентификации, обеспечение регистрации событий, контроль точности и полноты и правильности данных, поступающих в программу) и принципы проектирования к разрабатываемому программному обеспечению (рис. 3) [8].

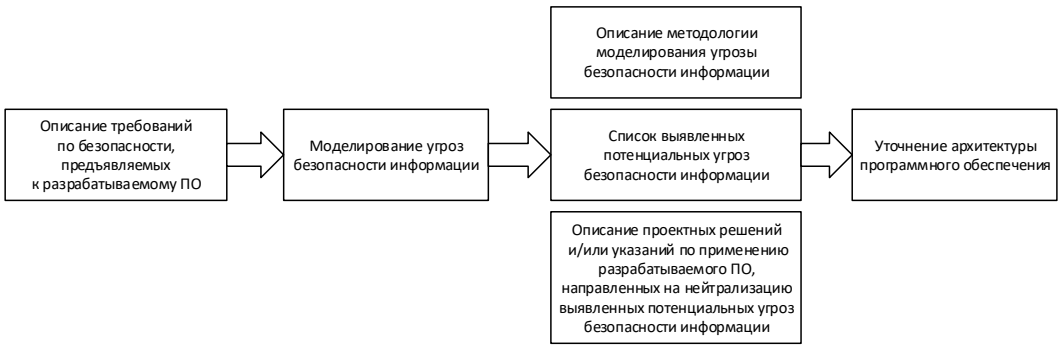


Рис. 2. Анализ требований и проектирование ПО

9. Реализация

СМРБПО должна определять к каждому процессу жизненного цикла ПО, установленных ГОСТ Р ИСО/МЭК 12207, меры по разработке безопасного ПО,

использую как базовый набор мер из ГОСТ Р 56939-2016 (табл.1), так и иные собственные меры. [9]

Таблица 1.

Соответствие процессов жизненного цикла ПО мерам по разработке безопасного ПО

Процесс жизненного цикла ПО	**Меры из ГОСТ Р 56939-2016**
Процесс анализа требований к ПО	П.5.1
Процесс проектирования архитектуры ПО	П.5.2.1
Процессы конструирования и комплексирования ПО	П. 5.3.1
Процесс квалификационного тестирования ПО	П. 5.4.1
Процессы инсталляции ПО и поддержки приемки ПО	П.5.5.1
Процесс решения проблем в ПО	П.5.6.1
Процесс менеджмента документации и конфигурации ПО	П.5.7.1
Процесс менеджмента инфраструктуры	П.5.8.1
Процесс менеджмента людских ресурсов	П.5.9

10. Оценка эффективности системы менеджмента

В СМРБПО необходимо определить способы оценки эффективности используемых мер. Возможны два подхода к способам оценки. В первом, организация самостоятельно должна определить способы оценки и режим мониторинга процессов в целях доказательства эффективности системы менеджмента. Во втором, требования к способам оценки эффективности мер должны быть определены и закреплены в стандарте.

11. Аудит

Должна быть определена периодичность и полнота внутреннего аудита СМРБПО. Аудит не должен ограничиваться проверкой документации.

12. Сертификация

После доработки законодательной базы, должна проводиться сертификация СМРБПО в целях повышения доверия к организациям, разрабатывающим ПО, снижения количества уязвимостей используемого ПО. [10]

В первую очередь обеспечение безопасности программного обеспечения необходимо для объектов критических информационных систем, государственных структур, предприятий оборонно-промышленно комплекса. Несмотря на строгие требования по обеспечению защиты таких систем, остаются бреши в виде уязвимостей и недекларированных возможностей используемого ПО. На данный момент угрозы, связанные с внутренними нарушителями в лице разработчиков операционных систем и ПО, рассматриваются как неактуальные, так как организации имеют репутационные риски. Ввиду наращивания рядом зарубежных стран возможностей информационно-технического воздействия на информационную структуру в военных целях и плохой геополитической обстановкой в том числе в сфере ИТ, вышеупомянутые угрозы необходимо признать актуальными и принять соответствующие меры.

Вывод

СМРБПО предназначена для организаций, занимающихся разработкой программного обеспечения. Ознакомившись с материалами данной статьи можно выделить следующие преимущества использования СМРБПО:

- обеспечивает прозрачность управления;

- благодаря использованию мер разработки безопасного ПО организация может существенно сократить затраты на подготовку ПО к процедуре оценки по «Общим критериям»;

- внедрение СМРБПО обеспечит уверенность клиентов в безопасности поставляемого ПО;

- позволит оптимизировать используемые ресурсы.

Литература

1. Барабанов А.В., Марков А.С., Фадин А.А., Цирлов В.Л. Статистика выявления уязвимостей программного обеспечения при проведении сертификационных испытаний // Вопросы кибербезопасности. 2017. № 2(20). С. 2-8.
2. Барабанов А.В., Марков А.С., Цирлов В.Л. 28 Магических мер разработки безопасного программного обеспечения // Вопросы кибербезопасности. 2015. № 5(13). С. 2-10.
3. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий /Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.
4. Райкова Н.О., Шахалов И.Ю. К вопросу об интегрировании систем менеджмента качества и информационной безопасности // Правовая информатика. 2014. № 2. С. 20-25.
5. Райкова Н.О., Шахалов И.Ю. Новейшие требования к системам менеджмента информационной безопасности // Молодежный научно-технический вестник # 04, апрель 2015.
6. Дорофеев А.В., Марков А.С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. № 1(2). С. 67-73.
7. Дорофеев А.В. Менеджмент информационной безопасности: переход на ISO 27001:2013 // Вопросы кибербезопасности. 2014. № 3(4). С. 69-73.
8. Барабанов А.В., Марков А.С., Цирлов В.Л. Методический аппарат анализа и синтеза комплекса мер разработки безопасного программного обеспечения//Программные продукты и системы. 2015. № 4 (112). С. 166-175.
9. Barabanov A., Markov A., Fadin A., Tsirlov V., Shakhalov I. Synthesis of Secure Software Development Controls. In Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08-10, 2015). SIN ‘15. ACM New York, NY, USA, 2015, pp. 93-97. DOI: 10.1145/2799979.2799998.
10. Barabanov A.V., Markov A.S., Tsirlov V.L. Methodological framework for analysis and synthesis of a set of secure software development controls // Journal of Theoretical and Applied Information Technology. 2016. V. 88. №1. P. 77-88.

Рецензент: Шахалов И.Ю., доцент кафедры ИУ8 МГТУ им. Н.Э. Баумана, is@cnpo.ru

Security Software Development Management System Conception

Raykova N.O.[63]

This article introduces conception description of secure software development management system. It based on the requirements of international and national standards in the field of information security. We evaluated the regulatory framework for the development of secure software.

Keywords: secure software development management system, secure software, software vulnerability.

[63] Raykova Natalya Olegovna, Information Security Department, BMSTU, Moscow,
e-mail: natalya_raykova@mail.ru

УДК 004.056

Актуальные вопросы определения местоположения мобильного устройства по анализу энергопотребления с помощью машинного обучения

Рауткин В.Ю.[64]

Пользователи мобильных устройств могут воздерживаться от предоставления случайным приложениям отслеживать каждое их движение с помощью GPS. Но известно, что многие датчики в современных мобильных устройствах позволяют раскрывать различную конфиденциальную информацию. В этой статье мы рассмотрим как может быть раскрыта информация о вашем местонахождении каждым приложением на вашем устройстве через другую, маловероятную утечку данных: энергопотребление телефона. Так как доступ к данным энергопотребления доступен любому приложению без разрешения пользователя - это создаёт серьезную угрозу конфиденциальности.

Ключевые слова: мобильный шпионаж, отслеживание местоположения, анализ энергопотребления, машинное обучение

Введение

Исследователи из Стэнфордского университета и израильской исследовательской группы Rafael создали технику, которую они называют PowerSpy, которая, по их словам, может собирать информацию о геолокации телефона, просто отслеживая его потребление энергии с течением времени. Эти данные, в отличие от GPS или отслеживания местоположения Wi-Fi, свободно доступны для любого установленного приложения без необходимости запрашивать разрешение пользователя [1-4]. Это представляет собой новый метод скрытного определения движений пользователя с точностью до 90%, хотя на данный момент этот метод действительно работает только при попытке различить определенное количество предварительно измеренных маршрутов [5-9].

Обзор тематики

Злоумышленники могут обманным путем загрузить определенное приложение, использующее технологию PowerSpy, или же менее опасные производители приложений смогут использовать эту технологию для отслеживания местоположения в рекламных целях. Приложению достаточно иметь выход в интернет для отправки данных на сторонний сервер, который будет обрабатывать входящие данные и формировать маршруты для отслеживания в режиме реального времени, так же сохраняя маски энергопотребления на различных маршрутах. PowerSpy использует тот факт, что сотовая связь телефона расходует больше энергии для подключения к ближайшей сотовой вышке, чем дальше он от этой вышки находится, или когда препятствия, такие как здания или горы, блокируют его сигнал. Эта корреляция между использованием батареи и такими переменными, как условия окружающей среды и расстояние между вышками сотовой связи, достаточно сильна, чтобы можно было отфильтровать мгновенные потери энергии, такие как телефонный разговор или использование другого энергоемкого приложения.

[64] Рауткин Владимир Юрьевич, студент 5-го курса кафедры ИУ8 МГТУ им. Н.Э. Баумана, г.Москва, vova.raut@bk.ru

Один из приемов машинного обучения, который исследователи использовали для обнаружения и фильтрации шума - это фокус на долгосрочные тенденции в потреблении энергии телефоном, а не на последние несколько секунд или минут. Достаточно длительное измерение энергопотребления позволяет алгоритму обучения фильтровать шум, и как следствие, измерение совокупного энергопотребления телефона с течением времени полностью раскрывает местоположение и движение телефона.

Тем не менее, PowerSpy имеет главное ограничение: для достоверного определения местоположения устройства заранее требуется карта масок энергопотребления для различных маршрутов . Это означает, что невозможно определить новый маршрут без наличия масок энергопотребления на данном пути, чтобы сделать какие-либо выводы о местоположении. Стэнфордские и израильские исследователи собирали данные о энергозатратах с телефонов, когда они проезжали по Калифорнийскому заливу и израильскому городу Хайфа. Затем они сравнили свой набор данных с энергопотреблением телефона цели, поскольку он неоднократно путешествовал по одному из этих маршрутов. Они обнаружили, что среди семи возможных маршрутов они могут определить правильный с 90-процентной точностью.

Если вы совершите одну и ту же поездку пару раз, вы увидите очень четкий профиль сигнала и профиль мощности. Этих сходств достаточно для того, чтобы распознать среди нескольких возможных маршрутов, по которым вы выбираете тот или иной маршрут, который прошла цель. Группа исследователей надеется улучшить свой анализ, чтобы применить тот же уровень точности для отслеживания телефонов по множеству других возможных путей и с различными телефонами. Исследователи также работают над тем, чтобы более точно определить, где на известном маршруте находится телефон в любой момент времени. В настоящее время точность этого измерения варьируется от нескольких метров до сотен метров в зависимости от того, как долго телефон путешествовал.

Исследователи пытались определить местонахождение телефонов, даже когда они путешествуют по маршрутам, профиль которых никогда раньше не был сохранен полностью. Это достигается путем объединения измерений небольших участков трасс, профили мощности которых уже были предварительно измерены. Для телефона с несколькими приложениями создающими дпополнительный шум, исследователи смогли определить точный путь устройства примерно в двух случаях из трех. Для телефонов с десятком дополнительных приложений, которые непредсказуемо потребляют энергию и добавляют шум к измерениям, они смогли определять часть пути примерно в 60 процентах случаев, а точный путь - только в 20 процентах случаев. Даже с его относительной неточностью и необходимостью более ранних измерений энергопотребления на возможных маршрутах, PowerSpy представляет серьезную проблему конфиденциальности.

Вывод

Это не первый случай, когда исследователи используют различные компоненты телефона для определения конфиденциальной информации пользователя. В прошлом году та же группа исследователей, которую возглавлял известный криптограф Дэн Бонех, обнаружила, что они могут использовать гироскопы в телефоне как микрофоны. Этот трюк с «гирофоном» был способен уловить цифры, произносимые вслух в телефон, или даже определить пол говорящего. Всякий раз, когда пользователь предоставляет какому-либо приложению доступ к датчикам на устройстве, он открывает потенциальные пути

компроментации информации злоумышленником. PowerSpy является еще одним напоминанием об опасности предоставления ненадежным приложениям доступа к датчикам, которые собирают больше информации, чем предполагалось. Android и IOS оставляет данные о потреблении энергии доступными для всех приложений с целью отладки. Но это означает, что эти данные легко могут быть ограничены разработчиками, что исключило бы их шансы стать закулисным методом определения местоположения пользователя.

Литература

1. Мошков А.Н. Новые информационные угрозы требуют идти в ногу со временем // Вопросы кибербезопасности. 2014. № 3 (4). С.2-6.
2. Шеремет И.А. Противодействие информационным и кибернетическим угрозам // Вестник академии военных наук. 2016. № 2 (55). С. 29-34.
3. Баранов А.П. Актуальные проблемы в сфере обеспечения информационной безопасности программного обеспечения // Вопросы кибербезопасности. 2015. № 1 (9). С. 2-5.
4. Petrenko S. Cyber Security Innovation for the Digital Economy a Case Study of the Russian Federation. - River Publishers, 2018. 458 p.
5. Andy Greenberg PowerSpy: Location Tracking using Mobile Device Power Analysis // 24th USENIX Security Symposium. 2015. P. 785–800
6. Yan Michalevsky, Gabi Nakibly Gyrophone: Recognizing Speech From Gyroscope Signals // Black Hat 2014
7. Bojinov, H., Michalevsky, Y., Nakibly, G., Boneh, D. Mobile device identification via sensor fingerprinting. arXiv preprint arXiv:1408.1416 (2014).
8. Carrol, A., Heiser, G. An analysis of power consumption in a smartphone. In USENIX Annual Technical Conference (2010).
9. Рауткин В.Ю. Обзор способов достоверной идентификации сетевых устройств // Вопросы кибербезопасности. 2013. № 3 (3). С. 54-60. URL: https://elibrary.ru/item.asp?id=22536189.

Рецензент: Шахалов И.Ю., доцент кафедры ИУ8 МГТУ им. Н.Э. Баумана, is@cnpo.ru

Locating a mobile device for analyzing power consumption using machine learning

Rautkiv V.U.[65]

Mobile users may refrain from providing random applications with their every movement using GPS. But it is known that many sensors in modern mobile devices allow you to disclose confidential information. In this article we will look at how information about your location can be disclosed to each application on your device through another, unlikely data leak: the power consumption of the phone. Since access to energy data is available to any application without user permission, this creates a serious privacy risk.

Keywords: mobile espionage, location tracking, power analysis, machine learning

[65] Vladimir Rautkin, 4-th year student IU-8, BMSTU, Moscow, vova.raut@bk.ru

УДК 004.93

Определение синтезированных биометрических образов

Рычков А.С. [66]

Аннотация. Работа посвящена способу определения искусственных биометрических образов отпечатков пальцев. В результате были рассмотрены следующие вопросы: способ синтеза искусственных биометрических образов отпечатков пальцев с помощью программы SFinGe; представлена блок–схема алгоритма распознания, его описание, а также описан способ адаптивной фильтрации в формульном виде. Представлены результаты применения алгоритма на естественных и синтезированных биометрических образов. Данные результаты показывают, что существует способ отличить синтезированный отпечаток пальца, от естественного отпечатка пальца при помощи рассмотрения шума на цифровом изображении.

Ключевые слова: отпечаток пальца, цифровое изображение, метод генерации отпечатков пальцев, гистограмма, фильтрация.

Введение

На сегодняшний день уже возможно с большой правдоподобностью создавать искусственные биометрические данные (данные с выходов первичных измерительных преобразователей физических величин, совокупность которых образует биометрический образ конкретного человека), что позволило находить новые способы для подделки, скрытия и искажения биометрических данных.

Существуют разнообразные алгоритмы, стандарты и готовые программные решения для синтеза биометрических данных. Среди них можно выделить ГОСТ 52633.2-2010 и программу SFinGe. Данная программа была создана для синтезирования большой базы данных выборок, чтобы тестировать алгоритмы распознавания. В ГОСТ 52633.2-2010 описаны требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации.

SFinGe

SFinGe (Synthetic Fingerprint Generator) [1] - программа для генерации синтезированных отпечатков пальцев, реализованное в Университете Болоньи. База данных отпечатков пальцев, созданная из разных версиях SFinGe, была одной из четырех баз данных FVC (Fingerprint Verification Contest) [2]. В каждом году (2000, 2002, 2004 и 2006 гг.) участники имели аналогичные результаты в синтетической базе данных и реальных базах данных отпечатков пальцев. Это означает, что SFinGe имеет межклассовые и внутриклассовые вариации синтетического отпечатка пальца, очень похожие на реальные [1].

Процесс формирования отпечатка пальца показан на рисунке 1. Верхняя часть, то есть часть, которая заканчивается созданным мастер-отпечатка, описана в разделе «Способы создания синтетических отпечатков пальцев». Для более реального вида отпечатков пальцев применяются некоторые методы моделирования повреждений. Они находятся в нижней части рисунка 1.

Первым шагом является выбор области контакта. Для имитации различных мест размещения пальца в области датчика производится случайный перевод рисунка гребня. Это делается без изменения глобальной формы и положения отпечатка пальца.

Вторым шагом является изменения в толщине гребня. Толщина гребня изменена для имитации различной влажности кожи и давления пальца. Влажная кожа и более высокое давление вызывают появление более толстого хребтов, и в этом случае используется

[66] Рычков Алексей Сергеевич, магистрант, МГТУ им. Н.Э. Баумана, Москва, rychkov.alexey.s@gmail.com

оператор эрозии. Сухая кожа и низкое давление делают хребты более тонкими, поэтому в этом случае необходим оператор растяжения. Случайно выбранная величина влажности и давления определяет какой из морфологических операторов будет использоваться.

Третий шаг — это искажение отпечатка пальца. На этом этапе имитируется деформация кожи в зависимости от расположения пальца на датчике. Пластичность кожи (сжатие или растяжение) и другое усилия, приложенные к каждой части пальца, создает нелинейное искажение. Для этого искажения используется интерполяционный многочлен Лагранжа.

Четвертый шаг - шумоподавление и рендеринг. На этом этапе моделируются многие малые факторы. К сожалению, эти небольшие факторы больше всего повреждают отпечатки пальцев. К ним относятся неравномерность гребней, неравномерное давление пальца, разный контакт гребней с датчиком, наличие небольших поры и другие шумы. Шум генерируется в четыре этапа. Во-первых, впадины (или белые пиксели) сохраняются отдельно. Во-вторых, добавляется шум в виде различных пятен. В-третьих, всё изображение сглаживается. Наконец, впадины, сохраненные на первом этапе, возвращаются обратно на изображение (чтобы предотвратить чрезмерное сглаживание на третьем шаге).

Пятый шаг - глобальный перевод или чередование. Этот шаг имитирует не полностью установленный палец на датчике. Поэтому он слегка переводит и / или поворачивает изображение целиком.

Последний шаг - генерация реалистического фона. Фон генерируется случайным образом из набора фоновых изображений и математического метода, основанного на теореме Карунена – Лоэва, который будет создавать новые фоны из находящихся в наборе. В конце этого этапа создается отпечаток пальца. Для генерации баз данных имеется несколько оттисков от одного мастер-отпечатка [2, 3, 4, 5].

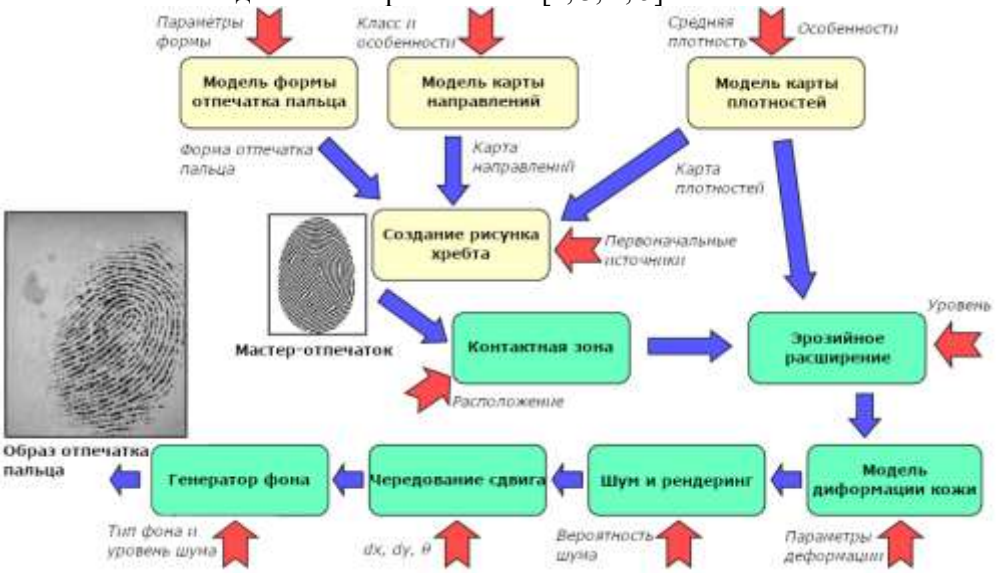


Рисунок 1. Процесс формирования отпечатка пальца SFinGe [4]

Пример алгоритма определения синтезированных отпечатков пальцев

Пример алгоритма для определения синтезированного отпечатка пальца и результаты его применения [6].

В качестве примера возьмем образ, синтезированный в программе SFinGe (см. рис. 2).

Рис. 2. Синтезированный зашумленный отпечаток

Выполним следующие шаги для определения синтезированного отпечатка:

1. Получаем полутоновое изображение.

В качестве исходного изображения возьмем рисунок 2 (уже полутоновое).

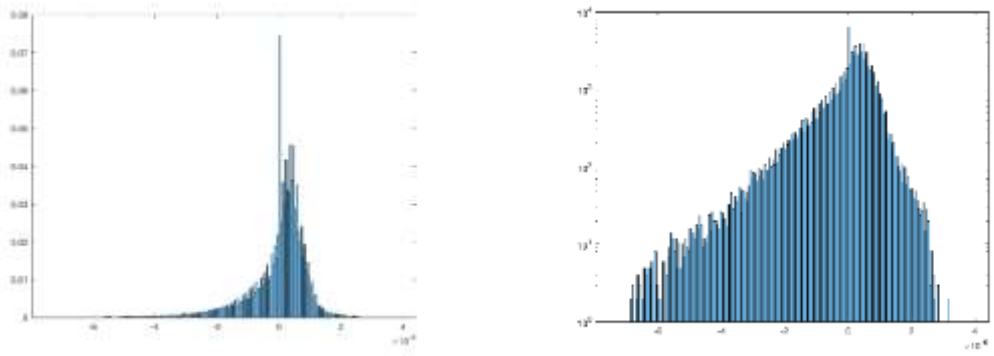
2. Фильтрация.

Так как на изображении присутствует несколько видов шумов необходимо провести несколько фильтраций или адаптивную фильтрацию [7].

3. Получение гистограммы шумов.

Для этого вычтем из полутонового изображения результаты фильтрации. Так как отфильтровать идеально не получится, то на изображении шумов будет не только шум.

Для пояснения ниже приведена гистограмма шума. Если изначальное изображение биометрического образа близко к идеалу, то на гистограмме мы увидим только максимум в нуле. Но так как в реальности разные шумы накладываются друг на друга (при создании синтезированного отпечатка пальца шумы то же накладываются друг на друга), останется фон на гистограмме (см. рисунок 3).



а б

Рис. 3. гистограмма шума (а); гистограмма шума в логарифмическом масштабе (б)

4. Анализ фона на гистограмме.

Теперь нужно оценить величину фона на гистограмме. Ошибки величины и формы фона складывается из неправильного выбора фильтров, не правильно выбранных коэффициентов фильтров, плохого качества исходного изображения и т.д. Вследствие чего можно говорить о достоверности отпечатка пальца только с некой долей вероятности.

Формульное представление алгоритма

Необходимо определить является ли изображение синтезированным. Для этого будем рассматривать шум на изображении, сравнивая его с шумом, возникающим на естественных и синтезированных отпечатках пальцев.

Любое цифровое изображение представляет собой набор пикселей с определенной интенсивностью на каждом.

$$I(x,y)=\begin{bmatrix} I(0,0) & I(0,1) & \cdots & I(0,W-1) \\ I(1,0) & I(1,1) & \dots & I(1,W-1) \\ \vdots & \vdots & & \vdots \\ I(H-1,0) & I(H-1,1) & \dots & I(H-1,W-1) \end{bmatrix} \quad (1)$$

где W – ширина изображения; H – высота изображения; $x \in [0,W]$, $y \in [0,H]$ – пиксели.

Описать зашумленный естественный образ отпечатка пальца можно следующим образом:

$$I'_n(x,y) = I_n(x,y) + N_n(x,y), \quad (2)$$

где $N_n(x,y)$ – вносимые шумы.

Для синтезированных образов отпечатков пальцев формула будет выглядеть следующим образом:

$$I'_s(x,y) = I_s(x,y) + N_s(x,y), \quad (3)$$

где $N_s(x,y)$ – вносимые шумы.

Для определения является ли образ синтезированным или естественным есть несколько способом.

Рассмотрение $I_s(x,y)$ и провести анализ изображения на основе известных алгоритмов синтезирования отпечатков.

Так как природа добавленного шума к изображению имеет разный источник в синтезированных и искусственных образах, то можно исследовать вносимые шумы $N_s(x,y)$.

Далее будет рассмотрен второй вариант, а именно анализ вносимого шума на цифровом изображении.

Для этого возьмем следующие исходные данные, цифровое изображение (не известно естественное или синтезированное).

$$I'(x,y) = I(x,y) + N(x,y) \quad (4)$$

Необходимо избавиться от $N(x,y)$, для этого необходимо отфильтровать изображение. Используем адаптивную фильтрацию [8].

На фильтр одновременно подаётся входные сигналы $I'(x,y)$ и $n(x,y)$. $I(x,y)$ не коррелирует с $N(x,y)$. Сигнал $n(x,y)$ является шумом коррелированный с $N(x,y)$, который нужен для формирования оценки сигнала $\hat{N}(x,y)$. Полезный сигнал оценивается следующим образом:

$$\hat{I}(x,y) = I'(x,y) - \hat{N}(x,y) = I(x,y) + N(x,y) - \hat{N}(x,y) \quad (5)$$

Возводим в квадрат:

$$\hat{I}^2(x,y) = I^2(x,y) + \left(N(x,y) - \hat{N}^2(x,y)\right) + 2I(x,y)\left(N(x,y) - \hat{N}(x,y)\right) \quad (6)$$

Вычисляем математическое ожидание:

$$M\left[\hat{I}^2(x,y)\right] = \\ = M\left[I^2(x,y)\right] + M\left[\left(N(x,y) - \hat{N}^2(x,y)\right)\right] + 2M\left[I(x,y)\left(N(x,y) - \hat{N}(x,y)\right)\right] \quad (7)$$

Последнее слагаемое в выражении равно нулю, так как сигнал $I(x,y)$ не коррелирует с сигналом $N(x,y)$ и $\hat{N}(x,y)$.

$M\left[I^2(x,y)\right] = W\left(I(x,y)\right)$ – мощность сигнала $I(x,y)$.

$M\left[\hat{I}^2(x,y)\right] = W\left(\hat{I}(x,y)\right)$ – оценка мощности сигнала $I(x,y)$ и общая выходная мощность.

$M\left[N(x,y) - \hat{N}^2(x,y)\right] = W(\xi_N)$ – остаточная мощность шума, который содержится в выходном сигнале.

При настройке адаптивного фильтра к оптимальному положению минимизируется мощность остаточного шума, а, следовательно, и мощность выходного сигнала:

$$\min W\left(\hat{I}(x,y)\right) = W\left(I(x,y)\right) + \min W(\xi_N) \quad (8)$$

На мощность полезного сигнала настройка не влияет, поскольку сигнал не коррелирован с шумом. Эффект минимизации общей выходной мощности будет выражаться в максимизации выходного отношения сигнал/шум. Если настройка фильтра обеспечивает равенство $\hat{N}(x,y) = N(x,y)$, то при этом $\hat{I}(x,y) = I(x,y)$. Если сигнал не содержит шума, адаптивный алгоритм должен устанавливать нулевые значения всем коэффициентам цифрового фильтра. В идеале необходимо отфильтровать изображение до его похожести на мастер-отпечаток (см. раздел «Способы создания синтетических отпечатков пальцев»).

Плюс адаптивной фильтрации в том, что можно сразу получить цифровое изображение шума. В противном случае необходимо было бы вычитать из оригинального изображения фильтрованное.

Необходимо проанализировать полученный шум $\hat{N}(x,y)$, при условии, что $\hat{N}(x,y) = N(x,y)$.

Нужно рассмотреть гистограмму $\hat{N}(x,y)$. Для понимания является ли изображение синтезированным необходимо иметь большую выборку синтезированных и естественных образов, а точнее их шумов. Ниже приведены примеры синтезированных (табл. 1) и естественных образов (табл. 2).

Таблица 1.
Синтезированные отпечатки пальцев и их гистограммы шума

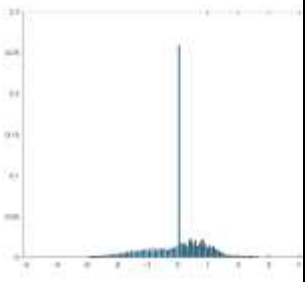
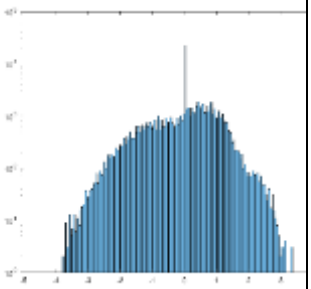
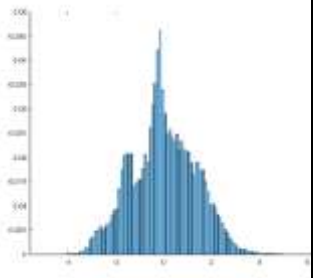
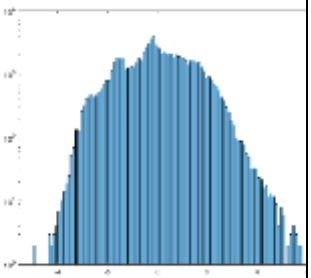
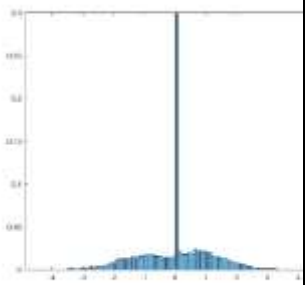
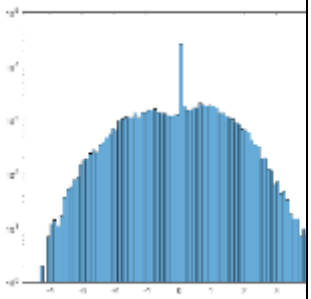
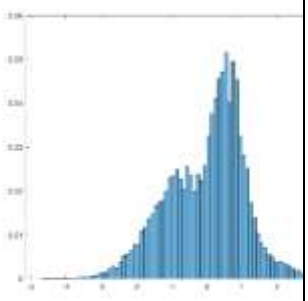
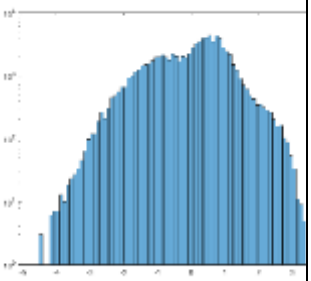
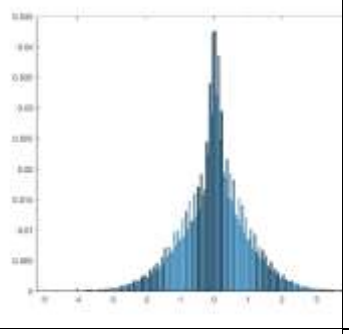
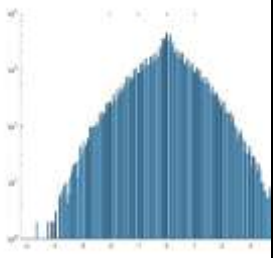
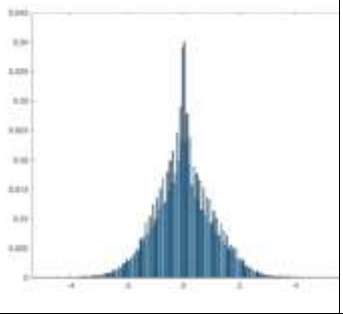
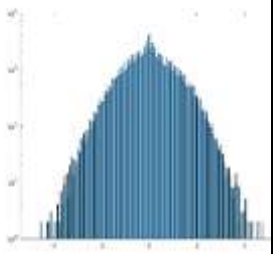
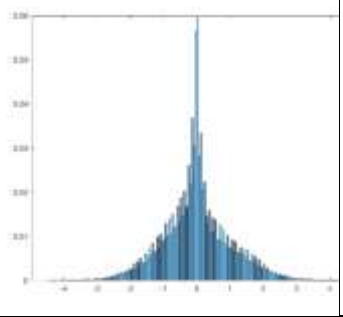
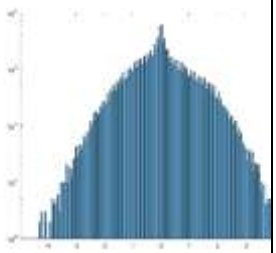
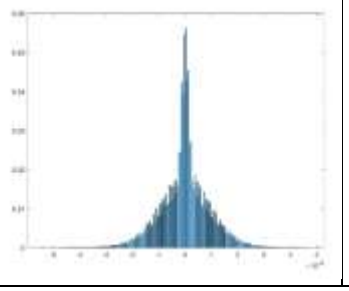
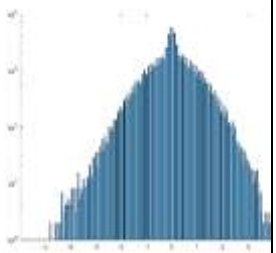
Отпечаток	Гистограмма	Гистограмма в логарифмическом масштабе
		
		
		
		

Таблица 2.
Естественные отпечатки пальцев и их гистограммы шума

Отпечаток	Гистограмма	Гистограмма в логарифмическом масштабе
		
		
		
		

При сравнении таблицы 1 и таблицы 2 видно, что гистограммы отличны по форме, в следствии чего можно заключить, что определение синтезированных образов возможно, но с некоторой долей вероятности, она зависит от условий сбора отпечатков, ошибок сканера (оптическая система и электронный тракт), фильтрации и т.д.

Блок-схема алгоритма определения синтезированного отпечатка пальца

На рисунке 4 представлена блок-схема, где реализован алгоритм распознания синтезированных биометрических образов.

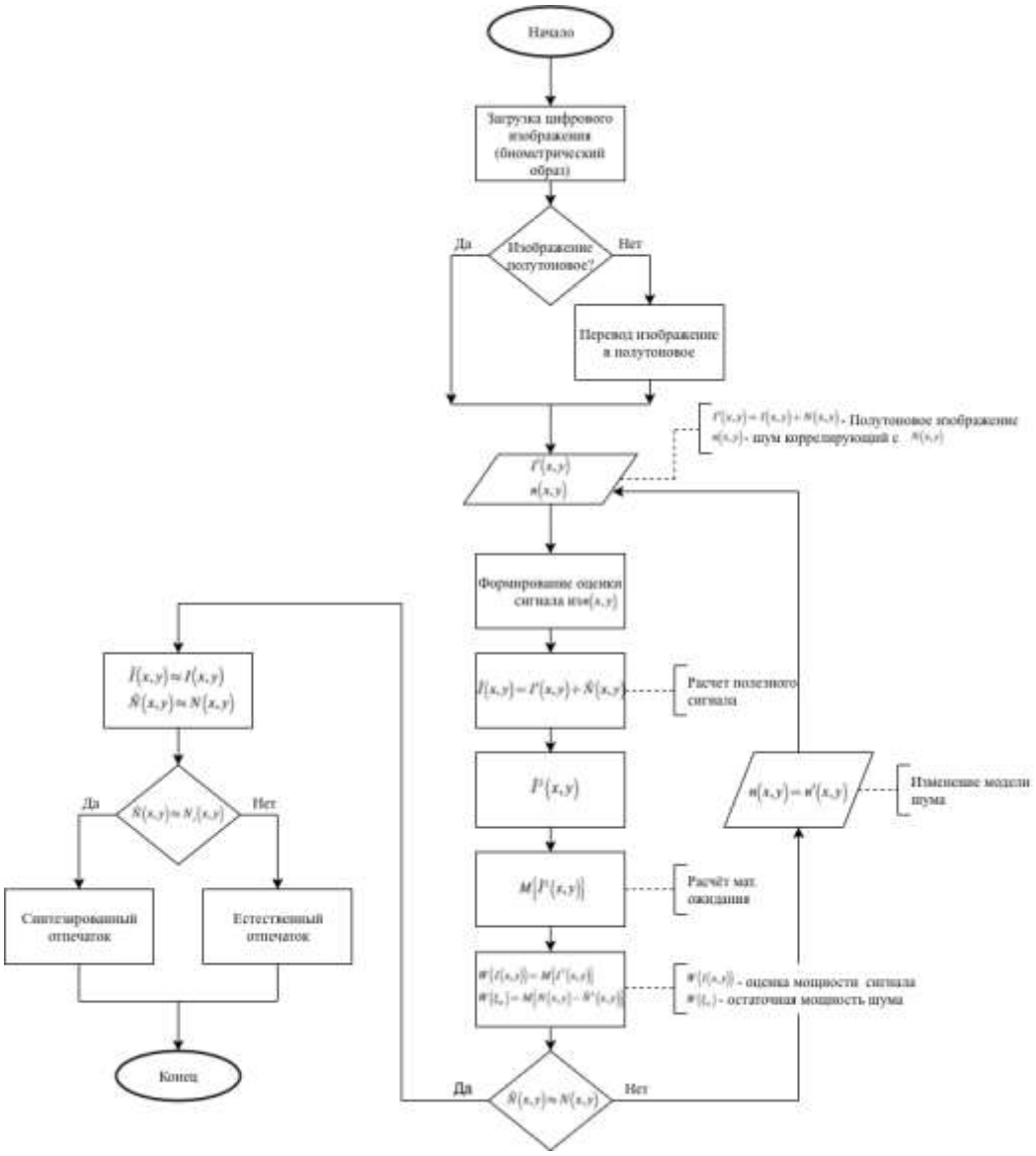


Рис. 4. Блок-схема алгоритма распознания синтезированных образов

Вывод

В статье рассмотрены:

программа для создания биометрических образов;

метод определения синтезированных биометрических образов;

блок–схема алгоритма определения синтезированных биометрических образов;

адаптивная фильтрация в формульном представлении.

Данный алгоритм определения синтезированных биометрических образов работает с некой долей вероятности, так как зависит от условий сбора отпечатков, ошибок сканера (оптическая система и электронный тракт), фильтрации и т.д.

Данные исследования необходимы поскольку синтезированные биометрические образы возможно использовать не только для тестирования разнообразных алгоритмов, их можно использовать и в других областях, а именно в не законной деятельности. Например, создание слоя с папиллярными линиями, на основе синтезированных образов. Инструкцию по созданию отпечатков можно найти в интернете в свободном доступе и для его создания все необходимое можно приобрести в свободной продаже. Также подменна естественных биометрических образов синтезированными, так как внешне они могут быть почти не отличимые (качество изображения, положение образа и т.д.).

Исследование способов определения синтезированных биометрических образов будет полезно в областях, связанных с безопасностью и идентификацией личности, таких как информационная безопасность, криминалистика и в некоторых случаях юриспруденция.

Литература

1. Biometric System Laboratory. DISI – University of Bologna. URL: http://biolab.csr.unibo.it/ (Дата обращения 06.10.2018)
2. Maltoni, D., Maio, D., Jain, A.K. and Prabhakar, S.: Handbook of Fingerprint Recognition. Springer, 2009, pages 512. ISBN 978-1-8488-2254-2.
3. Zhao, Q., Jain, A.K., Paulter, N.G., Taylor, M.: Fingerprint image synthesis based on statistical feature models, 2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS), pages 23-30, ISBN 978-14-673-1384-1, URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6374554&isnumber=6374538.
4. Cappelli, R.: SFinGe: an Approach to Synthetic Fingerprint Generation, In BT 2004 - International Workshop on Biometric Technologies. Calgary, Canada: 2004, pages 147-154.
5. Cappelli, R., Maio, D., Maltoni, D.: Synthetic Fingerprint-Database Generation, 16th International Conference on Pattern Recognition (ICPR2002), Québec City, Canada: 2002, pages 744-747. ISBN 0-7695-1695-X
6. Рычков А.С. Алгоритм анализа искусственных биометрических данных с использованием модели шумов. Сборник трудов Восьмой всероссийской научно-технической конференции «Безопасные информационные технологии» (БИТ-2017) / Под. ред. М.А.Басараба. – М.: МГТУ им. Н.Э.Баумана, НУК «Информатика и системы управления», 2017. С. 374-379.
7. Джиган В.И. Адаптивная фильтрация сигналов: теория и алгоритмы. Москва, Техносфера, 2013, 528 с.
8. Widrow B. Thinking about thinking: the discovery of the LMS algorithm – DSP history // IEEE Signal Processing Magazine. 2005. Vol. 22. № 1. P. 100–106.

Научный руководитель: Басараб Михаил Алексеевич, д.ф.-м.н., заведующий кафедрой ИУ8 «Информационная безопасность», basarab.iu8@gmail.com.

Definition of synthetic biometric images

Rychkov A.S.[67]

Abstract. The work is devoted to the method of definition of synthetic biometric images of fingerprints. As a result, the next problem was considered: a method for synthesizing synthetic biometric fingerprint images with using the SFinGe software; a flowchart of the recognition algorithm, its description is presented, and a method of adaptive filtering in the formula form is described. The results of applying the algorithm on natural and synthetic biometric images are presented. These results show that there is a way to differ a synthetic fingerprint from a natural fingerprint by considering the noise in a digital image.

Keywords: fingerprint, digital image, fingerprint generation method, histogram, filtration.

[67] Alexey Rychkov, Master's Degree student, Bauman Moscow State Technical University, Moscow, rychkov.alexey.s@gmail.com

УДК 004.056

Алгоритмы анонимной идентификации устройства

Смольникова М.С., студент, МГТУ им. Н.Э. Баумана, Москва, smolnikova@stego.su

В данной работе рассмотрены некоторые существующие методы анонимной идентификации устройства, а также предложен алгоритм для анонимной идентификации устройства в системе дистанционного банковского обслуживания. Алгоритм работает на основе технологии Browser Fingerprint – сбор информации об удаленном устройстве для дальнейшей идентификации. Массив данных для устройства кодируется строкой (отпечатком) с помощью нечетких хэш-функций. Отпечатки могут быть получены даже когда cookie выключены.

Ключевые слова: Browser Fingerprint, нечеткий поиск, нечеткая хэш-функция, расстояние Левенштейна, cookie, идентификация.

Введение

Анонимная идентификация устройства, или получение цифрового отпечатка устройства – присвоение устройству некого внутреннего идентификатора на основе внешних параметров устройств. Данная технология может быть применена во многих сферах, например,

1) Персональная реклама
2) Внутренняя аналитика (Google Analytics и Яндекс активно используют)
3) Системы антифрода (борьбы с мошенничеством, фрод-мониторинг Интернет-ресурсов.

Методы анонимной идентификации устройства

Основной и самый распространенный способ идентифицировать устройство – сессионные cookie [1], т.е. выставление небольшого фрагмента данных веб-сервером, которые хранятся на компьютере пользователя. Они могут быть самые разные, набирают популярность evercookie, но основной их недостаток – пользователь может их легко удалить или подменить. Более стойкой и стабильной является другая технология – Browser Fingerprint.

Принцип работы очень простой – с помощью скриптовых языков программирования стал возможным сбор более индивидуальной информации, такой как операционная система, браузер с установленными плагинами и шрифтами, данные о видеокарте, процессоре, ip-адрес, провайдер, город и другие. Ассимиляция такой информации вместе в одну строку дает уникальный отпечаток компьютера. Концепция отпечатка устройства связана с практической ценностью отпечатков пальцев человека. В идеале все машины имеют разное значение отпечатка (различие) и это значение никогда не поменяется (стабильность). В таком случае можно было бы однозначно определять каждую машину в сети без согласия пользователя.

Алгоритм применения Browser Fingerprint основан на нечетком поиске [1] с использованием нечетких хэш-функций. Под нечетким поиском понимается поиск по ключевым словам с учётом возможных произвольных ошибок в написании ключевого слова или, напротив, ошибок написания слова в целевом запросе. Ключевым моментом построения грамотного поиска является выбор меры сходства между словами или, как еще принято называть, функции расстояния между словами. Другим важным аспектом является правильная индексация

элементов для быстрого и надежного поиска. Наиболее распространенной метрикой является метрика Левенштейна [3].

Расстояние Левенштейна — это наименьшее расстояние редактирования такое, что одна строка переходит в другую. В случае сравнения строк, предпочтительней высчитывать расстояние для каждого слова отдельно, а не для строки целиком. Вычисление расстояния Левенштейна имеет квадратичную сложность, поэтому очень важно выбрать в исходном словаре множество, которое могло бы содержать исходный запрос [4].

Программная реализация алгоритма анонимной идентификации устройства

Fuzzy hashing fingerprint – алгоритм получения отпечатка устройства, основанный на нечетких хеш-функциях. Отпечаток – строка, представляющая собой конкатенацию двух строк: device _hash и geo_hash (рис. 1).

Device_hash – нечеткая хеш-функция от параметров, определяющих устройство (ОС, canvas, webgl, browser). Geo_hash – нечеткая хеш-функция от параметров, определяющих местоположение устройства (город, time зона, провайдер, внешний ip, внешний ip (web rtc), локальный ip (webrtc)).

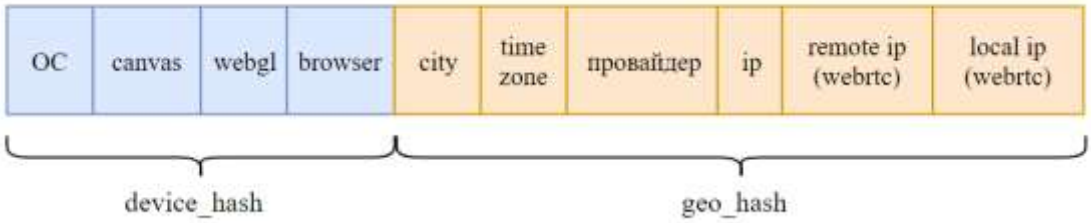


Рис.1 Структура Fuzzy hashing fingerprint

При этом итоговый отпечаток может иметь разную длину в зависимости от разных входных данных (например, если отсутствует какой-либо параметр, или их пришло несколько за сессию).

Такие отпечатки были получены для 289 тыс. устройств и сгруппированы по расстоянию Левенштейна в 58105 групп (число различий меньше 15). В каждой группе от 2 до 194 отпечатков.

Рассмотрим группу со 194 отпечатками (рис. 2). Она образована 66 устройствами. Последующая проверка показала, что все устройства связаны 95 логинами следующим образом:

Рис.2 Связи между найденными устройствами

Последующий анализ групп с похожими отпечатками дал аналогичный результат: все объединенные устройства имеют общие логины.

Выводы

Защита от отпечатков браузера, или fingerprints, довольно трудна. Но и эта технология кроме очевидных плюсов имеет свои минусы. Самый большой - сложность реализации. Для достижения высокой точности необходимо хранить большие массивы данных, для которых требуются стабильные (чаще нереляционные) базы данных. Кроме того, каждый отпечаток имеет определённый срок жизни, по оценкам аналитиков это около двух недель. Но несмотря на недостатки, Browser Fingerprint остается самой популярной и востребованной технологией анонимной идентификации устройства.

Литература

1. Рауткин В.Ю. Обзор способов достоверной идентификации сетевых устройств // Вопросы кибербезопасности. 2013. № 3 (3). С. 54-60. URL: https://elibrary.ru/item.asp?id=22536189.
2. Фролов А. С. Разработка алгоритма нечеткого поиска на основе хэширования // Молодой ученый. — 2016 — №13. — С. 357-360.
3. Машечкин И.В., Петровский М.И., Попов Д.С., Царёв Д.В. Латентно-семантический анализ в задаче автоматического аннотирования // Программирование. — Наука, 2011 — Т. 37 — № 6 — С. 67-77.
4. Петровский М.И., Глазкова В.В., Царёв Д.В. О выборе модели представления текстовой информации для задачи анализа и фильтрации Интернет-трафика // Математические методы распознавания образов: 13-я Всероссийская конференция. — М.: МАКС Пресс, 2007 — С. 519-522.

Научный руководитель: Басараб Михаил Алексеевич, доктор технических наук, профессор, МГТУ им. Н.Э. Баумана, basarab.iu8@gmail.com

ALGORITHMS OF ANONYMOUS IDENTIFICATION OF THE DEVICE

M. Smolnikova, student, Bauman Moscow State University, Moscow, smolnikova@stego.su

In this paper, we consider some of the existing methods of anonymous identification of the device, and propose an algorithm for anonymous identification of the device in the remote banking service system. The algorithm works based on technology Browser Fingerprint - collecting information about the remote device for further identification. The data array for the device is encoded by a string (fingerprint) using fuzzy hash functions. Imprints obtained even when cookies turned off.

Keywords: Browser Fingerprint, fuzzy search, fuzzy hash function, Levenshtein distance, cookie, identification.

УДК 004.056

К вопросу об использовании методов оценки рисков в системах менеджмента информационной безопасности

Ж. Шаршеева[68]

Аннотация. Проведен анализ методов оценки рисков в контексте информационной безопасности. Рассмотрены особенности систем менеджмента информационной безопасности. Выделены общие и редко используемые методы анализа риска. Даны рекомендации по использованию методов оценки рисков систем менеджмента информационной безопасности.

Ключевые слова: безопасность, риск, методы оценки рисков, управление рисками, стандарт.

Деятельность организации тесным образом связана с рисками, а точнее с процессами и процедурами по их оценке, обработке, контролю и управлению [5]. Общий подход к управлению рисками в области информационной изложен в стандарте ГОСТ Р ИСО/МЭК 27005, при этом методический аппарат обоснования анализа рисков достаточно подробно представлен в литературе [1-18]. В то же время остается актуальным вопрос комплексирования различных способ и техник анализа рисков в рамках организации системы менеджмента организации. Наиболее известными стандартами, в которых описаны методы анализа рисками являются ГОСТ Р ИСО 31010-2011 и PMBOK. К сожалению, указанные стандарты не предлагают каких-либо рекомендаций по применению указанных методов в области именно информационной безопасности [12, 13, 17].

Основываясь на данных [9, 10], оценка риска представляет собой часть по процессу управления рисками, предусматривающая определенный по структуре процесс, который выявляет возможно затронутые цели, а также проводит анализ рисков с позиции вероятных последствий и до момента принятия решения. Для проведения оценки риска необходимым является ответить на некоторые вопросы:

- Что может случиться и по какой причине?
- Какими могут быть последствия?
- Насколько вероятно их будущее появление?
- Существуют ли факторы, смягчающие последствия риска или уменьшающие вероятность его возникновения?

В докладе будет представлены результаты исследования применимости методов анализа рисков к сфере информационной безопасности[69]. Часть результатов представлены в табл.1.

Таблица 1 - Оценка применимости методов оценки рисков для СМИБ

Метод	Объём подготовительных работ	Доступность входных данных	Применимость выходных данных	Наглядность результатов	Удобство анализа
Мозговой штурм	Н	Н	С	С	С
Структурированное интервью	Н	С	Н	С	Н
Метод Дельфи	Н	Н	С	С	С
Подготовительная оценка рисков	Н	С	В	В	В

[68] Жибек Шаршеева, аспирант, Финансовый университет при Правительстве Российской Федерации, г. Бишкек, Киргизия, jsharsheeva.rc@gmail.com

[69] ГОСТ Р ИСО 31010-2011. Менеджмент риска. Методы оценки риска.

(PHA)					
Анализ риска и работоспособности (HAZOR)	C	C	C	C	C
Обзор воздействий(BIA)	C	C	C	C	C
Оценка видов и последствий отказов (FMEA)	C	H	B	C	B
Оценка дерева неисправностей (FTA)	H	C	C	B	B
Исследование дерева событий (ETA)	B	B	B	B	B
Попарный анализ "причина-последствие"	C	C	B	B	B
Обзор уровней защиты (LOPA)	C	C	B	C	C
Оценка дерева решений	B	C	C	B	C
Оценка влияния человеческого фактора (HRA)	C	B	C	C	C
Оценка "галстук-бабочка"	B	B	C	C	C
Марковский анализ	B	B	C	B	B
Форма последствий и вероятностей	C	B	B	B	B
Обзор эффективности затрат (CBA)	B	C	C	B	B
Мультикритериальная оценка решений (MCDA)	B	C	B	B	B

В табл.1 представлены обозначения уровней, которые приняты по международным и отечественным стандартам, где H – низкий, C – средний, B – высокий. Согласно табл. 1, в расположении находится достаточно широкий комплекс методов, а именно:

- информационно-статистический подход;
- экспертное оценивание;
- Марковский анализ;
- событийно-логический подход;
- оценка видов, последствий и критичности отказов (FMECA);
- анализ дерева неисправностей (FTA);
- анализ дерева событий (ETA).

Следует отметить что в процессе анализа рисков необходимо учитывать практические ситуации, при которых желаемая альтернатива формируется, основываясь на действующем законодательстве [5, 9, 10].

Литература

1. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий. Москва, ДМК Пресс, 2017, 224 с.
2. Бельфер Р.А., Калюжный Д.А., Тарасова Д.В. Анализ зависимости уровня риска информационной безопасности сетей связи от экспертных данных при расчетах с использованием модели нечетких множеств // Вопросы кибербезопасности. 2014. №1 (2). С. 33-39.
3. Бердюгин А.А. Управление риском нарушения информационной безопасности в условиях электронного банкинга // Вопросы кибербезопасности. 2018. № 1 (25). С. 28-38.
4. Булдакова Т.И., Миков Д.А. Реализация методики оценки рисков информационной безопасности в среде MATLAB//Вопросы кибербезопасности. 2015. №4 (12). С. 53-61.
5. Дорофеев А.В. Менеджмент информационной безопасности: управление рисками//Вопросы кибербезопасности. 2014. № 2 (3). С. 66-73.
6. Дорофеев А.В., Марков А.С. Менеджмент информационной безопасности: основные концепции//Вопросы кибербезопасности. 2014. № 1(2). С. 67-73.
7. Казарин О.В., Репин М.М. Особенности анализа рисков утечки конфиденциальной информации по техническим каналам при создании радиоэлектронных средств. Вопросы кибербезопасности, 2015, № 4(12), с. 62-69.
8. Калашников А.О. Управление информационными рисками объектов критической информационной инфраструктуры Российской Федерации // Вопросы кибербезопасности. 2014. В 3(4). С. 35-41.
9. Петренко С.А. Модель киберугроз по аналитике инноваций DARPA // Труды СПИИРАН. 2015. № 2 (39). С. 26-41.
10. Петренко С.А., Беляев А.В. Управление рисками ИТ-безопасности: SOA 404 // Защита информации. Инсайд. 2007. № 5 (17). С. 24-29.
11. Разработка методики проверки сведений, предоставляемых при заключении договора о банковском обслуживании, на основе риск-ориентированного подхода / Шеремет И.А., Дворянкин С.В., Евсеев В.Л., Скородумов Б.И., Велигура А.Н., Крылов Г.О., Овчинникова Ю.Е., Устинов Р.А., Бердюгин А.А., Воеводин А.Ю. - Отчет о НИР № ВТК-ГЗ-42-17 от 02.05.2017 (Правительство РФ).
12. Райкова Н.О. Влияние новых требований ISO/IEC 27001 на международную сертификацию организаций // В сборнике: Безопасные информационные технологии Сборник трудов Восьмой всероссийской научно-технической конференции. НУК «Информатика и системы управления». Под. ред. М.А.Басараба. 2017. С. 351-354.
13. Райкова Н.О. Сравнительный анализ стандартов менеджмента качества и информационной безопасности // Труды международного симпозиума Надежность и качество. 2014. Т. 2. С. 270-274.
14. Ревенков П.В., Бердюгин А.А. Расширение профиля операционного риска в банках при возрастании DDoS-угроз. // Вопросы кибербезопасности, 2017, № 3(21), с. 16-23.
15. Тарасова Н.А. Факторы организационных рисков, возникающих в системах обеспечения информационной безопасности // Вопросы кибербезопасности. 2013. В2. С.63-68.
16. Чукляев И.И. Научно-методическое обеспечение комплексного управления рисками нарушения защищенности функционально-ориентированных информационных ресурсов информационно-управляющих систем // Вопросы кибербезопасности, 2016, № 4(17), с. 61-71.
17. Шахалов И.Ю., Райкова Н.О. К вопросу об интегрировании систем менеджмента качества и информационной безопасности // Правовая информатика. 2014. В 2. С. 20-26.
18. Probabilistic Modeling in System Engineering / By ed. A. Kostogryzov. – London: IntechOpen, 2018. 278 p.

УДК 004.056.5

Создание прототипа системы биометрической аутентификации по геометрии лица с помощью методов машинного обучения

Соков Б.Б.[70]

Аннотация. Настоящее исследование посвящено решению проблемы разработки метода биометрической аутентификации. В работе рассматривается решение задачи аутентификации по геометрии лица с помощью методов машинного обучения. Подход гарантирует высокие результаты аутентификации с точки зрения монотонной комбинации вероятностей ошибок первого и второго рода. Полученные результаты могут быть применены, в частности, при построении многофакторной системы аутентификации.

Ключевые слова: нейронная сеть, гиперпараметры, биометрическая аутентификация.

Введение

В наши дни у каждой системы есть электронные средства защиты. В качестве примера можно привести социальные сети. Для того, чтобы зайти под своим аккаунтом, пользователь должен пройти двухфакторную аутентификацию, другими словами, пользователь сначала вводит логин и пароль, а затем система отправляет одноразовый пароль на номер телефона, привязанный к аккаунту пользователя.

Несомненно, каждая информационная система нуждается в защите. И чем выше фактор риска, чем больше финансовые потери, тем более надежный уровень защиты понадобится системе.

В настоящее время существует достаточно большое количество способов и довольно разнообразные методы защиты системы от несанкционированного доступа. У каждого метода есть свои особенности, свои плюсы и минусы. Например, аутентификация по отпечатку пальца является довольно распространенным и наиболее изученным методом, которому в данной момент по точности распознавания и финансовым характеристикам практически нет равных. Но метод это довольно старый и ученные давно ищут альтернативу этому методу аутентификации. В то время как, например, аутентификация по геометрии лица, на сегодняшний день, является довольно перспективной темой исследований, набирающей обороты[71].

Биометрическая аутентификация в 95% случаев включает в себя математическую статистику. В связи с этим, самым удобным методом аутентификации личности является аутентификация при помощи нейронных сетей, где происходит сравнение полученных данных с эталонными (например, [1-5]).

Биометрические сканеры

Для того, чтобы собирать точную биометрическую информацию о человеке, нужен биометрический сканер, показывающий высокое качество съема биометрической информации. Основная функция сканера – это проверка того, подделан объект биометрии или нет. При этом разные сканеры имеют различный набор способностей. Важно помнить, что сканеры очень сильно влияют на полученную статистику FAR и FRR[72]. Чаще всего в роли сканеров в методе

[70] Соков Басанг Батыревич, Бакалавр, МГТУ им. Н.Э. Баумана, Москва, ssokov09@mail.ru

[71] Современные биометрические методы идентификации: https://habr.com/post/126144/

[72] Биометрическая идентификация: www.techportal.ru/glossary/biometricheskaya_identifikaciya.html

аутентификации по геометрии лица выступает обычная камера. Метод, реализующий накопление информации о лице, включает в себя наиболее приемлемые характеристики работы с камерой. Суть заключается в том, что при занесении личности в базу он поворачивает голову и алгоритм соединяет изображение воедино, создавая 3d шаблон.

Статистические показатели метода

Полные данные о FRR и FAR для алгоритмов этого класса на сайтах производителей открыто не приведены. Но для лучших моделей фирмы Bioscript (3D EnrolCam, 3D FastPass), работающих по методу проецирования шаблона при FAR = 0.0047%, FRR составляет 0.103%. Считается, что статистическая надежность метода сравнима с надежностью метода идентификации по отпечатку пальца.

Преимущества и недостатки метода

Преимущества метода. Не происходит контакта со сканирующим устройством. Внешние факторы незначительно влияют на точность распознавания, как на самом человеке (появление очков, бороды, изменение прически), так и в его окружении (освещенность, поворот головы). Высокий уровень точности распознавания, сравнимый с метом идентификации по отпечатку пальца.

Недостатки метода. Оборудование является относительно дорогим. Изменения мимики лица и помехи на лице ухудшают статистическую надежность метода. Метод еще недостаточно хорошо разработан, особенно в сравнении с давно применяющейся дактилоскопией, что затрудняет его широкое применение.

Выбор архитектуры нейронной сети.

Чтобы в дальнейшем правильно использовать полученные данные, необходимо выбрать наиболее подходящий метод для работы с данными аутентификации по геометрии лица. В ходе исследования было выявлено, что наиболее подходящим метод являются древовидные оценочные функции Парзена [6].

В данном алгоритме работа происходит с гиперпараметрами. Гиперпараметры – это совокупность особенностей архитектуры, количество нейронов на каждом слое, их тип, количество слоев, первоначальная инициализация сети, а также методика обучения [7].

Данный метод основан на использовании древовидных оценочных функций Парзена. На начальном этапе алгоритм схож с методом гауссовского процесса с ожидаемым улучшением. В дальнейшем строится дерево решений и по нему проводится поиск. Эффективность данного метода оценивается высоко, здесь определяются направления в пространстве гиперпараметров методом вычислений. Вычислительная сложность метода можно определить, как среднюю, она приблизительно равна использованию поиска по дереву, что в свою очередь значительно сокращает время поиска [8].

Древовидные оценочные функции Парзена не имеют тех недостатков, которые встречаются в методе гауссовских процессов с ожидаемым улучшением. На каждой итерации собираются новые данные, и в конце каждой итерации алгоритм сам решает какой набор параметров будет использован в следующей итерации. В начале работы алгоритма нужно определить какое распределение для гиперпараметров будет начальным. Как видите, наиболее эффективными и

удобными в практических задачах выступают древовидные оценочные функции Парзена. Но для удобства правильнее будет воспользоваться поиском по матрице с переменным шагом для получения характеристик классификаторов на основе ИНС в пространстве гиперпараметров. Затруднение в использовании полносвязных ИНС для распознавания изображений состоит в потребности разложения трехмерного массива, описывающего изображение, в одномерный вектор. Для этого можно использовать два основных метода: построчное разложение и разложение с помощью скользящего окна. При использовании построчного разложения изображения в одномерный вектор изменяются последовательности представления цветовых каналов[73] [9]. Также можно встретить разновидности метода с применением предварительного перевода изображения в черно-белый — уменьшение числа каналов с 3 до 1. В методе скользящего окна применяется концепция окон для трехцветного изображения. Происходит последовательная запись в окне соответствующего размера цветовой составляющей каждого пикселя.

Вектор размерностью w x h x 3 генерируется окном, где w – ширина окна, h – высота окна. Разновидностями этого метода являются изменения параметров сдвига и размера окна [10, 11].

Вывод

В ходе проделанной работы теоретически и экспериментально обоснован новый подход к решению разработки метода биометрической аутентификации. Подход затрагивает решение задачи аутентификации по геометрии лица с помощью методов машинного обучения. Данный метод находится на стадии разработки, но гарантирует высокие результаты аутентификации с точки зрения монотонной комбинации вероятностей ошибок первого и второго рода.

В дальнейшем планируется провести проверку работоспособности предложенного подхода при построении многофакторной системы аутентификации в мобильных устройствах.

[73] Применение локальных бинарных шаблонов к решению задачи распознавания лиц: https://habr.com/post/193658/

Литература

1. Качайкин Е.И., Иванов А.И. Идентификация авторства рукописных образов с использованием нейросетевого эмулятора квадратичных форм высокой размерности // Вопросы кибербезопасности. 2015. № 4 (12). С. 42-47.
2. Качайкин Е.И., Иванов А.И., Безяев А.В., Перфилов К.А. Оценка достоверности нейросетевой автоматизированной экспертизы авторства рукописного почерка // Вопросы кибербезопасности. 2015. № 2 (10). С. 43-48.
3. Крутохвостов Д.С., Хиценко В.Е. Парольная и непрерывная аутентификация по клавиатурному почерку средствами математической статистики // Вопросы кибербезопасности. 2017. № 5 (24). С. 91-99.
4. Ложников П.С., Сулавко А.Е., Бурая Е.В., Писаренко В.Ю. Аутентификация пользователей компьютера на основе клавиатурного почерка и особенностей лица // Вопросы кибербезопасности. 2017. № 3 (21). С. 24-34.
5. Рыжков А.П., Катков О.Н., Морозов С.В. Нейросетевые технологии при решении задач разграничения доступа // Вопросы кибербезопасности. 2016. № 3 (16). С. 69-76.
6. Фукунага К. Введение в статистическую теорию распознавания образов, М.: Наука, 1979. — 368 с.
7. Хайкин С., Нейронные сети. Полный курс, Издательство: Вильямс, 2016, 1104 с
8. А.Н. Голубинский, А.А. Толстых Выбор архитектуры искусственной нейронной сети на основе сравнения эффективности методов распознавания изображений- – 2018 - № 1 - С. 27-37
9. Математические основы информационной безопасности / Басараб М.А., Булатов В.В., Булдакова, Т.И., Гордеев Э.Н., Жуков А.Е., Ключарев П.Г., Медведев Н.В., Троицкий И.И., Чичварин Н.В. и др.: Под ред. Матвеева В.А. – М.: НИИ РиЛ МГТУ им.Н.Э.Баумана, 2013. -244 с.
10. Ершов К.С., Романова Т.Н. Анализ и классификация алгоритмов кластеризации // Новые информационные технологии в автоматизированных системах. 2016. № 19. С. 274-279.
11. Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы: Пер. с польск. И. Д. Рудинского. М.: Горячая линия -Телеком, 2006. 452 с. URL: http://sernam.ru/book_gen.php

Научный руководитель: Коннова Наталья Сергеевна, доцент кафедры «Информационная безопасность», кандидат технических наук, МГТУ им. Н. Э. Баумана, Доцент, nkonnova@bmstu.ru.

The creation of a prototype system for biometric authentication to the geometry of the face using methods of machine learning

Sokov B.B.[74]

Annotation. This study is devoted to the problem of developing a method of biometric authentication. The paper deals with the problem of face geometry authentication using machine learning methods. The approach ensures the results the results of the authentication methods from the point of view of monotonic combinations of probabilities of errors of first and second kind. The results can be applied, in particular, in the construction of a multi-factor authentication system.

Keywords: neural network, hyperparameters, neural network architecture.

[74] Sokov Basang, bachelor, Bauman Moscow State Technical University, Moscow, ssokov09@mail.ru

УДК 347.734

Оценка рисков информационной безопасности в рамках проекта Положения Банка России о требованиях к системе управления операционным риском для кредитной организации

Титов А.Ю.[75]

В работе проведён анализ разделов 7 и 8 проекта Положения Банка России «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» (по состоянию на 18.09.2018 г.) с точки зрения оценки рисков информационных систем и информационной безопасности. Снижение операционного риска кредитной организации, связанного с нарушением безопасности информации, обеспечивается путём надлежащего выбора, повышения полноты и качества применения соответствующих мер защиты информации. Для противостояния угрозам безопасности информации и их влиянию на операционный риск, организациям требуется определить достаточность и адекватность состава и содержания мер защиты информации, что невозможно без знания всех актуальных угроз безопасности информации.

Ключевые слова: банковское регулирование, операционные риски, риски информационной безопасности, киберриск.

Введение

Деятельности кредитных организаций присущ операционный риск, связанный, помимо прочего, с возможностью отказов в используемых информационных системах и нарушениями безопасности информации. Понизить этот риск можно лишь до определённого остаточного уровня. Снижение операционного риска, связанного с рисками ИБ и ИТ, обеспечивается путём надлежащего выбора, повышения полноты и качества применения соответствующих мер, обеспечивающих непрерывность деятельности и защиту информации.

Переход Банка России на риск-ориентированный подход в регулировании, характеризующийся требованием оценки возможных потерь от операционного риска с целью выделения резервов на их покрытие, в перспективе должен обеспечить поднадзорным организациям адекватный уровень платёжеспособности и финансовой устойчивости, гарантирующий бесперебойное обслуживание клиентов.

Роль рисков ИБ в структуре операционных рисков

Операционный риск (ОР) – это риск прямых или косвенных потерь кредитной организации в результате:

- неадекватных или ошибочных внутренних процессов;
- действий персонала;
- нарушение штатной работы информационных систем;
- внешних событий.

В ОР входят разные виды рисков в зависимости от видов бизнес-процессов:

- риски информационной безопасности;
- риски, связанные с персоналом;
- риски недостатков внутреннего контроля;
- риски информационных систем;
- риски проектов;

[75] Титов Андрей Юрьевич, студент группы ИУ8-25, МГТУ им. Н.Э. Баумана, г. Москва, andyut@mail.ru

- риски обеспечения непрерывности и восстановления деятельности.

Структура рисков ИБ с точки зрения управления ОР представлена на Рис. 1.

Рис.1. Структура рисков ИБ с точки зрения управления ОР [1].

Основной особенностью управления ОР является децентрализованность

управления отдельными видами ОР, в том числе на основе специализированных стандартов, например, [2] для рисков ИБ.

Требования к системе управления операционными рисками

В соответствии с [3] кредитным организациям потребуется создать базу данных о событиях ОР и убытках, понесённых вследствие реализации ОР, содержащую следующую информацию:

- размер убытков;
- даты возникновения;
- дата отражения убытка на балансе организации;
- источник возникновения события (подразделение, автоматизированная система, бизнес-процесс);
- поступившие возмещения;
- информация о причинах и обстоятельствах возникновения событий.

Назначение базы данных – контроль над уровнем фактически понесённых (прямых) убытков организации. В случае превышения среднегодовых потерь, рассчитанных на основе этой базы данных, над минимальным регуляторным капиталом устанавливается надбавка (буфер капитала).

Классификация событий риска ИБ

В [3] предусматривается следующая классификация событий для риска ИБ:

- Связанные с переводами и платежами:
  - возникшие в результате использования электронных средств платежа клиентов кредитных организаций без их согласия;
  - связанные с переводами и снятиями денежных средств в результате несанкционированного доступа к объектам информационной инфраструктуры;
  - возникшие в результате списания денежных средств с корреспондентских счетов участников платёжной системы без их согласия и (или) с использованием искажённой информации;
  - связанные с неоказанием кредитной организацией услуг по

переводу денежных средств;
    - возникшие в результате нарушений и недостатков обеспечения ИБ и управления рисками нарушения ИБ.
- Возникшие в результате несанкционированного доступа и (или) реализации компьютерных атак на объекты информационной инфраструктуры и (или) информационные системы (в соответствии с [4]):
    - связанные с несанкционированным доступом к объектам информационной инфраструктуры и (или) информационным системам
    - возникшие в результате атак типа «отказ в обслуживании» (DDOS-атаки), предпринимаемых с целью блокирования нормального функционирования
    - возникшие в результате воздействия компьютерных вирусов
    - связанные с эксплуатацией уязвимостей в программном обеспечении информационных систем.
- Связанные с обработкой (хранением, уничтожением) информации без использования средств автоматизации:
    - связанные с утечкой конфиденциальной информации;
    - связанные с хищением или утратой носителей информации.

Сравнение с классификацией по ГОСТ Р 57580.1-2017

Банком России разработан стандарт [2], который содержит требования к содержанию базового состава мер защиты информации (требования к системе защиты информации) для информационных систем финансовых организаций, выбор которых производится с учётом модели угроз и нарушителей безопасности информации.

При разработке Модели угроз и нарушителей оцениваются:

В качестве типов источников угроз:

- антропогенные источники угроз;
- техногенные источники угроз;
- стихийные источники угроз.

В качестве источников угроз:

- криминальные элементы;
- компьютерные злоумышленники (хакеры);
- конкуренты;
- поставщики программно-технических средств, расходных материалов, услуг;
- подрядчики, осуществляющие монтаж, пусконаладочные работы оборудования;
- работники организации;
- неблагоприятные события природного характера;
- неблагоприятные события техногенного характера.

В качестве уязвимостей:

- потенциальная подверженность воздействию природных и техногенных факторов;
- ошибки в проектировании информационной системы финансовой организации;

- физические, моральные, психологические особенности работников;
- недостатки в организации охраны и технической защиты;
- восприимчивость программного обеспечения к вредоносным программам и компьютерным вирусам;
- наличие уязвимостей программного и аппаратного обеспечения;
- сбои и отказы технических средств;
- ошибки при подготовке и использовании программного обеспечения;
- наличие уязвимостей (слабостей) системы защиты информации;
- неполная регламентация вопросов взаимодействия с поставщиками и подрядчиками;
- несоответствие регламентов текущему состоянию информационной системы кредитной организации.

Очевидны расхождения в классификации видов рисков ИБ с точки зрения стандартов риск-менеджмента и подходов к ИБ, которое необходимо устранить в финальной версии Положения [3], чтобы не было разночтений.

Требования к системе управления рисками ИБ в составе ОР

Одним из подходов к расчёту величины необходимого капитала на покрытие операционного риска в составе величины собственных средств (капитала) кредитной организации является формула [1]:

$$К_{необходимый,ОР} = \underbrace{К_{мин\_регуляторн,ОР}}_{\text{№ 346-П}} + \underbrace{\Delta_{ИБ} + \Delta_{ОР}}_{\text{№ 3624-У}} \quad (1)$$

где $К_{мин\_регуляторн,ОР}$ – минимальный капитал, выделяемый на покрытие операционного риска, необходимый для соблюдения минимального значения норматива достаточности капитала;

$\Delta_{ИБ}$ – компонента необходимого капитала на покрытие совокупных убытков от реализации рисков ИБ, определяемая в случае превышения контрольного показателя склонности к риску в части ИБ в течение года;

$\Delta_{ОР}$ – компонента необходимого капитала на покрытие совокупных убытков от реализации ОР без учёта $\Delta_{ИБ}$, определяемая в случае превышения контрольного показателя склонности к риску в части ОР (без учёта ИБ) в течение года.

Контрольные показатели склонности к риску (риск аппетита) устанавливаются кредитной организацией самостоятельно и должны базироваться на внутренней оценке с учётом предыдущих надзорных оценок качества систем ИТ и ИБ и реализованных фактических потерь, покрываемых минимальным регуляторным капиталом на ОР. Если фактические потери за предыдущие года (год) превысили минимальный регуляторный капитал, то размер превышения включается в $\Delta_{ИБ}$ и $\Delta_{ОР}$ соответственно.

Заключение

В [5] отмечается, что документ [3] пока сырой, но в целом понятен службам ИБ. Разделы 7 и 8 Положения целиком касаются ИТ и ИБ непосредственно. Текущую Политику ИБ предлагается дополнить:

- требованием по обмену информацией о событиях риска ИБ и предоставляемых данных в ФинЦЕРТ, в соответствии с нормативными актами Банка России;
- показателями и методиками оценки эффективности обеспечения ИБ и управления рисками ИБ;

- ссылкой на выполнение требований Положения.

Положение о Службе ИБ предлагается дополнить обязанностью по направлению информации о событиях риска ИБ в ФинЦЕРТ.

Согласно проекту Положения кредитные организации должны планировать выделение средств на защиту от рисков ИБ и ИС.

Кредитные организации должны соответствовать Положению к 01.01. 2020.

Литература

1. Доклад на X Уральском форуме «Информационная безопасность финансовой сферы» [Электронный ресурс]: Перспективы развития регулирования операционных рисков в части киберрисков / начальник управления моделирования рисков департамента банковского регулирования Бухтин М.А. 15.02.2018. URL: https://ural.ib-bank.ru/files/files/materials2018/31%20Bukhtin.pdf (дата обращения: 12.11.2018).

2. ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. // СПС КонсультантПлюс.

3. Центральный Банк Российской Федерации [Электронный ресурс]: Проект Положения Банка России «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» (по состоянию на 18.09.2018) URL: https://cbr.ru/StaticHtml/File/41186/180918-41_1.pdf (дата обращения: 12.11.2018).

4. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. // СПС КонсультантПлюс.

5. SecurityLab.ru [Электронный ресурс]: Что интересного по ИБ в проекте Положения Банка России «О требованиях к системе управления операционным риском…». / Валерий Естехин. 26.09.2018. URL: https://www.securitylab.ru/blog/personal/estekhin/344841.php (дата обращения: 12.11.2018).

Научный консультант: Левиев Дмитрий Олегович, Старший преподаватель кафедры Информационная безопасность (ИУ8) НУК Информатика и системы управления (ИУ) МГТУ им. Н. Э. Баумана, leviev@bmstu.ru.

Information Security Risk Assessment According to the Draft Regulations of the Central Bank of the Russian Federation on Requirements to Operational Risk Management System for Credit Institution and Banking Group

Titov A.[76]

Abstract. The analysis of draft banking regulations is conducted relating to operational risk assessment with respect to information systems and information security risks of the credit institution. Operational risk related to information security breaches is mitigated by the proper choice of, the coverage of, and the quality of implementation of appropriate protection measures. To resist to information security threats and their influence on operational risk, the credit institution should identify the adequacy and configuration of protection measures, that is impossible to perform without knowledge of all relevant information security threats. The conclusion is made on the reasonable preparatory actions implied by the draft regulation to the credit institution.

Keywords…banking regulations, operational risk, information security, cyberrisk

[76] Andrei Titov, student of IU8-25 group, Bauman Moscow State Technical University, andyut@mail.ru

УДК 004.056

Обнаружение ботов в онлайновой социальной сети Twitter с помощью алгоритма машинного обучения «Случайный лес»

Хачатрян М.Г.[77]

В статье рассматривается возможность использования алгоритма машинного обучения «Случайный лес» для обнаружения ботов в социальной сети «Twitter». Цель исследования – дать количественную оценку точности обнаружения ботов. Было проведено тестирование алгоритма методом кросс-валидации по десяти блокам на выборке из нескольких тысяч аккаунтов Twitter, состоящей как из настоящих пользователей, так и из различных видов ботов. В результате проведенного тестирования было получено значение F_1-метрики равной 0.982. Данное значение является довольно высоким показателем точности обнаружения ботов по сравнению с большинством предыдущих работ по обнаружению ботов в онлайновой социальной сети Twitter.

Ключевые слова: решающие деревья, кросс-валидация, социальные сети, боты.

Введение

За последнее десятилетие социальные сети, такие как «Twitter» хорошо зарекомендовали себя в качестве инструмента для коммуникации в реальном времени. Социальные сети затрагивают практически все слои населения и эффективно структурируют пользователей по их интересам, политическим, религиозным и иным взглядам [1]. Однако, несмотря на все удобства, которые предоставляют социальные сети, безусловно, существуют проблемы, связанные с злоупотреблениями [2], которые довольно часто проводятся с помощью ботов [3]. Боты – это программное обеспечение, предназначенное для имитации поведения реального пользователя в социальных сетях. В данной работе произведено исследование по применению алгоритма классификации «Случайный лес» для обнаружения ботов в социальной сети «Twitter».

Алгоритм классификации «Случайный лес»

«Случайный лес» [4] – это множество решающих деревьев. В задаче классификации решение принимается голосованием по большинству среди выданных ответов. Все деревья строятся независимо по следующей схеме:

1. Выбирается подвыборка обучающей выборки размера N с повторениями, по которой строится дерево (для каждого дерева своя подвыборка).
2. Для построения каждого расщепления в дереве просматриваются m (квадратный корень из общего количества признаков M) случайных признаков.
3. Выбираются наилучшие признак и расщепление по нему (в данной работе по критерию Джини [5]). Дерево строится, до исчерпания выборки (пока в листьях не останутся представители только одного класса), если не заданы ограничения (например, глубина дерева).

Исходные данные для обучения и тестирования алгоритма

Данные, используемые в этой работе находятся в открытом доступе и были представлены в статье [6]. Для обучения и тестирования алгоритмов машинного обучения используются данные групп, представленных в таблице 1. Каждая группа представляет собой таблицу, где строки представляют собой различные аккаунты, а столбцы – признаки аккаунта (например, количество групп, к которых состоит аккаунт), по которым определяется, является аккаунт ботом или нет.

[77] Хачатрян Микаэл Гагикович, МГТУ им. Н.Э. Баумана, Москва, 5019973@mail.ru

Таблица 1.

Используемые группы из базы данных

Группа	Описание	Количество аккаунтов
genuine accounts	Аккаунты обычных пользователей	3474
social spambots #1	Ретвитеры[78] некоего итальянского политического деятеля	991
social spambots #2	Спамеры[79] платных приложений для мобильных устройств	3457
social spambots #3	Спамеры продуктов на продажу в Amazon.com	464
traditional spambots #1	Тренировочный набор данных спамеров, используемых в статье [7]	1000
traditional spambots #2	Спамеры зловредных ссылок	100
traditional spambots #3	Спамеры рассылающие предложения о работе	433

Методика оценки эффективности алгоритма

Оценка эффективности производится методом кросс-валидации по k блокам с выбором оптимальных гиперпараметров (некоторые параметры, которые не изменяются в процессе обучения алгоритма), который состоит из следующих шагов [8]:

1. Доступные данные делятся на две подгруппы: тренировочные и тестовые.
2. На данном этапе тренировочные данные подаются на вход алгоритму обучения с различными гиперпараметрами. Для каждой конфигурации гиперпараметров производятся следующие действия:
   2.1. Тренировочные данные делятся на k блоков
   2.2. Производится k итераций обучения и тестирования алгоритма. Для обучения используется $k-1$ блоков, для тестирования 1, при этом после проведения k итераций каждый блок должен участвовать в тестировании.
   2.3. Результаты тестирования усредняются.
3. Производится обучение алгоритма с наилучшими гиперпараметрами на тренировочных данных и оценка точности на тестовых.

В качестве метрики для оценки точности была выбрана F_1-мера:

$$F_1 = 2 \cdot \frac{Pre \cdot Rec}{Pre + Rec}, \quad (3)$$

где $Pre = \frac{TP}{TP+FP}$ – точность;

$Rec = \frac{TP}{TP+FN}$ – полнота;

TP – число объектов положительного класса, идентифицируемых как объекты положительного класса;

TN – число объектов отрицательного класса, идентифицируемых как объекты отрицательного класса;

FP – число объектов отрицательного класса, идентифицируемых как объекты положительного класса;

FN – число объектов положительного класса, идентифицируемых как объекты отрицательного класса.

Обучение и тестирование алгоритма

[78] боты, которые совершают размещения записи на своей странице для определенного аккаунта

[79] боты, которые распространяют спам

Реализация и тестирование алгоритмов было произведено с помощью языка программирования Python и его библиотек. При тестировании методом кросс-валидации по 10 блокам данные были разделены на тренировочные и тестовые (90% тренировочных, 10% тестовых) методом стратификации.

В таблице 2 представлена зависимость F_1 метрики от количества решающих деревьев N и от максимальной глубины деревьев d на тренировочных данных.

Таблица 2.

Зависимость значения метрики F_1 от гиперпараметров при использовании метода кросс-валидации.

N \ d	1	2	3	4	5	6	7	8	9
1	0.735	0.827	0.914	0.931	0.977	0.977	0.970	0.968	0.978
2	0.976	0.973	0.976	0.986	0.977	0.984	0.984	0.983	0.979
3	0.976	0.976	0.979	0.985	0.981	0.986	0.985	0.984	0.987
4	0.976	0.978	0.978	0.984	0.982	0.988	0.987	0.982	0.988
5	0.976	0.976	0.979	0.984	0.985	0.989	0.987	0.989	0.989
6	0.976	0.974	0.977	0.984	0.985	0.987	0.986	0.990	0.986
7	0.976	0.976	0.976	0.983	0.986	0.987	0.987	0.989	0.989
8	0.976	0.976	0.977	0.984	0.985	0.989	0.986	0.989	0.989
9	0.976	0.977	0.979	0.984	0.984	0.988	0.987	0.989	0.989

Как видно, наилучшие результаты достигаются при глубине дерева d равном 8 и числе решающих деревьев N равном 6.

После обучения алгоритма на тренировочных данных с полученными оптимальными гиперпараметрами было произведено тестирование на тестовых данных и получено значение F_1 метрики равной 0.982.

Выводы

В данной статье было рассмотрено обнаружение ботов в социальной сети «Twitter» при помощи алгоритма «Случайный лес». В качестве исходных данных для экспериментальной оценки эффективности выбранного алгоритма были использованы данные, представленные в статье [6]. Оценка эффективности алгоритма производилась методом кросс-валидации по 10 блокам.

В результате экспериментальной оценки эффективности было получено, что значение F_1-метрики на тестовых данных равно 0.982, что является довольно высоким показателем, если сравнивать с предыдущими работами по обнаружению ботов в социальной сети Twitter [7,9,10,11].

Литература

1. Алымов А.С., Баранюк В.В., Смирнова О.С. Детектирование бот-программ, имитирующих поведение людей в социальной сети «Вконтакте» // International Journal of Open Information Technologies. 2016. Том 4, № 8. С. 55 – 60.
2. Ключарёв П.Г. Социальные сети: Перспективные направления исследований // Безопасные информационные технологии. Сборник трудов Седьмой всероссийской научно-технической конференции. – М.: НУК Информатика и системы управления, 2016, С. 164-167.
3. Лыфенко Н.Д. Виртуальные пользователи в социальных сетях: мифы и реальность // Вопросы кибербезопасности. 2014. №5(8). С. 1-4.
4. A. Liaw, M. Wiener. Classification and Regression by RandomForest // R News. 2002. Vol. 2. Issue 3.
5. Yu-Shan Shih. Families of splitting criteria for classification trees // Statistics and Computing. 1999, Vol 9, pp. 309-315
6. Stefano Cresci, Roberto Di Pietro, Marinella Petrocchi, Angelo Spognardi, Maurizio Tesconi. The paradigm-shift of social spambots: Evidence, theories, and tools for the arms race // In Proceedings of the 26th International Conference on World Wide Web Companion. International World Wide Web Conferences Steering Committee. 2017. P. 963-972. DOI: 10.1145/3041021.3055135

7. C. Yang, R. Harkreader, and G. Gu. Empirical evaluation and new design for fighting evolving Twitter spammers // IEEE Trans. Inform. Forens. Sec. 2013. Vol. 8. Issue 8. P. 1280-1293. DOI: 10.1109/TIFS.2013.2267732

8. Sebastian Raschka. Model evaluation, model selection, and algorithm selection in machine learning. 2018, URL: https://sebastianraschka.com/pdf/manuscripts/model-eval.pdf

9. S. Cresci, R. Di Pietro, M. Petrocchi, A. Spognardi, and M. Tesconi. DNA-inspired online behavioral modeling and its application to spambot detection. // IEEE Intelligent Systems. 2016. Vol. 5. Issue 31. P. 58-64

10. F. Ahmed and M. Abulaish. A generic statistical approach for spam detection in online social networks // Computer Communications. 2013. Vol. 36. Issue 10. P. 1120-1129

11. Z. Miller et al. Twitter spammer detection using data stream clustering // Information Sciences. 2014. Vol. 260. P. 64-73

Научный руководитель: Ключарев Петр Георгиевич, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э.Баумана, канд. техн. наук, pgkl@yandex.ru

Bots detection in the Twitter online social network using «Random Forest» machine learning algorithm

Khachatrian M. G.[80]

The study discusses the possibility of using the «Random Forest» machine learning algorithm to detect bots in social network «Twitter». The purpose of the study is to quantify the accuracy of bot detection. The algorithm was tested by cross-validation through ten blocks on a sample of several thousand Twitter accounts, consisting of both real users and different types of bots. The result of the testing is 0.982 of F_1-metric. This result is a fairly high indicator of the accuracy of bot detection compared to most previous works on the detection of bots in the online social network Twitter.

Keywords: decision trees, cross-validation, social networks, bots.

[80] Khachatrian Mikael Gagikovich, Bauman Moscow State Technical University, 5019973@mail.ru

УДК 004.056.55

EVHEN 2.0. Новая схема быстрого асимметричного шифрования и цифровой подписи на публичном ключе

Щелкунов Д.А.[81] , Чиликов А.А.[82]

Аннотация

Описывается разработанный авторами подход к созданию схемы высокоскоростного асимметричного шифрования и цифровой подписи на публичном ключе на базе механизмов white-box-криптографии.

Ключевые слова: асимметричная криптография, white-box-криптография, обфускация, цифровая подпись

Введение

В связи с развитием облачных технологий, Интернета вещей и общим ростом скорости Интернет-коммуникаций, а также объёмов и качества передаваемой по сети информации актуализируются угрозы информационной безопасности информационных систем.

В частности часто бывает необходимо шифровать данные с высокой скоростью (например, данные телеметрии) на публичном ключе. Существующие асимметричные алгоритмы шифрования либо недостаточно производительны, либо в принципе не позволяют осуществлять полноценное шифрование (только подпись).

Существовал ряд попыток создать быстрые асимметричные шифры на базе симметричных посредством механизмов white-box-криптографии. Однако на текущий момент не существует стойких white-box-реализаций, позволяющих заменить ими алгоритмы асимметричного шифрования.

Разработанный алгоритм позволяет осуществлять шифрование на публичном ключе со сложностью $O(n)$, благодаря использованию табличных вычислений. Сложность расшифрования с использованием приватного ключа составляет $O(n^3)$.

Перед дальнейшими рассуждениями введём ряд обозначений. $GF(2)$- поле Галуа размерностью 2. $GF(2^n)$- поле Галуа порядка 2^n(расширение поля$GF(2)$). $s_i(x_i)$- инъективное таблично заданное преобразование следующего вида:$s_i(x_i)\colon x_i^{(t)} \to z_i^{(k)}$, где t и k соответственно размерность входного и выходного векторов. $F_i^j(x)$- функция, заданная таблично, осуществляющая преобразование следующего вида: $F_i^j(x)\colon x_i^{(k)} \to \left(\beta_i^j\right)^{(h)}$, где kи $h = \frac{v}{2}$соответственно размерность входного и выходного векторов. Операция $q \cdot m$означает умножение двух полиномов над$GF(2)$.M_i^j- квадратная обратимая матрица над$GF(2)$, а операция$M \times a$означает умножение квадратной обратимой матрицы M размерности$k \times k$на вектор a размерности k из векторного пространства над$GF(2)$

Рассмотрим систему следующего вида:

$$\begin{cases} y_0^i = M_0^i \times s_i(x_i) + \lambda_0 \cdot F_0^i(x_i) \\ y_1^i = M_1^i \times s_i(x_i) + \lambda_1 \cdot F_1^i(x_i) \\ \dots \\ y_{n-1}^i = M_{n-1}^i \times s_i(x_i) + \lambda_{n-1} \cdot F_{n-1}^i(x_i) \end{cases} \quad (1)$$

В каждом из уравнений системы (1) входной векторx_i размерности t подвергается нелинейному инъективному преобразованию$s_i(x_i)\colon x^{(t)} \to z^{(k)}$, умножается на обратимую матрицуM_i^j, а затем складывается в векторном пространстве над$GF(2)$с произведением

81 Щелкунов Дмитрий Анатольевич, к.т.н., КФ МГТУ имени Н.Э. Баумана, г. Калуга, d.schelkunov@gmail.com

82 Чиликов Алексей Анатольевич, к. ф.-м.н., Московский Государственный Технический Университет им. Н. Э. Баумана, факультет Информатика и системы управления, кафедра ИУ-8 Информационная безопасность; Московский Физико-Технический Институт, факультет инноваций и высоких технологий, лаборатория продвинутой комбинаторики и сетевых приложений; Passware, Research Department;Москва, chilikov@passware.com

случайно выбранного полиномаλ^jразмерности hи однонаправленной функции. $F_i^j(x): x_i^{(k)} \to \left(\beta_i^j\right)^{(h)}$При этом соблюдается следующее соотношение размеров векторов:

$$t \le k < \frac{1}{2}v \qquad (2)$$

Из системы (1) очевидно, что между заданными таблично функциями$y_0^i, y_1^i \dots y_{n-1}^i$существует линейная зависимость, замаскированная суммами с произведениями вида $\lambda_j \cdot F_j^i(x_i)$. Как будет показано ниже, при правильном выборе параметров описываемой системы и неизвестности функций$s_i(x_i)$ и$F_j^i(x_i)$ сложность установления линейной зависимости между векторами$y_0^i, y_1^i \dots y_{n-1}^i$составляет$O(2^v)$. Т.е. нахождение вышеуказанной линейной зависимости при корректно выбранных параметрах является сложной задачей, что может быть использовано для построения алгоритмов асимметричного шифрования.

Шифрование

Рассмотрим пример алгоритма шифрования. Шифрование осуществляется поблочно. Размер блока *l* байт. Каждый блок делится на$n = \frac{l}{t}$входных векторов. При этом l кратно *t*. Для каждого из n векторов сгенерирована своя собственная таблица подстановок$s_i(x_i): x_i^{(t)} \to z_i^{(k)}, i \in [0, n-1], k \ge t$. Этот набор таблиц подстановок является секретом. Сгенерируем MDS-матрицу$H^{n\times n}$, элементами которой будут обратимые подматрицы $M^{k\times k}$. Таким образом матрица$H^{n\times n}$является блочной и выглядит следующим образом:

$$\begin{matrix} M_0^0 & M_0^1 & \dots & M_0^{n-1} \\ M_1^0 & M_1^1 & \dots & M_1^{n-1} \\ \dots & \dots & \dots & \dots \\ M_{n-1}^0 & M_{n-1}^1 & \dots & M_{n-1}^{n-1} \end{matrix} \qquad (3)$$

Шифрование осуществляется посредством умножения матрицы$H^{n\times n}$на вектор-результат подстановок$s_i(x_i)$, как видно из формулы ниже:

$$\begin{bmatrix} M_0^0 & M_0^1 & \dots & M_0^{n-1} \\ M_1^0 & M_1^1 & \dots & M_1^{n-1} \\ \dots & \dots & \dots & \dots \\ M_{n-1}^0 & M_{n-1}^1 & \dots & M_{n-1}^{n-1} \end{bmatrix} \times \begin{bmatrix} s_0(x_0) \\ s_1(x_1) \\ \dots \\ s_{n-1}(x_{n-1}) \end{bmatrix} = \begin{bmatrix} M_0^0 \times s_0(x_0) + \dots + M_0^{n-1} \times s_{n-1}(x_{n-1}) \\ M_1^0 \times s_0(x_0) + \dots + M_1^{n-1} \times s_{n-1}(x_{n-1}) \\ \dots \\ M_{n-1}^0 \times s_0(x_0) + \dots + M_{n-1}^{n-1} \times s_{n-1}(x_{n-1}) \end{bmatrix} \qquad (4)$$

Произведение (4) сводится к следующей сумме векторов:

$$\begin{bmatrix} M_0^0 \times s_0(x_0) \\ M_1^0 \times s_0(x_0) \\ \dots \\ M_{n-1}^0 \times s_0(x_0) \end{bmatrix} + \dots + \begin{bmatrix} M_0^{n-1} \times s_{n-1}(x_{n-1}) \\ M_1^{n-1} \times s_{n-1}(x_{n-1}) \\ \dots \\ M_{n-1}^{n-1} \times s_{n-1}(x_{n-1}) \end{bmatrix} \qquad (5)$$

Каждое слагаемое в сумме (5) будем называть *T-box*-ом. Очевидно, что между элементами каждого из *T-box*-ов существует линейная зависимость над *GF(2)*. Добавив к каждому из *T-box*-ов маскирующие преобразования, описанные в системе (1), получим следующую формулу:

$$\begin{bmatrix} M_0^0 \times s_0(x_0) + \lambda_0 \cdot F_0^0(x_0) \\ M_1^0 \times s_0(x_0) + \lambda_1 \cdot F_1^0(x_0) \\ \dots \\ M_{n-1}^0 \times s_0(x_0) + \lambda_{n-1} \cdot F_{n-1}^0(x_0) \end{bmatrix} + \dots + \begin{bmatrix} M_0^{n-1} \times s_{n-1}(x_{n-1}) + \lambda_0 \cdot F_0^{n-1}(x_{n-1}) \\ M_1^{n-1} \times s_{n-1}(x_{n-1}) + \lambda_1 \cdot F_1^{n-1}(x_{n-1}) \\ \dots \\ M_{n-1}^{n-1} \times s_{n-1}(x_{n-1}) + \lambda_{n-1} \cdot F_{n-1}^{n-1}(x_{n-1}) \end{bmatrix} \qquad (6)$$

В формуле (6) мы видим модифицированные *T-box*-ы, заданные таблично, как функции от x_i. Если функции функции$s_i(x_i)$ и$F_i^j(x_i)$, а также полиномыλ_iвыбраны корректно, то восстановить линейную зависимость между элементами таким *T-box*-ов является сложной задачей. Такие *T-box*-ы являются публичным ключом алгоритма.

Расшифрование

Как очевидно из системы (6), результатом шифрования будут *n* векторов размером *v* каждый, система которых будет выглядеть следующим образом:

$$\begin{cases} \hat{z_0} = \left(M_0^0 \times s_0(x_0) + \ldots + M_0^{n-1} \times s_{n-1}(x_{n-1})\right) + \lambda_0 \cdot \left(F_0^0(x_0) + \ldots + F_0^{n-1}(x_{n-1})\right) \\ \hat{z_1} = \left(M_1^0 \times s_0(x_0) + \ldots + M_1^{n-1} \times s_{n-1}(x_{n-1})\right) + \lambda_1 \cdot \left(F_1^0(x_0) + \ldots + F_1^{n-1}(x_{n-1})\right) \\ \ldots \\ \hat{z_{n-1}} = \left(M_{n-1}^0 \times s_0(x_0) + \ldots + M_{n-1}^{n-1} \times s_{n-1}(x_{n-1})\right) + \lambda_{n-1} \cdot \left(F_{n-1}^0(x_0) + \ldots + F_{n-1}^{n-1}(x_{n-1})\right) \end{cases}$$

(7)

Для расшифрования необходимо редуцировать систему (7). Для этого возьмём остаток от деления каждого из векторов $\hat{z_i}$на соответствующий ему полином λ_i. В результате получим редуцированную систему векторов следующего вида:

$$\begin{cases} z_0' = M_0^0 \times s_0(x_0) + \ldots + M_0^{n-1} \times s_{n-1}(x_{n-1}) \\ z_1' = M_1^0 \times s_0(x_0) + \ldots + M_1^{n-1} \times s_{n-1}(x_{n-1}) \\ \ldots \\ z_{n-1}' = M_{n-1}^0 \times s_0(x_0) + \ldots + M_{n-1}^{n-1} \times s_{n-1}(x_{n-1}) \end{cases}$$

(8)

В матричной форме система (8) будет выглядеть следующим образом:

$$Z' = M \times S(x) \qquad (9)$$

Умножим выражение (9) на матрицу *H*, обратную матрице *M*, получив таким образом образом следующую систему:

$$\begin{cases} z_0 = s_0(x_0) \\ z_1 = s_1(x_1) \\ \ldots \\ z_{n-1} = s_{n-1}(x_{n-1}) \end{cases} \qquad (10)$$

Теперь применим к векторам системы (10) преобразования $g_i(s_i(x_i) = z_i)$: $s_i(x_i)^{(k)} \to x_i^{(t)}$, отменяющие преобразования $s_i(x_i)$.

Параметры системы шифрования

Ключевым моментом, определяющим стойкость описанной выше системы шифрования, являются параметры *t, k, v*, а также структура преобразований $s_i(x_i)$и $F_i^j(x_i)$. Идеальным вариантом для преобразований $s_i(x_i)$и $F_i^j(x_i)$являлось бы отсутствие линейных комбинаций следующего вида:

$$\exists a_i^j \neq 0, a_i^j \in GF(2), \sum_{j=0}^{t-1} \sum_{i=0}^{n-1} a_i^j \cdot s_i\left(x_i^j\right) = 0 \qquad (11)$$

$$\exists a_i^j \neq 0, a_i^j \in GF(2), \sum_{i=0, j=0}^{n-1} a_i^j \cdot F_i^j(x_i) = 0 \qquad (12)$$

Предположим, что равенство (12) не выполняется. В этом случае множество значений функций $F_i^j(x_i)$должно быть базисом векторного пространства размерностью $2^{(t \cdot n)^2}$. Т.е. при минимальном *t* размером 4 бита и декларируемой корневой стойкости 128 бит мы получим векторное пространство размерностью 2^{65536}, что делает описанную систему сложно применимой на практике.

Предположим, что при определённых коэффициентах a_i^jвыполняется равенство (11). В этом случае мы получим набор выражений следующего вида:

$$\sum_{j=0}^{t-1} \sum_{i=0}^{n-1} a_i^j \cdot \left(\lambda_c \cdot F_c^j\left(x_i^j\right)\right) = \alpha_c \qquad (13)$$

В равенстве (13) *c* – некоторое фиксированное целое число (номер строки из суммы (6)). Очевидно, что из равенства (13) можно получить следующее равенство:

$$\lambda_c \cdot \sum_{j=0}^{t-1} \sum_{i=0}^{n-1} a_i^j \cdot F_c^j\left(x_i^j\right) = \alpha_c \qquad (14)$$

Таким образом, разложив α_cна множители, мы сможем вычислить λ_c. Вычислив все λ_cдля $c = 0 \ldots n-1$, мы сможем получить *T-box*-ы из суммы (5) и в дальнейшем достаточно установить линейные зависимости между коэффициентами *T-box*-ов, вычислить обратную матрицу, а следовательно, получить приватный ключ шифрования, взломав таким образом вышеописанную систему. Основной задачей для успешного взлома

данным способом является установление зависимости (14). Иначе говоря, необходимо доподлинно убедиться, что равенство (11) выполнено. В противном случае вместо равенства (14) мы получим следующее выражение:

$$\lambda_c \cdot \left(\sum_{j=0}^{t-1}\sum_{i=0}^{n-1} a_i^j \cdot F_c^j\left(x_i^j\right)\right) + e_c = \alpha_c \qquad (15)$$

Т.к. мы не знаем значения e_cи не знаем, выполняется ли равенство (11) (каких-либо маркеров его выполнения при наличии только описанных выше наборов *T-box*-ов у нас нет), мы не можем достоверно утверждать, что в результате разложения α_cна множители мы получаем именно λ_c, а не некоторое другое значение $\hat{\lambda_c}$. Убедиться в том, что $e_c = 0$и $\hat{\lambda_c} = \lambda_c$, мы можем только проверив, является ли редуцированный по модулю $\hat{\lambda_c}c$-й элемент *T-box*-а помноженным на некоторый коэффициент матрицы *M s-box*-ом. Для этого нам необходимо, предположив, что $\hat{\lambda_c} = \lambda_c$и перебрав коэффициенты матрицы *M* для следующего элемента *T-box*-а (ещё не редуцированного, т. к. мы нашли предполагаемый λ_cтолько для *c*-го элемента *T-box*-а), вычислить $\lambda_{c+1(\hat{mod}n)}$и попытаться проверить наличие линейной зависимости во всех остальных *T-box*-ах. Для нахождения $\hat{\lambda_c} = \lambda_c$в случае выполнения равенства (11) необходимо перебрать $n \cdot tk$-значных значений. Таким образом сложность взлома таким способом составит $2^{n \cdot k \cdot t}$. При *t*=4, *k*=16, *n*=64 мы получим величину 2^{4096}, что значительно превышает корневую сложность 2^{128}для тех же параметров.

Предположим, что равенство (12) выполняется для каких-либо a_i^j. В этом случае рассуждения аналогичны предыдущим для равенства (11). Также как и в случае равенства (11) основной задачей является выявление параметров a_i^j. Не стоит забывать того факта, что аналитику не доступны функции $F_i^j(x_i)$в чистом виде. Элементы *T-box*-ов «замаскированы» суммой с преобразованиями вида $M_j^i \times s_i(x_i)$. Предположим, что удалось найти выражение следующего вида:

$$\sum_{i=0,j=0}^{n-1} a_i^j \cdot T_i^j\left(x_j\right) = d^{(k)} \qquad (16)$$

В формуле (16) $T_i^j\left(x_j\right) = M_i^j \times s_j\left(x_j\right) + \lambda_i \cdot F_i^j\left(x_j\right)$- *i*-й элемент *j*-го *T-box*-а, а $d^{(k)}$- вектор размерности *k* (старшие $v - k$бит вектора равны 0). Иными словами вектор $d^{(k)}$достаточно мал по сравнению с векторами T_i^j. В этом случае формула (16) сводится к следующему виду:

$$\sum_{i=0,j=0}^{n-1} a_i^j \cdot \left(M_i^j \times s_j\left(x_j\right) + \lambda_i \cdot F_i^j\left(x_j\right)\right) = d^{(k)} \qquad (17)$$

Обозначим $low_k\left(\lambda_i \cdot F_i^j\left(x_j\right)\right)$вектор размерностью *v*, младшие *k* бит которого взяты из произведения $\lambda_i \cdot F_i^j\left(x_j\right)$, а старшие $v - k$бит равны 0. Обозначим $high_k\left(\lambda_i \cdot F_i^j\left(x_j\right)\right)$вектор размерностью *v*, младшие *k* бит которого равны 0, а старшие $v - k$бит взяты из произведения $\lambda_i \cdot F_i^j\left(x_j\right)$. Тогда формула (17) может быть представлена следующим образом:

$$\sum_{i=0,j=0}^{n-1} a_i^j \cdot \left(M_i^j \times s_j\left(x_j\right) + low_k\left(\lambda_i \cdot F_i^j\left(x_j\right)\right) + high_k\left(\lambda_i \cdot F_i^j\left(x_j\right)\right)\right) = d^{(k)} \qquad (18)$$

Из равенства (18) очевидно, что младшие *k* бит «замаскированы» суммой с преобразованиями вида $M_i^j \times s_j\left(x_j\right)$. Т.е. выполнение равенства (18) не означает, что выполняется равенство (12) и нахождение маленьких векторов решётки, образованной векторами $T_i^j\left(x_j\right)$не несёт практического смысла.

Предположим, например, аналитику удалось найти маленький вектор $d^{(k)}$в решётке, образованной всеми значениями *i*-го элемента *j*-го *T-box*-а для фиксированных *i* и *j*. Без потери общности будем считать *i*=*j*=0 и возьмём все *t* значений 0-го элемента 0-го *T-box*-а. Предположим, аналитику удалось найти маленький вектор $d^{(k)}$в решётке этих значений, размер которых составляет *v* бит. Это даст нам следующее равенство:

$$\sum_{i=0}^{t-1} a_i \cdot \left(M_0^0 \times s_0(i) + low_k\left(\lambda_0 \cdot F_0^0(i)\right) + high_k\left(\lambda_0 \cdot F_0^0(i)\right)\right) = d^{(k)} \quad (19)$$

Очевидно, что равенство (19) является частным случаем равенства (18) и, исходя из рассуждений, приведённых выше для равенства (18), нахождение маленького вектора $d^{(k)}$не несёт практического смысла.

В силу вышеизложенного мы допускаем выполнение равенства (12) и вводим более слабые ограничения:

$$\forall c \in [0 \dots n-1], \sum_{j=0}^{t-1} a^j \cdot s_c\left(x_c^j\right) = 0 \Rightarrow a^j = 0, j \in [0, t-1] \quad (20)$$

Неравенство (20) говорит нам о том, что в множестве *T-box*-ов для одного *t*-битового входа не будет линейных зависимостей между значениями функции $s_c\left(x^{(t)}\right)$. Исходя из этого, для *t*=4 бита размер выхода функции$s_c\left(x^{(t)}\right)$не может быть меньше 16-и бит. Т.е. принимаем *k*=16.

Соотношение (2) говорит нам о том, что *v* не может быть меньше 33 бит. Принимаем *v*=34.

Из структуры схемы шифрования видно, что старшая часть элементов *T-box*-ов представляет собой $high_k\left(\lambda_i \cdot F_i^j\left(x_j\right)\right)$. При этом размер каждого из этих элементов составляет 34 бита. Для противодействия гипотетическим атакам на не замаскированную старшую часть увеличим размер каждого из элементов *T-box*-а до 64-х бит. Выделим в старших 47-и битах 30 произвольных позиций таким образом, что эти позиции будут совпадать для каждой из «строк» формулы (6) или для порядкового номера элемента *T-box*-а. В эти позиции поместим случайно выбранные значения. Это позволит замаскировать старшую часть $high_k\left(\lambda_i \cdot F_i^j\left(x_j\right)\right)$, т. к. аналитику неизвестны эти позиции. Т.к. операция сложения в формуле (6) подразумевает под собой сложение по модулю 2, биты в этих позициях не влияют на результат сложения других бит. При расшифровании мы учитываем эти позиции и редуцируем размер каждого из 64-х битовых векторов результат до 34-х бит посредством набора сдвигов, уникальных для каждого из 64-х битовых векторов. Вышеозначенные случайно выбранные биты назовём маскирующими битами. Исходные биты будем называть информационными. Операцию добавления маскирующих бит обозначим $Ex_i^j(x): x^{(v)} \to y^{(l)}$. В нашем случае *l=64*. Операцию извлечения информационных бит обозначим $Dex_i(x): x^{(l)} \to y^{(v)}$.

Предположим, аналитик имеет возможность узнать, является ли результат расшифрования валидным или нет. Очевидно, что при замене маскирующих бит результат расшифрования не изменится и останется валидным, т. к. их значения не учитываются в процессе расшифрования. Чтобы избежать этого, каждый из *l*-битных элементов *T-box*-а можно умножить на обратимую матрицу $L_i^{l \times l}$над $GF(2)$. При этом эти матрицы будут различаться для всех элементов одного *T-box*-а и будут идентичными для элементов *T-box*-ов, имеющих одинаковые позиции. Формально это будет выглядеть следующим образом:

$$\begin{bmatrix} L_0 \times Ex_0^0\left(M_0^0 \times s_0(x_0) + \lambda_0 \cdot F_0^0(x_0)\right) \\ L_1 \times Ex_1^0\left(M_1^0 \times s_0(x_0) + \lambda_1 \cdot F_1^0(x_0)\right) \\ \dots \\ L_{n-1} \times Ex_{n-1}^0\left(M_{n-1}^0 \times s_0(x_0) + \lambda_{n-1} \cdot F_{n-1}^0(x_0)\right) \end{bmatrix} + \dots$$

$$\dots + \begin{bmatrix} L_0 \times Ex_0^{n-1}\left(M_0^{n-1} \times s_{n-1}(x_{n-1}) + \lambda_0 \cdot F_0^{n-1}(x_{n-1})\right) \\ L_1 \times Ex_1^{n-1}\left(M_1^{n-1} \times s_{n-1}(x_{n-1}) + \lambda_1 \cdot F_1^{n-1}(x_{n-1})\right) \\ \dots \\ L_{n-1} \times Ex_{n-1}^{n-1}\left(M_{n-1}^{n-1} \times s_{n-1}(x_{n-1}) + \lambda_{n-1} \cdot F_{n-1}^{n-1}(x_{n-1})\right) \end{bmatrix} \quad (21)$$

Подобно формуле (6) *T-box*-ы в формуле (21) также задаются таблично. Для расшифрования, очевидно, перед редукцией по модулю λ_iнеобходимо умножить каждый элемент полученного в результате выполнения формулы (21) вектора на матрицу, обратную соответствующей матрице $L_i^{l\times l}$, а затем применить операцию Dex_i, чтобы исключить маскирующие биты и сформировать вектор, эквивалентный результату формулы (7).

Подпись с помощью EVHEN 2.0. Метод коллизий

Для дальнейших рассуждений введём несколько дополнительных обозначений. $Msg^{(N)}$- исходное сообщение длиной *N* бит. $Hash\left(Msg^{(N)}\right): Msg^{(N)} \rightarrow hash^{(l)}, N \geq l$- хэш-функция, трансформирующая сообщение длиной *N* бит в последовательность длиной *l* бит, где *l* – размер блока шифрования для EVHEN 2.0.

В схеме проверки подписи будут использоваться два открытых ключа: Pub_1иPub_2. Как было показано выше, открытым ключом является набор таблиц подстановок — *T-box*-ов. При формировании подписи будет использоваться набор параметров, который мы будем именовать закрытым ключом — *Priv*.

В процедуре формирования и проверки подписи участвуют Алиса и Боб. Чтобы подписать сообщение Алиса подсчитывает его хэш-сумму$Hash(Msg) = hash^{(l)}$. После этого, используя закрытый ключ, Алиса формирует последовательность бит $digest^{(l)}$такую, что $Pub_1\left(hash^{(l)}\right) = Pub_2\left(digest^{(l)}\right)$. После этого Алиса отправляет Бобу следующую последовательность: $Msg|digest^{(l)}$, где | - операция конкатенации.

Для проверки подписи Боб подсчитывает $Pub_1\left(Hash(Msg)\right)$ и сравнивает результат с $Pub_2\left(digest^{(l)}\right)$. Если результаты равны, то проверка подписи считается пройденной успешно.

Такой подход к формированию и проверке электронной подписи мы называем ***Методом коллизий***. Сложность взлома определяется сложностью формирования последовательности $digest^{(l)}$, такой, что $Pub_1\left(hash^{(l)}\right) = Pub_2\left(digest^{(l)}\right)$ при известных $hash^{(l)}$и двух наборов *T-box*-ов — открытых ключейPub_1иPub_2.

Опишем принцип построения открытых ключей Pub_1иPub_2. В первую очередь сгенерируем ключевую пару *Priv* и Pub_1, как описано в предыдущих пунктах настоящей работы. Напомним, что открытый ключ — это набор таблично заданных функций — *T-box*-ов ($T_i, i \in [0, \ldots, n-1]$).

Для создания открытого ключа Pub_2введём нелинейное биективное отображение $v_i(x_i): x_i^{(t)} \rightarrow x'^{(t)}_i$.

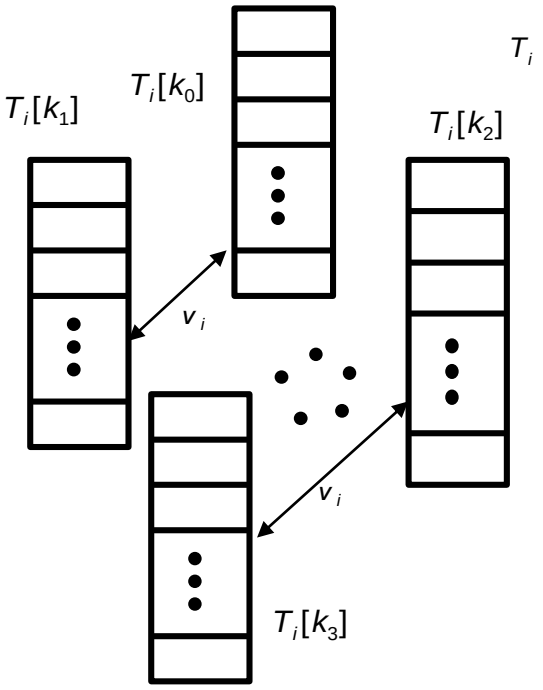


Рисунок 1. «Перемешивание» *T-box*-а посредством $v_i(s_i)$

Отображение $v_i(x_i)$, по сути, «перемешивает» элементы каждой из таблиц подстановокT_i между собой уникальным для каждой из этих таблиц способом. Можно считать, что перед *s-box*-ами из (1) применяется ещё одна нелинейная подстановка. Получим таким образом набор модифицированных *T-box*-ов ($T'_i, i \in [0, \dots, n-1]$).

Просуммируем каждый из модифицированных на предыдущем шаге *T-box*-ов с соответствующим ему вектором $MASK_i, i \in [0, \dots, n-1]$. Напомним, что результата применения каждого из *T-box*-ов можно представить в виде вектора размерности *n*, координатами которого являются двоичные векторы размерности *v*. Маскирующие линейные преобразования $MASK_i$также являются векторами размерности *n*, координатами которых являются двоичные векторы размерности *v*. Фактически, вектор $MASK_i$, как и вектор $T'_i[k], k \in [0, \dots, t]$ принадлежит векторному пространству размерности n над векторным пространством размерности *v*. Операция сложения векторов осуществляется покоординатно, а каждая из координат одного вектора складывается с соответствующей ей координатой другого вектора по модулю 2.

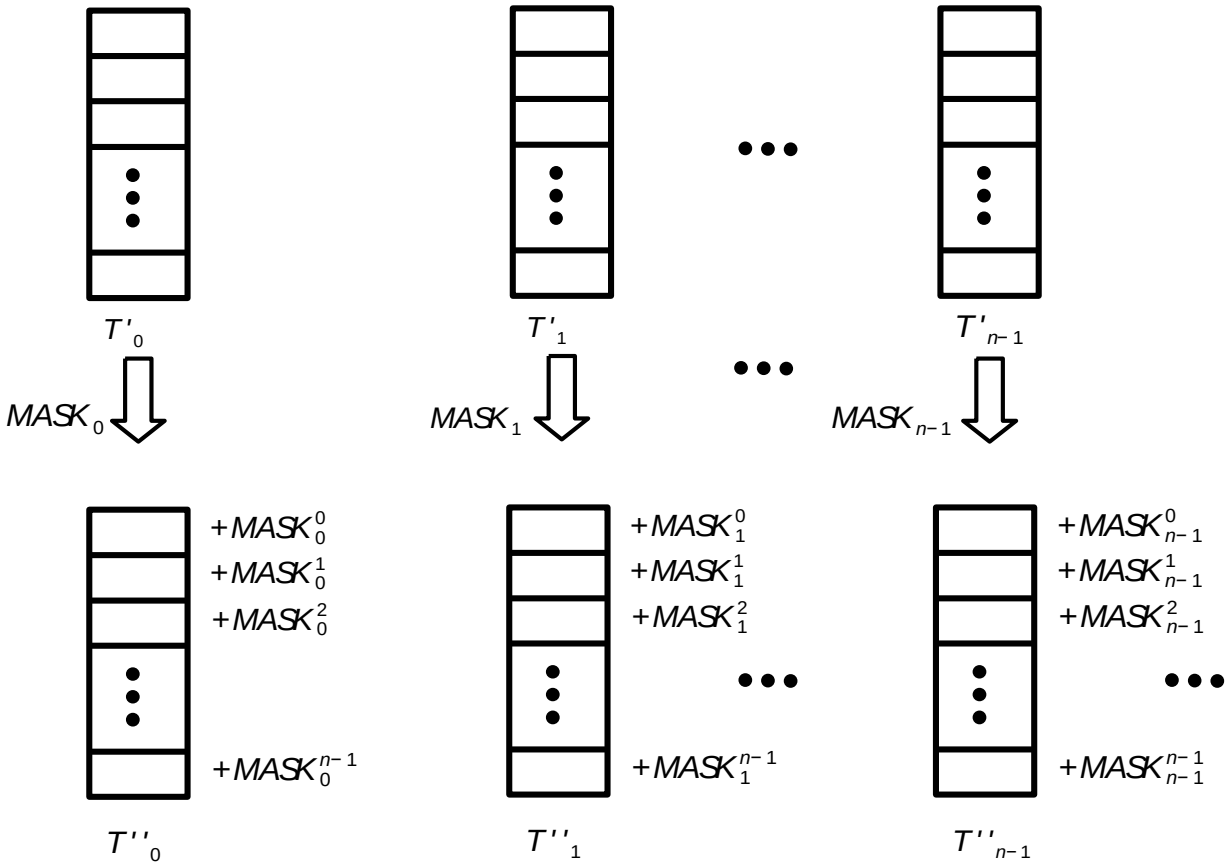


Рисунок 2. Применение линейных маскирующих преобразований$MASK_i$по отношению к *T-box*-ам

Визуально сложение с$MASK_i$показано на рисунке 2. Напомним, что T'_i (впрочем, как и T_i) - это множество, состоящее из k векторов. Операция сложения с $MASK_i$ подразумевает сложение каждого из этих векторов с $MASK_i$. Основное требование к преобразованиям $MASK_i$ заключается в следующем:

$$\sum_{i=0}^{n-1} MASK_i = 0 \qquad (22)$$

Полученные в результате сложения с $MASK_i$*T-box*-ы обозначим T''_i.

На следующем этапе перемешаем полученные *T-box*-ы между собой.

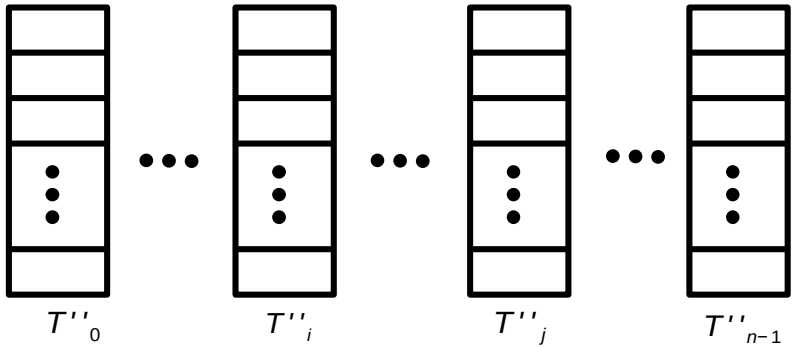


Рисунок 3. Перемешивание *T-box*-ов

Пример такого перемешивания изображён на рисунке 3. По сути, данная операция осуществляет перемешивание индексов *T-box*-ов. Например, 0-й координате входного

вектора будет соответствовать не T''_0, как до операции, а T''_j. Полученные в результате наборы *T-box*-ов обозначим $T'''_i, i \in [0, \ldots, n-1]$. Данное обратимое преобразование обозначим *TMIX*.

Следующее преобразование заключается в том, что отдельные элементы из разных *T-box*-ов меняются местами друг с другом. Пусть $[index, value]$ - пара значений, первое из которых — индекс таблицы подстановок (соответствующего *T-box*-а), второе — значение, передаваемое этому *T-box*-у. Иными словами, пара $[index, value]$ однозначно определяет$T'''_{index}[value]$. Множество *IVSET* – упорядоченное множество всех возможных пар $[index, value]$. Упорядочивание осуществляется в первую очередь по возрастанию значения *index*, во вторую — по возрастанию значения *value* (пары с одинаковым значением *index* сортируются по возрастанию значения *value*). Введём перестановку множества *IVSET* и обозначим её $SUBST(IVSET)$. В результате этой перестановки, например, пара $[i, k]$ переместится на место пары $[j, k]$, а пара $[j, k]$, в свою очередь, переместится на место пары $[l, k]$и т. д. Таким образом перестановка $SUBST(IVSET)$ формирует новый набор *T-box*-ов.

На рисунке 4 показан визуально показан пример одного из таких перемещений. Полученные в результате такой перестановки *T-box*-ы обозначим $T''''_i, i \in [0, \ldots, n-1]$.

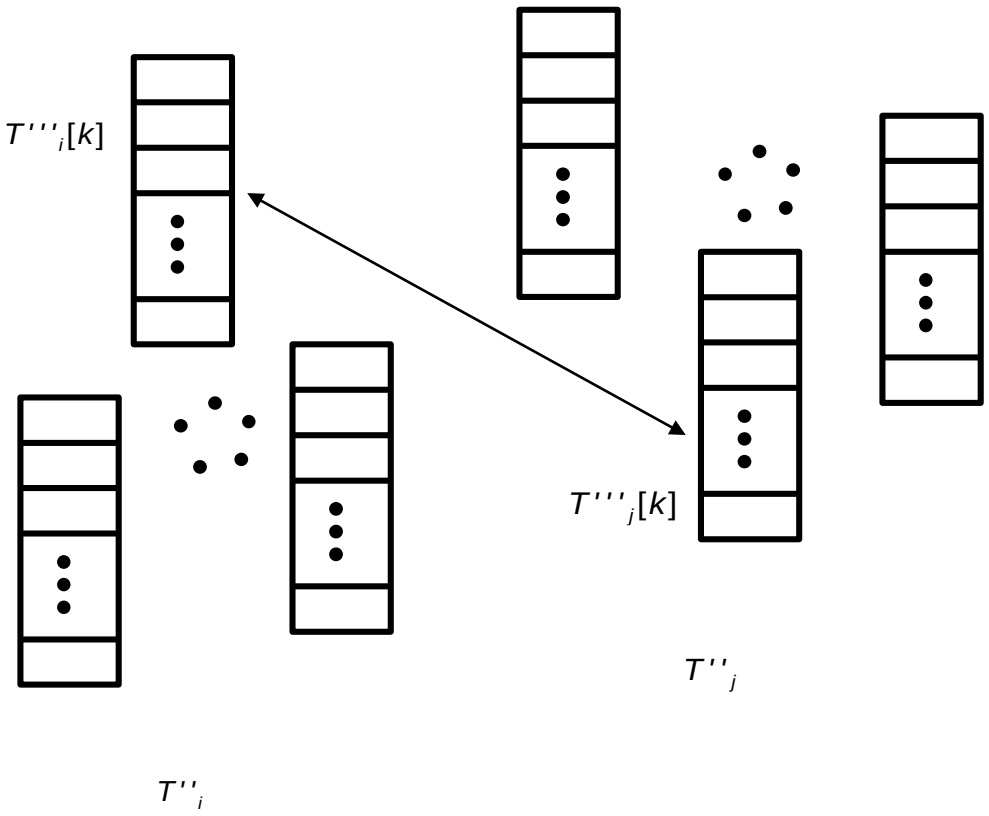


Рисунок 4. «Перемещение» элемента *T-box*-а

Последним из преобразований при формировании открытого ключа Pub_2 будет объединение нескольких *T-box*-ов в один, как показано на рисунке 5.

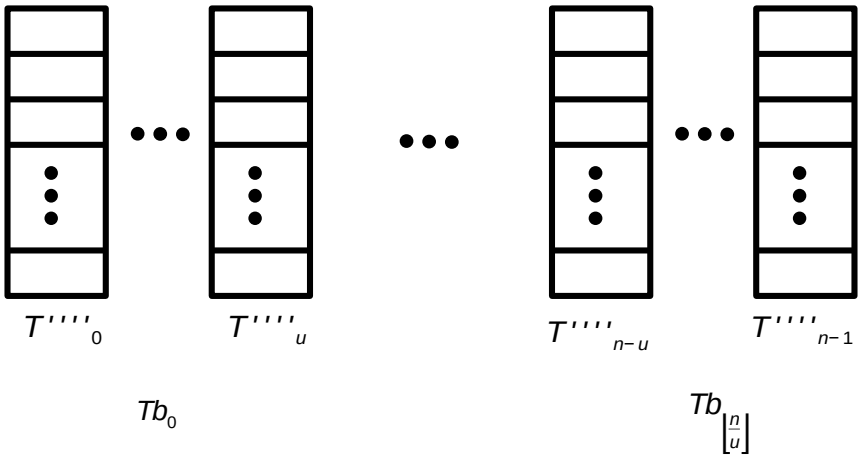


Рисунок 5. Объединение *T-box*-ов

Это преобразование мы назовём *JOIN*. Как видно из рисунка, оно объединяет u соседних *T-box*-а в один. Очевидно, что полученные в результате *T-box*-ы $Tb_{0,\dots}, Tb_{\lfloor \frac{n}{u} \rfloor}$получают на вход $k \cdot u$ бит. Они и будут являться вторым открытым ключом Pub_2. При это секретными параметрами являются: ключ $Priv_1$, множество биективных отображений $\nu_i, i \in [0, \dots, n-1]$, обратимое преобразование *TMIX*, обратимая перестановка *SUBST*.

Приведём алгоритм построения последовательности $digest^{(l)}$, зная секретные параметры и исходную последовательность $hash$.

Пусть ν_i^{-1} - набор преобразований, обратных соответствующим ν_i. Применив покоординатоно преобразования ν_i^{-1} к вектору $hash$ (последовательность $hash$ можно представить, как вектор размерности *n*, координатами которого являются *t*-битные числа). В результате получим вектор $hash'$.

Применим преобразование *TMIX,* которое суть есть перемешивание индексов *T-box*-ов, по отношению к вектору $hash'$, перемешав таким образом его координаты. В результате получим вектор $hash''$.

Теперь нам осталось учесть преобразование *SUBST*, которое, как было сказано выше, перемешивает элементы *T-box*-ов (векторы-значения) с разными индексами, но с одинаковыми входными значениями. Для каждой из *l* координат вектора $hash''$мы глядим, был ли перемещён соответствующий значению этой координаты вектор *T-box*-а и, если да, то на какую позицию (координату). На эту новую позицию мы помещаем это значение в результирующий вектор $digest^{(l)}$.

Совершенно очевидно, что $Pub_2\left(digest^{(l)}\right)$ будет равен $Pub_1\left(hash^{(l)}\right)$ по построению.

Литература

1. S. Chow, P. Eisen, H. Johnson, P.C. van Oorschot, A White-Box DES Implementation for DRM Applications, 2002.
2. S. Chow, P. Eisen, H. Johnson, P.C. van Oorschot, White Box Cryptography and an AES Implementation, 2002.
3. Julien Bringer, Herve Chabanne, Emmanuelle Dottax, White Box Cryptography: Another Attempt, 2006.
4. Hamilton E. Link, William D. Neumann, Clarifying Obfuscation: Improving the Security of White-Box Encoding.
5. B. Wyseur, "White-Box Cryptography," PhD thesis, Katholieke Universiteit Leuven, B. Preneel (promotor), 169+32 pages, 2009. URL: http://www.cosic.esat.kuleuven.be/publications/thesis-152.pdf

6. Щелкунов Д.А. О практическом применении White-Box криптографии., // Международная конференция РусКрипто, 2009.
7. Щелкунов Д.А. Разработка методик защиты программ от анализа и модификации на основе запутывания кода и данных, Диссертация на соискание ученой степени кандидата технических наук, Мазин А.В. (научный руководитель), 126+18 стр, 2009.
8. Щелкунов Д.А. White-Box криптография, обфускация и защита ПО. Основные направления развития., // Международная конференция РусКрипто, 2010.
9. Dmitry Schelkunov. White-Box Cryptography and SPN ciphers. LRC method. URL: http://eprint.iacr.org/2010/419
10. Щелкунов Д.А. Асимметричный SPN-шифр на базе white-box-криптографии и хаотических отображений., // Международная конференция РусКрипто, 2017.
11. Чиликов А.А. Анализ стойкости криптосистемы EVHEN 1.0. // Безопасные информационные технологии. Сборник трудов Восьмой Всероссийской научно-практической конференции \ Москва: Издательство: МГТУ им. Баумана – 2017.
12. Щелкунов Д.А., Чиликов А.А. EVHEN 2.0. Высокоскоростное асимметричное шифрование на публичном ключе. // Безопасные информационные технологии. Сборник трудов Восьмой Всероссийской научно-практической конференции \ Москва: Издательство: МГТУ им. Баумана – 2017.
13. Щелкунов Д.А., Чиликов А.А. О высокоскоростном асимметричном шифровании на публичном ключе на базе white-box-криптографии. // Международная конференция РусКрипто, 2018.

Schelkunov D.A.[83] , Chilikov A.A.[84]

Abstract
In this work we describe a new approach to fast asymmetric encryption and digital signatture. This method is based on the white-box cryptography.
Keywords: asymmetric cryptography, white-box cryptography, obfuscation

83 Щелкунов Дмитрий Анатольевич, к.т.н., КФ МГТУ имени Н.Э. Баумана, г. Калуга, d.schelkunov@gmail.com
84 Чиликов Алексей Анатольевич, к. ф.-м.н., Московский Государственный Технический Университет им. Н. Э. Баумана, факультет Информатика и системы управления, кафедра ИУ-8 Информационная безопасность; Московский Физико-Технический Институт, факультет инноваций и высоких технологий, лаборатория продвинутой комбинаторики и сетевых приложений; Passware, Research Department;Москва, chilikov@passware.com

УДК 004.056:519.237

Определение количества информации по Шеннону в дискретном канале связи с аддитивным шумом

Якубов Р.Ж.[85]

Данная работа посвящена исследованию дискретных каналов передачи данных с аддитивным шумом и вопросу применения к ним статистической меры, известной как информация по Шеннону. Представлена математическая модель канала связи. Также предложены определения информации по Шеннону и энтропии. Приведены некоторые математические выкладки, позволяющие оценить количество информации, передаваемого в одном информационном сообщении. Кроме того, заложена база для дальнейшей работы с двумерными каналами связи. Результаты работы могут применяться при построении систем передачи данных.

Ключевые слова: информация, энтропия, канал передачи, статистика, компьютерное моделирование.

Введение

Данная работа является логическим продолжением [1] – [5], посвященным задаче распознавания дискретного сигнала в аддитивном шуме[6]-[11]. Одной из характеристик канала связи является количество информации по Шеннону. Данное понятие является частью теории передачи информации, которая фактически является теорией статистических мер информации в каналах связи. При этом основные ее критерии – это сохранение передаваемой информации от искажений и оптимизация пропускной способности каналов связи.

Модель канала передачи

Объектом исследования является дискретный канал связи, содержащий аддитивный шум. Для проведения работы предлагается использовать его математическую модель (1):

$$y = \frac{a}{2}\eta + \varepsilon \quad (1)$$

$$\eta = \begin{cases} 1, \text{с вероятностью } P = 0{,}5 \\ -1, \text{с вероятностью } P = 0{,}5 \end{cases}$$

Шум в каналах связи моделируется случайными величинами $\varepsilon \sim N(0, \sigma_\varepsilon^2)$

$a = |m_1 - m_{-1}|$ – амплитуда полезного сигнала в канале y.

$P\left(y/\eta = 1\right)$, $P\left(y/\eta = -1\right)$ подчинены нормальному закону с параметрами $N(m_1, \sigma_\varepsilon^2)$ и $N\ (m_{-1}, \sigma_\varepsilon^2)$.

В данной модели возможно два сообщения: $\eta = 1, \eta = -1$, соответствующие логическим «1» и «0», соответственно.

Определение количества информации и значения энтропии

В соответствии с источником [10], количество информации в канале связи y (1) можно выразить, как:

$$I(\eta, y) = H(y) - H(y/\eta) \quad (2)$$

$$H(y) = \int_{-\infty}^{\infty} f(y) \log\big(f(y)\big)\, dy, \quad (3)$$

[85] Якубов Р. Ж., аспирант кафедры ИУ8 МГТУ им. Н.Э. Баумана, Москва, yakubov_rustam@inbox.ru

где $f(y)-$ плотность функции распределения случайной величины, описывающей канал y.

Поскольку $\eta = \begin{cases} 1, \text{с вероятностью } P = 0{,}5 \\ -1, \text{с вероятностью } P = 0{,}5 \end{cases}$, для канала (4) плотность функции распределения представляется следующим образом:

$$\begin{aligned} f(y) &= \frac{1}{2} f\left({}^{y}/_{\eta = 1}\right) + \frac{1}{2} f\left({}^{y}/_{\eta = -1}\right) \\ &= \frac{1}{2}\frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{\left(x-\frac{a}{2}\right)^2}{2\sigma^2}} + \frac{1}{2}\frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{\left(x+\frac{a}{2}\right)^2}{2\sigma^2}} \\ &= \frac{1}{2\sigma\sqrt{2\pi}}\left(e^{-\frac{\left(x-\frac{a}{2}\right)^2}{2\sigma^2}} + e^{-\frac{\left(x+\frac{a}{2}\right)^2}{2\sigma^2}} \right) \end{aligned} \tag{4}$$

Подставив это значение в $H(y)$, получим, что

$$\begin{aligned} H(y) = \int_{-\infty}^{\infty} & \frac{1}{2\sigma\sqrt{2\pi}} e^{-\frac{\left(y+\frac{a}{2}\right)^2}{2\sigma^2}} \left(e^{\frac{ay}{\sigma^2}} + 1\right) \left(\log\left(\frac{1}{2\sigma\sqrt{2\pi}}\right) + \log\left(e^{-\frac{\left(y+\frac{a}{2}\right)^2}{2\sigma^2}} \right) \right. \\ & \left. + \log\left(e^{\frac{ay}{\sigma^2}} + 1\right) \right) dy \\ = 1 &- \frac{1}{2}\log e - \frac{a^2}{2\sigma\sqrt{2}}\log e \\ - \int_{-\infty}^{\infty} & \frac{1}{2\sigma\sqrt{2\pi}} e^{-\frac{\left(y+\frac{a}{2}\right)^2}{2\sigma^2}} \left(e^{\frac{ay}{\sigma^2}} + 1\right) \log\left(e^{\frac{ay}{\sigma^2}} + 1\right) dy \end{aligned} \tag{5}$$

Выразим условную энтропию $H(y/\eta)$:

$$H\left({}^{y}/_{\eta}\right) = \sum_{j=1}^{2} p(\eta_j)\, H\left({}^{y}/_{\eta_j}\right) \tag{6}$$

$j = (1{:}\,2)$, т.к. случайная величина η принимает значения только логических «1» и «0». $H\left({}^{y}/_{\eta_j}\right)$ – энтропия, которая остается после того, как адресат принял сигнал с определенным значением η. $p(\eta_j) = 0.5$ Отсюда:

$$\begin{aligned} H\left({}^{y}/_{\eta}\right) &= -\frac{1}{2} H\left({}^{y}/_{\eta = -1}\right) - \frac{1}{2} H\left({}^{y}/_{\eta = 1}\right) \\ &= -\frac{1}{2} H\left(\frac{a}{2} + \varepsilon\right) - \frac{1}{2} H\left(-\frac{a}{2} + \varepsilon\right) \end{aligned} \tag{7}$$

$$H\left({}^{y}/_{\eta = 1}\right) = H\left(\frac{a}{2} + \varepsilon\right) = H\left(\frac{a}{2}\right) + H(\varepsilon) = H(\varepsilon) \tag{8}$$

Так как случайная величина ε распределена по нормальному закону, в соответствии с [10]: $H(\varepsilon) = \log\left(\sigma\sqrt{2\pi}\right)$

Тогда $H\left({}^{y}/_{\eta = 1}\right) = \log\left(\sigma\sqrt{2\pi}\right)$ (9)

Поскольку $H\left(\frac{a}{2}\right) = H\left(-\frac{a}{2}\right) = 0$:

$$H\left({}^{y}/_{\eta=1}\right) = H\left({}^{y}/_{\eta=-1}\right) \quad (10)$$

Очевидно, что $H\left({}^{y}/_{\eta}\right) = -\frac{1}{2}\log\left(\sigma\sqrt{2\pi}\right) - \frac{1}{2}\log\left(\sigma\sqrt{2\pi}\right) = -\log\left(\sigma\sqrt{2\pi}\right)$

Таким образом, количество информации в канале передачи данных y:

$$I(\eta, y) = 1 - \frac{1}{2}\log e - \frac{a^2}{2\sigma\sqrt{2}}\log e - \int_{-\infty}^{\infty} \frac{1}{2\sigma\sqrt{2\pi}} e^{-\frac{\left(y+\frac{a}{2}\right)^2}{2\sigma^2}} \left(e^{\frac{ay}{\sigma^2}} + 1\right) \log\left(e^{\frac{ay}{\sigma^2}} + 1\right) dy + \log(\sigma\sqrt{2\pi}) \quad (11)$$

Пусть амплитуда сигнала $a = 1$. Вычислим количество информации в канале y (1) для $\sigma = 3$. В таком случае $I(\eta, y) \approx 2.21634$. Если увеличить интенсивность шума до $\sigma = 10$, то количество информации будет равно $I(\eta, y) \approx 3.875$

Полученные результаты согласуются с (2), так как при усилении шума в канале связи растет значение $H(y)$, что в свою очередь приводит к увеличению количества информации в канале y.

В рамках усложнения данной задачи предлагается использовать систему каналов передачи данных (12)

$$\begin{cases} Y_1 = \frac{a}{2}\eta + \varepsilon \\ Y_2 = \frac{b}{2}\eta + \sigma \end{cases} \quad (12)$$

По аналогии с каналом y (1), в данном случае a и b являются амплитудами дискретных сигналов, ε и σ являются нормально распределенными случайными величинами, с коэффициентом корреляции $r_{\varepsilon,\sigma}$.

В данном случае количество информации в данной системе каналов связи равно

$$I(\eta, Y_1, Y_2) = H(Y_1, Y_2) - H(Y_1, Y_2/\eta) \quad (13)$$

Исследование величины (12) может стать основной для последующих исследований. Интерес представляет влияние корреляции каналов связи на величину энтропии и количества информации в передаваемых сообщениях.

Выводы

В рамках данной работы была проведена аналитическая работа, позволившая рассмотреть возможность применения теории статистических мер информации к дискретным каналам связи с аддитивным шумом. Полученные формулы позволяют определить количество информации по Шеннону в заданном канале связи. Продемонстрировано влияние аддитивного шума в канале связи на энтропию сигнала и ее влияние на количество информации. В рамках статьи намечены направления будущих исследований, заложена база для них.

Литература

1. Якубов Р. Ж. Двумерное распознавание сигнала на основе метода k ближайших соседей // Молодежный научно-технический вестник, 2015. № 7. с. 40-46. URL:

2. Троицкий И. И., Басараб М. А., Матвеев В. А. Использование двух каналов передачи информации для решения задачи распознавания дискретного сигнала в аддитивном шуме // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение, 2015. № 4. с. 106-112. DOI: 10.18698/0236-3933-

3. Троицкий И.И., Якубов Р.Ж., Моделирование процесса распознавания дискретного сигнала в аддитивном шуме для двух каналов передачи информации на основе метода k ближайших соседей при наличии общего шума. // Вопросы кибербезопасности. 2017. № 1 (19). С. 57-62.

4. Троицкий И.И., Якубов Р.Ж., Сравнительный анализ линейной фильтрации дискретного сигнала в аддитивном шуме для двух каналов передачи информации с методом k ближайших соседей. // Вопросы кибербезопасности. 2018. № 2 (26). С. 59-69. DOI: 10.21681/2311-3456-2018-2-

5. Troickiy I.I. Yakubov R.Z., Using of potential functions method for recognition of two channels in additive noise(BIT 2017) CEUR Workshop Proceedings, 2017, Vol-2081, pp. 131-134.

6. Малла С. Вейвлеты в обработке сигналов. М: Мир, 2005. 672 с.

7. Горелик А. Л., Скрыпник В. А. Методы распознавания. М.: Высшая школа, 1989. 232 с.

8. Джиган В. И. Адаптивная фильтрация сигналов. Теория и алгоритмы. М: Техносфера, 2013. 528 с.

9. Дуда Р., Харт П. Распознавание образов и анализ сцен. М.: Мир, 1976. 510 с.

10. Кульбак С. Теория информации и статистика. М.: Наука, 1967. 408 с.

11. Probabilistic Modeling in System Engineering / By ed. A. Kostogryzov. – London: IntechOpen, 2018. 278 p.

Научный руководитель: Троицкий Игорь Иванович, к.т.н., доцент кафедры ИУ8 МГТУ им. Н.Э. Баумана, Москва, iitroickiy@mail.ru

SEARCHING OF AMOUNT OF INFORMATION OF SHANNON IN A DISCRETE CHANNEL WITH ADDITIVE NOISE

Yakubov R. Zh.[86]

This article is devoted to researching of binary information channels with additive noise and a question of application of statistical measure, which is known as Shannon information. A mathematical model of channel is presented. Defenitions of Shannon information and entropy are also attached. There are added some mathematical calculations, which allow to estimate amount of information in one message. Besides, there are offered the base for future investigations. Results of this work can be applied at creation of transmission system of data.

Keywords: information, entropy, transmission channel, statistics, computer modeling.

[86] Yakubov Rustam Zhafarovich, post-graduate student of Information security department of BMSTU, Moscow, e-mail: yakubov_rustam@inbox.ru

УДК 004.056

АНАЛИЗ ОРГАНИЗАЦИОНЫХ МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Шахалов И.Ю., Чепик П.И.[87]

Аннотация: Целью защиты информации в автоматизированных системах является предотвращение или существенное затруднение утечки обрабатываемой информации, а также НСД к ним. Информация об угрозах является важным компонентом эффективной защиты, что даёт возможность предсказать допустимые атаки и подготовиться к ним заранее. Для достижения высокого уровня безопасности необходимо принятие соответствующих организационных мер.

Ключевые слова: угрозы, информационная безопасность, автоматизированная система.

Введение

Обеспечение безопасности автоматизированной системы предполагает создание препятствий для любого несанкционированного вмешательства в процессе ее функционирования [5, 11]. Для эффективной защиты информации в автоматизированных системах обработки информации требуется разработка и принятие организационных мероприятий [4, 6, 8].

Актуальность проблемы

Значительный объём информации хранится, обрабатывается и передаётся на автоматизированных системах (далее – АС). Под автоматизированной системой обработки информации понимается организационно-техническая система, которая представляет собой совокупность следующих взаимосвязанных компонентов: средства вычислительной техники; программное обеспечение; каналы связи; информации на различных носителях; персонал и пользователи системы [1-3, 10, 11]. В данном процессе задействован каждый участник по выполнению действий обработки, хранения и передачи информации.

Существуют основные организационные и организационно-технические мероприятия по созданию и поддержанию функционирования комплексной системы защиты: разовые мероприятия; мероприятия, проводимые при осуществлении или возникновении определенных изменений в самой защищаемой АС или внешней среде; периодически проводимые мероприятия; постоянно проводимые мероприятия.

Организационно – технические меры АС и средства защиты информации исключают доступ посторонних лиц к информационным ресурсам и средствам защиты информации, возможность появления нарушителя в среде обслуживающего персонала, возникновение угроз со стороны пользователей и технического персонала.

Угрозы безопасности обрабатываемой информации в АС

В АС встречаются следующие угрозы безопасности [10, 13]:

- угрозы техногенного характера, основными из которых являются:
- аварии (отключение электропитания, системы заземления, разрушение инженерных сооружений и т.д.);
- неисправности, сбои аппаратных средств, нестабильность параметров системы электропитания, заземления и т.д.;
- помехи и наводки, приводящие к сбоям в работе аппаратных средств;
- ошибочные действия и (или) нарушения тех или иных требований лицами, санкционировано взаимодействующими с возможными объектами угроз;

[87] Шахалов Игорь Юрьевич, доцент кафедры ИУ8, МГТУ им. Н.Э. Баумана, Москва, is@cnpo.ru
Чепик Полина Игоревна, МГТУ им. Н.Э. Баумана, Москва, p.chepik@bmstu.net

- умышленные угрозы, направленные на нарушение целостности и доступности информации.

Описание потенциального нарушителя в АС

Поведём анализ потенциальных нарушителей АС [14], которые имеют возможность доступа к ресурсам, обрабатываемых в АС и могут быть подразделены на следующие категории:

Категория I – это лица, не имеющие права доступа в контролируемую зону. К нарушителю данной категории можно отнести физических лиц, целенаправленные действия которых, направлены на нарушение работоспособности АС, в том числе и средств защиты информации и криптографических средств, а также на нарушение целостности и доступности информационных ресурсов АС. Данная категория нарушителей может осуществлять атаки только с территории, расположенной вне контролируемой зоны объекта. Нарушители данной группы потенциально имеют следующие возможности:

- технический съем (перехват) информации с внешних каналов связи АС;
- попытки осуществления компьютерных атак и вирусного заражения программно-технических средств АС.

Категория II – это лица, имеющие право постоянного или разового доступа в контролируемую зону, но не имеющие права доступа к техническим средствам АС.

Кроме того, потенциальные нарушители подразделяются на:

- внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны информационной системы;
- внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны информационной системы.

Внешними нарушителями могут быть как лица категории I, так и лица категории II, внутренними нарушителями могут быть только лица категории II.

Всех нарушителей II категории можно разделить на:

- обслуживающий персонал объекта;
- лиц из числа сотрудников сторонних организаций;
- других лиц сторонних организаций, имеющие доступ в контролируемую зону;
- пользователей АС;
- технического персонала.

Таким образом, в качестве потенциальных нарушителей АС рассматриваются лица категории I. Кроме того, не исключена возможность реализации угроз со стороны обслуживающего персонала из пределов контролируемой зоны (внешний нарушитель категории II), а также непреднамеренных угроз со стороны пользователей и технического персонала вследствие ошибочных действий, нарушения регламентов проведения работ и пр.

Мероприятия по защите информации

Мероприятия по защите информации, обрабатываемой в АС от НСД предусматривают:

– физическая охрана технических средств (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строго пропускного режима, специальное оборудование помещений с размещенными средствами;

– учет всех машинных носителей информации;

– ведение двух копий дистрибутивов программных средств системы защиты: на сервере и на оптических дисках;

– периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств.

Для проведения работ по защите информации в АС допускаются сотрудники, имеющие специальную подготовку по защите информации и практические навыки работы со средствами вычислительной техники (СВТ), прошедших подготовку для выполнения

обязанностей администратора безопасности информации.

В случае отсутствия в штатной структуре должности администратора информационной безопасности, ответственными за обеспечение безопасности информации назначаются специалисты из числа наиболее подготовленных по защите информации.

В своей работе администратор по информационной безопасности должен руководствоваться основными документами по защите информации, инструкцией по защите от НСД АС и средств защиты информации, входящих в ее состав.

На лиц, ответственных за обеспечение безопасности информации от НСД, возлагаются следующие основные задачи и функции:

– первоначальная настройка и корректировка параметров идентификации и полномочий доступа субъектов доступа к защищаемым ресурсам;

– первоначальная настройка и корректировка перечня компонентов программного и информационного обеспечения подлежащих контролю целостности;

– первоначальная настройка и корректировка перечня регистрируемых событий безопасности в АС, настройка и корректировка содержания журналов регистрации и учета событий безопасности;

– контроль состояния и работоспособности программных средств защиты информации от НСД в АС, а также оперативное восстановление функций СЗИ при сбоях;

– тестирование всех функций СЗИ от НСД с помощью программных средств тестирования с периодичностью не реже одного раза в месяц;

– учет всех защищаемых носителей информации с помощью их маркировки, учет защищаемых носителей в журнале (картотеке) с регистрацией их выдачи (приема);

– организация работы с печатающими средствами, входящими в состав, АС, в режиме печати с маркировкой твердых копий (с колонтитулами) и без нее с обязательным ведением журналов учета размножения документов.

Действия сотрудников при эксплуатации АС фиксируются в техническом журнале с указанием даты и времени и заверяются подписью лиц, производивших действия. В техническом журнале фиксируются следующие события (действия и их результаты):

– установка ОС и производимые настройки СЗИ;

– установка и настройки СЗИ от НСД;

– проверка целостности файлов и ее результат;

– появление сообщений о неисправности носителей парольной информации или сбоях в работе ПО и предпринятые при этом действия;

– действия должностных лиц и администраторов при компрометации СЗИ.

Выводы

Для достижения высокого уровня безопасности необходимо принятие организационных мер, которые должны быть направлены на обеспечение правильного функционирования механизмов защиты и выполняться администратором системы. Также, со стороны руководства организации должны быть введены правила автоматизированной обработки информации, включая правила её защиты и установлены меры ответственности за нарушение этих правил.

Литература

1. Быков А.Ю., Панфилов Ф.А., Зенькович С.А. Модель и методы многокритериального выбора классов защищенности для объектов распределенной информационной системы и размещения баз данных по объектам//Вопросы кибербезопасности. 2016. № 2 (15). С. 9-20.

2. Вильям Л. Саймон, Кевин Митник Искусство обмана, Москва, 2004. 14 с.

3. Гришин М.И., Марков А.С., Барабанов А.В. Формальный базис и метабазис оценки соответствия средств защиты информации объектов информатизации // Известия Института инженерной физики. 2011. Т. 3. № 21. С. 82-88.

4. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности АС и ИВС/Котенко И.В., Котухов М.М., Марков А.С и др. -СПб: ВУС, 2000. 190 с.

5. Барабанов А.В., Марков А.С., Цирлов В.Л. Методический аппарат оценки соответствия автоматизированных систем требованиям безопасности информации//Спецтехника и связь. 2011. № 3. С. 48-52.

6. Математические основы информационной безопасности / Басараб М.А., Булатов В.В., Булдакова Т.И. и др.; Под. ред. В.А.Матвеева. М.: НИИ РиЛТ МГТУ им. Н.Э.Баумана, 2013. 244 с.

7. Меняев М.Ф. Информационный менеджмент, Москва, 2017. 280 с.

8. Оладько В.С. Модель выбора рационального состава средств защиты в системе электронной коммерции//Вопросы кибербезопасности. 2016. № 1 (14). С. 17-23. 3

9. Цирлов В.Л. Основы информационной безопасности автоматизированных систем, 2008.

10. Чепик П.И. Обзор существующих угроз в информационной безопасности. В сборнике: Безопасные информационные технологии Сборник трудов Восьмой всероссийской научно-технической конференции. НУК «Информатика и системы управления». Под. ред. М.А.Басараба. 2017. С. 509-512.

11. Чобанян В.А., Шахалов И.Ю. Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры//Вопросы кибербезопасности. 2013. № 1(1). С. 17-27.

12. Чобанян В.А., Шахалов И.Ю., Райков О.В. Некоторые аспекты расчета эффективности средств защиты информации перспективных автоматизированных систем военного назначения // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2014. № 7-8. С. 46-49.

13. Шеремет И.А. Противодействие информационным и кибернетическим угрозам//Вестник академии военных наук. 2016. № 2 (55). С. 29-34.

14. Паршуткин А.В. Концептуальная модель взаимодействия конфликтующих информационных и телекоммуникационных систем // Вопросы кибербезопасности. № 5(8). 2014. С. 2-6.

ANALYSIS ORGANIZACION OF MEASURES TO ENSURE THE PROTECTION OF INFORMATION IN AUTOMATED SYSTEMS

Shakhalov I.Yu., Chepik P.I.[88]

Abstract: The purpose of information protection in automated systems is to prevent or significantly complicate the leakage of processed information, as well as unauthorized access to them. Information about threats is an important component of effective protection and provides an opportunity to predict possible attacks and prepare for them in advance them. In order to achieve a high level of security, it is necessary to take appropriate organizational measures.

Keywords: threats, information security, automated system

[88] Igor Shakhalov, docent, BMSTU, is@cnpo.ru
Polina Chepik, BMSTU, Moscow, p.chepik@bmstu.net

УДК 004.056

Консолидация технологий мониторинга IT-инфраструктуры

Селезнев С.Н.[89]

Аннотация. В статье мы обсудим, каким образом можно качественно улучшить мониторинг IT-инфраструктуры предприятия и адаптировать его для решения различных задач, в том числе в области информационной безопасности.

Ключевые слова: зонтичный мониторинг, системы управления информационной безопасности, мониторинг бизнес-процессов

Введение

Ввиду широкого распространения систем мониторинга ИТ-инфраструктуры проблематика оценки эффективности их применения для решения бизнес-задач становится одним из важных аспектов жизнедеятельности организации [1-7]. Нами рассмотрены ограничения, которые возникают при эксплуатации классических систем мониторинга, а также систем управления событиями информационной безопасности (СУСИБ), сформированы задачи и требования к системам мониторинга нового поколения.

Функции систем мониторинга

Основные функции систем мониторинга ИТ-инфраструктуры включают:

1. Сбор данных – получение данных о функционировании из подключенных источников различными способами.
2. Анализ данных в реальном времени – данные передаются в аналитические модули, где происходит генерация событий и инцидентов по определенным правилам.
3. Визуализация данных и событий – представление данных в виде временных графиков или диаграмм.
4. Оповещение администраторов о возникновении событий и инцидентов.
5. Формирование отчетов – сведение аналитической и статистической информации в отчеты, которые используемые для дополнительного анализа.
6. Хранение исторических данных с возможностью их поиска и фильтрации.

Ограничения классических систем мониторинга

Несмотря на видимую простоту решений и достаточно широкие функциональные возможности существующих решений, эффективность их применения ограничивается следующими факторами:

7. Неправильно или недостаточно хорошо настроенные правила формирования событий и отсутствие мониторинга отдельных объектов ИТ-инфраструктуры делают невозможным получение полной и достоверной картины функционирования ИТ-инфраструктуры в целом.
8. Количество предоставляемых данных и событий, генерируемых системой может быть очень большим и выделить из них важную информацию или обнаружить проблему администратору в этом случае затруднительно.
9. В большинстве случаев в системе мониторинга будут отсутствовать эффективные механизмы выявления тенденций или прогнозирования событий, а также механизмы оперативного реагирования на возникающие проблемы.
10. Классическая система мониторинга оперирует метриками и правилами

[89] Селезнев Сергей Николаевич, АО «Эшелон Технологии», Москва, ss@cnpo.ru

в отношении отдельно взятых объектов мониторинга, не имея информации об их взаимном влиянии, и не обладает оперативной информацией об изменениях в ИТ-инфраструктуре.

Проблематика эффективного применения инструментов мониторинга не ограничивается указанными факторами, а, в том числе, заключается в отсутствии системного подхода к проектированию решения, соответствующего нуждам организации.

Системы управлениями событиями информационной безопасности

СУСИБ позволяют осуществлять мониторинг информационных систем, анализировать события безопасности в режиме реального времени, возникающие на объектах мониторинга. Собранные и проанализированные данные помогают обнаружить инциденты ИБ или аномалии, оставшиеся незаметными для специализированных средств защиты [2, 3].

Областью применения СУСИБ являются:

1. Управление информационной безопасностью.
2. Управление событиями безопасности.

В СУСИБ данные и события собираются из ряда систем инфраструктурного мониторинга, логов ИТ и безопасности, предоставляемых средствами защиты информации (СЗИ).

В дополнение функциям классических систем мониторинга, внедрение СУСИБ реализует:

1. Прием событий, генерируемых подключенными СЗИ.
2. Формирование правил, которые генерируют события и инциденты информационной безопасности.
3. Контроль конфигурации некоторых объектов ИТ-инфраструктуры и получение от них подробной информации.

Ограничения СУСИБ

Применение СУСИБ как самостоятельного решения или в комплексе с классическими системами мониторинга также имеет ряд ограничений:

1. Существенные временные затраты на внедрение СУСИБ в организациях с развитой ИТ-инфраструктурой.
2. Необходимость привлечения дополнительных специалистов в области ИБ для обслуживания СУСИБ.
3. Ложные срабатывания в СУСИБ – это ситуации, в которых происходит ошибочное принятие за инцидент ИБ нормального поведения сетевого трафика или пользователя.
4. Отчеты СУСИБ обычно не содержат такую важную информацию, как состояние объекта до и после изменений и трудны в восприятии.

Системы мониторинга нового поколения

Системы зонтичного мониторинга (ЗСМ) – это мощный инструмент сбора и выявление корреляции данных о событиях, которые используют возможности различных систем мониторинга нижнего уровня. ЗСМ ориентированы на решение следующего круга приоритетных задач:

1. Формирование единого пространства событий по состоянию контролируемых объектов ИТ-инфраструктуры.
2. Работа со всей информацией в едином графическом интерфейсе на разных уровнях абстракции.
3. Автоматизация учета, управления и сбора данных о состоянии объектов ИТ-инфраструктуры.

4. Выявление первопричин событий и инцидентов (в т.ч. ИБ).
5. Обогащение данных проходящих через ЗСМ дополнительной информацией.

Рис. 1. Уровень зонтичного мониторинга

Требования к созданию ЗСМ

Исследование, проведенное в рамках данной работы, позволило сформулировать требования к ЗСМ, реализация которых будет способствовать созданию качественно нового уровня управления ИТ-инфраструктурой организации. ЗСМ должна:

1. Обеспечивать двустороннюю интеграцию с системами сбора информации.
2. Обеспечивать возможность интеграции систем мониторинга различного назначения («классических» и СУСИБ).
3. Автоматизировать задачи комплексной диагностики проблем и устранения инцидентов (в том числе обеспечивать их приоритизацию).
4. Предоставлять централизованную базу знаний по всем аспектам функционирования ИТ-инфраструктуры.
5. Обеспечивать накопление информации о ложных срабатываниях.
6. Система мониторинга должна обеспечивать работу с любыми типами данных и любыми источниками.

Рис. 2. Схема зонтичного мониторинга

Заключение

Результаты проведенного исследования успешно применяются разработчиками новой отечественной системы зонтичного мониторинга eZont компании «Эшелон Технологии».

Литература

1. Горбачев И.Е. Концепция итерационного внешнего проектирования облика проактивных систем информационной безопасности // Вопросы кибербезопасности. 2017. № 5 (24). С. 50-63.
2. Кузнецов А.В., Ненашев С.М. Способ определения регистрируемых событий // Вопросы кибербезопасности. 2015. № 5 (13). С. 23-25.
3. Марков А., Фадин А. Конвергенция средств защиты информации // Защита информации. Инсайд. 2013. № 4 (52). С. 80-81.
4. Марков А.С. Сервисное и программно-техническое обеспечение ситуационных центров по информационной безопасности // В книге: The 2017 Symposium on Cybersecurity of the Digital Economy (CDE'17). 2017. С. 255-260.
5. Петренко С.А., Цирлов В.Л. Импортозамещение решений IDS и SIEM//Защита информации. Инсайд. 2017. № 5 (77). С. 46-51.
6. Котенко И.В., Федорченко А.В., Саенко И.Б., Кушнеревич А.Г. Технологии больших данных для корреляции событий безопасности на основе учета типов связей // Вопросы кибербезопасности. 2017. № 5 (24). С. 2-16.
7. Шеремет И.А. Противодействие информационным и кибернетическим угрозам//Вестник академии военных наук. 2016. № 2 (55). С. 29-34.

Научный консультант

Цирлов Валентин Леонидович, кандидат технических наук, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, z@cnpo.ru

CONSOLIDATION OF MONITORING TECHNOLOGIESIT INFRASTRUCTURE

Seleznev S.N.[90]

Annotation. In the article we will discuss how to qualitatively improve the monitoring of the IT infrastructure of an enterprise and adapt it for solving various tasks, including in the field of information security.

Keywords: umbrella monitoring, SIEM, SEM, SIM

[90] Seleznev Sergey Nikolaevich, Echelon Technologies, Moscow, ss@cnpo.ru

Оглавление

Барков В.В. Проектирование и разработка экспертно-аналитической системы «Система анализа трафика» для исследования алгоритмов классификации трафика мобильных устройств под управлением операционной системы Android 2
Бельфер Р. А., Борисов С. М., Макаров И. М. Алгоритм функций устройств абонентского доступа имитатора сети ПД категории специального назначения, подлежащих реализации на специально разработанных аппаратно-программных устройствах..... 14
Бельфер Р.А., Макаров И.М., Никулина Т.П. Алгоритм формирования маршрутизации от источника в имитаторе сети ПД категории специального назначения..... 20
Бердюгин А.А. Подход к управлению защитой информации в системах электронного банкинга 24
Бондарев В.В. Психологические аспекты информационной безопасности 28
Быков А.Ю., Крыгин И.А., Гришунин М.В. Алгоритм поиска седловой точки в смешанных стратегиях на основе модификации метода Брауна-Робинсона для решения задачи выбора защищаемых объектов 33
Варфоломеев А.А. Современные ручные шифры и их использование в учебных курсах по криптографии на примере шифра Elsiefour 39
Глинская Е.В., Чичварин Н.В. Специфика конструирования бортовой аппаратуры модульной авионики с учетом требований информационной безопасности 43
Волосатова Т.М., Чичварин Н.В. Способы моделирования аппаратуры модульной авионики в условиях вредоносных воздействий..... 58
Горшков Ю.Г. Средства криминалистического исследования фонограмм..... 64
Давыдов В.Н. Методы применения машинного обучения для первичного анализа внутреннего программного обеспечения..... 68
Давыдов В.Н. Выявление аномальной активности пользователей интернет-ресурсов 72
Демченко И.А. Передача скрытых сообщений с использованием протоколов без гарантированной доставки пакетов. 77
Жоголев Г.Д. Клеточные автоматы в криптографии 81
Климцов В.Е., Чиликов А.А. Автоматизация дифференциального криптоанализа по ошибкам вычислений применительно к поточным аппаратно-реализуемым шифрам..... 86
Ключарёв П.Г. О производительности и статистических свойствах некоторых криптографических алгоритмов, основанных на обобщенных клеточных автоматах..... 91
Ковынёв Н.В. Стеганографический метод идентификации авторского права на аудиофайл 95
Кондрашев И.В. Сжатие биометрических сигналов с помощью дискретного косинусного преобразования и дискретного преобразования Чебышева..... 102
Крыгин И. А. Математическая постановка задачи распределения вычислительных ресурсов между средствами защиты информации на основе дискретно-непрерыной игры 107
Лебедев А. Н. Новые арифметические операции конечного коммутативного кольца и их использование в криптографии..... 112
Лебедев А. Н. Способ многофакторной аутентификации электронных документов с визуализацией и использованием дополнительного канала 116
Магомедова Д.И. Повышение стойкости стеганографических алгоритмов при использовании фрактальных ключей 119
Макаров А.О. Схема пост-квантовой агрегированной подписи на основе теории алгебраического кодирования..... 124
Маркова И.А. Обзор методов защиты персональных данных пользователя в web-приложениях..... 129

Маркова И.А. Особенности обеспечения безопасности персональных данных при работе в информационных системах обработки персональных данных..... 133
Медведев Н. В. Выравнивание загрузки узлов компьютерной сети 137
Медведев Н. В., Глинская Е. В. Вероятностные характеристики обнаружения скрытых изображений 140
Миронов С.В. Методика тестирование программного обеспечения при ограниченном доступе к исходным текстам..... 143
Островский А.С., Малахов М.В. Использование бинарной инструментации кода в динамическом анализе программного обеспечения 148
Райкова Н.О. Анализ нормативной базы в области разработки безопасного программного обеспечения 152
Рауткин В.Ю. Актуальные вопросы определения местоположения мобильного устройства по анализу энергопотребления с помощью машинного обучения..... 157
Рычков А.С. Определение синтезированных биометрических образов 160
Смольникова М.С. Алгоритмы анонимной идентификации устройства..... 169
Шаршеева Ж. К вопросу об использовании методов оценки рисков в системах менеджмента информационной безопасности 172
Соков Б.Б. Создание прототипа системы биометрической аутентификации по геометрии лица с помощью методов машинного обучения 175
Титов А.Ю. Оценка рисков информационной безопасности в рамках проекта Положения Банка России о требованиях к системе управления операционным риском для кредитной организации 179
Хачатрян М.Г. Обнаружение ботов в онлайновой социальной сети Twitter с помощью алгоритма машинного обучения «Случайный лес»..... 184
Щелкунов Д.А., Чиликов А.А. EVHEN 2.0. Новая схема быстрого асимметричного шифрования и цифровой подписи на публичном ключе 188
Якубов Р.Ж. Определение количества информации по Шеннону в дискретном канале связи с аддитивным шумом..... 199
Шахалов И.Ю., Чепик П.И. Анализ организационных мероприятий по обеспечению защиты информации в автоматизированных системах …….. 203
Селезнев С.Н. Консолидация технологий мониторинга IT-инфраструктуры ……. 207

Издательство МГТУ им. Н.Э.Баумана
Россия, Москва, 105005, ул.2-я Бауманская, д.5, стр.1.
Тел. (499)263-6391, Факс: (499) 267-4844
Подписано в печать 29.12.2018, Заказ 015678
Формат 60x90.8. Гарнитура Times New Roman
Усл. печ. 29.12. Тираж 100 экз.