МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Брянский государственный технический университет

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ

Материалы X Межрегиональной научно-практической конференции

30 апреля 2018 г.
г. Брянск

БРЯНСК
ИЗДАТЕЛЬСТВО БГТУ
2018

ББК 75.7

Информационная безопасность и защита персональных данных. Проблемы и пути их решения: Материалы X Межрегиональной научно-практической конференции [Электронный ресурс]/ под ред. О.М. Голембиовской, М.Ю.Рытова. – Брянск: БГТУ, 2018. – 187 с.

ISBN 978-5-906967-92-3

Приведены материалы докладов участников X Межрегиональной научно-практической конференции «Информационная безопасность и защита персональных данных. Проблемы и пути их решения», состоявшейся 30 апреля 2018 года в Брянском государственном техническом университете.

Материалы конференции предназначены для студентов, а также могут быть полезны магистрантам, аспирантам, занимающимся научно-исследовательской работой.

Редактор Т.И. Королева
Компьютерный набор К.А. Синицкая

Темплан 2018 г., п. 25

Подписано в печать 25.05.2018 Формат 60x84 1/16. Бумага офсетная. Офсетная печать. Печ.л. 14,27 Уч.-изд.л. 14,27

Издательство Брянского государственного технического университета
241035, Брянск, бульвар 50 лет Октября, 7, БГТУ, 58-82-49.
Лаборатория оперативной полиграфии БГТУ, ул. Институтская,16.

ISBN 978-5-906967-92-3

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.942

Баянов Булат Ильмирович, *студент кафедры «Системы информационной безопасности» КНИТУ-КАИ*
Мухаматханов Ренат Маратович, *студент кафедры «Системы информационной безопасности» КНИТУ-КАИ*
Хаматнуров Ильдар Ильнатович, *студент кафедры «Системы информационной безопасности» КНИТУ-КАИ*
Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ, Казань, Россия
e-mail: bayanov_bulat@mail.ru

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ WEB-РЕСУРСА В СФЕРЕ ЭЛЕКТРОННЫХ УСЛУГ

Разработана общая методика формирования автоматизированной системы защиты информации, направленной на обеспечение информационной безопасности организации, использующей web-ресурс.

В настоящее время множество организаций использует электронные ресурсы для автоматизации процессов в собственной инфокоммуникационной системе для упрощения выполнения множества задач. В качестве электронного ресурса в данной статье рассматривается web-ресурс. Электронный ресурс может выполнить следующие задачи: оптимизацию документооборота, использование передовых технологий взаимодействия с пользовательскими интерфейсами системы, сокращение времени на заполнение документов и минимизации ошибок при их заполнении, облегчение принятия управленческих решений. Множество предприятий, работающих с конфиденциальной информацией, также может использовать и персональные данные пользователей системы, поэтому инфокоммуникационная система требует обеспечения защиты данной информации [1].

Зачастую у автоматизированной системы (АС), такой как web-ресурс, система защиты также является автоматизированной [3]. Для построения автоматизированной системы защиты информации (АСЗИ) специалисты по информационной безопасности пользуются методикой, в которой применяются документы по стандартизации автоматизированных систем, специальные правовые документы, нормативные документы ФСТЭК, а также руководящие документы в сфере защиты информации [2].

Данная методика построена с использованием следующего документа: ГОСТ 34.601-90 "Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания", который регламентирует стадии и этапы создания АС, т.е. производится проектирование АСЗИ.

На первом этапе выполняется анализ объекта автоматизации (в нашем случае объектом АСЗИ является web-ресурс), затем к АСЗИ выдвигается список требований по обеспечению защиты информации. Результатом данного этапа является акт обследования. В акте обследования указывается назначение, цели, субъекты АСЗИ, общая информация об объекте исследования, ее структура [4]. Так как объект автоматизации использует конфиденциальную информацию, прежде чем приступить к следующему этапу формирования АСЗИ и необходимых документов, требуется выполнить оценку уровня конфиденциальности информации, с которой работает субъект АС. Оценка уровня конфиденциальности зависит от выдвинутых АСЗИ требований по защите информации, при этом специалист по информационной безопасности руководствуется документом ГОСТ 34.602-89 "Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы". Данный ГОСТ устанавливает состав, содержание, правила оформления документа "Техническое задание на создание (развитие или модернизацию) системы".

Следующим этапом формирования АСЗИ является разработка таких документов, как техническое задание и технический проект. Каждый из данных документов взаимосвязан друг с другом, поэтому множество разделов одного из документов основывается на разделах другого. Техническое задание является основным документом, определяющим требования и порядок создания АС, а технический проект является документом, определяющим порядок действий для ввода в эксплуатацию АС. Согласно ГОСТ 34.602-89 техническое задание выдвигает ряд требований по защите информации, учитывая класс защищенности конфиденциальной информации. Класс защищенности определяется специалистом согласно руководящему документу "Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации". Настоящий руководящий документ устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов. Так как объектом защиты является web-ресурс при формировании документов, которые в последующем послужат основой для создания АСЗИ web-ресурса, также должен учитываться Федеральный закон №149 "Об информации, информационных технологиях и о защите информации" [6]. В данном документе выдвигаются обязанности владельца web-ресурса для обеспечения защиты конфиденциальной информации пользователей web-ресурса. Если web-ресурс работает с персональными данными, то также стоит учесть обязанности, прописанные в Федеральном законе №152 "О персональных данных" [5]. Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Указанный список документов является достаточным для формирования АСЗИ web-ресурса.

Согласно 34.601-90 последний этап создания АСЗИ является ввод АСЗИ в действие. К данному этапу можно отнести подготовку объекта автоматизации к вводу АС в действие, подготовку персонала, проведение предварительных испытаний, проведение опытной эксплуатации и прочее.

Таким образом, стандарты существенно упрощают процесс создания АСЗИ. Так как в качестве электронного ресурса предприятия и организации при работе с информацией зачастую используют именно web-ресурс, формирование АСЗИ web-ресурса производится с учетом правовых документов по защите информации web-ресурсов.

Список литературы

1 Бондарев, В.В. Введение в информационную безопасность автоматизированных систем: учебное пособие/В.В. Бондарев. – 2016. – М.: МГТУ им. Н.Э. Баумана. – С. 252.

2 Сердюков, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие/В.А. Сердюков. – М.: Издательский дом Высшей школы экономики, 2015. – С. 574.

3 Защита конфиденциальной информации на автоматизированных рабочих местах на базе автономных ПЭВМ [Электронный ресурс]. Режим доступа: https://studfiles.net/preview/2566963/page:9. Дата обращения (11.04.18.);

4 Классификация сетевых атак [Электронный ресурс]. Режим доступа: http://www.internet-technologies.ru/articles/article_237.html. Дата обращения (16.04.18.);

5 Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция) [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/. Дата обращения (12.04.18.).

6 Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция) [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/. Дата обращения (15.04.18.).

Материал поступил в редколлегию 23.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 621.394

***Белим Сергей Викторович**, д.ф.-м.н., профессор, заведующий кафедрой информационной безопасности ОмГУ им. Ф.М. Достоевского*
***Белим Светлана Юрьевна**, к.п.н., доцент, доцент кафедры информационной безопасности ОмГУ им. Ф.М. Достоевского*
Омский государственный университет им. Ф.М. Достоевского, Омск, Россия
e-mail: sbelim@mail.ru

ИСПОЛЬЗОВАНИЕ KDP-СХЕМЫ ПРЕДВАРИТЕЛЬНОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ДЛЯ РЕАЛИЗАЦИИ МАНДАТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА

Рассмотрена возможность использования KDP-схемы предварительного распределения ключей для реализации мандатного разграничения доступа в распределенных системах с иерархией пользователей. Предложен модифицированный алгоритм предварительного распределения ключей. Разработана методика построения семейства подмножеств для решения поставленной задачи.

Мандатное разграничение доступа считается более строгим по сравнению с дискреционным аналогом. Однако для его реализации, как правило, необходима централизованная подсистема безопасности, требующая централизованного принятия решений на основе сравнения мандатов доступа. Данная задача легко решается в локальных системах, но сталкивается с рядом трудностей в распределенных системах. На сегодняшний день эта проблема решается с помощью сертификатов открытых ключей. Тем не менее, такое решение нельзя считать удовлетворительным. Использование сертификатов приводит к необходимости привлечения асимметричных криптографических алгоритмов, которые работают достаточно медленно. Кроме этого не решается полностью задача отказа от централизации, так как необходим центр подтверждения сертификатов. Мандатное разграничение доступа опирается на множество меток безопасности, которые образуют алгебраическую решетку. Метки безопасности присваиваются как пользователям, так и информационным объектам. При запросе на доступ происходит сравнение меток безопасности. Решение принимается на основе некоторого логического условия, накладываемого на метки безопасности.

Пусть в распределенной системе задано множество пользователей U. Для пользователей системы существует отношение порядка. Ограничимся отношением порядка, описываемым графом в виде дерева. Доминирование пользователя u_i над пользователем u_j обозначим $u_i > u_j$. Возможна также ситуация, когда пользователи несравнимы друг с другом, тогда будем использо-

вать обозначение $u_i <> u_j$. Ограничимся случаем мандатного разграничения доступа, в котором разрешены только информационные потоки снизу вверх. Данный случай соответствует мандатной политике безопасности по обеспечению конфиденциальности информации. В этом случае для двух пользователей $u_i > u_j$ разрешен только информационный поток от u_j к u_i. Для двух несравнимых пользователей запрещены информационные потоки в обе стороны.

Поставим задачу формирования ключевой схемы, позволяющей обмениваться информацией в соответствии с мандатным разграничением доступа. Для этого построим схему предварительного распределения ключей, вырабатывающую парные ключи только для разрешенных каналов.

Для решения задачи модифицируем KDP-схему предварительного распределения ключей. Для системы без разграничения доступа в KDP-схеме формируется набор ключевых материалов $K=\{k_1,\ldots,k_n\}$, предварительно рассылаемый всем участникам по защищенным каналам. Для выработки парных ключей используется система подмножеств $S=\{S_1,\ldots,S_m\}$ множества $\{1,\ldots,n\}$, где m – количество пользователей системы. Множество S является открытым. Для обмена информацией с пользователем u_j пользователь u_i извлекает подмножества S_i и S_j. Далее он вычисляет элементы, входящие в пересечение множеств $S_{ij}=S_i \cap S_j$. Парный ключ обмена сообщениями вычисляется с использованием набора ключевых материалов K, и подмножества S_{ij}: $k_{ij}=\oplus k_l \quad (l \in S_{ij})$.

Эти же операции выполняет пользователь u_j при получении сообщения от u_i.

Описанная схема подразумевает обмен сообщений каждого с каждым в обоих направлениях. Модифицируем схему, введя в нее асимметричность ключей $k_{ij} \neq k_{ji}$. Для этого также используем множество ключевых материалов K и множество подмножеств S. Для выработки ключа шифрования канала от u_j к u_i используем разность двух множеств: $\Delta S_{ij}=S_i \setminus S_j$. $k_{ij}=\oplus k_l \quad (l \in \Delta S_{ij})$.

Такой подход приводит к автоматическому выполнению требования асимметричности ключей. Для чтения сообщений пользователь u_i $(i=1,\ldots,m)$ будет использовать ключи k_{ij} $(j=1,..,m)$, а для отправки сообщений - ключи k_{ji} $(j=1,..,m)$. Предложенная схема основана на симметричном шифровании, что существенно ускоряет процессы шифрования и расшифрования.

Реализуем теперь запрет на каналы обмена информацией. Для этого потребуем, чтобы соответствующие парные ключи были нулевыми $k_{ji}=0$, то есть $\Delta S_{ij}=\varnothing$. Отсюда вытекают требования к множеству подмножеств S. Наиболее распространенным подходом к построению множества S является использования семейств Шпернера [1]. Семейством Шпернера [2] называется семейство подмножеств $D=\{D_1,...,D_n\}$ таких, что, если $D_i \cap D_j \subseteq D_t$, то либо $t=i$, либо $t=j$. В немодифицированной KDP-схеме на основе элементов семейства Шпернера D_i формируются подмножества S_{ij}. Используем аналогичный подход для решения поставленной задачи. Сформируем семейство Шпернера с количеством элементов, равным числу пользователей $D=\{D_1,...,D_m\}$. Множество S

будем формировать, двигаясь по дереву иерархии пользователей от листьев к корню. Выделим «листовых» пользователей u_1, …, u_l, где l – число листовых вершин дерева. Приравняем, соответствующие им элементы множества S, элементам семейства Шпернера $S_i=D_i$ (i=1,…,l). Поднимемся от листьев к корню дерева. Если вершина u_i имеет ближайших потомков u_{i1},…, u_{ik}, то этому пользователю соответствует множество:

$S_i=S_{i1}\cup S_{i2}\cup\ldots\cup S_{ik}\cup D_i$.

Данный алгоритм формирования множества S приводит к выполнению требуемого условия мандатного разграничения доступа: если $u_i > u_j$, то $S_i \supset S_j$, а, следовательно, $S_i \setminus S_j \neq \varnothing$, тогда как $S_j \setminus S_i = \varnothing$. Таким образом, пользователи могут сформировать парный ключ только для разрешенных каналов передачи информации. Также выполняется требование для несравнимых пользователей: если $u_i <> u_j$, то выполняются равенства $S_j \setminus S_i = \varnothing$ и $S_i \setminus S_j = \varnothing$.

Список литературы

1. O'Keefe C.M. Applications за finite geometries in information security // Australas. J. Combin. 1993. V. 7, P. 195 - 212.

2. Dyer M., Fenner T., Frieze A., Thomason A. On key storage in secure networks // J. Cryptology. 1995. V. 8, P. 189 - 200.

Материал поступил в редколлегию 23.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.7

Беляев Дмитрий Леонидович, *к.т.н., сотрудник*
Орлов Алексей Вячеславович*, сотрудник*
Олейник Светлана Игоревна*, сотрудник*
Академия Федеральной службы охраны Российской Федерации, г. Орёл, Россия
e-mail: dbelyaew@mail.ru

АНАЛИЗ ВАРИАНТОВ ПРИМЕНЕНИЯ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ ДЛЯ ОРГАНИЗАЦИИ СОРЕВНОВАНИЙ ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Проанализирован подход к применению облачной инфраструктуры под управлением OpenStack для организации и проведения соревнований по компьютерной безопасности.

Для разработки и тестирования новых приложений, а также развертывания облачных, мобильных и веб-приложений, получающих все необходимые для работы ресурсы может быть использован комплекс проектов свободного программного обеспечения OpenStack. Платформа Red Hat Enterprise Linux OpenStack Platform позволяет создавать частные облака для тестирования новых конфигураций и выполнения пилотных проектов, предъявляющих специфические требования к инфраструктуре и программному обеспечению.

Основные компоненты OpenStack и их взаимодействие представлены на рис. 1.

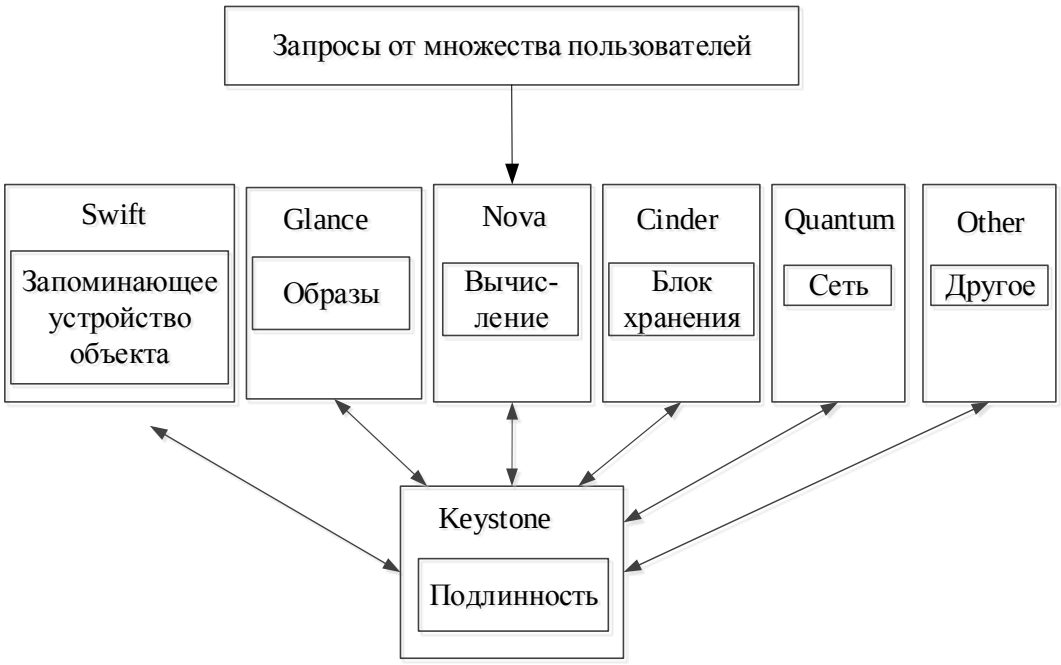

Рис.1. Компоненты OpenStack

На рис. 1 представлены:

- Swift – облачное файловое хранилище;
- Glance – библиотека образов виртуальных машин, обычно с бэкендом в Swift;
- Nova – контроллер вычислительных ресурсов;
- Cinder – служба работы с блочными устройствами хранения данных;
- Quantum – сервис «подключение к сети как услуга» между интерфейсами устройств (vNIC), которые управляются другими сервисами OpenStack;
- Keystone – сервис идентификации;

Специфика соревнований по компьютерной безопасности заключается в необходимости развёртывания:

- тестовых и лабораторных стендов;
- среды запуска программного обеспечения;
- среды разработки;
- среды автоматизированного тестирования.

Особенностью проведения таких соревнований является:

- срок существования виртуальных серверов для отработки тестовых задач, как правило, не превышает 1 недели.
- частое развёртывание однотипных служб;
- аппаратные ресурсы для развёртывания информационной инфраструктуры соревнований довольно часто выделяются по остаточному принципу, при этом, не обеспечивая требуемой производительности.

Единая облачная среда позволяет запускать и выполнять отдельно взятые виртуальны машины на различных аппаратных средствах, в наименьшей степени загруженных в текущий момент времени.

Ускорить развёртывание тестового окружения, сократить трудозатраты на моделирование различных ситуаций возможно с помощью облачной инфраструктуры, такой как OpenStack, позволяющей объединить вычислительные ресурсы. Развёртывание информационных сервисов на базе OpenStack является наиболее целесообразным решением.

С применением комплексного подхода, ориентированного на масштаб облачной среды веб-приложений, требуется разработать новые парадигмы пользовательского интерфейса, управления информацией и контроля доступа. Вместе они должны создать базу для организации и проведения соревнований по компьютерной безопасности, включающей площадки для развёртывания уязвимых информационных сервисов, задания по сетевой тематике и веб-приложения для оценивания результатов.

Список литературы

1. Хороших, Д. OpenStack и модель групповых политик/ Д. Хороших// Открытые системы. СУБД. – 2015. – № 1. – С.18-19.

2. Комашинский, В. В. Концептуальные и технологические основы защищённого управления информационной инфраструктурой сети: монография / В. В. Комашинский. – Орёл : Академия ФСО России, 2017. – 201 с.

Материал поступил в редколлегию 20.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.056

Беляев Дмитрий Леонидович, *к.т.н., сотрудник*
Титов Владислав Геннадьевич, *сотрудник*
Академия ФСО России, *Орёл, Россия*
e-mail: *dbelyaew@mail.ru*

ОЦЕНКА ВЛИЯНИЯ КРИПТОГРАФИЧЕСКИХ ТУННЕЛЕЙ НА КАЧЕСТВО ПРЕДОСТАВЛЕНИЯ МУЛЬТИСЕРВИСНЫХ УСЛУГ

Представлены результаты исследования по определению степени влияния криптографических туннелей на параметры качества обслуживания, а также результаты разработки программного средства данной направленности.

Актуальность повышения качества обслуживания растет пропорционально увеличению количества передаваемого трафика. Данная закономерность диктует свои требования к обеспечению необходимого качества обслуживания путём управления параметрами QoS. Задержка видео- или аудио- данных может сильно отразиться на восприятии доносимой информации и как следствие - повлиять на оперативность и результативность принятия решений. Изображения и текстовые файлы не относятся к информации, чувствительной к задержкам, поэтому особое внимание отдается повышению качества обслуживания при организации видеоконференций и IP-телефонии.

В процессе взаимодействия пользователей на удаленном расстоянии причинами ухудшения представленных параметров являются неправильная настройка коммутационного оборудования или перегруженность канала из-за передачи больших объёмов информации. Величина задержки, а также других параметров QoS зависит от степени загруженности криптографической подсистемы маршрутизатора. При увеличении числа пакетов, для которых необходимо выполнить криптографические преобразования возможно увеличение очередей, приводящих к возникновению задержек и снижающих производительность интерфейсов.

Для организации безопасной передачи информации между пользователями сети используется большое число криптографически защищённых соединений. При этом они могут устанавливаться как с помощью средств из состава рабочих мест пользователей, так и с помощью специализированных маршрутизаторов с функциями криптозащиты. Использование криптотуннеля обеспечивает безопасную передачу данных, но из-за привлечения дополнительной вычислительной мощности на реализацию криптографических алгоритмов происходит изменение параметров QoS, которое отрицательно сказывается на качестве передачи данных.

Учитывая необходимость обеспечения безопасности передаваемых данных, а также обеспечение поддержания высокого качества обслуживания, было проведено исследование, которое позволило определить степень влияяния криптотуннелей на параметры QoS. Исследуемая топология сети представлена на рис. 1.

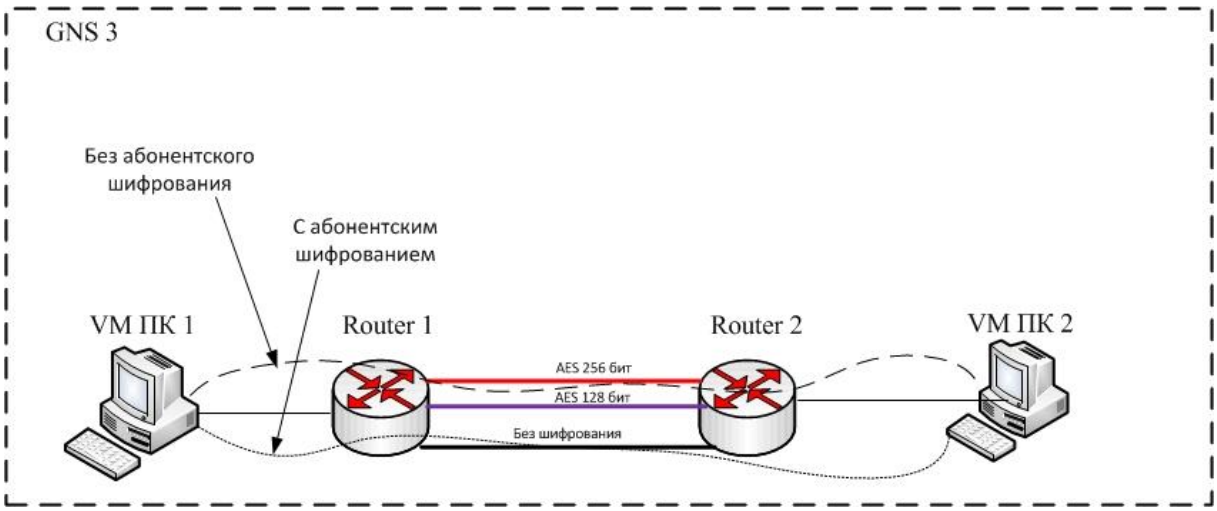

Рис. 1. Исследуемая топология сети

Данная структура позволяет имитировать работу мультисервисной сети использующей криптографические туннели при передаче данных, а также работу службы качества обслуживания. Ключевыми элементами топологии являются два маршрутизаторы которые в физической сети могут быть представлены в виде криптошлюзов, маршрутизаторов или криптомаршрутизаторов.

Для организации криптотуннеля на маршрутизаторах настроена работа по протоколу IPsec. Данный протокол используются для безопасной передачи данных, голоса и видео. Шифрование данных реализовано по алгоритму AES. Между маршрутизаторами исследуемой топологии установлено несколько соединений, что обеспечивает независимость и полноту исследования, а так же позволяет осуществить передачу данных по зашифрованному или незашифрованному каналу в соответствии с наличием шифрования на абонентской стороне.

Настройка службы качества обслуживания осуществляется посредством конфигурирования соответствующих политик. Мониторинг изменения параметров QoS реализован с помощью настройки SLA-теста на маршрутизаторах.

Для генерации маркированного трафика между виртуальными машинами VM1 и VM2 используется программа jperf. Данная утилита имитирует работу сети в режиме предоставления мультисервисных услуг и позволяет нагрузить виртуальные каналы до состояния сети при ее перегрузке.

В мультисервисных сетях процесс настройки криптотуннелей и службы качества обслуживания не автоматизирован. Использование программного

средства, изображенного на рис. 2, позволяет построить криптотуннели и настроить технологию качества обслуживания, а также повысить производительность сети и снизить временные затраты на конфигурацию маршрутизирующего оборудования. Программное обеспечение устанавливается непосредственно на оконечном оборудовании и осуществляет заданные настройки путём подсоединения к удаленным маршрутизаторам по протоколу telnet. Для разграничения доступа к данному ПО реализована функция аутентификации по логину и паролю.

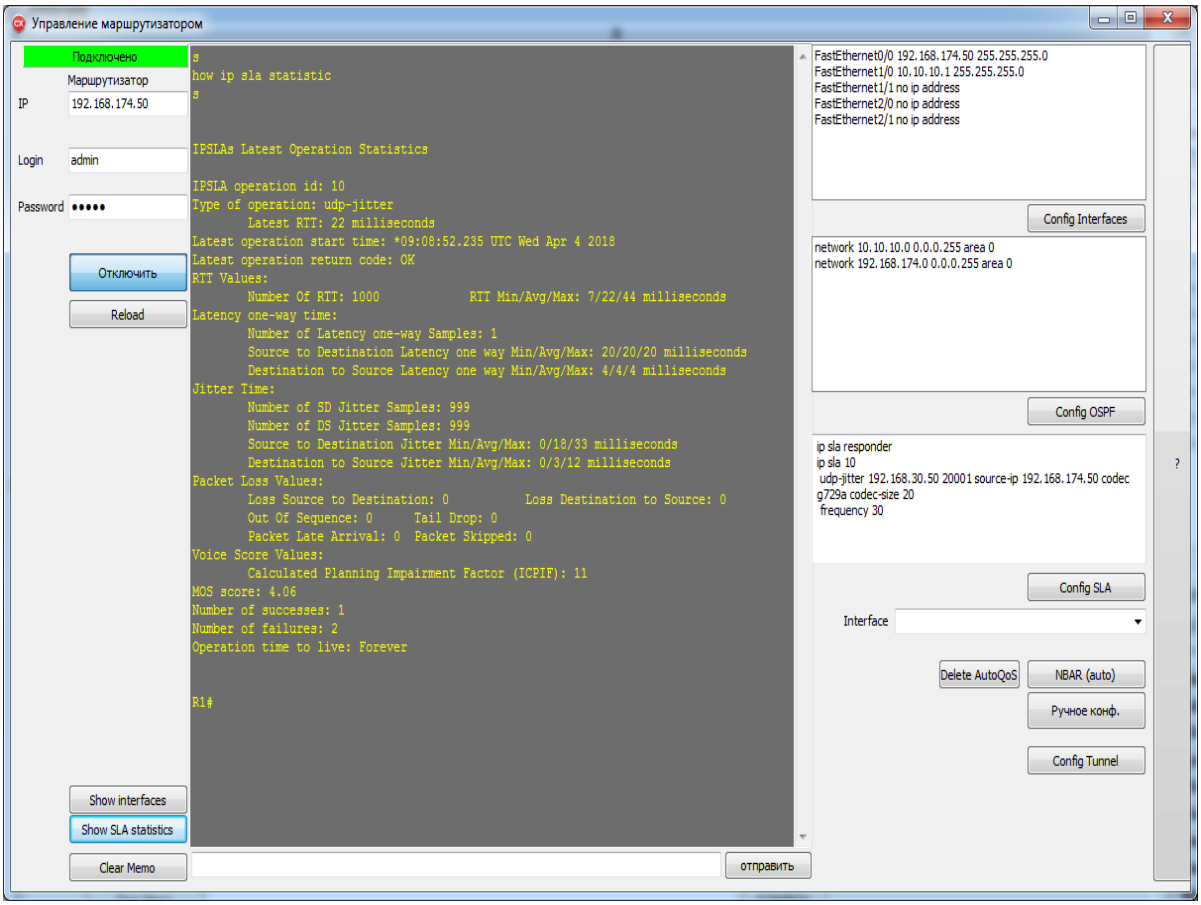

Рис. 2. Интерфейс программного средства

Основными функциями программного средства является настройка криптотуннелей с различной длиной ключа шифрования, для анализа изменения параметров качества обслуживания при передаче одного трафика по различным криптотуннелям, а также добавления политик качества обслуживания. Помимо основных функций, в программе реализован сбор информации о маршрутизаторе и представлении ее в удобном виде, к данной информации относятся сведения об интерфейсах и маршрутизации. Программное средство позволяет быстро производить базовую настройку маршрутизатора как в автоматическом режиме путем использования соответствующих кнопок, так и в ручном режиме по аналогии с работой через консоль маршрутизатора.

Программное средство осуществляет сбор данных о параметрах QoS в определённые промежутки времени. Задача вывода полученных значений в виде графика на настоящий момент является нерешённой, поэтому все графики построены в ручном режиме на основе данных, полученных при помощи программы.

Данные об изменении процента потерянных пакетов и джиттера представлены на рис. 3, 4 соответственно.

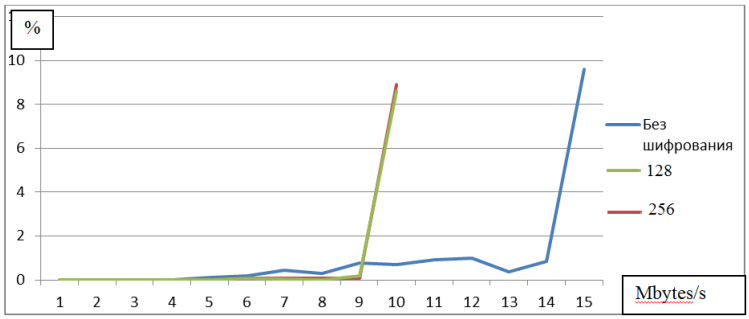

Рис. 3. График зависимости количества потерянных пакетов от скорости передачи и длины ключа шифрования

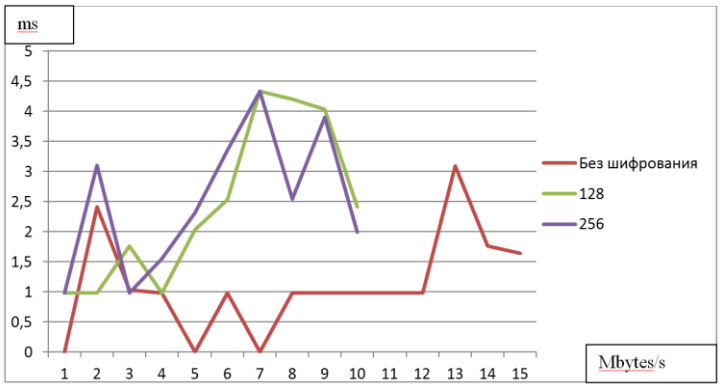

Рис. 4. График зависимости джиттера задержки от скорости передачи и длины ключа шифрования

Как видно из представленных графиков, в ходе исследования было выявлено увеличение числа потерянных пакетов и величины джиттера задержки при передаче данных по зашифрованному каналу по сравнению с передачей того же типа данных по каналу без шифрования. Это связано с привлечением дополнительной вычислительной мощности из-за подключения криптоядра маршрутизатора при шифровании трафика. Для анализа параметров QoS была выбрана передача UDP пакетов, которые являются чувствительными к джиттеру и потере пакетов. По результатам работы стенда получили значения параметров QoS при прохождении через криптотуннели с длиной ключа 128 и 256 бит.

На основе полученных данных можно сформировать общий вывод. Криптотуннели вносят задержку передачи и вызывают дополнительную потерю па-

кетов, это связано с потребностью в трате некоторого времени t на шифрование пакета данных прежде чем начинается его передача. Влияние криптотуннелей на скорость передачи выражено, в первую очередь, в ее ограничении. Конечно же, следует отметить, что данные показатели при использовании другого оборудования будут иметь отличные значения, но в общем влияние криптотуннеля на параметры QoS очевидно.

Дальнейшим направлением исследования является автоматизация построения графиков по полученным параметрам QoS и автоматизация перенаправления трафика по каналам в соответствии с текущей характеристикой защищённости данных, приходящих на маршрутизатор. Решение таких задач позволит повысить производительность сети и, как следствие, улучшит значения параметров качества обслуживания.

Список литературы

1. Беляев, Д.Л. Разработка приложений для конфигурирования политик качества обслуживания в маршрутизаторах Cisco / Д. Л.Беляев, М. Х. Нгуен // Информационная безопасность и защита персональных данных. Про блемы и пути их решения: Материалы IX Межрегиональной научно-практической конференции [Электронный ресурс]/ под ред. О. М. Голембиовской, М.Ю.Рытова. – Брянск: БГТУ, 2017. – С. 23-26.

Материал отправлен в редколлегию 20.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.056

Васинёв Дмитрий Александрович, *к. т. н. сотрудник*
Кушнир Кирилл Евгеньевич, *сотрудник*
Академия ФСО России*, Орёл, Россия*
e-mail: kirill.kysh06041996@yandex.ru

РАЗРАБОТКА И ОБОСНОВАНИЕ ТЕХНИЧЕСКИХ РЕШЕНИЙ ПО МОДЕРНИЗАЦИИ УЗЛА КОММУТАЦИИ С ИСПОЛЬЗОВАНИЕМ ОТЕЧЕСТВЕННОГО ДОВЕРЕННОГО ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ

Представлено исследование существующего узла доступа к сети с коммутацией пакетов на основе телекоммуникационного оборудования Cisco. Рассмотрен разработанный прототип узла на основе отечественного доверенного оборудования АПКШ «Континент». Предложено решение по построению узла на основе изделия М-479Р, являющегося полнофункциональным маршрутизатором и шифратором.

В настоящее временя для организации обмена данными по различным каналам связи и с использованием различных технологий используется мультипротокольное оборудование Cisco и Juniper. Данное оборудование показывает себя надежно в различных условиях и удовлетворяет в большинстве случаев требованиям заказчика.

У большинства развивающихся организаций, филиалы которых находятся в разных городах, странах, возникает проблема соединения локальных сетей организаций в единую сеть организации. Данная проблема решается путем аренды каналов у оператора связи.

Основными сервисами, предоставляемыми оператором связи для соединения разрозненных точек какой-либо организации, являются сервисы находящиеся на втором либо третьем уровне эталонной модели взаимодействия открытых систем. В настоящее время в транспортной сети оператора связи распространена технология MPLS. При установке на стороне пользователя оборудования иностранного производства, такого как Cisco или Juniper, проблемы взаимодействия пользователя и оператора не возникает. Использование иностранного оборудования у пользователя снижает уровень доверия к сети. Существуют требования по использованию телекоммуникационного оборудования, а именно:

– телекоммуникационное оборудование должно быть российского производства;

– используемое телекоммуникационное оборудование должно быть сертифицировано ФСБ России.

При выполнении данных требований возникает проблема взаимодействия оборудования отечественного производства и оборудования оператора связи. В настоящее время оборудования российского производства, реализующего технологию MPLS, нет.

У технологий, работающих на втором и третьем уровне, имеются свои преимущества и недостатки. На третьем уровне возможна реализация распространённого защитного механизма IPSec, механизмов качества обслуживания. На втором же уровне сохраняется адресная схема сети, возможность использования одной сети для разрозненных точек организации, также реализация технологии второго уровня намного проще.

Особое место при организации связи является подключение удалённых абонентов. При подключении определённых абонентских устройств необходимо предоставить данным абонентам определённые услуги связи: IP-телефония, видеосвязь, передача сообщений в рамках сервиса электронной почти. В зависимости от вида сервиса определяется его чувствительность к задержкам, пропускной способности.

Исходное решение узла коммутации СКП было основано на использовании оборудования фирмы Cisco. Оборудование данного производителя обеспечивает удовлетворение требований как чувствительных к задержке сервисов (видеоконференцсвязь, IP-телефония), так и не чувствительных к ней (передача данных, система документальной связи). На уровне доступа используется коммутатор Cisco 2960. За маршрутизацию в данной реализации узла доступа к СКП отвечает маршрутизатор Cisco 2911. Для сохранения адресации использовались L2VPN каналы. Маршрутизация трафика осуществлялась с использованием технологии VRF. Для каждого канала имелась своя таблица маршрутизации, что разграничивало трафик, передающийся по различной физической среде. Схема связи, реализованная на основе данного оборудования, представлена на рис. 1.

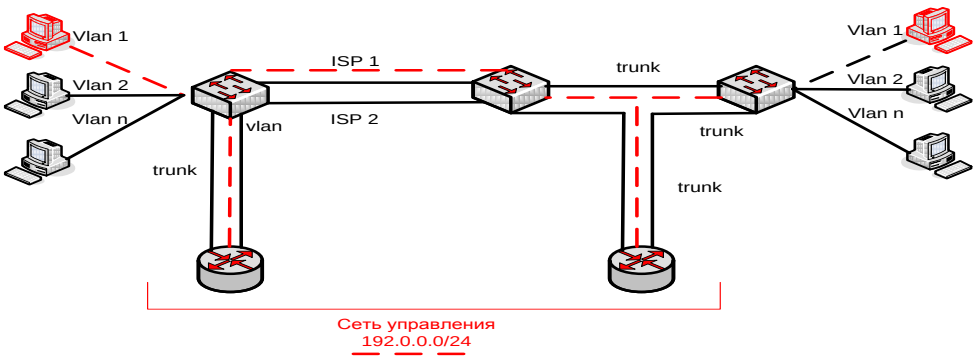

Рис. 1. Схема организации узла коммутации на основе оборудования Cisco

Технология L2VPN в отличие от технологии L3VPN может передавать трафик не только по протоколу IP, но и с помощью многих других протоколов в

рамках технологии AToM. Для работы телекоммуникационной составляющей данной схемы, то есть корректной передачи трафика различных сервисов, для каждой услуги, в том числе управления оборудованием, был выделен отдельный L2VPN канал. Абонентские устройства подключались через различные VLAN коммутатора доступа. Уже на данном этапе реализовывался механизм безопасности.

Оборудование Cisco является специализированным, отличается высокой производительностью и надежностью и по большей части удовлетворяет требованиям современных мультимедийных услуг по пропускной способности, резервированию маршрутов, способности к восстановлению после сбоев. Однако операционные системы данного оборудования являются закрытыми, что, в свою очередь, снижает степень доверия к сети. Производство данного оборудования также производится за рубежом.

Обозначенная проблема была решена в ходе исследований возможности применения отечественного коммуникационного оборудования. В рамках исследования применялось оборудование АПКШ "Континент" в качестве устройства организации L2VPN каналов, Поток-К в качестве абонентского коммутатора и Поток-КМ в качестве граничного устройства при соединении с оператором связи, выполняющего маршрутизацию трафика во внешние сети. Данные устройства отечественного производства и имеют сертификат ФСБ. Результатом исследований был разработан стенд, представленный на рис. 2.

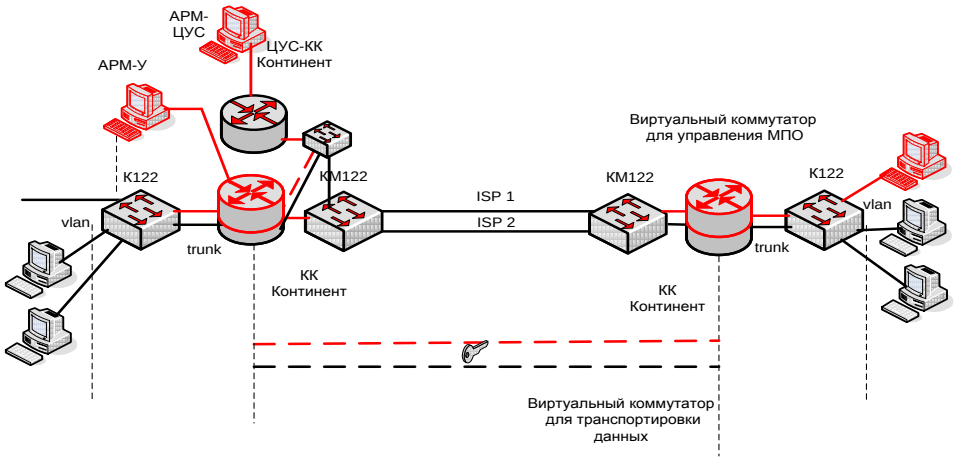

Рис. 2. Схема организации узла коммутации на основе оборудования АПКШ "Континент"

Из всей линейки АПКШ "Континент" был выбран криптокуммутатор. Выбор данного устройства был обусловлен следующими факторами:

– сохранение существующей схемы адресации;
– быстрота работы;
– нагрузка канала;
– реализация механизмов безопасности.

Аппаратно-программный комплекс шифрования реализует систему защиты информации в виде централизованной системы управления, СКЗИ, межсетевого экрана и детектора атак [1].

Разработанная схема имеет существенные недостатка:

– стоимость оборудования;

– невозможность реализации механизмов качества обслуживания на данных версия программного обеспечения телекоммуникационных устройств;

– невозможность работы по каналам L3, то есть фактическое количество каналов уменьшается.

Решением данных проблемы может послужить узел коммутации сети с коммутацией пакетов, построенный на основе отечественного доверенного коммуникационного оборудования Поток-К122 и М479-Р. Схема данного узла представлена на рис. 3.

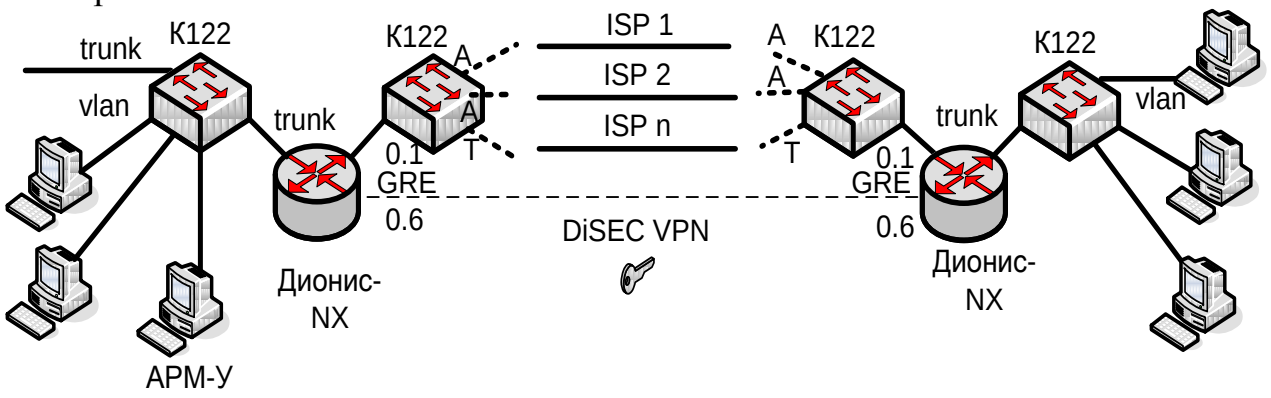

Рис. 3. Схема организации узла коммутации на основе оборудования "Дионис"

Данная схема относительно разработанных и представленных ранее обладает следующими преимуществами:

– узел коммутации разработан полностью на отечественном коммуникационном оборудовании;

– стоимость данной схемы организации узла существенно ниже схемы, построенной на основе оборудования АПКШ "Континент";

– существует возможность реализации механизмов обеспечения качества обслуживания [2].

Направление дельнейших исследований представляет собой проведение экспериментов над разработанной схемой, проверка реализации механизмов качества обслуживания и выполнения требований информационной безопасности.

Список литературы

1. ООО "Информзащита". [Электронный ресурс]. – URL: http://securitycode.ru (Дата обращения 10.03.2018).

2. "ФАКТОР-ТС". [Электронный ресурс]. – URL: http://factor-ts.ru (Дата обращения 16.03.2018).

Материал поступил в редколлегию 23.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.056

Васинёв Дмитрий Александрович, *к. т. н., сотрудник*
Вафин Дамир Фаритович, *сотрудник*
Академия ФСО России*, Орёл, Россия*
e-mail: damir.romanov11@gmail.com

РАЗРАБОТКА И ОБОСНОВАНИЕ ТЕХНИЧЕСКИХ РЕШЕНИЙ ПО МОДЕРНИЗАЦИИ УЗЛА КОММУТАЦИИ С ИСПОЛЬЗОВАНИЕМ ОТЕЧЕСТВЕННОГО ДОВЕРЕННОГО ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ

Представлены схемы модернизации узла связи, с использованием отечественного доверенного мультипротокольного оборудования, рассмотрены пути решения для достижения требуемого качества обслуживания для различного рода трафика, а также обеспечение резервирования каналов передачи данных.

Современное состояние сетей с коммутацией пакетов характеризуются широким применением различных технологий построения сетей у операторов связи, предоставлением широкого спектра транспортных услуг абоненту, а также поддержки современных инфокоммуникационных услуг, с учетом возможностей устаревающего парка коммуникационного оборудования.

В настоящее время инфраструктура сетей с коммутацией пакетов (СКП) характеризуется применением структурирующего коммуникационного оборудования, как правило, иностранного производства, например Cisco, Juniper и другие, которое позволяет строить сети, удовлетворяющие заданным требованиям, предоставляющие мультимедийные услуги. При этом важно отметить, что ни уровень развития применяемого оборудования, ни качество разработки программных продуктов, реализующих функционал операционной системы, не дают гарантии безошибочной работы коммуникационного оборудования СКП. Оборудования данных компаний удовлетворяют многим требованиям, таким как производительность, высокая отказоустойчивость, пропускная способность, масштабируемость и многое другое. Это оборудование производится в иностранных государствах, что осложняет обеспечение информационной безопасности и снижает уровень доверия к сети. Использование отечественного доверенного телекоммуникационного оборудования помогает решить данную проблему.

В связи с этим имеется необходимость перехода на сети с коммутацией пакетов, в основе которых будет функционировать коммуникационное оборудование отечественного производства.

Основной целью развития СКП является создание специальной телекоммуникационной инфраструктуры, отвечающей требованиям по информа-

ционной безопасности и обеспечивающей устойчивое функционирование в различных условиях обстановки.

Для защиты системы управления и телекоммуникационной инфраструктуры СКП от несанкционированного доступа, компьютерных атак и других действий вероятных нарушителей безопасности информации применяется система информационной безопасности СКП.

В данном случае особый интерес представляют разработки компаний "Код Безопасности" и «ИнфоТекс», реализующие в виде аппаратно-программного комплекса шифрования систему защиты информации в виде централизованной системы управления, СКЗИ, межсетевого экрана и детектора атак.

АПКШ "Континент" позволяет реализовать защиту (шифрование и межсетевое экранирование) каналов связи и управления при передаче информации ограниченного доступа между сегментами сложных распределенных сетей федерального масштаба по открытым и выделенным (ведомственные и корпоративные СПД) каналам связи, обеспечивая резервирование и балансировку имеющихся каналов связи, а также возможность приоритезации сетевого трафика, обеспечивает возможность работы с сетями IPv6. АПКШ "Континент" содержит интегрированную систему обнаружения вторжений и позволяет строить как L3, так и L2 VPN туннели [1].

АПКШ «Континент» также поддерживает следующие дополнительные возможности [1]:

- поддержка распространенных каналов связи;
- работа с высокоприоритетным трафиком;
- резервирование гарантированной полосы пропускания за определенными сервисами;
- поддержка VLAN;
- скрытие внутренней сети. Поддержка технологий NAT/PAT;
- NAT внутри VPN-связей;
- интеграция с внешними системами анализа событий безопасности;
- маршрутизация трафика (Статическая, RIP, OSPF, BGP);
- поддержка NTP на ЦУСе;
- режим повышенной безопасности;
- возможность интеграции с системами обнаружения атак;
- защита от DoS-атак типа SYN-flood;
- функционал DHCP сервера на КШ.

Физическая модель для исследования мультипротокольного оборудования (АПКШ «Континент», коммутаторы «Поток – К-122» и «Поток – КМ-122») отечественного производства на предмет оптимизации схемы организации транспортировки данных в СКП.

В настоящий момент транспортировка данных осуществляется на оборудовании иностранного производства таких как Cisco, Juniper и др. Общая схема взаимодействия двух узлов изображена на рис. 1.

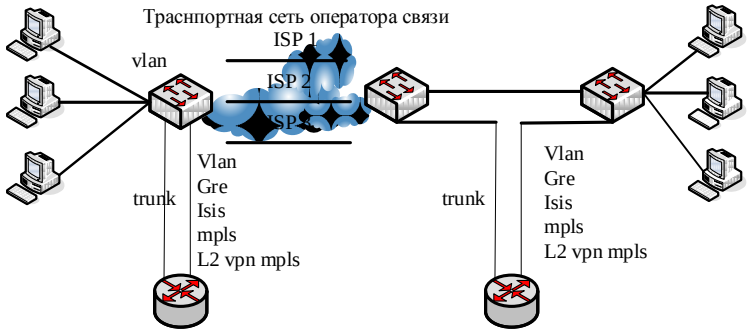

Рис. 1. Схема взаимодействия узлов на оборудовании Cisco

Существуют некоторые требования к системам связи:

– обеспечение конфиденциальности и целостности данных, передаваемых по каналам связи;

– поддержка единого адресного пространства для защищаемой ЛВС систем связи;

– быстродействие и производительность;

– масштабируемость;

– отказоустойчивость.

Для реализации защиты каналов связи между географически распределёнными системами связи рекомендуется использовать технологию VPN (виртуальные защищенные сети). Классические технологии VPN, широко представленные на рынке (IPsec, SSL VPN, ViPNet VPN), разработаны для построения защиты каналов связи в тех случаях, когда в системах связи используется различное адресное пространство и общение серверов, объектов сети производится посредством маршрутизации данных. Особенностью эластичных систем связи является то, что общение всех объектов ЛВС систем связи происходит напрямую без использования маршрутизации данных. Достигается этот эффект благодаря использованию специализированного оборудования, объединяющего ЛВС всех систем связи в единый домен общения. В такой ситуации классические технологии построения VPN уступают.

Для решения поставленной задачи компания «Код Безопасности» разработала технологию L2OverIP. L2OverIP — это технология построения VPN, которая позволяет организовать защиту распределенных сегментов ЛВС систем связи, использующих единое адресное пространство, на канальном уровне модели OSI. В результате узлы из разных сегментов могут взаимодействовать друг с другом так, как если бы они находились в одном сегменте с прямой видимостью.

Функционал L2OverIP позволяет объединить несколько сегментов сети, в том числе сегменты, разделенные на виртуальные локальные сети (VLAN). При этом возможны различные варианты объединения:

– объединение сегментов без VLAN;

– объединение нескольких или одной из используемых VLAN в разных сегментах;

– объединение одного из используемых VLAN сегмента с сегментами без VLAN.

Преимуществом последних версий криптокоммутаторов является то, что они позволяют обеспечивать качество обслуживания для различного вида трафика.

Коммутатор «Поток – К-122» будет использоваться для создания сегментов локальной вычислительной сети. На устройстве поддерживается до 1024 VLAN 802.1q. Каждый порт может быть «приписан» к какой-либо VLAN - как тегированный порт или как не тегированный порт. С помощью данного коммутатора с использованием протокола 802.1q будут разделяться различные виды трафика и присваиваться различные метки качества обслуживания [2].

Коммутатор маршрутизирующий «Поток – КМ-122» поддерживает до 4096 VLAN 802.1q. Каждый порт, включая порты стекирования и агрегированные порты, может быть «приписан» к какой-либо VLAN - как тегированный порт или как не тегированный порт. Для надежности маршрутизации реализован механизм резервных маршрутов. При реализации отказоустойчивых подключений 3-го уровня следует использовать именно механизм маршрутизации с резервными маршрутами, и не использовать статические маршруты [3].

Таким образом, применение криптографических коммутаторов «Континент», коммутаторы «Поток – К-122» и «Поток – КМ-122» схема взаимодействия узлов будет следующей (рис. 2).

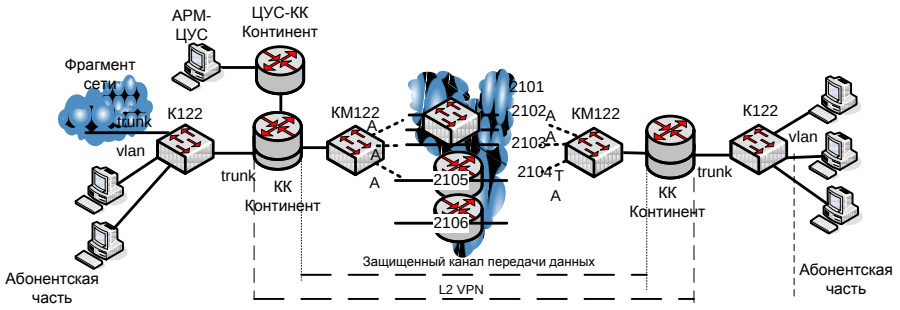

Рис. 2. Схема взаимодействия узлов с использованием отечественного оборудования

Направлением дальнейшей работы является в условиях повышенной загружённости обеспечить необходимое качество обслуживания для разного вида передаваемой информации, так как существуют виды трафика критичные к за-

держке, например видео. Для этого на коммутаторе «Поток – К-122» будут присваиваться метки качества обслуживания, а затем передаваться на криптокоммутатор «Континент». С учетом того, что последние версии криптокоммутаторов поддерживают обработку тегированного трафика, будет обеспечиваться необходимый уровень качества обслуживания передаваемой информации. Для недопущения прерывания передачи по каналу связи используется «Поток – КМ-122», который с определенной периодичностью проверяет работоспособность канала и обеспечивает его резервирование.

Альтернативной схемой решения проблем возникших с качеством обслуживания и обеспечения отказоустойчивости является схема, представленная на рис. 3.

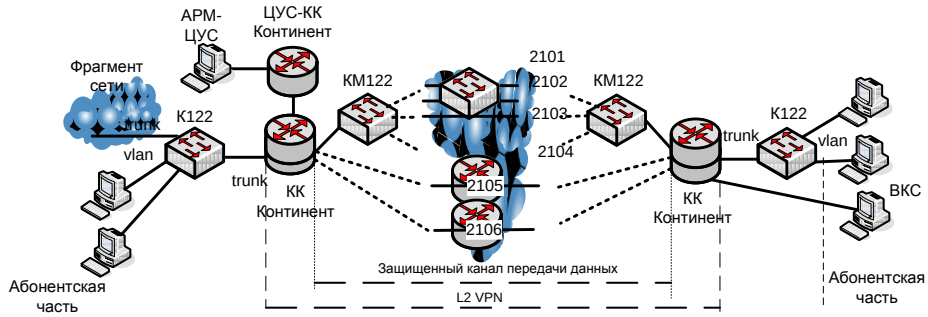

Рис. 3. Структура защищенной сети с раздельным подключением каналованалогов L2 и L3 к криптокоммутатору

В данной схеме решается проблема с обеспечением приоритетного обслуживания видео трафика, выполнения требований по отказоустойчивости с помощью реализованных механизмов резервирования каналов на устройстве АПКШ «Континент» и устройстве «Поток – КМ-122».

Список литературы

1. Комплект документации «Руководство администратора АПКШ «Континент». Централизованное управление комплексом» – М.: Информзащита, 2015.
2. ЕКВМ.465235.006РЭ.
3. ЕКВМ.465235.010РЭ_122Ф.

Материал поступил в редколлегию 23.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.056

Голембиовская Оксана Михайловна, *к.т.н., доц. каф. «Системы информационной безопасности»*
Шинаков Кирилл Евгеньевич, *асс. каф. «Системы информационной безопасности»*
Карюк Елена Александровна, *магистрант каф. «Системы информационной безопасности»*
ФГБОУ ВО «Брянский государственный технический университет»
г. Брянск, Россия
Bryansk-tu@yandex.ru

АНАЛИЗ ВОЗМОЖНЫХ ФИНАНСОВЫХ ПОТЕРЬ ОТ НАРУШЕНИЯ СВОЙСТВ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Рассмотрены различные виды финансовых потерь, связанные с нарушением свойств безопасности конфиденциальной информации.

На сегодняшний день одним из немаловажных факторов при определении целесообразности финансовых трат при построении системы защиты информации на предприятии является понимание руководством возможного ущерба от разглашения, удаления и изменения конфиденциальной информации. Так, в случае если ущерб будет рассчитан как превышающий сумму затрат на построение СЗИ, то данное направление представляется целесообразным и необходимым к финансированию.

Ввиду этого рассмотрим возможные случаи финансовых потерь от нарушения обозначенных свойств безопасности конфиденциальной информации:

1.Финансовые потери, связанные с прерыванием сервиса

Остановка в работе предприятия обязательно приведет к финансовым потерям, так как предприятие, в первую очередь, не сможет получать прибыль от оказания услуг или реализации товара. Также предприятие понесет дополнительные финансовые потери, связанные с прерыванием сервиса, такие как оплата аренды помещения и оплата коммунальных услуг. Таким образом, финансовые потери, связанные с прерывание сервиса можно описать как:

$$P_{itrrpt} = (\text{Размер ежедневной прибыли} + \text{Стоимость коммунальных услуг/день} + \text{Стоимость аренды/день}) * \text{Количество дней простоя предприятия.}$$

2.Финансовые потери, связанные с утратой клиентов

Нарушение свойств безопасности информации неизбежно приводит к утрате доверия клиентов и соответственно к отказу от сотрудничества с предприятиями. Таким образом, финансовые потери, связанные с утратой клиентов, можно описать как:

$$P_{client} = \text{Размер прибыли от 1 клиента} * \text{Количество потерянных клиентов.}$$

3.Финансовые потери, связанные с нарушением внутреннего функционирования

Нарушение свойств безопасности может привести к нарушению функционирования одного или нескольких отделов предприятия. Потери, связанные с нарушение внутреннего функционирования, связаны с оплатой труда сотрудников, работа которых приостановлена в результате нарушения. Таким образом, финансовые потери, связанные с нарушением внутреннего функционирования, можно описать как:

$P_{function}$ = (Заработная плата сотрудника, работа которого остановлена в результате нарушения/час * Количество часов, затраченных на восстановление работоспособности) * Количество сотрудников, работа которых остановлена в результате нарушения.

4.Финансовые потери, связанные с нарушением условий договора

В случае нарушения условий договора сторона ответственная за это несет убытки в размере неустойки, предусмотренной в договоре, а также в размере ожидаемой прибыли, предусмотренной условиями исполнения договора. Также сторона, нарушившая условия договора, несет ответственность за данное деяние в соответствии со ***ст. 7.32 КоАП РФ Нарушение порядка заключения, изменения контракта.***

Таким образом, финансовые потери, связанные с нарушение условий договора можно описать как:

1. $P_{contract}1$ = Размер неустойки, предусмотренный договором + Размер ожидаемой прибыли.

или

2. $P_{contract}2$ = {$P_{contract}21$, $P_{contract}22$, $P_{contract}23$, $P_{contract}24$, $P_{contract}25$, $P_{contract}26$, $P_{contract}27$, $P_{contract}28$, $P_{contract}29$, $P_{contract}210$ }, (табл. 1):

Таблица 1

Финансовые потери, связанные с нарушением условий договора

$P_{contract}2x$	Ст. 7.32 КоАП РФ	Штраф
$P_{contract}21$	п.1	*Административный штраф для ЮЛ* – 1 % от начальной (максимальноц) цены контракта, но не менее 50 000 и не более 300 000 рублей
$P_{contract}22$	п.2	*Административный штраф для ЮЛ* – Двукратный размер дополнительно израсходованных средств
$P_{contract}23$	п.3	-
$P_{contract}24$	п.4	*Административный штраф для ЮЛ* – 200 000 рублей
$P_{contract}25$	п.5	*Административный штраф для ЮЛ* – Двукратный размер дополнительно израсходованных средств
$P_{contract}26$	п.6	*Административный штраф для ЮЛ* – 200 000 рублей

Окончание табл. 1

$P_{contract}27$	п.7	*Административный штраф для ЮЛ* – 1-3х кратный размер стоимости неисполненных обязательств, предусмотренных контрактом, но не менее 300 000 рублей
$P_{contract}28$	п.8	-
$P_{contract}29$	п.9	-
$P_{contract}210$	п.10	-

5.Финансовые потери, связанные с нарушением неприкосновенности частной жизни персонала/пользователя

Незаконный сбор или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, наказываются штрафом или иным образом, предусмотренным ***Ст. 137 п.1 УК РФ Нарушение неприкосновенности частной жизни.***

Таким образом, финансовые потери, связанные с нарушением неприкосновенности частной жизни персонала/пользователей, можно описать как:

$P_{privacy}$ ***= 200 000 рублей (заработная плата или иной доход за период до 18 месяцев.)*** – Ст. 137 п.1 УК РФ.

6.Нарушение норм/законов

Нарушение свойств безопасности непосредственно связано с нарушением законодательства РФ. Ниже рассмотрим основные статьи Уголовного Кодекса и Кодекса об административных правонарушениях РФ. Финансовые потери вследствие нарушения норм/законов РФ будем определять суммой вероятных штрафов, предусмотренных соответствующими статьями УК РФ и КоАП РФ. Таким образом, финансовые потери, связанные с нарушением норм/законов РФ, можно описать как:

P_{fine} ***= {Pfine1,*** P_{fine}***2,*** P_{fine}***3,*** P_{fine}***4,*** P_{fine}***5,*** P_{fine}***6,*** P_{fine}***7,*** P_{fine}***8,*** P_{fine}***9,*** P_{fine}***10,*** P_{fine}***11,*** P_{fine}***12,*** P_{fine}***13},*** (табл. 2)

Таблица 2

Финансовые потери, связанные с нарушением норм/законов РФ

$P_{fine}x$	Статья	Штраф
УК РФ		
Pfine1	Ст. 147 п.1 Нарушение изобретательских и патентных прав	*Штраф* в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев
Pfine2	Ст. 159.6 п.1 Мошенничество в сфере компьютерной информации	*Штраф* в размере до 120 000 рублей или в размере заработной платы или иного дохода осужденного за период до 1 года
Pfine3	Ст. 172.1 Фальсификация финансовых документов учета и отчетности финансовой организации	*Штраф* в размере от 300 000 до 1 000 000 рублей или в размере заработной платы или иного дохода осужденного за период от 2х до 4х лет

Pfine4	Ст. 183 п.2 Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну	*Штраф* в размере до 1 000 000 рублей или в размере заработной платы или иного дохода осужденного за период до 2х лет
Pfine5	Ст. 272 п.1 Неправомерный доступ к компьютерной информации	*Штраф* в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев
Pfine6	Ст. 272 п.2 Неправомерный доступ к компьютерной информации	*Штраф* в размере от 100 000 до 300 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 2х лет
	КоАП РФ	
Pfine7	Ст. 5.27 п.6 Нарушение трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права	*Административный штраф* на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, - от 1 000 до 5 000 рублей; на юридических лиц - от 30 000 до 50 000 рублей.
Pfine8	Ст. 5.29 Непредоставление информации, необходимой для проведения коллективных переговоров и осуществления контроля за соблюдением коллективного договора, соглашения	*Административный штраф* в размере от 1 000 до 3 000 рублей
Pfine9	Ст. 7.12 п.2 Нарушение авторских и смежных прав, изобретательских и патентных прав	*Административный штраф* на юридических лиц - от 30 000 до 40 000 рублей.
Pfine10	Ст. 13.11 п.4 Нарушение законодательства РФ в области персональных данных	*Административный штраф* на индивидуальных предпринимателей - от 10 000 до 15 000 рублей; на юридических лиц - от 20 000 до 40 000 рублей.
Pfine11	Ст. 13.11 п.5 Нарушение законодательства РФ в области персональных данных	*Административный штраф* на индивидуальных предпринимателей - от 10 000 до 20 000 рублей; на юридических лиц - от 25 000 до 45 000 рублей.
Pfine12	Ст. 13.11 п.6 Нарушение законодательства РФ в области персональных данных	*Административный штраф* на индивидуальных предпринимателей - от 10 000 до 20 000 рублей; на юридических лиц - от 25 000 до 50 000 рублей.
Pfine13	Ст. 13.12 п.1 Нарушение правил защиты информации	*Административный штраф* на юридических лиц - от 15 000 до 20 000 рублей.

7.Финансовые потери, связанные с затратами на разработку проекта

На каждом этапе разработки проекта предприятие неизбежно понесет финансовые потери вследствие нарушения свойств безопасности коммерческой тайны и информации о сущности изобретения, полезной модели или промышленного образца до момента официальной публикации сведений о них. Рассмотрим 3 основных этапа жизненного цикла проекта – проектирование, разработка и выпуск продукции.

Нарушение свойств безопасности на этапе проектирования приведет к финансовым потерям в размере заработной платы персонала, работающего над проектом. Таким образом, финансовые потери на этапе проектирования опишем как

$P_{project\_design}$ = заработная плата персонала работающего над проектом.

Нарушение свойств безопасности на этапе разработки приведет к финансовым потерям в размере заработной платы персонала, работающего над проектом, стоимости сырья, затраченного на момент нарушения, и стоимость обслуживания оборудования, используемого для разработки. Таким образом, финансовые потери на этапе разработки опишем как:

$P_{project\_dvlp}$ = заработная плата персонала работающего над проектом + стоимость сырья + стоимость обслуживания оборудования.

Нарушение свойств безопасности на этапе выпуска также приведет к финансовым потерям в размере заработной платы персонала, работающего над проектом, стоимости сырья, затраченного на момент нарушения, и стоимость обслуживания оборудования, используемого для разработки. Таким образом, финансовые потери на этапе выпуска продукции опишем как:

$P_{project\_prelease}$ = заработная плата персонала работающего над проектом + стоимость сырья + стоимость обслуживания оборудования.

8.Возмещение вреда персоналу/пользователям.

Нарушение свойств безопасности при обработке информации конфиденциального характера может привести к негативным последствиям для персонала предприятия, а также клиентов. Клиенты и персонал будут вынуждены понести финансовые потери, связанные с восстановлением вследствие утраты, либо признания недействительными юридически значимых документов. Лицо, которое понесло потери согласно законодательству РФ, вправе обратиться в соответствующую судебную инстанцию с требованием возмещения причинённого вреда. Финансовые потери, связанные с возмещением вреда клиентам/персоналу, опишем как совокупность государственной пошлины по делам рассматриваемым в судах соответствующей инстанции и размером государственной пошлины, предусмотренной законодательством РФ за совершение различных юридически значимых действий.

Таким образом, финансовые потери, связанные с возмещением вреда клиентам/персоналу, опишем как:

$$P_{harm} = P_{harm}1 + P_{harm}2,$$

где $P_{harm}1$- размер государственной пошлины по делам, рассматриваемым в судах соответствующей инстанции. Определен ст. 333.19, 333.21, 333.23 Налогового Кодекса РФ.

$P_{harm}2$ - размер государственной пошлины, предусмотренной законодательством РФ за совершение различных юридически значимых действий. Определен ст. 333.24, 333.26, 333.28, 333.30, 333.33 Налогового Кодекса РФ.

Размер государственной пошлины по делам, рассматриваемых в судах РФ, определен ст. 333.19, 333.21, 333.23 Налогового Кодекса РФ.

Таким образом, имея прогностическую картину возможных финансовых потерь от нарушения свойств информационной безопасности, оператор конфиденциальной информации может сформулировать целесообразность траты финансовых средств на такое направление, как построение системы защиты информации на предприятии.

Материал поступил в редколлегию 23.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.054

***Голямин Дмитрий Сергеевич**, магистрант каф. «Системы информационной безопасности» БГТУ*

***Боровых Надежда Евгеньевна,** студент каф. «Системы информационной безопасности»*

ФГБОУ ВО Брянский государственный технический университет, г. Брянск, Россия

e-mail: dmgolyamin@gmail.com

РАЗРАБОТКА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ОЦЕНКИ ЗАЩИЩЕННОСТИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Рассмотрен алгоритм работы автоматизированный системы оценки защищенности государственных информационных систем.

В ходе выполнения работы был проведен анализ нормативно-правовой базы в области защиты государственных информационных систем, анализ авторских методик оценки защищенности государственных информационных систем и существующих программных продуктов формирования рекомендаций по защите информационных ресурсов. Была разработана методика определения степени ущерба, предложены меры и средства защиты в соответствии с требованиями ФСТЭК России и разработана автоматизированная система оценки защищенности государственных систем.

Основные этапы разработанной автоматизированной системы оценки защищенности государственных информационных систем:

1. Ввод первичных показателей информационной системы.

Автоматизированная система методом экспертного опроса получает от оператора данные об информационной системе: первичную степень возможного ущерба, первичный уровень значимости информации и первичный класс защищенности.

2. Получение данных об используемых средствах защиты информации.

На данном этапе также методом экспертного опроса автоматизированная система получает данные о средствах защиты информации, используемых в информационной системе. Выбор и сравнение средств защиты информации проводился с помощью метода анализа иерархий. На основании этих данных определяется степень возможного ущербаи класс защищенности информационной системы.

3. Получение данных о полном перечне реализованных мер защиты.

Методом экспертного опроса автоматизированная система получает данные о перечне реализованных технических, организационных и программно-аппаратных мерах и средствах защиты. Оценивается достаточность реализованных мер и средств защиты в соответствии с требованиями ФСТЭК России.

4. Сравнение показателей автоматизированной системы с первичными показателями.

Выполняется проверка на соответствие полученного во втором пункте класса защищенности информационной системы первичному классу защищенности информационной системы. В случае соответствия первичный класс защищенности признается итоговым классом защищенности информационной системы. В обратном случае класс защищенности, полученный автоматизированной системой, признается итоговым классом защищенности.

5. Оценка защищенности.

6. Вывод конечных результатов.

На данном этапе автоматизированная система выдает результат оценки защищенности информационной системы, даёт рекомендации по обеспечению уровня информационной безопасности государственных информационных систем, в частности для оцениваемой государственной информационной системы, в соответствии с действующей нормативно-правовой базой в области защиты государственных информационных систем.

На основании данных этапов сформирован алгоритм автоматизированной системы оценки защищенности государственных информационных систем (рис. 1).

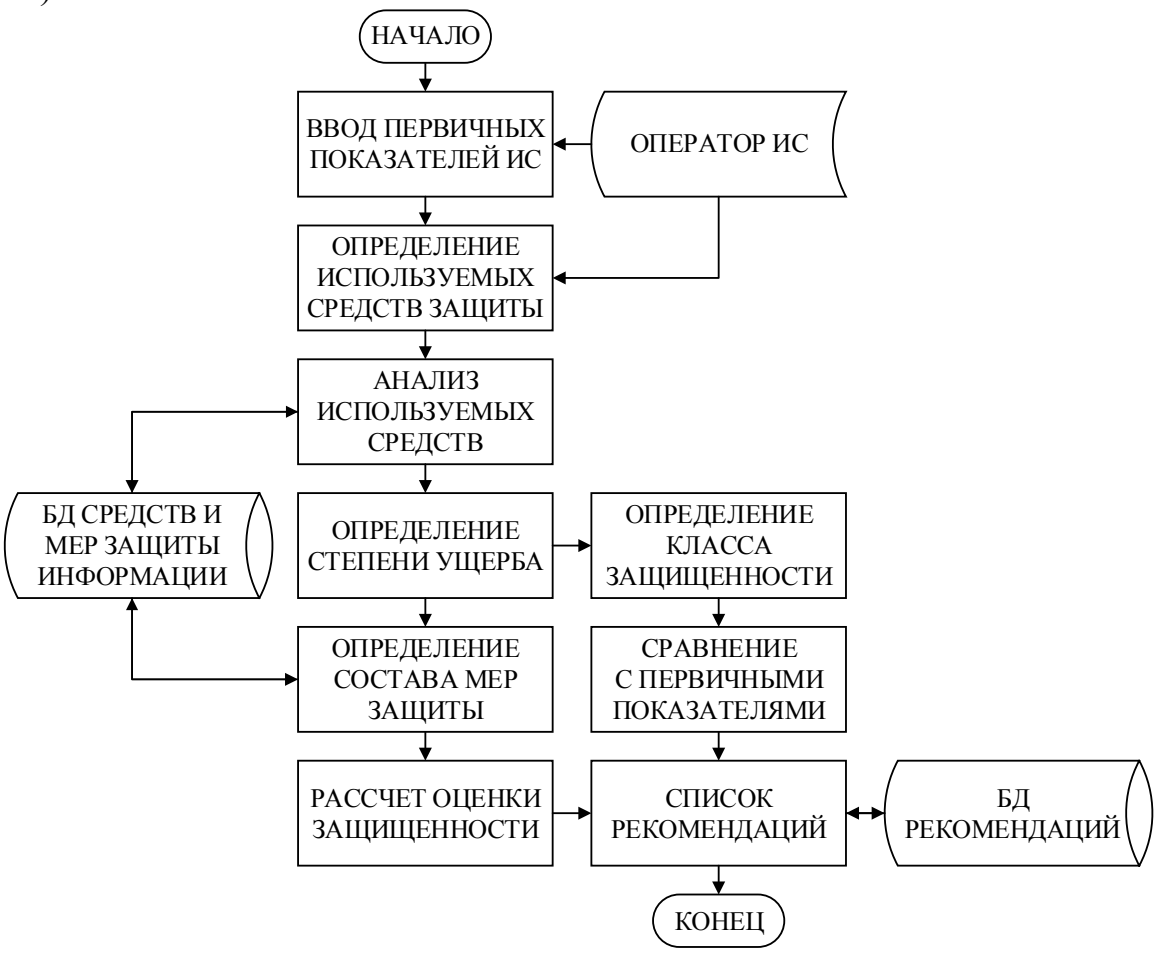

Рис. 1. Алгоритм автоматизированной системы оценки защищенности государственных информационных систем

На основании алгоритма составляем формулу оценки защищенности:

$$OZ = \left(\frac{SMZ}{13} * SU \right) * 100\%,$$

где OZ – оценка защищенности информационной системы;

SMZ – реализация состава мер защиты;

SU – степень возможного ущерба.

Разработанная автоматизированная система является достаточно гибкой для последующего внесения изменений, а также простой в использовании. Система предполагает свое использование как экспертами, так и невысококвалифицированными в вопросах информационной безопасности сотрудниками оператора.

Данная автоматизированная система предназначена для проведения оценки уровня защищенности государственных информационных систем. Практическая значимость использования выражается в повышении эффективности проведения процедуры оценки, оптимизации временных и финансовых затрат.

Материал поступил в редколлегию 22.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.056

Горбачев Павел Николаевич, *сотрудник*
Борисов Андрей Константинович, *сотрудник*
Академия ФСО России*, Орёл, Россия*
e-mail: pavel.gorbachev@list.ru

ОБНАРУЖЕНИЕ СЕТЕВЫХ АТАК В ОБЛАКАХ НА БАЗЕ OPENSTACK

Проведено исследование сетевого взаимодействия компонентов облачной платформы OpenStack с целью определения наиболее приемлемой точки анализа сетевого трафика в виртуальных сетях, развернутых в облачных платформах с применением программного коммутатора Open vSwitch

Для обеспечения защиты виртуальных машин и компонентов виртуальной сетевой инфраструктуры облачных платформ от сетевых компьютерных атак, а также для диагностики виртуальных сетей необходимо определить наиболее приемлемые точки мониторинга сетевого трафика виртуальных устройств. Анализа сетевого трафика между вычислительными узлами инфраструктуры облака зачастую недостаточно, так как в этом случае невозможно обеспечить мониторинг трафика виртуальных машин и виртуальных компонентов сетевой инфраструктуры (например, маршрутизаторов), функционирующих на одном вычислительном узле.

Для выбора точки получения копии сетевого трафика виртуальной машины или виртуального маршрутизатора необходимо рассмотреть прохождение трафика на уровне устройств и каналов виртуализации в облачной платформе OpenStack при использовании средств Open vSwitch.

Коммутация в случае сетевого взаимодействия двух виртуальных машин, размещенных на одном вычислительном узле в одной виртуальной сети, производится с помощью VLAN, определенного для сетевого моста внутренних соединений BR-INT, который функционирует на базе средства виртуализации сетевых устройств и каналов Open vSwitch (рис. 1).

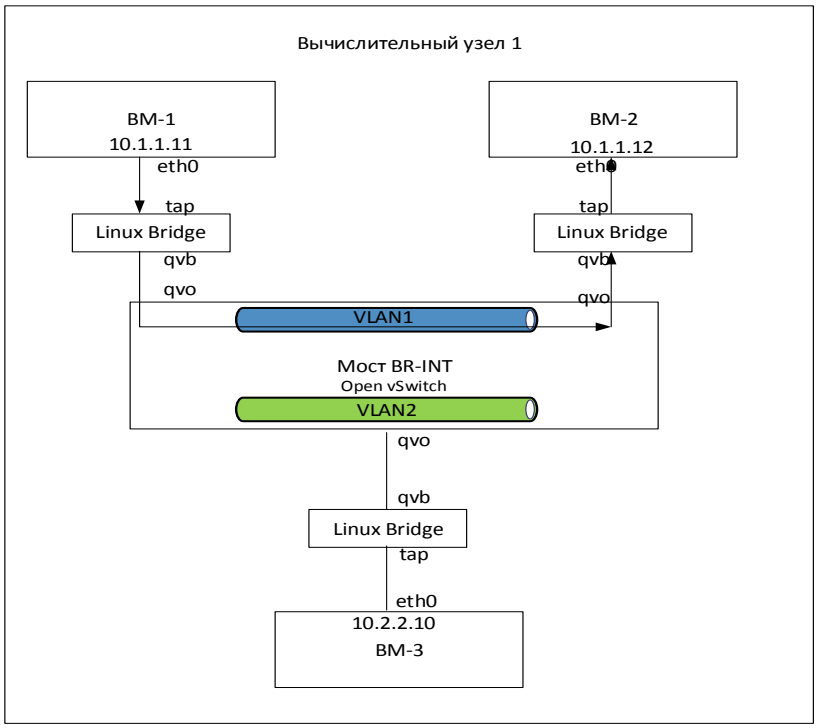

Рис. 1. Коммутация в одной виртуальной сети на одном вычислительном узле

Если виртуальные машины расположены на разных вычислительных узлах, но в одной виртуальной сети коммутация пакетов обеспечивается мостом межузловой связи BR-TUN через физическую сеть. В этом случае используются интерфейсы типа eth, tap, qvb, qvo (рис. 2).

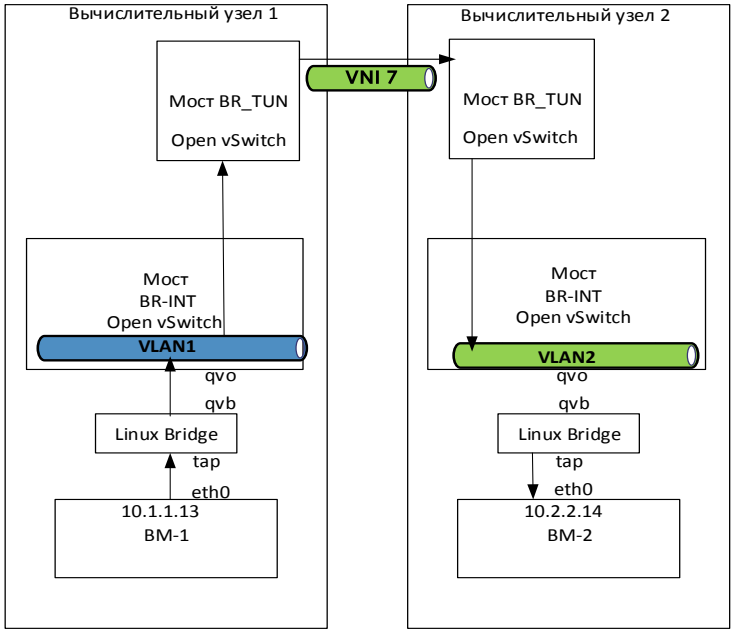

Рис. 2. Коммутация в одной виртуальной сети
на разных вычислительных узлах

Для сетевого взаимодействия двух виртуальных машин из разных сетей при размещении их на одном вычислительном узле соединение между двумя VLAN моста внутренних соединений BR-INT обеспечивается с помощью виртуального маршрутизатора OpenStack. Интерфейсы типа qr виртуального маршрутизатора соединяют сети через соответствующие VLAN
(рис. 3).

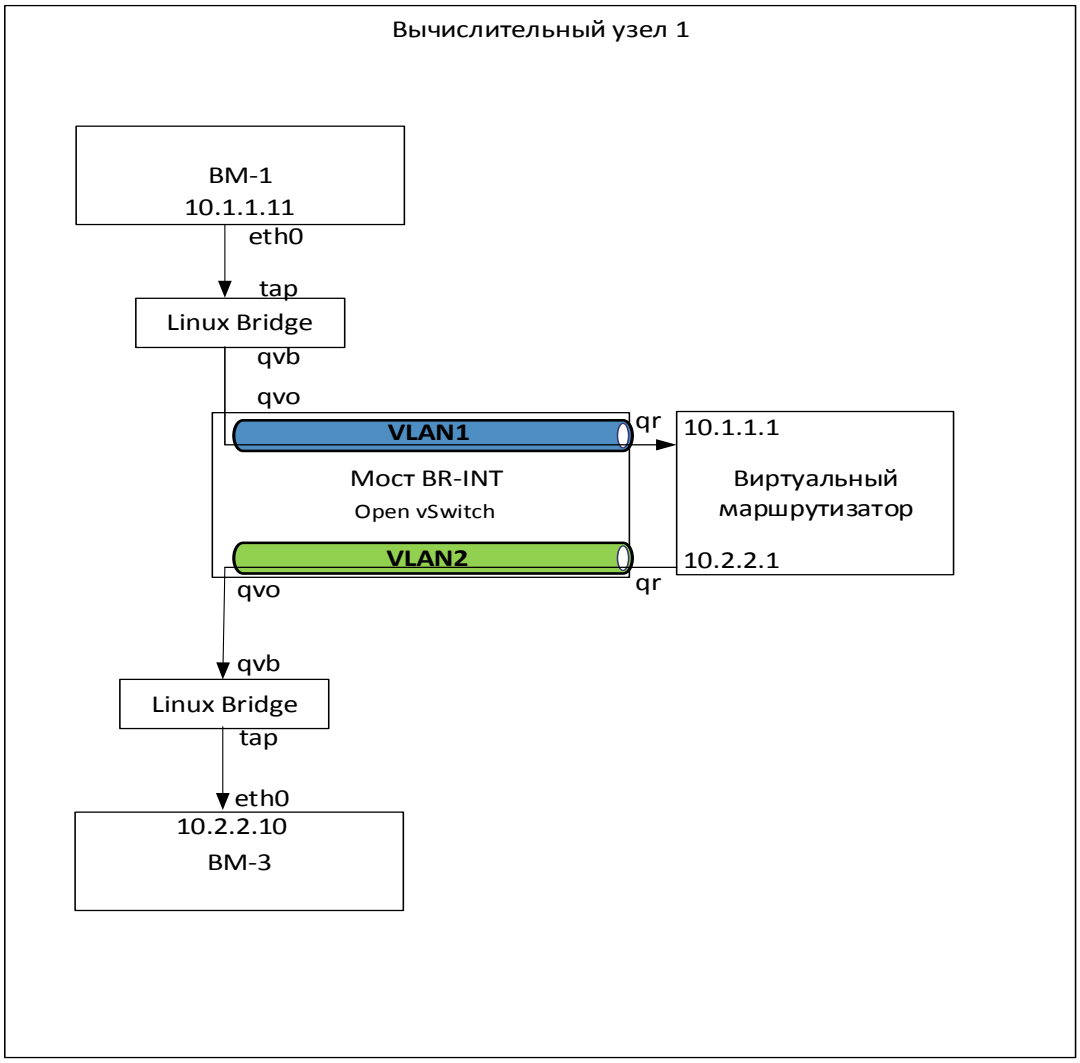

Рис. 3. Маршрутизация в разных виртуальных сетях
на одном вычислительном узле

Если виртуальные машины расположены на разных вычислительных узлах и при этом в разных виртуальных сетях трафик от виртуальной машины до виртуального маршрутизатора проходит аналогичным образом, то после пакеты направляются через сетевой мост BR-TUN на соответствующий вычислительный узел и далее попадают в VLAN сети назначения (рис. 4).

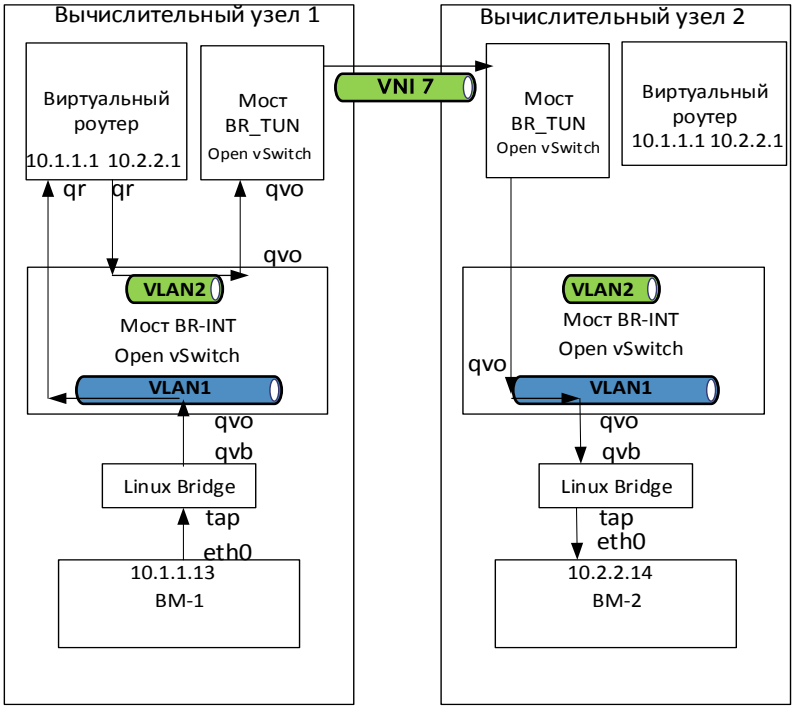

Рис. 4. Маршрутизация в разных виртуальных сетях
на разных вычислительных узлах

Для обеспечения сетевого взаимодействия виртуальной машины облака с сетевыми устройствами за пределами облака используется привязка внутреннего IP адреса виртуальной машины к одному из внешних адресов облака. Это повсеместно реализуется для обеспечения возможности доступа к информационным ресурсам, развернутым в виртуальной сети облака.

Сетевое взаимодействие реализуется аналогично взаимодействию между маршрутизируемыми сетями, с той лишь разницей, что задействуется сетевой интерфейс qg виртуального маршрутизатора для перенаправления сетевого трафика на мост внешних соединений BR-EX. При этом на выходе интерфейса qg внутренний IP адрес виртуальной машины заменяется на назначенный внешний.

Когда нет необходимости использовать выделенный внешний IP адрес для виртуальной машины, подмена адреса происходит на сетевом контроллере на адрес соответствующего выходного интерфейса. Эта схема задействуется для обеспечения доступа из облака к информационным ресурсам, расположенным за его пределами. Соединение между вычислительным узлом и сетевым контроллером происходит через BR-TUN мост. В этом случае задействуются все перечисленные ранее виртуальные интерфейсы (рис. 5).

Во всех рассмотренных случаях трафик на уровне вычислительного узла проходит через сетевые интерфейсы tap, qvb и qvo. При этом интерфейсы tap и qvb входят в сетевой мост QBR, работающий на базе Linux Bridge, а qvo – в BR-

INT мост, функционирующий на базе Open vSwitch. Сетевые мосты BR-INT, BR-TUN и BR-EX, которые включают в себя интерфейсы qvo, qr, qg, поддерживают расширенные возможности работы с пакетами.

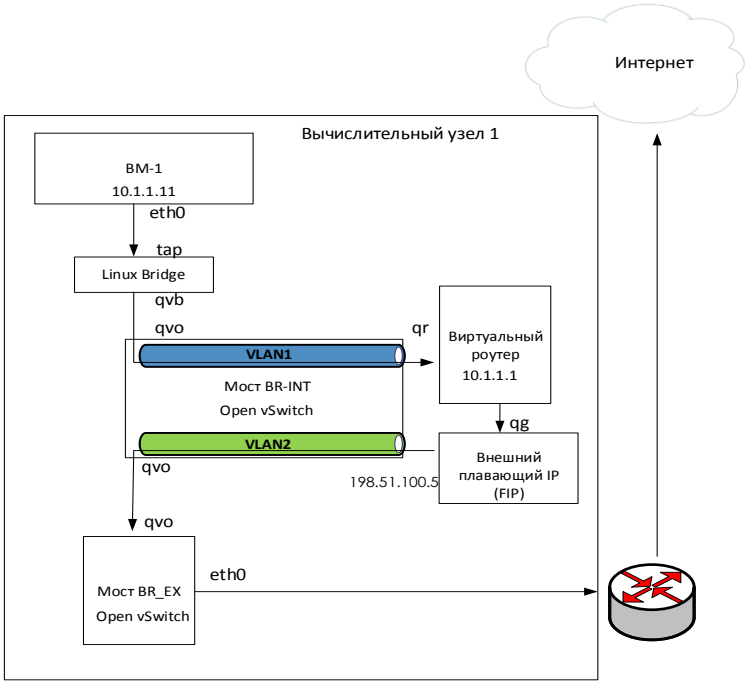

Рис. 5. Маршрутизация во внешнюю сеть с применением внешнего плавающего IP

Исходя из особенностей прохождения сетевых пакетов и возможностей виртуальной сетевой инфраструктуры, нужно выбрать точки получения копии сетевого трафика для дальнейшего анализа на предмет наличия или отсутствия сетевых атак.

Вариант 1 – анализировать трафик с tap интерфейса

В OpenStack интерфейс виртуальной машины, например eth0, подключается к виртуальному tap устройству, функционирующему на вычислительном узле, интерфейс которого имеет подобный формат имени – tap6c7ae61e-05.

Этот интерфейс наиболее удобно использовать для частного анализа трафика с вычислительного узла, потому что он непосредственно подключен к виртуальному сетевому интерфейсу виртуальной машины.

Использовать его для последующей отправки копии трафика на удаленное средство безопасности возможно только с помощью копирования сторонними утилитами (например, tc) сетевых пакетов захваченных сниффером, который, в свою очередь, должен функционировать на каждом вычислительном узле. Это затрудняется необходимостью доустановки соответствующих приложений, координацией их работы и контролем работоспособности.

Вариант 2 – добавление зеркала интерфейсов типа qvo, qr, qg в мост BR-INT средствами Open vSwitch.

Этот интерфейс не подключен к виртуальной машине непосредственно, так как он расположен между tap интерфейсом и виртуальными устройствами Open vSwitch.

Этот подход наиболее целесообразно использовать для централизованной системы анализа трафика, так как с указанными сетевыми интерфейсами можно производить различные операции на уровне моста BR-INT. Также на этих интерфейсах отсутствуют правила безопасности в отличие от tap, это позволит обнаружить сам факт возникновения атаки ещё до её возможной блокировки межсетевым экраном.

Для построения системы защиты и основы её программной реализации выбран второй вариант - зеркалирование сетевого трафика облака средствами Open vSwitch.

Open vSwitch позволяет направлять копию сетевого трафика одного или нескольких интерфейсов на нужный адрес. Может зеркалироваться только входящий или исходящий трафик, а также оба направления. Подход позволяет не использовать сниффер и сторонние утилиты копирования трафика на вычислительных узлах.

На основе рассмотренного подхода предлагается способ перенаправления копии трафика на любой доступный для вычислительного узла адрес назначения путем передачи копий сетевых пакетов для анализа через GRE-туннель. Это позволит построить комплексную защиту облака с возможностью обнаружения сетевых атак, источником которых является как внешний злоумышленник, так и ресурс внутри облака (например, виртуальная машина с вредоносным программным обеспечением, которое может быть занесено в систему в обход средств безопасности, размещенных на входе облака).

Предложенный подход позволит “вытащить” копию сетевого трафика из скрытого от большинства программных или программно-аппаратных анализаторов трафика сегмента центра обработки данных. Анализируемый трафик целесообразно перенаправлять на систему обнаружения или предотвращения сетевых атак, находящуюся в локальной сети центра обработки данных, чтобы обеспечить максимально быстрое реагирование при приемлемой загрузке сетевой инфраструктуры. При небольшом количестве точек мониторинга, средство безопасности можно разместить в отдельной виртуальной сети в качестве виртуальной машины с установленным средством безопасности.

Список литературы

1. Воробьев А.А. Установка, настройка и эксплуатация частного облака на базе Openstack: учебное пособие / А. А. Воробьев, А.В. Потемкин, Б.И. Соловьев, А.В. Яковлев. – Орёл: Академия ФСО России, 2017.

2. Маркелов, А.С. OpenStack: практическое знакомство с облачной операционной системой/А.С. Маркелов // Оформление, ДМК Пресс, 2016.

Материал поступил в редколлегию 22.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.056

***Горлов Алексей Петрович**, к.т.н., доц. каф. «Системы информационной безопасности»*
***Гулак Максим Леонидович**, к.т.н., доц. каф. «Системы информационной безопасности»*
***Лексиков Евгений Вячеславович**, ст. преподаватель каф. «Системы информационной безопасности»*
Брянский государственный технический университет, Брянск, Россия
E-Mail: apgorlov@gmail.com

АВТОМАТИЗАЦИЯ ПРОЦЕССА ОЦЕНКИ ЭФФЕКТИВНОСТИ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Рассмотрена автоматизация процесса оценки эффективности комплексных систем защиты информации путем создания автоматизированной системы, основными функциями которой являются проведение аудита информационной безопасности (ИБ), формирование модели угроз ИБ, рекомендаций по созданию системы защиты информации, комплекта организационно-распорядительной документации.

На сегодняшний день проблема защиты конфиденциальной информации стоит особенно остро. Ущерб от искажения, уничтожения, хищения, разглашения конфиденциальной информации превышает миллионы рублей.

Согласно статистике, за 2017 год на территории РФ зафиксировано около 120 тысяч преступлений в сфере информационной безопасности. К этим преступлениям относятся неправомерный доступ к конфиденциальной информации, разглашение сведений, составляющих коммерческую тайну, создание, использование или распространение вредоносных программ для ЭВМ или машинных носителей с такими программами.

Практический опыт создания систем защиты информации на объектах свидетельствует, что чаще всего специалистам приходится дорабатывать и систематизировать уже внедренные на объекте средства и методы защиты информации. Также для поддержания высокого уровня защищенности информации необходимо периодически проводить аудит информационной безопасности и оценивать эффективность функционирования КСЗИ.

При решении рассматриваемой проблемы одной из важнейших задач является разработка математических моделей, информационного обеспечения и программного комплекса автоматизации оценки уровня защищенности и эффективности комплексных систем защиты информации [2,4].

В основу предлагаемой методики положена оценка защищенности объекта информатизации согласно положениям законодательной базы РФ, требованиям государственных стандартов, а также проверка наличия организационно-

распорядительной документации, регламентирующей защищенную обработку конфиденциальной информации.

Преимуществом данной методики является возможность снизить трудоемкость работ, сократить временные и материальные затраты на проведение оценки уровня информационной безопасности, повысить качество проектных решений.

Наиболее распространена практика создания единой системы защиты из разрозненных элементов, когда к уже существующей информационной среде добавляются средства защиты информации. Современные условия диктуют другой подход, который заключается в том, что информационная среда изначально проектируется с точки зрения защиты всех ее компонентов. Это предполагает возможность оценить еще на этапе проектирования целесообразность использования той или иной СЗИ, а также моделировать взаимодействие СЗИ в едином информационном пространстве [3].

Состав и функциональность проектируемой СЗИ должны соответствовать актуальным для рассматриваемой информационной системы угрозам. Для удовлетворения этого требования необходимо на этапе проектирования выявить существующие уязвимости и угрозы информационной безопасности, определить степень актуальности этих угроз и вероятность их реализации, а также возможный ущерб от их реализации. Этот этап проектирования СЗИ является одним из наиболее важных и трудоемких, так как от результата выявления угроз информационной безопасности зависит то, какими средствами будет обеспечиваться защита конфиденциальной информации.

Для автоматизации данного процесса необходимо разработать математическую модель выявления уязвимостей системы защиты информации.

Ввод исходных данных представляет собой заполнение опросных анкет, позволяющих выявить вид обрабатываемой информации, существующие средства защиты информации, угрозы ИБ, уязвимости системы защиты информации, а также прочие данные, необходимые для составления информационной модели объекта информатизации.

Следующим этапом является оценка состояния защищенности ОИ. Выделяются 3 основных направления оценки защищенности:

- оценка на соответствие требованиям стандартов (ГОСТ, СТР-К, ISO);
- определение наличия технических средств защиты информации на объекте информатизации;
- выявление организационно-распорядительной документации, регламентирующей защищенную обработку конфиденциальной информации.

По результатам данного этапа формируется отчет о состоянии защищенности объекта информатизации.

На этапе формирования модели угроз информационной безопасности формируется описание системы обработки информации, выявляются пользователи данной системы, определяется уровень исходной защищенности, степень актуальности угроз, рассчитывается вероятность реализации угроз.

Актуальность рисков определяется, исходя из типа обрабатываемой информации, объема обрабатываемых в системе данных, структуры информационной системы, режима обработки данных и т.д.

Для того чтобы определить актуальность угроз для данного объекта информатизации, целесообразно выделить критерии актуальности каждой конкретной угрозы. Так, для угрозы сетевой атаки можно выделить такие критерии актуальности, как наличие доступа к глобальной сети, наличие в структуре локальной вычислительной сети средств межсетевого экранирования, антивирусной защиты и т.д.

Заключительным этапом является формирование организационно-распорядительной документации, регламентирующей защиту конфиденциальной информации.

На данном этапе проводится проверка наличия организационно-распорядительной документации на объекте, выявляются недостающие документы и, если нужно, проводится сбор данных, необходимых для формирования дополнительных документов.

Выходными данными этого блока является комплект организационно-распорядительной документации, регламентирующей защиту конфиденциальной информации.

Результаты работы автоматизированной системы представлены на рис. 1.

Рис. 1. Результаты работы автоматизированной системы оценки эффективности КСЗИ

Таким образом, на выходе автоматизированной системы формируется комплект документов включающий модель угроз информационной безопасности рассматриваемого объекта, комплект организационно-распорядительной документации, регулирующей защиту конфиденциальной информации и рекомендации по усовершенствованию системы защиты информации.

Поведение сложных информационных систем, подверженных внешним и внутренним деструктивным воздействиям – является неоднородным стохастическим процессом. С целью получения информации о динамике многомерной задачи, требуется определить критерии в соответствии с которыми будет осуществляться выбор инструмента математического моделирования (табл. 1).

Анализ данных критериев показал, что наиболее подходящий инструмент для моделирования процессов защиты информации является математический аппарат раскрашенных, вероятностных, ингибиторных сетей Петри.

Раскрашенные сети – позволяют разделить фишки угроз безопасности и методов противодействия.

Вероятностные сети – позволяют настроить вероятность совершения переходов (возникновение угроз и реагирование методов противодействия).

Ингибиторные сети – позволяют реализовать процесс предотвращения угрозы безопасности методом противодействия.

Предлагается способ формального задания математической модели, построенной на базе ингибиторных, вероятностных и раскрашенных сетей Петри: $F =< P,T,I,O >$, где $P = \{p1, p2, p3, p4, p5, p5'\}$: $p1$ – возникновение источника угрозы, $p2$ – возникновение угрозы безопасности, $p3$ – прохождение угрозы через уязвимое звено, $p4$ возникновение метода противодействия, $p5$ – нанесение деструктивного действия, $p5'$ – предотвращение угрозы безопасности, $T = \{t1, t2, t3, t3'\}$ – множество переходов, I – входные позиции, O – выходные позиции.

Таблица 1

Требования к математической модели

№ п/п	Требования к математической модели
1	Возможность учета вероятностей реализации и предотвращения угроз
2	Возможность моделирования процессов защиты во времени
3	Возможность моделирования одновременной реализации угроз во времени
4	Возможность учета своевременности реагирования средств защиты на угрозы безопасности

Для моделирования реагирования средств защиты на угрозы безопасности, фишки в данной сети определены в множестве $Color = \{red, blue\}$, причем фишки $Color = red$ соответствуют угрозам безопасности, а фишки $Color = blue$

методам противодействия. При этом в позициях $\{p1, p2, p3, p5\}$ могут находиться только фишки $Color = red$, $\{p4, p5'\}$ - только фишки типа $Color = blue$.

Для записи в формализованном виде каждого из способов срабатывания перехода $T = \{t1, t2, t3, t3'\}$ введем дополнительные операнды и параметры:

$F(p_i)$ – функция, отражающая наличие фишки в позиции p_i;

φ(P) – функция, отражающая совершение/отражение угрозы с вероятностью P;

P_{threat} – вероятность совершения угрозы;

$P_{reaction}$ – вероятность устранения угрозы;

Правила срабатывания задаются с помощью терминальных языков[5] описания сетей Петри:

$$P1^i \rightarrow \tau_i = t1^i(F_{P1i}), t2^i(F_{P2i}, \varphi(P_{threat(n)})), t3^i(F_{P3i}, , \varphi(P_{reaction(m)}, t3'^i(F_{P3i}, \varphi(P_{reaction(m)}) \rightarrow P5^i, P5'^i; \quad (1)$$

На основе исходных данных по рассматриваемому защищаемому объекту моделирования строится сеть Петри, фрагмент которой представлен на рис. 2.

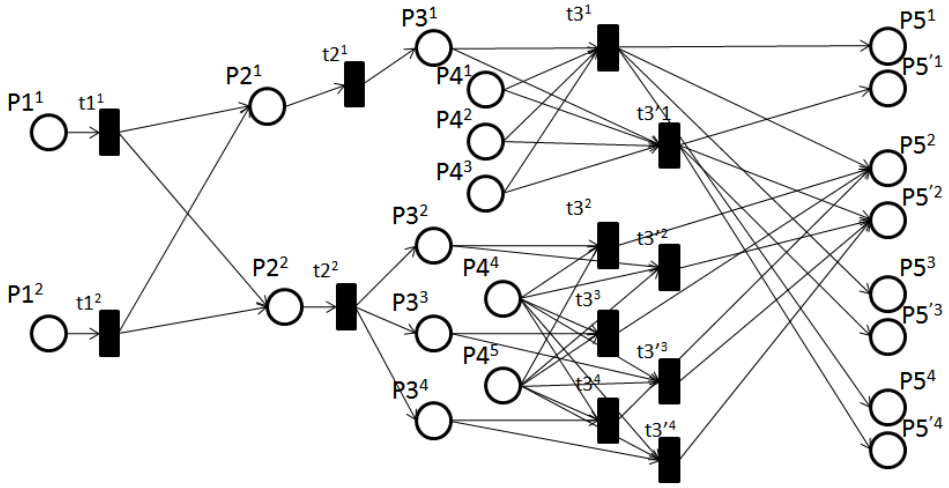

Рис. 2. Фрагмент построенной сети Петри

Данная сеть является раскрашенной, вероятностной и ингибиторной, что позволяет реализовать следующие возможности:

1) вероятностная сеть позволяет учесть, как средства нападения, так и средства отражения угроз безопасности за счет настройки вероятностей совершения переходов;

2) раскрашенная сеть Петри позволяет идентифицировать фишки, ассоциируемые с угрозами безопасности и методами противодействия;

3) ингибиторная сеть Петри обеспечивает реализацию механизма предотвращения угроз безопасности методами противодействия.

Для разграничения действий злоумышленника и средств защиты в сети Петри представлены фишки двух типов: фишки типа *color=blue* – это фишки методов противодействия, а фишки типа *color=red* – это угрозы безопасности. Варианты развития событий изображены на рис. 4.

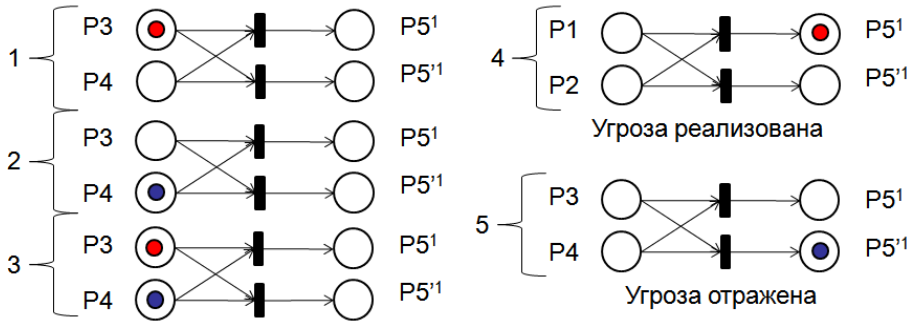

Рис.3. Варианты развития событий

Отличительной особенностью данной сети (рис. 2) является то, что она позволяет учитывать, как действия угроз, так и действия средств защиты. Это обеспечивается тем, что переходы t2 данной сети настраиваются в соответствии с вероятностью совершения угрозы. А переходы t3 - в соответствии с расчетной вероятностью предотвращения угрозы методами противодействия. Это способствует более глубокому исследованию процессов защиты информации.

Далее для оценки эффективности моделируемой комплексной системы защиты информации предлагается использовать специально разработанную весовую функцию.

В основе весовой функции лежит ряд критериев, отражающих вероятности совершения и отражения угрозы, а также степень опасности угрозы. Данная весовая функция будет накапливаться при отражении каждой угрозы, тем самым показывая эффективность системы защиты информации.

Далее предлагается рассчитать весовую функцию для каждой выявленной угрозы и присвоить расчетные значения переходам, соответствующим отражению угрозы t3'. Таким образом, суммарное значение весовой функции будет накапливаться каждый раз, когда происходит событие ликвидации какой-либо угрозы (вариант номер 5 на рис. 4). Данный критерий отличается тем, что основывается на результатах моделирования угроз безопасности, то есть отражает динамическое состояние СЗИ.

В результате анализа работ в области защиты информации обоснована формула для расчета весовой функции за счет ликвидации воздействия i-угрозы

$$W = \frac{P_{threat} + q_i^{threat} + (1 - P_{reaction})}{3}; \in [0,1], \quad (2)$$

где P_{threat} - вероятность совершения угрозы;

$P_{reaction}$ - вероятность предотвращения угрозы;

q_i^{threat} - коэффициент опасности угрозы.

Так как настоящее исследование опирается на нормативно-правовые акты ФСТЭК и ФСБ России, то для расчета вероятности совершения угрозы безопасности P_{threat} используется «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах

персональных данных», утвержденная ФСТЭК. Исходя из данной методики вероятность совершения угрозы будет определяться соотношением:

$$P_{threat} = Y_1 + Y_2 / 20, \qquad (3)$$

где Y_1 - степень исходной защищенности;

Y_2 - вероятность реализации угрозы.

В рамках рассматриваемой проблемы для расчета вероятности устранения угрозы безопасности $P_{reaction}$ предлагается применить методику, предложенную Домаревым В.В., которая позволяет учитывать количественные и качественные требования по предотвращению угроз безопасности, а также их важность. Она заключается в том, что вероятность устранения угрозы безопасности представляется в виде функциональной зависимости:

$$P_{reaction}(x_1 \ldots x_m) = \sum_{i=1}^{k} \omega_i \cdot \bar{x}_i + \sum_{i=k+1}^{m} \omega_i \cdot \mu(x_i), \qquad (4)$$

где $\bar{x}_i$ - количественные требования к КСЗИ;

ω_i - вес i-го требования;

$\mu(x_i)$ - качественные требования к КСЗИ;

k - число количественных требований;

m - число качественных требований.

Предлагаемый подход к оценке уровня информационной безопасности объекта информатизации позволяет значительно сократить материальные и временные затраты на проведение аудита информационной безопасности, а так же повысить качество проектных решений при создании и внедрении комплексных систем защиты информации.

Математический аппарат раскрашенных, вероятностных, ингибиторных сетей Петри позволяет оценить эффективность системы защиты объекта с учетом своевременности реагирования средств противодействия и одновременности реализации угроз.

Список литературы

1. Аверченков, В.И. Организационная защита информации/ В. И. Аверченков, М.Ю. Рытов.– Брянск: Изд-во БГТУ, 2010. – 184 с. – (Серия «Организация и технология защиты информации»).

2. Аверченков, В.И. Аудит информационной безопасности/ В. И. Аверченков. – Брянск: Изд-во БГТУ, 2010. – 210 с. – (Серия «Организация и технология защиты информации»).

3. Аверченков, В.И. Автоматизация проектирования комплексных систем защиты информации: могорафия/ В. И. Аверченков, М.Ю. Рытов. – Брянск: Изд-во БГТУ, 2012. – 147 с. – (Серия «Организация и технология защиты информации»).

4. Аверченков, В.И. Разработка системы технической защиты информации/ В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – Брянск: БГГУ, 2008. – 187 с. – (Серия «Организация и технология защиты информации»).

5. Хопкрофт, Дж., Мотвани, Р., Дж. Ульман. Введение в теорию автоматов, языков и вычислений/ Дж. Хопкрофт, Р. Мотвани, Дж. Ульман. – М.: Вильямс, 2002 (пер. издания Addison Wesley). – 528 с. – ISBN 5-8459-0261-4.

Материал поступил в редколлегию 23.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.056

***Горлов Алексей Петрович**, к.т.н., доц. каф. «Системы информационной безопасности»*

***Ивашков Алексей Юрьевич**, студент каф. «Системы информационной безопасности»*

ФГБОУ ВО «Брянский государственный технический университет», Брянск, Россия

E-Mail: apgorlov@gmail.com

АВТОМАТИЗАЦИЯ ПРОЦЕССА ВЫБОРА ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Рассматривается процесс автоматизации оценки состояния защищенности объекта информатизации, с применением аппарата ингибиторных, вероятностных и раскрашенных сетей Петри.

Комплексная система защиты информации - это система, в которой действуют в единой совокупности правовые, организационные, технические, программно-аппаратные и другие нормы, методы, способы и средства, обеспечивающие защиту информации от всех потенциально возможных и выявленных угроз и каналов утечки. Элементы КСЗИ, в свою очередь, в общем виде состоят из средств, устройств и способов защиты информации, а также методов их использования.

Понятие защиты информации в настоящее время ассоциируется, как правило с проблемами обеспечения информационной безопасности в информационных системах (ИС).

Комплексная система защиты информации (КСЗИ) в самом общем виде может быть определена как организованная совокупность всех средств, методов и мероприятий, выделяемых в ИС для решения в ней выбранных задач защиты. Задачи же защиты информации решаются с целью нейтрализации дестабилизирующего воздействия причин нарушения целостности информации при обеспечении физической целостности информации или с целью перекрытия каналов несанкционированного получения информации – при защите от несанкционированного получения информации.

Отсутствие на объектах информатизации систем защиты информации приводит к утечке конфиденциальной информации так как разработка и внедрение таких систем является достаточно затратной процедурой. Автоматизированная система оценки уровня ИБ позволит привести систему ОИ в соответствие установленным требованиям, противостоять актуальным угрозам, снизить трудоемкость работ, сэкономить время и значительно сократить материальные затраты на проведение аудита и разработку СЗИ.

Ввиду этого разработка системы автоматизированной оценки уровня информационной безопасности объекта информатизации представляется актуальной.

В большинстве своем существует практика создания единой системы защиты из существующих разрозненных элементов, где к уже существующей информационной среде добавляются средства защиты информации. Современные условия диктуют другой подход, который заключается в том, что изначально вся информационная среда проектируется с точки зрения защиты всех ее компонентов. Это предполагает возможность оценить еще на этапе проектирования целесообразность использования той или иной СЗИ, а также моделировать их взаимодействие в едином информационном пространстве.

Состав и функциональность проектируемой СЗИ должны соответствовать актуальным для рассматриваемой информационной системы угрозам. Для обеспечения этого требования необходимо на этапе проектирования выявить существующие уязвимости и угрозы информационной безопасности, определить степень актуальности этих угроз и вероятность их реализации, а также возможный ущерб от их реализации. Этот этап проектирования СЗИ является одним из наиболее важных и трудоемких, так как от результата выявления угроз информационной безопасности зависит то, какими средствами будет обеспечиваться защита конфиденциальной информации.

Для автоматизации данного процесса необходимо разработать математическую модель выявления уязвимостей системы защиты информации.

На рис.1 этот процесс представлен блоком оценки состояния защищенности. На данном этапе на основе результатов оценки соответствия требованиям нормативно-правовой базы требуется выявить уязвимости информационной системы.

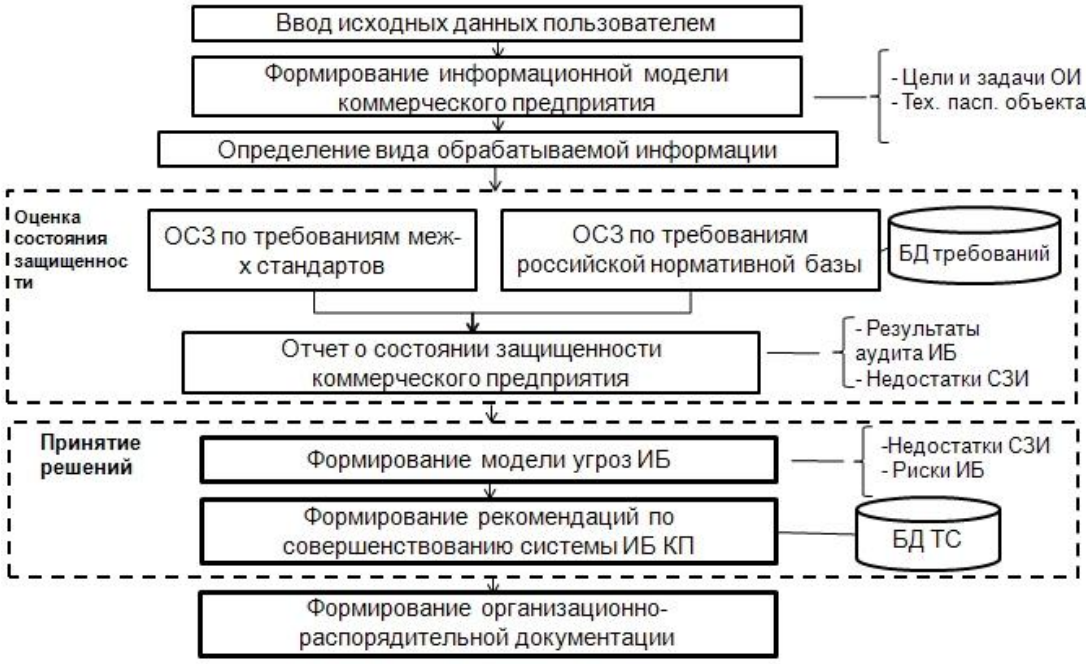

Рис. 1. Алгоритм работы автоматизированной системы

На предыдущем этапе работы системы был сформирован информационный портрет объекта информатизации, который позволяет определить объекты и субъекты информационной безопасности, другими словами, определяется информация, подлежащая защите.

Предлагается способ формального задания математической модели, построенной на базе ингибиторных, вероятностных и раскрашенных сетей Петри: $F =< P,T,I,O >$, где $P = \{p1, p2, p3, p4, p5, p5'\}$: $p1$ – возникновение источника угрозы, $p2$ – возникновение угрозы безопасности, $p3$ – прохождение угрозы через уязвимое звено, $p4$ возникновение метода противодействия, $p5$ – нанесение деструктивного действия, $p5'$ – предотвращение угрозы безопасности, $T = \{t1, t2, t3\}$ – множество переходов, I – входные позиции, O – выходные позиции. Для моделирования своевременности реагирования средств защиты на угрозы безопасности фишки в данной сети определены на множестве $Color = \{red, blue\}$, причем фишки $Color = red$ ассоциируются с угрозами безопасности, а фишки $Color = blue$ с методами противодействия. При этом в позициях $\{p1, p2, p3\}$ могут находиться только фишки $Color = red$, $\{p4\}$ – только фишки типа $Color = blue$, а в позициях $\{p5, p5'\}$ как те, так и другие.

Для записи в формализованном виде каждого из способов срабатывания перехода $T = \{t1, t2, t3\}$ введем дополнительные операнды и параметры:

$Q(p^i)$ – отражает наличие фишки в позиции i;

$\varphi(T,t)$ – отражает вероятность совершения перехода Т;

$++(p^i, C, \varphi)$ – увеличивает число фишек цвета С с вероятностью φ в позиции p на 1;

$--(p^i, C, \varphi)$ – уменьшающий число фишек цвета С с вероятностью φ в позиции p^i на 1;

$Time$ – время моделирования в тактах;

P_{threat} – вероятность совершения угрозы;

$P_{reaction}$ – вероятность устранения угрозы;

$Y(p3^i, p4^j, t3^h)$ - возвращает 1, если позиции $p3^i$ и $p4^j$ связаны с переходом $t3^h$.

Используя продукционные правила, которые успешно применяются для описания логики работы системы, представим правило срабатывания перехода $t1$:

$$\forall t \in t1^i (Input(p1^i, t1^i, t, \mu)) \Rightarrow$$
$$AddSort(TR, t, 1))$$
$$\forall t \in TR(Max(TR, t)) \Rightarrow$$
$$I(p1^i, t1^i, \mu) O(p2^i, t1^i, \mu) Rem(TR, t).$$

Перехода $t2$:

$\forall t \in t2^i(Input(p2^i, t2^i, t, \mu)) \Rightarrow$

$AddSort(TR, t, \varphi(t2^i, t))$

$\forall t \in TR(Max(TR, t)) \Rightarrow$

$I(p2^i, t2^i, \mu)O(p3^i, t2^i, \mu)Rem(TR, t)$, где $\varphi(t2^i, t) = P^i_{threat}$

Перехода $t3$:

$((\forall t \in TR(Max(TR, t))) \cap (Y(p3^i, p4^k, t3^h) = 1) \Rightarrow$

$I(p3^i, p4^k, t, \mu)O(p5'^m, t, \mu)Rem(TR, t) \cap$

$\cap (W = W + W(t3^h, t)) \cap (++(p5'^m, blue, 1))) \cup$

$((\forall t \in TR(Max(TR, t))) \cap (Y(p3^i, p4^k, t3^h) = 0) \Rightarrow$

$I(p3^i, p4^k, t, \mu)O(p5'^m, t, \mu)(Rem(TR, t)) \cap$

$(++(p5^i, red, 1)))$;

Фрагмент сети Петри (цветная, ингибиторная, вероятностная), используемой для выявления уязвимостей СЗИ и угроз, представлен на рис. 2:

1) вероятностная сеть позволяет учесть как средства нападения, так и средства отражения угроз безопасности за счет настройки вероятностей совершения переходов;

2) раскрашенная сеть Петри позволяет идентифицировать фишки, ассоциируемые с угрозами безопасности и методами противодействия;

3) ингибиторная сеть Петри обеспечивает реализацию механизма предотвращения угроз безопасности методами противодействия.

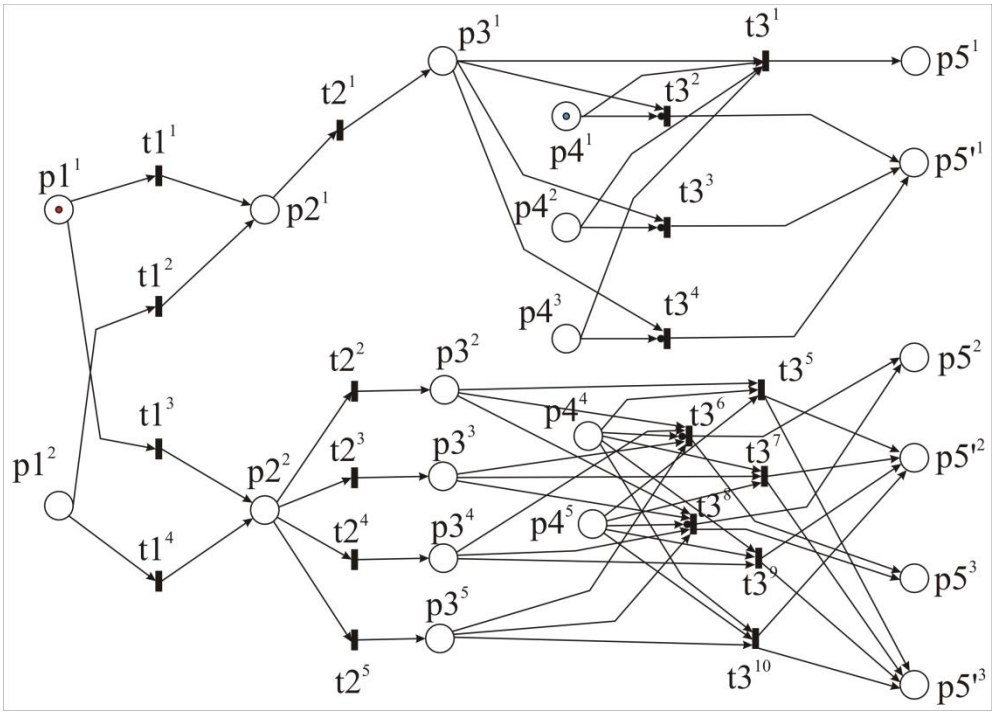

Рис.2. Фрагмент сети Петри

Таким образом, использование ингибиторных, вероятностных и раскрашенных сетей Петри позволяет реализовать эффективный выбор технических

средств защиты информации, а также учесть одновременность совершения атак и своевременность противодействия защитных механизмов.

Список литературы

1. Аверченков, В.И. Разработка системы технической защиты информации/ В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – Брянск: БГГУ, 2008. – 187 с. – (Серия «Организация и технология защиты информации»).

2. Герасименко, В.А. Защита информации в автоматизированных системах обработки данных: в 2 кн./В.А. Герасименко. – М.: Энергоатомиздат, 1994.– Кн.1. – 400 с.

3. Гришина, Н.В. Организация комплексной системы защиты информации/ Н.В. Гришина. – М.: Гелиос АРВ, 2007. – 256 с.

4. Питерсон, Дж. Теория сетей Петри и моделирование систем. – М: Мир, 1984. – 264 с.

5. Котов, В.Е. Сети Петри/В.Е. Котов. – М: Наука, 1984. – 160 с.

Материал поступил в редколлегию 23.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.056

Гулак Максим Леонидович, *к.т.н., доц. каф. «Системы информационной безопасности» БГТУ*
Лысов Дмитрий Андреевич, *студент*
ФГБОУ ВО «Брянский государственный технический университет», Брянск, Россия
e-mail: gml13@yandex.ru, lysovdmitriia@gmail.com

ОБЩИЕ ПОДХОДЫ К МОДЕЛИРОВАНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Описаны общие подходы к моделированию инфомрационных систем, рассмотрены вопросы обеспечения информационной безопасности ИС. Сформулирована модель угроз безопасности. Приведены рекомендации, позволяющие сформулировать элементы политики безопасности информационных систем.

На сегодняшний день проблема защиты конфиденциальной информации стоит особенно остро. Ущерб от искажения, уничтожения, хищения, разглашения конфиденциальной информации превышает миллионы рублей.

В I полугодии 2016 года в мире обнародовано и зарегистрировано 840 случаев утечки конфиденциальной информации, что на 16% превышает количество утечек, зарегистрированных за аналогичный период 2015 года. Внешние атаки стали причиной 33% утечек данных. В 67% случаев утечка данных произошла под воздействием внутреннего нарушителя. За I полугодие 2016 году зафиксировано 23 «мега-утечки». В результате каждой «утекло» более 10 млн персональных данных. На «мега-утечки» пришлось 92% всех скомпрометированных записей. В 67% случаев виновными в утечке информации оказались сотрудники компаний. В 1% случаев – высшие руководители организаций. Россия заняла второе место по числу утечек, ставших достоянием общественности. В исследуемый период зарегистрировано 110 случаев утечки конфиденциальной информации из российских компаний и государственных организаций.

Бурный рост конфиденциальной и коммерческой информации, а также существенное увеличение фактов ее хищения вызывает повышенный интерес все большего числа организаций к созданию собственных защищенных информационных систем.

Проектирование защищенных информационных систем – процесс довольно сложный, который предполагает наличие соответствующих знаний и опыта у ее создателей.

Потребитель может не вникать в разработку такого проекта и подробности его развития, однако он обязан контролировать каждый его этап на предмет соответствия техническому заданию и требованиям нормативных документов. В свою очередь, персональный опыт проектировщиков требует использования

существующих нормативных документов в данной области для получения наиболее качественного результата.

Таким образом, процесс проектирования защищенных информационных систем должен основываться на знании и строгом выполнении требований существующих нормативных документов как со стороны ее разработчиков, так и со стороны заказчиков.

Необходимым условием достижения требуемой степени информационной безопасности в информационных системах является формирование комплексной защиты, включающей принятие разнообразных мер защиты: правовых, организационных, технических. Таким образом, построение системы защиты информации ИС не должно ограничиваться простым выбором тех или иных средств защиты. Следует различать следующие основные фазы жизненного цикла системы информационной безопасности: разработка, внедрение и эксплуатация, сопровождение

Сформируем основные этапы построения системы безопасности ИС:

- анализ физической и логической архитектуры;
- выявление уязвимых элементов;
- анализ и классификация возможных угроз;
- разработка политики безопасности;
- разработка системы защиты информации.

Анализ физической и логической архитектуры ИС происходит с учетом оценки аппаратных средств, программного обеспечения, схем распределения его компонентов между узлами сети. Кроме того, анализируются протоколы взаимодействия, сетевой трафик на различных уровнях сетевой модели взаимодействия, технологии использования мобильных программ (JAVA, ActiveX, JavaScript, VBScript и т.д.). Обязательным является проведение анализа согласованности аппаратной и программной конфигурации узлов сети и анализа подсистем защиты информации на различных уровнях программно-аппаратных средств.

Для выявления уязвимостей модулей системы диагностируются элементы аппаратных средств и каналы связи, используемые ИС, в т.ч. локальные сети, сетевые устройства концентрации и маршрутизации каналов межсетевого взаимодействия, а также каналов коммуникации с глобальными сетями. Кроме того, анализируются уязвимые элементы операционных систем и систем управления базами данных ИС. При этом важным направлением является оценка уязвимости элементов сетевых программных средств ИС (в т.ч. совместной работы, утилит администрирования, мобильных программ и сервисов).

Необходимо оценить и классифицировать угрозы несанкционированного использования аппаратных и программных ресурсов (например, возможности хищения, подлога, разрушения и потери информации, отказов в работе программно-аппаратных средств), а также угрозы некорректного использования информационных ресурсов (например, нарушения физической и логической целостности данных, работоспособности компьютерных систем). Кроме того,

подход к постороению безопасности ИС требует оценки угроз проявления ошибок пользователей, операторов и администраторов, а также угроз безопасности сетевого взаимодействия (безопасности информационного обмена и нарушений протоколов взаимодействия).

Необходимо сформировать политику безопасности для элементов ИС как совокупность концептуальных решений, направленных на эффективную защиту информации и ассоциированных с ней ресурсов. Предполагается формирование стратегических целей обеспечения информационной безопасности и определение требований к системе защиты информации. На этом же этапе разрабатывается концепция защиты от реализации преднамеренных и случайных угроз, составляется общий план восстановления на случай негативного воздействия на компьютерные ресурсы, а также разрабатываются организационные мероприятия и технические меры по созданию условий безопасной обработки информации в ИС.

Разработка системы защиты ИС требует формирования детальной спецификации компонентов системы информационной безопасности, проектирования комплексной системы защиты для рабочих станций, серверов, а также компьютерной сети в целом, подбора сертифицированных средств обработки и защиты информации. Таким образом, итогом формирования системы защиты информации на этапах ее разработки, построения и ввода в эксплуатацию является максимальная защищенность ИС. На рис. 1 показаны этапы жизненного цикла ИС на примере спиральной модели.

Рис. 1. Спиральная модель жизненного цикла ИС

В ходе эксплуатации ИС необходимо регулярно проводить анализ динамики угроз безопасности, а ранее выявленные актуальные угрозы подлежат периодической переоценке. Периодичность переоценки определяется индивидуально для конкретной ИС, исходя из особенностей ее функционирования (но не реже одного раза в год). В процессе выявления новых уязвимостей должны

быть учтены возможные источники угроз безопасности элементов защищаемой информационной системы.

Источниками угроз безопасности ИС будем считать нарушителей, осуществляющих целенаправленное или неумышленное деструктивное воздействие. С учетом наличия прав доступа и возможностей по доступу к информации и (или) к компонентам информационной советующей системы выделим два типа нарушителей:

- внешние нарушители – лица, не имеющие постоянного права доступа к информационной системе, ее отдельным компонентам или реализующие угрозы безопасности информации из-за границ информационной системы;
- внутренние нарушители – лица, имеющие право постоянного или периодического доступа к информационной системе, ее отдельным компонентам.

Наибольшими возможностями по реализации угроз безопасности обладают внутренние нарушители. Таким образом, при оценке их возможностей необходимо учитывать принимаемые организационные меры по допуску к работе в ИС. Возможности внутреннего нарушителя зависят от установленного порядка допуска физических лиц к ИС и ее компонентам, а также мер по контролю за доступом и работой этих лиц. В зависимости от имеющихся прав доступа нарушители могут иметь легитимный физический (непосредственный) и (или) логический доступ к компонентам информационной системы и (или) содержащейся в них информации или не иметь такого доступа. В качестве внутренних нарушителей безопасности информации информационной советующей системы могут выступать:

- лица, осуществляющие преднамеренные действия с целью доступа к информации (воздействия на информацию), содержащейся в информационной системе, или нарушения функционирования информационной системы или обслуживающей ее инфраструктуры (преднамеренные угрозы безопасности информации);
- лица, имеющие доступ к информационной системе, непреднамеренные действия которых могут привести к нарушению безопасности информации (непреднамеренные угрозы безопасности информации).

Анализ прав доступа пользователей к ИС проводится, как минимум, в отношении следующих компонент информационной системы:

- устройств ввода/вывода (отображения) информации;
- беспроводных устройств;
- программных, программно-аппаратных и технических средств обработки информации;
- съемных машинных носителей информации;
- машинных носителей информации, выведенных из эксплуатации;
- активного (коммутационного) и пассивного оборудования каналов связи;
- каналов связи, выходящих за пределы контролируемой зоны.

Определение угроз для разрабатываемой информационной советующей системы в процессе обмена информацией на всех уровнях в соответствии с эталонной семиуровневой моделью ISO/OSI (Open systems interconnection basic reference model, ГОСТ Р ИСО/МЭК 7498-1-99) может быть представлено по следующим уровням:

- на физическом уровне: обрыв канала связи, перепад напряжения;
- канальном уровне: перехват фреймов, прием фрейма с чужим MAC-адресом, подмена хоста, попытка подмена VLAN;
- сетевом уровне: подмена шлюза по умолчанию, нарушение процесса маршрутизации, DDOS-атака;
- транспортном уровне: подмена UDP (User Datagram Protocol) пакетов, атаки LAND;
- сеансовом уровне: подмена подлинности сертификатов, подмена электронной подписи, атака «человек посередине» в связке «клиент-сервер», перехват/подмена сеансовых ключей;
- уровне представления: дешифрование потока данных;
- прикладном уровне: нарушение разграничений прав доступа.

Реализация угроз безопасности ИС возможна как на уровне сетей, сетевых приложений и сервисов, так и на уровне операционной системы. Соответственно, определяя типы объектов, подверженных угрозе безопасности на раличных уровнях ISO/OSI, выделим для:

- для сетевого уровня – маршрутизаторы, коммуникаторы, концентраторы и сетевые карты;
- уровня сетевых приложений и сервисов – программные компоненты обеспечения взаимодействия сетевых аппаратных средств и передачи данных по компьютерным сетям;
- уровня операционных систем – файлы данных.

Приведенные рекомендации позволяют сформулировать элементы политики информационной безопасности ИС с учетом динамичности среды функционирования аппаратных и программных компонентов информационной системы.

Материал поступил в редколлегию 23.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 006.067

***Гулак Максим Леонидович**, к.т.н., доц. каф. «Системы информационной безопасности» БГТУ*

***Горлов Алексей Петрович**, к.т.н., доц. каф. «Системы информационной безопасности» БГТУ*

***Лексиков Евгений Вячеславович**, ст. преподаватель каф. «Системы информационной безопасности» БГТУ*

ФГБОУ ВО «Брянский государственный технический университет», Брянск, Россия

e-mail: gml13@yandex.ru

О НЕКОТОРЫХ ПОЛОЖЕНИЯХ ГОСТ Р 57580.1-2017

Проведен краткий обзор стандарта России ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер». Рассмотрены основная нормативная база Банка России в области защиты информации, некоторые положения нового стандарта, его текущий статус для финансовых организаций.

В банковском секторе российской экономики вопросы обеспечения информационной безопасности требуют самого пристального внимания. В этой сфере присутствуют реальные риски хищения денежных средств, а это требует реализации инструментария безопасности не только на словах или на бумаге, но и на практике.

В соответствии с законодательно закрепленными требованиями финансовые организации выстраивают системы защиты информации, которые, кроме того, учитывают технический, практический аспект безопасности.

Наряду с основными регуляторами в области обеспечения информационной безопасности (ФСТЭК России и ФСБ России), предъявляющими определенные требования, у финансовых организаций России есть и ведомственный регулятор – Центральный банк Российской Федерации (Банк России), также выдвигающий целый ряд требований, направленных на обеспечение безопасности.

На протяжении многих лет Банк России выпускает различные нормативные документы, регламентирующие деятельность финансовых организаций в области защиты информации. Некоторые из этих нормативных документов обязательны для выполнения, другие же носят необязательный рекомендательный характер. Так, в число обязательных к исполнению нормативных актов относятся многочисленные Положения Банка России, такие, как Положение Банка России №382-П от 9 июня 2012 г. «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспече-

нию защиты информации при осуществлении переводов денежных средств», Положение Банка России №552-П от 24 августа 2016 г. «О требованиях к защите информации в платежной системе Банка России». Кроме Положений, Банк России утвердил стандарты и рекомендации в области информационной безопасности (стандарты СТО БР ИББС и рекомендации РС БР ИББС). Важнейшим в этом ряду документом является Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2014). Все указанные документы носят лишь рекомендательный характер. Они обязательны к исполнению только при решении конкретного банка о присоединении к данному стандарту.

Следовательно, при построении системы защиты информации банки должны одновременно учитывать требования нескольких нормативных документов, направленных на выполнение всех необходимых требований по безопасности, что, несомненно, значительно увеличивает нагрузку на службы информационной безопасности. К тому же, необязательность выполнения стандарта СТО БР ИББС-1.0-2014 привела к тому, что Банк России не может заставить финансовые организации создавать полнофункциональные системы защиты информации. Поскольку не во всех банках и иных финансовых организациях информационная безопасность финансируется должным образом, это вызывает различные инциденты информационной безопасности.

Потому и появились планы по переработке существующих стандартов и разработке нового стандарта, определяющего некоторый конечный перечень мер защиты информации и являющегося обязательным для всех финансовых организаций.

В итоге был разработан национальный стандарт по защите информации в финансовых организациях, утвержденный Федеральным агентством по техническому регулированию и метрологии 8 августа 2017 года.

Положения разработанного Стандарта распространяются на различные финансовые организации: кредитные организации, некредитные финансовые организации, указанные в ч.1 ст. 76.1 Федерального закона «О Центральном банке Российской Федерации (Банке России)», и на субъекты национальной платежной системы. Следовательно, область действия Стандарта значительно расширилась. Помимо банков, требования стандарта теперь распространяются и на некредитные финансовые организации, такие как микрофинансовые и страховые компании.

К основным новеллам Стандарта можно отнести прописанные в документе уровни защиты информации. Таким образом, Банк России перешел от обязательного к исполнению перечня мер защиты к предоставлению финансовым организациям возможности самостоятельного определения необходимых и достаточных мер защиты информации. Это нововведение сравнимо с подходом ФСТЭК России, не первый год использующим классы защищенности для определения требований по защите информации для ГИС и АСУ ТП, ИСПДн.

Стандарт вводит 3 уровня защиты информации, позволяющих определить базовый состав защитных мер: уровень 3 – минимальный, уровень 2 – стандартный, уровень 1 – усиленный. Устанавливается уровень защиты информации для определенного контура безопасности (информационная система, реализующая бизнес-процессы единой степени критичности, для которых применяется единый режим защиты информации), которых в соответствии с нормативными документами Банка России в финансовой организации может быть один или несколько. Однако до настоящего времени Банк России не утвердил нормативные документы для определения уровня защиты информации.

Поскольку у финансовых организаций появилась возможность формирования конечного перечня мер защиты информации, финансовая организация, определив уровень защиты информации и, следовательно, соответствующий этому уровню базовый состав мер защиты, может адаптировать его к своим потребностям, учитывая при этом модели угроз и нарушителей информационной безопасности, структурные и функциональные характеристики объектов информатизации, используемые в организации информационные технологии, установленные нормативно-правовыми актами требования к защите информации.

Помимо этого, при невозможности технической реализации либо экономической нецелесообразности отдельных выбранных мер защиты информации Стандарт дает возможность использовать компенсирующие меры.

В Стандарте приведен базовый состав мер защиты информации для каждого установленного уровня защиты информации, а для каждой защитной меры документ определяет способы ее реализации: «О» – реализация с помощью организационной меры защиты информации, «Т» – реализация с помощью технической меры защиты информации, «Н» – реализация не обязательна.

Все приведенные в Стандарте меры защиты информации делятся на 3 больших категории, в которых выделены различные подгруппы (процессы, направления, стадии жизненного цикла): требования к системе защиты информации; требования к организации и управлению защитой информации; требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений.

В части технической защиты персональных данных, что должно быть учтено любой финансовой организацией, Стандарт не предлагает никаких специальных защитных мер. В тексте документа лишь выполнено соотнесение уровней защиты информации с уровнями защищенности ПДн, установленными в Постановлении Правительства Российской Федерации от 01.10.2012 г. №1119.

Можно сделать вывод, что рассмотренный Стандарт, с одной стороны, включает в себя уже устоявшиеся практические меры по обеспечению безопасности, с другой, – вводит и новые направления обеспечения информационной безопасности.

Статус Стандарта на сегодняшний день не определен. Хоть он и был утвержден в августе 2017 года и введен в действие с 1 января 2018 года, но пока данный ГОСТ носит рекомендательный характер. Банк России не включил

ссылку на Стандарт в свои нормативные документы, без чего Стандарт станет обязательным для исполнения в финансовых организациях. Помимо этого, пока нет утвержденных документов, которые бы устанавливали правила определения уровней защиты информации в финансовых организациях.

Учитывая, что Банк России переведет Стандарт в ранг обязательного, финансовым организациям уже сейчас следует ознакомиться с его положениями и разобраться, какие работы и изменения в действующих системах обеспечения информационной безопасности необходимо будет провести для выполнения его требований.

Материал поступил в редколлегию 22.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.007

Емельяненко Юлия Александровна, *магистрант кафедры «Системы информационной безопасности»*
Голембиовская Оксана Михайловна, *к.т.н., доц. кафедры «Системы информационной безопасности»*
ФГБОУ ВО «Брянский государственный технический университет», Брянск, Россия
e-mail: gorkye@yandex.ru

РАЗРАБОТКА МЕТОДИКИ ОЦЕНКИ РИСКОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Представлена разработка методики оценки рисков персональных данных.

Закон РФ «О персональных данных» № 152-ФЗ (Утвержден Президентом Российской Федерации 27.07.2006 года) дает следующее определение персональным данным физических лиц: «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)».

В настоящее время на рынке информационной безопасности представлен большой перечень автоматизированных средств, позволяющих произвести оценку рисков персональных данных для субъекта малого, среднего и крупного бизнесов, однако развитие информационного общества не стоит на месте, и поэтому необходимо постоянно расширять базу знаний и дополнять базы программных продуктов новыми данными.

Целью данной работы является разработка методики оценки рисков персональных данных с учётом предыдущих алгоритмов и методов произведения оценки.

Данная методика позволяет выполнить анализ и оценку рисков без привлечения высококвалифицированных специалистов в несколько этапов:

1. Идентификация активов организации.

Активы системы информационных технологий являются компонентом или частью общей системы, в которую предприятие напрямую вкладывает средства и которые, соответственно требуют защиты со стороны предприятия.

Составляются списки активов организации в процессе сбора администратором ИБ данных для анализа рисков путем опроса сотрудников предприятия с целью выявления используемых активов. При идентификации активов следует иметь в виду, что всякая система информационных технологий включает в себя не только аппаратные средства, но и программное обеспечение.

1. Информация/данные (файлы, содержащие информацию о платежах или продукте).
2. Аппаратные средства (компьютеры, принтеры).

3. Программное обеспечение, включая прикладные программы (программы обработки текстов, программы целевого назначения).

4. Оборудование для обеспечения связи (телефоны, медные и оптоволоконные кабели).

5. Программно-аппаратные средства (электронные носители информации).

6. Документы (контракты).

7. Продукция предприятия.

8. Услуги (информационные, вычислительные услуги).

9. Конфиденциальность и доверие при оказании услуг (услуг по совершению платежей).

10. Оборудование, обеспечивающее необходимые условия работы.

11. Персонал организации.

12. Престиж (имидж) организации.

2. Определение вероятности реализации угроз.

Определение вероятности возникновения неблагоприятных событий и актуальность угроз ИБ определяется специалистом или группой специалистов, занимающихся разработкой модели угроз. По завершении этапа формируется список актуальных угроз на каждый актив или группу активов.

3. Определение риска несоответствия требований законодательства в области ИБ.

Любая организация, имеющая информационные системы или работа которой связана с использованием информационных технологий для ведения бизнеса, должна соблюдать федеральные законы в этой отрасли. Невыполнение данных требований может повлечь за собой гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность. Риск невыполнения требований законодательства влияет на общий риск ИБ МСБ. Алгоритм определения риска несоответствия требований законодательства в области ИБ включает в себя проведение всестороннего анализа состояния системы защиты с целью выявления выполнения требований в соответствии с требованиями законодательства. В ходе проведения анализа всем требованиям, которые выполняются, присваивается значение «1», в обратном случае – «0». Все значения, которым присвоено значение «1», суммируются, остальные значения не учитываются. В заключение анализа необходимо определить уровень риска несоответствия требований по ИБ, который определяется по табл. 1.

Таблица 1

Уровень риска несоответствия требований по ИБ

Сумма выполненных требований	Риск несоответствия требованиям законодательства (Rn)
1	2
40–51	0,01

Окончание табл. 1

27–39	0,25
Менее 26	0,5
Не выполняются	0,9

4. Проведение количественной оценки рисков:

• Выявление актуальных угроз - при помощи модели угроз составляется список актуальных угроз. Идентифицированные активы сопоставляются с направленными на них угрозами.

• Определение вероятности наступления угрозы - на один актив могут влиять одновременно несколько угроз. Следует выяснить вероятность того, что хотя бы одна угроза реализуется по отношению к выбранному активу.

• Определение ценности активов в рублях.

• Определение возможности применения технических и организационных уязвимостей - вероятность применения организационных уязвимостей проводится экспертным методом.

• Расчет численного значения риска.

5. Определение допустимого уровня риска.

Допустимый принято считать тот риск, который в данной ситуации считают приемлемым при существующих общественных ценностях.

6. Рекомендации.

В результате выполнения данных операций при необходимости вносятся изменения в политику безопасности организации, обновляется список актуальных угроз и формируется перечень контрмер. Выявленные уязвимости устраняются технически и документально.

Риск реализации хотя бы одной угрозы из всего перечня актуальных угроз с учетом наличия уязвимостей по отношению к конкурентному активу определяется по общей формуле:

$$R = R_{угр.} \cdot R_{н} \cdot C \cdot \left(\frac{K_{о} + K_{т} + K_{п}}{3} \right) \cdot 100\% , \quad (1)$$

где R – численная величина риска реализации угроз ИБ;

Rугр. – вероятность реализации хотя бы одной угрозы из всего перечня актуальных угроз;

Rн – риск несоответствия требованиям законодательства;

C − ценность актива;

Ko – вероятность использования организационных уязвимостей;

Kт – вероятность использования технических уязвимостей;

Kп– вероятность использования программных уязвимостей.

Таким образом, учитывая все обозначенные этапы, разработанная методика будет решать следующие задачи:

1. Проведение оценки риска персональных данных в организации при помощи собственных ресурсов, без привлечения высококвалифицированных специалистов;

2. Наглядное отражение степени выполнения требований законодательства при защите персональных данных на предприятии;

3. Использование результата оценки рисков для выработки рекомендаций по снижению уровня риска.

Материал поступил в редколлегию 16.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.056

Ерёменко Владимир Тарасович, *д.т.н., профессор, заведующий кафедрой «Информационная безопасность» ОГУ им. Тургенева*
Скуридина Юлия Сергеевна*, студентка каф. «Информационная безопасность» ОГУ им.Тургенева*
Орловский государственный университет им. И.С.Тургенева, Орёл, Россия
e-mail: wladimir@orel.ru

ВНУТРЕННИЙ И ВНЕШНИЙ АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Рассматривается вопросы аудита и проверки информационной безопасности. Рассмотрены принципы поведения и организации систем внешнего и внутреннего аудита информационной безопасности.

Введение. Управление ИБ – неотъемлемая часть управления любой современной организацией в целом, независимо от её размера и сферы деятельности.

Управление ИБ является сложным непрерывным процессом, перед которым стоит множество целей и задач, являющихся обеспечивающими вспомогательными по отношению к основным бизнес-целям и задачам объектов информатизации. Они формулируются в различных документах: концепциях, стратегиях, стандартах, инструкциях и т.д.

Для успешного управления ИБ должна быть создана учитывающая специфику организации и адекватная её требованиями в отношении обеспечения ИБ система управления информационной безопасности (СУИБ)

Для организации и проверок СУИБ необходимо определить их виды (мониторинг, самооценка, аудит), а далее осуществить сами проверки и анализ СУИБ со стороны руководства.

Оценка и проверка СУИБ и ИБ как часть системы обеспечения ИБ объектов информатизации и, как результат, выявление признаков деградации используемых защитных мер могут проводится путём выполнения следующих процессов на уровне как всей организации, так и её отдельных процессов активов-систем, сетей, сервисов, самой информации:

1. Мониторинга и контроля используемых защитных мер (как непрерывные во времени, постоянно проводимые процессы).
2. Самооценки ИБ (проводимые в рамках заданного интервала времени с установленными программой и планом проведения).
3. Внешнего и внутреннего аудита ИБ (проводимые с установленными программой и планом проведения).
4. Анализа функционирования СУИБ (в том числе со стороны руководства) (также проводимые с установленной периодичностью).

Основываясь на этом, необходимо детально рассмотреть внешний и внутренний аудит ИБ объектов информатизации, который является неотъемлемой частью систем безопасности.

Особенности внутреннего аудита ИБ объектов информатизации

Через запланированные интервалы времени объекты информатизации должны проводить внутренние аудиты ИБ, рассматривая их как важнейшую форму контроля руководством функционирования СУИБ.

Аудит ИБ объектов информатизации - проверка состояния защищенности интересов/целей объектов в процессе их реализации в условиях внутренних и внешних угроз ИБ, а также предотвращение утечки защищаемой информации и возможных несанкционированных и непреднамеренных воздействий на неё.

Аудит ИБ объектов информатизации систем информационных технологий (ИТ) - проверка состояния защищенности конфиденциальной информации в организации от внутренних и внешних угроз ИБ, а также ПО и АО, от которого зависит бесперебойное функционирование систем ИТ.

Технический аудит осуществляется семейством программных и технических средств контроля, обеспечивающих деятельность по регистрации событий ИБ, а также (возможно) по исследованию нарушений ИБ на основе данных регистрации. Во время его проведения дается общая оценка архитектуры и информационных потоков (Интернет, электронная почта, веб-приложения, файлы и т. д.), проверяется наличие и текущее состояние СОИБ, актуальность применяемых политик, технических регламентов и инструкций.

Внутренний аудит ИБ объектов информатизации как регламентированную внутренними документами деятельность по контролю функционирования СУИБ и различных аспектов ОИБ, осуществляемую представителями специального контрольного органа — подразделения организации в рамках помощи органам управления организации. В стандартах ISO/IEC и ГОСТ Р ИСО/МЭК 19011 внутренний аудит называется аудитом *первой* стороной, который проводится организацией или от её имени[5,6].

Цели внутренних аудитов ИБ объектов информатизации

Целями внутренних аудитов ИБ является определение следующего [1,2,7,8]:

1. Соответствуют и адекватны ли документы, деятельности и результаты в области управления ИБ требованиям применяемых международных, национальных и иных стандартов в области ИБ и относящихся к ним законов или норм.
2. Соответствуют и адекватны ли деятельности и результаты в области управления ИБ выявленным требованиям по ОИБ, разработанным самой организацией.
3. Эффективно ли реализуются и поддерживаются в рабочем состоянии запланированные мероприятия по управлению и обеспечению ИБ.
4. Выполняются ли, как ожидается, цели, средства, процессы и процедуры СУИБ организации.

Внутренний аудит ИБ объектов информатизации обеспечивает руководство информацией об эффективности и продуктивности СУИБ.

Результаты внутренних аудитов ИБ служат основой входных данных для анализа СУИБ со стороны руководства и дают полезную информацию независимым экспертам проведении внешних аудитов ИБ.

Требования к организации системы внутреннего аудита ИБ[10-12].

1. Ущемление интересов - необходимо создавать специальные условия, при которых любые отклонения ставят или подразделение организации в невыгодное положение и побуждают их к регулированию «узких мест».
2. Недопущение концентрации прав первичного контроля в руках одного лица.
3. Заинтересованность и должное участие руководства объектов информатизации.
4. Приемлемость/пригодность методологии внутреннего аудита ИБ.
5. Непрерывность развития и совершенствования.
6. Приоритетность - абсолютный контроль над обычными незначительными операциями не имеет смысла и только отвлекает силы от более важных задач.
7. Исключение ненужных этапов шагов процедур в проведении внутреннего аудита ИБ.
8. Персональная ответственность - каждая отдельная контрольная функция должна быть закреплена только за одним ответственным.
9. Аудитор оценивает законность всех операций, но ответственность он несет за необнаруженные операций с негативными последствиями
10. Потенциальное замещение функций
11. Регламентация - подчиненность аудиторской деятельности.

Особенности внешнего аудита ИБ объектов информатизации

Чтобы обеспечить долгосрочность, адекватность и результативность подхода организации к управлению ИБ, а также оценить возможности улучшения за счет внедрения корректирующих действий и потребность в изменениях и подходе к защите, включая политику и цели в области управления ИБ, нужен внешний аудит ИБ объектов информатизации.

Внешний аудит ИБ объектов информатизации — систематический, независимый и документируемый процесс получения свидетельств деятельности объектов информатизации, по ОИБ и установления степени выполнения в ней критериев аудита ИБ.

Согласно стандартам ISO/IEC и ГОСТ Р ИСО/МЭК 19011 внешние аудиты включают так называемые аудиты *второй* и *третьей* сторонами[5,6]. Аудиты *второй* стороной проводятся сторонами, заинтересованными в деятельности организации, например потребителями или другими лицами от их имени. Аудиты *третьей* стороной проводятся внешними независимыми аудиторскими организациями, например такими, которые обеспечивают сертификацию/регистрацию соответствия стандартам ISO 9001, 14001 или 27001.

Существуют такие аудиты, как *первичные сертификации, надзорные аудиты, аудиты повторной сертификации и специальные аудиты*. Все они проводятся в строгой последовательности по истечении определённых сроков.

Цели внешнего аудита ИБ определяет заказчик аудита - организация или лицо, его заказавшее. Обычно требуется подтверждение одного или сразу двух положений:

1. Проверяемая организация придерживается собственных политики, целей и процедур в области ОИБ;
2. Соответствие СУИБ проверяемой организации всем требованиям стандартов ISO/IEC и ГОСТ Р ИСО/МЭК 27001 и целям политики организации.

Основными документами внешнего аудита являются:

1. Программа внешнего аудита
2. План внешнего аудита
3. Аудиторское заключение

Программа аудита ИБ объектов информатизации — план деятельности по проведению одного или нескольких аудитов ИБ (обязательно внешних плюс возможно внутренних и самооценок), запланированных на конкретный период времени и направленных на достижение конкретной цели.

План аудита ИБ объектов информатизации — описание деятельности и мероприятий по какому-либо конкретному аудиту ИБ.

Аудиторское заключение объектов информатизациим (заключение по результатам аудита ИБ) – качественная и/или количественная оценки соответствия установленным критериям аудита ИБ, представленные аудиторской группой после рассмотрения всех выводов аудита ИБ в соответствии с целями аудита ИБ.

Выводы аудита ИБ объектов информатизации - результат оценки собранных свидетельств аудита ИБ на соответствие критериям аудита ИБ. Выводы аудита ИБ указывают на несоответствие/соответствие и степень соответствия ИБ организации критериям аудита ИБ или возможность улучшения.

Аудитор (эксперт) *объектов информатизации* - лицо, обладающее компетентностью для проведения аудита ИБ.

Аудиторская группа объектов информатизации - один или несколько аудиторов, проводящих аудит ИБ, при необходимости поддерживаемые техническими экспертами

Технический эксперт объектов информатизации - лицо, предоставляющее аудиторской группе свои знания и/или опыт по специальным вопросам, включая ИБ.

Принципы проведения внешнего аудита

Проведение внешнего аудита ИБ основывается на ряде принципов, следование которым является предпосылкой для обеспечения объективных заключений по результатам внешнего аудита ИБ [4-9].

К принципам внешнего аудита ИБ относят:

Независимость – основа беспристрастности при проведении внешнего аудита ИБ и объективности при формировании заключения по результатам аудита ИБ.

Полнота – необходимое условие для формирования объекта, заключения по результатам аудита ИБ. Аудит ИБ должен охватывать области ИБ, соответствующие аудиторскому заданию

Оценка на основе свидетельств аудита ИБ объектов информатизации – основа для достижения надёжных воспроизводимых (повторяемых) заключений внешнего аудита ИБ в процессе систематического аудита ИБ. Свидетельство аудита основано на выборках существующей информации, поскольку аудит осуществляется в ограниченный период времени и с ограниченными ресурсами.

Достоверность свидетельств аудита ИБ объектов информатизации – основа получения достоверных и полных заключений внешнего аудита ИБ. Доверие к фактам, полученным при опросе сотрудников проверяемых подразделений, повышается при подтверждении данных фактов из различных источников.

Необходимость понимания аудитором деятельности проверяемой в объектах информатизации – условие получения достоверных и полных заключений внешнего аудита ИБ. Компетентность, этичность и беспристрастность - основа профессионализма. Доверие к процессу внешнего аудита ИБ зависит от компетентности тех, кто проводит аудит ИБ, и от этичности их поведения. Этичность поведения подразумевает ответственность, неподкупность, умение хранить тайну, осмотрительность. Беспристрастность означает обязательство представлять правдивые и точные отчеты. Выводы внешних аудитов ИБ, включения по результатам аудита и записи отражают правдиво и точно.

Ответственность – за соответствие требованиям несет проверяемая организация, а за оценку достаточности объективных свидетельств, являющихся основанием для принятия решений, и сами принимаемым решения-аудиторская организация.

Открытость – принцип доступности и раскрытия соответствующей информации.

Конфиденциальность – аудиторская организация должна обеспечивать конфиденциальность частных сведений о проверяемой организации.

Реагирование на жалобы – в случае призвания обоснованными жалобы сторон соответствующим образом учитываются, рассматриваются, находятся пути их решения проблем.

Заключение. В любой организации должна быть оценка и проверка деятельности. Аудит ИБ объектов информатизации как внешний, так и внутренний необходим для целостной и организованной работы предприятий и компаний. Конечно, здесь затронуты далеко не все его аспекты. Причина состоит только в том, что на постановку задач и методы его проведения влияет очень много факторов, поэтому подход в каждом конкретном случае строго индиви-

дуален. К тому же методы и средства аудита информационной безопасности могут быть разными для различных ИС.

Список литературы

1. ISO/IEC 19011.2002 «Guidelines for quality and/or environmental management systems auditing».
2. ISO/IEC 27001:2005 «Information technology. Securit techniques. Information ли security management systems. Requirements».
3. ISO/IEC 27002:2005 «Information technology. Security techniques Code of practice for information security management
4. ISO/IEC 27006:2011 «Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems».
5. Бурцев, В.В. Внутренний аудит компании: вопросы организации и управления/ В.В. Бурцев // Финансовый менеджмент. – 2003. – № 4. – С. 20-24.
6. ГОСТ Р ИСО 19011-2003 «Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента»
7. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и J средства обеспечения безопасности. Системы менеджмента информацион¬ной безопасности требования». – М.: Стандартинформ. – 2008.
8. ГОСТ Р ИСО/МЭК 27006:2008 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, обеспечиваю-щим аудит и сертификацию систем менеджмента ИБ».
9. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью».
10. Концепция аудита информационной безопасности систем информационных технологий и организаций. Государственная техническая комиссия при Президенте Российской Федерации, Воронеж, 2004.
11. Петренко, С. А. Анализ рисков в области защиты информации/ С.А. Петренко: Информационно-методическое пособие по курсу повышения квалификации «Управление информационными рисками». – СПб.: Издательский дом «Афина, 2009.

Материал поступил в редколлегию 23.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 331.108.26

***Лексиков Евгений Вячеславович**, ст. преподаватель каф. «Системы информационной безопасности»*
***Гулак Максим Леонидович,** к.т.н., доц. каф. «Системы информационной безопасности»*
***Горлов Алексей Петрович** к.т.н., доц. каф. «Системы информационной безопасности»*
ФГБОУ ВО «Брянский государственный технический университет», Брянск, Россия
e-mail: JL32@yandex.ru

ИСПОЛЬЗОВАНИЕ НЕЧЕТКОГО КОГНИТИВНОГО МОДЕЛИРОВАНИЯ ДЛЯ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ПОРТАЛОВ РЕГИОНАЛЬНЫХ ОРГАНОВ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ

Рассмотрен процесс использования нечетного когнитивного моделирования для проведения аудита информационной безопасности информационных порталов региональных органов исполнительной власти.

Обеспечение региональных органов исполнительной власти единой точкой доступа к информационным, производственным и экономическим ресурсам позволяет оптимизировать и автоматизировать процесс принятия управленческих решений. Однако внедрение информационного портала в такую обширную и сложную область не является мгновенным и легким процессом. Информационный портал (ИП) неотъемлемая часть усовершенствования процесса принятия управленческих решений для органов государственной и исполнительной власти, призванной решать критические проблемы информационных процессов. Также следует отметить, что в настоящее время процесс разработки информационных порталов региональных органов исполнительной власти не типизирован и не позволяет оперативно создавать информационные порталы для различных регионов на основе типовых проектных решений с целью обмена и обработки данных.

Для региональных органов исполнительной власти необходимо, чтобы информационный портал выполнял роли АИС и ИСУ.

АИС (автоматизированная информационная система) – это система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы.

ИСУ (информационная система управления) – это единый набор находящихся в отношениях и связях друг с другом элементов, позволяющий осуществлять сбор, обработку, хранение и предоставление информации о деятельности региональных ОИВ для принятия управленческих решений.

Разработка информационного портала региональных органов исполнительной власти является сложным процессом (рисунок). Перед разработкой информационного портала выполняются длительные и масштабные работы по сбору первичных требований, их анализу и проектированию будущего программного решения, оценке угроз и рисков. В целом весь этот длительный процесс называется аудитом информационной безопасности.

Условно первый этап процесса разработки ИП можно разделить на 4 уровня, которые выполняются строго последовательно:

1. Проведение аудита ИБ.

2. Подготовка ТЗ. Формируется техническое задание на разработку АИС (в обиходе «ТЗ по конкурсу»), в котором оформляются первичные требования различных направлений к АИС.

3. Выбор вида ИП. Выбирается основное техническое решение для поставленной в ТЗ задачи.

4. Выдача проекта и прогнозирование рисков. На выходе после первых трех уровней должен получиться технический проект по реализации заданной АИС.

Рассматривая процесс аудита ИБ организации, остановимся на первом уровне.

На первом уровне происходит осознание потребности в информационном портале, поиск первичной информации по запрашиваемой тематике. Формируются первичные требования к информационному порталу, а также перечень целей и задач, которые он должен будет выполнять.

Затем на основе первичных требований необходимо проводить аудит информационной безопасности (далее аудит ИБ). Аудит ИБ определен как аудит, охватывающий изучение и оценку по всем аспектам (или части из них) систем автоматизированной обработки информации, в том числе связанных неавтоматизированных процессов и интерфейса, который их собирает [1].

Аудит ИБ представляет собой деятельность по сбору и оценке ряда доказательств для определения того, является ли информационная система безопасной, поддерживает ли целостность переработанных и внесенных данных, позволяет ли достичь стратегических целей субъекта и насколько эффективно использует информационные ресурсы.

Активное развитие информационных технологий способствовало разработке и последующему совершенствованию методологий аудита при использовании компьютеров и комплектующих средств. Информационные технологии сегодня применимы на всех этапах проведения процедуры аудита: во время планирования, осуществления, документирования аудиторской работы, оформления аудиторского вывода. Поэтому вопрос автоматизации процесса аудита является очень важным на данный момент.

В настоящее время достаточно сложно представить аудиторское исследование без использования информационных технологий. С одной точки зрения, компьютер – это универсальное средство, призванное помогать аудиторам ре-

шать различные повседневные задачи, в круг которых входят в информационном обслуживании - ускорение процессов получения и обработки информации из баз данных клиента, документальная обработка информации, полученной аудиторами в ходе проверки; в методическом обслуживании - разработка аналитических электронных таблиц, создание прикладных аудиторских программ, ускорение применения аудиторских процедур; редактирование текстов и электронных таблиц, создание баз данных и пр. Однако, с другой точки зрения, использование клиентом автоматизированных информационных систем предъявляет особые требования к организации проведения исследования и выбора аудиторских процедур, что усложняет данный процесс.

На современном этапе организациям необходим структурированный подход в области аудита и управления информационными технологиями, который позволит гарантировать безопасность. Анализ показывает, что существующие подходы к проведению аудита ИБ не учитывают взаимное влияние ИТ-процессов друг на друга, объясняемое наличием ограничений на общий потребляемый ресурс.

Система управления ИТ-процессами организации является сложным организационно-техническим объединением. Именно поэтому механизм управления ее элементами является слабоструктурированным, допускающим формализацию в основном на качественном уровне, где изменение параметров системы может приводить к труднопредсказуемым изменениям в ее структуре [3].

В связи с этим для решения задачи анализа информации, имеющей такого рода нечеткости, особую актуальность приобрели нечеткие модели, т.е. модели, опирающиеся на теорию нечетких множеств, представляющую собой обобщение и переосмысление важнейших направлений классической математики. Для формализации подобных сложных систем чаще всего используется метод нечеткого моделирования для слабоструктурированных систем, который базируется на понятии нечетких множеств.

В основе метода нечеткого моделирования лежит понятие нечеткой когнитивной карты (НКК), впервые предложенное Б. Коско.

Информация о системе или процессе представляется в виде набора значимых факторов (концептов) и связывающих их причинно-следственных связей, при этом узлы получаемого нечеткого ориентированного графа представляют собой нечеткие множества, а направленные ребра определяют степень влияния (вес) связываемых концептов, что, в отличие от других методов, дает возможность формализации численно неизмеримых факторов, использования неполной нечеткой информации [2].

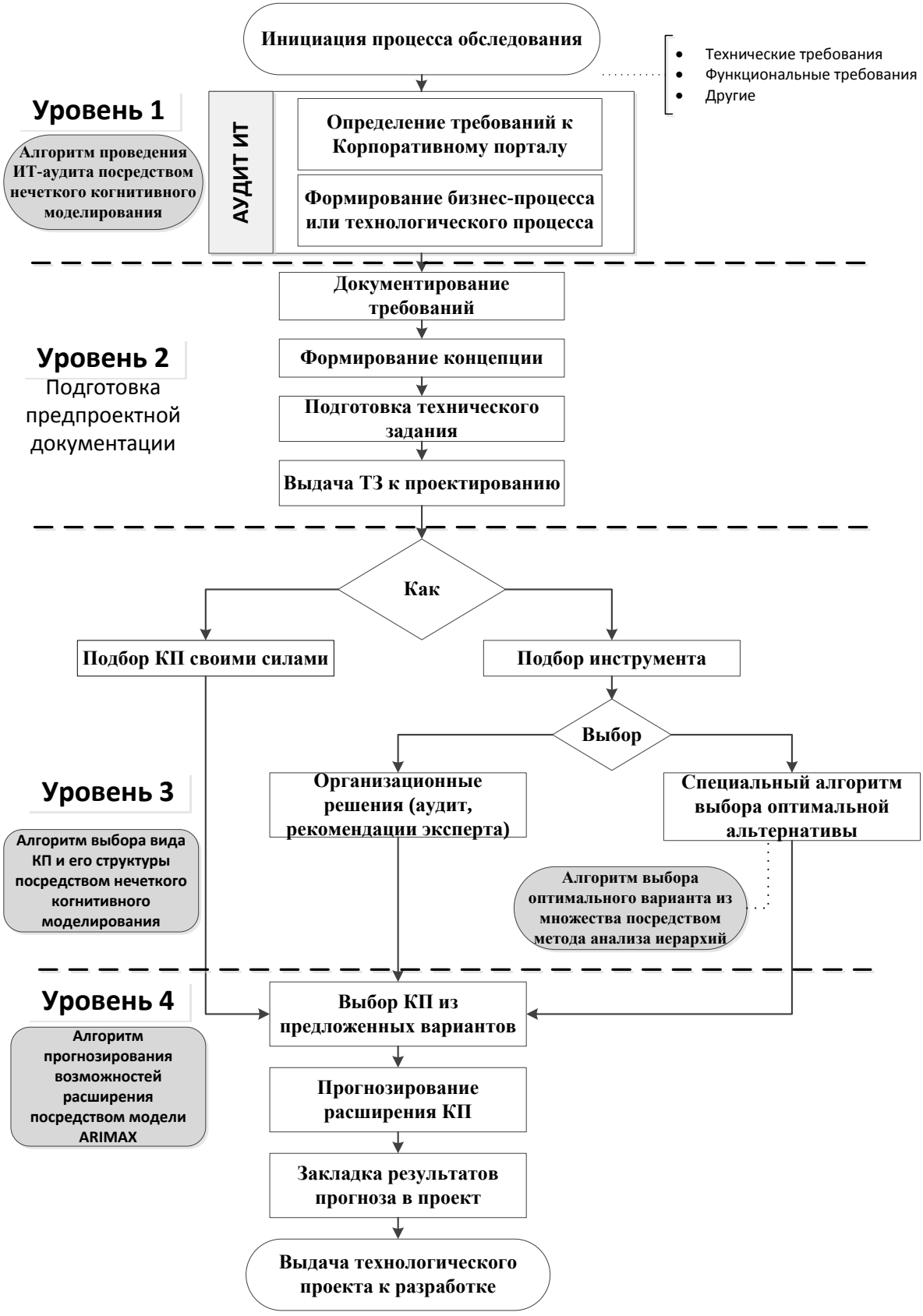

Рис.1. Алгоритм разработки информационного портала

Общая процедура применения аппарата НКК к решению задачи оценки обеспеченности ИТ-стратегии на заданном интервале планирования предусматривает реализацию следующего конечного множества этапов, которые задаются стандартным способом построения НКК.

Этап 1. Ввод множеств концептов:

- Шаги 1-4. Формирование множеств концептов, которые характеризуют различные параметры.

Для моделирования НКК необходимо задать множества концептов, которые в дальнейшем определят структуру нечеткой когнитивной модели исследуемого процесса.

В данном случае рассматривается ИТ-аудит предприятия перед проектированием ИП. Берутся множества угроз, рисков, ИТ-целей, уровни возможностей ИТ-процессов, а также ключевые показатели эффективности ИТ-процессов [4].

Каждое множество концептов имеет следующий вид:

$K^{\text{У}} = (K_1^{\text{У}}, K_2^{\text{У}}, \dots, K_i^{\text{У}})$,

где $\text{К}_\text{i}^{\text{У}}$ - концепт, характеризующий уровень влияния угроз безопасности (i =1, …, I).

Таким способом задаются все остальные множества концептов.

- Шаг 5. Формирование когнитивной модели исследуемого процесса.

Результатом выполнения шагов 1–4 первого этапа является структура нечеткой когнитивной модели:

$K = (\propto_1 K^{\text{У}}, \propto_2 K^a, \propto_3 K^b, K^{KPI})$,

где $\propto_1$, $\propto_2$, $\propto_3$ - бинарные функции, определяющие перечень критичных бизнес-целей, ИТ-целей и ИТ-процессов для конкретного профиля организации; К^a, К^b, К^{KPI} – множества концептов, которые были заданы в шагах 2-4.

Этап 2. Формирование отношений влияний между множествами:

- Шаги 1-4. Формирование отношений влияния между концептами из всех введенных на 1-м этапе множеств.

В качестве примера рассмотрим множество $\text{К}^{\text{У}}$. Отношения влияния между концептами из множества $\text{К}^{\text{У}}$ представляются в виде весов $\text{w}_{\text{ij}}^{\text{У}} \in [-1,1]$ и рассматриваются как элементы нечеткой матрицы смежности $\text{W}^{\text{БЦ}}$:

$$W^{\text{ПР}} = \begin{bmatrix} W_{11}^{\text{У}} & W_{12}^{\text{У}} & \dots & W_{1i}^{\text{У}} \\ W_{21}^{\text{У}} & W_{22}^{\text{У}} & \dots & W_{2i}^{\text{У}} \\ \dots & \dots & \dots & \dots \\ W_{j1}^{\text{У}} & W_{j1}^{\text{У}} & \dots & W_{ji}^{\text{У}} \end{bmatrix}$$

Эти отношения, отображаемые в виде дуг ориентированного графа, описывающего нечеткие причинно-следственные связи между концептами, могут быть положительными, отрицательными или нейтральными, характеризующими соответствующее влияние концептов друг на друга.

- Шаг 5. Для определения взаимовлияния концептов от исходной нечеткой матрицы смежности W с положительно-отрицательными нечеткими связями нужно перейти к нечеткой матрице положительных связей V размером $2I \times 2I$, элементы которой определяются из матрицы W размером $I \times I$ с помощью следующей замены:

- если $w_{ij} > 0$, то $v_{2i-1,2j-1} = w_{ij}, v_{2i,2j} = w_{ij}$;

- если $w_{ij} < 0$, то $v_{2i-1,2j-1} = -w_{ij}, v_{2i,2j} = -w_{ij}$.

Остальные элементы принимают нулевые значения.

В случае амбивалентности в исходной матрице положительно-отрицательная пара весов влияния преобразуется по аналогичному алгоритму, только вместо нулей на диагоналях ставятся определенные значения.

- Шаг 6. Согласованные отношения взаимовлияния концептов определяются в результате транзитивного замыкания:

$$V = VvV^2v \ldots V^n,$$

где степени нечетких матриц вычисляются на основе операции max–T-композиции.

После этого результат представляется в виде модифицированной матрицы, состоящей из положительно-отрицательных пар весов $W = \|w_{i,j}, \overline{w}_{ij}\|$, полученных по следующему правилу:

$$\begin{cases} w_{ij} = \max\left(v_{2i-1,2j-1}, v_{2i,2j}\right); \\ \overline{w}_{ij} = -max\left(v_{2i-1,2j-1}, v_{2i,2j}\right). \end{cases}$$

В результате этапа 2 формируется нечеткая когнитивная карта, отображающая системные факторы анализируемой системы (процесса, проблемы).

Этап 3. Формирование нечетких моделей. Модели формируются исходя из влияния одного концепта на другой. Так, в случае аудита ИБ можно построить НКМ влияния угроз, рисков на ИТ-процессы и БЦ региональных ОИВ.

В итоге получаются нечеткие когнитивные модели, отражающие все ключевые параметры, а также влияние каждого параметра на остальные. Таким образом, можно получить полную картину и взвесить все плюсы и минусы при планировании разработки программного решения.

Для региональных ОИВ, планирующих внедрение информационного портала, данный метод проведения аудита ИБ может сыграть немаловажную роль, так как позволяет установить зависимость между предполагаемыми угрозами, рисками и бизнесцелями, ИТ-возможностями информационного портала, определив эффективность использования такого мобильного инструмента централизованного управления практически всеми организационными и информационно-технологическими процессами ОИВ, и оценить риски при принятии управленческих решений.

Материал поступил в редколлегию 23.04.18.

УДК 331.108.26

***Лексиков Евгений Вячеславович**, ст. преподаватель каф. «Системы информационной безопасности» БГТУ*
Голиш Евгений Геннадьевич, магистрант каф. «Системы информационной безопасности» БГТУ
ФГБОУ ВО «Брянский государственный технический университет», Брянск, Россия
e-mail: JL32@yandex.ru

СНИЖЕНИЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С УЧЕТОМ ЛОЯЛЬНОСТИ ПЕРСОНАЛА

Рассмотрен процесс снижения рисков информационной безопасности с учетом лояльности персонала.

В процессе становления рыночных отношений, создания правовой основы цивилизованного предпринимательства, усиления недобросовестной конкуренции и криминализации отдельных сегментов экономики важная роль ложится на службы безопасности коммерческих предприятий, которые во многих случаях оказались не подготовленными к их решению.

Проблема оценки информационной безопасности государства, региона, отрасли или организации в последнее время приобрела особую актуальность. Однако, несмотря на большой интерес к ней отечественных и зарубежных ученных и практиков, следует отметить, что существующие разработки в основном посвящены различным аспектам национальной и региональной безопасности и в значительно меньшей степени – вопросам экономической и информационной безопасности отдельных предприятий. В настоящее время организации сталкиваются с целым рядом инсайдерских угроз: утечкой конфиденциальной информации, мошенничеством, злоупотреблением сетевыми ресурсами и саботажем. Наиболее опасной угрозой является утечка корпоративных секретов, в то время как остальные риски наносят значительно меньший ущерб.

Такая ситуация обусловлена тем, что утечка конфиденциальной информации приводит к снижению конкурентоспособности и ухудшению имиджа организации.

По статистике 2016 года, рейтинг самых опасных угроз ИБ трансформировался в следующий список: как и ранее на первом месте остается кража информации, однако на втором месте оказалась халатность сотрудников, а на третьем месте – саботаж. Таким образом, очевидно, что инсайдеры превалируют над вредоносными программами, хакерскими атаками, финансовым мошенничеством и аппаратно-программными сбоями[2].

Поэтому актуальной задачей, требующей безотлагательного решения, является формализация процесса оценки лояльности персонала для снижения рисков информационной безопасности объекта защиты.

Воздействию угроз экономической безопасности на предприятии, фирме, коммерческой организации может подвергаться следующая информация:

Сведения коммерческого содержания:

- данные о конкурентах, их слабые и сильные стороны;
- данные о поставщиках;
- данные о рынках сбыта;
- условия финансовой деятельности;
- технологические секреты;
- меры, предпринимаемые конкурентами в отношении своих противников;
- данные о потенциальных партнерах, проверка их на недобросовестность;
- информация о месте хранения грузов, времени и маршрутах их перевозки;
- выявление уязвимых звеньев среди сотрудников; выявление лиц, перспективных для вербовки путем подкупа, шантажа или иного метода;
- связи и возможности руководства;
- выявление круга постоянных посетителей.

Сведения личного характера:

- источники доходов;
- истинное отношение к тем или иным общественным явлениям, 'сильным мира сего;
- уклад личной жизни руководителя и членов его семьи;
- расписание и адреса встреч - деловых и личных;
- данные о размерах финансового благополучия;
- информация о человеческих слабостях;
- пагубные пристрастия;
- вредные привычки;
- сексуальная ориентация;
- данные о друзьях, подругах, местах проведения досуга, способах и маршрутах передвижения;
- информация о местах хранения ценностей;
- место жительства;
- супружеская неверность;
- проблемы отцов и детей.

Получить достоверную информацию о деятельности фирмы незаконным путем маловероятно, если фирма с пониманием относится к сохранности коммерческой тайны и созданию соответствующей системы защиты.

В то же время многие под безопасностью понимают, прежде всего, физическую защищенность, иногда включая отдельные требования информационной защиты коммерческих интересов, что не способствует решению проблем безопасности в комплексе. Вывод один - необходимо обеспечивать информационную безопасность, благодаря которой субъекты предпринимательской деятельности являются участниками выгодного внутреннего и международного

обмена товаром и знаниями, имея от этого прибыль. Причем каждый коммерческий объект должен строить свою систему информационной защиты на концептуальной основе, исходя из назначения объекта, его размеров, условий размещения, характера деятельности и т.д.

Опираясь на результаты статистических исследований, очевидно, что при снижении рисков человеческого фактора снижаются риски информационной безопасности в целом. В общем виде процесс анализа рисков ИБ сводится к следующей последовательности:

1 Описание исследуемой информационной системы (ИС).

2 Идентификация и оценка угроз.

3 Идентификация и оценка уязвимостей.

4 Идентификация существующих и планируемых мер защиты информации.

5 Расчет и оценка рисков ИБ.

6 Выработка предложений по снижению рисков.

Рассмотрим ключевые аспекты процесса анализа рисков ИБ с учетом рисков человеческого фактора.

Расчет риска ИБ заключается в определении его уровня, выраженного в количественной или качественной величине, а оценка риска - в сравнении этого уровня с максимально допустимым (приемлемым) уровнем, а также уровнем других рисков.

В простейшем случае расчет риска производят по двум факторам: вероятность происшествия и тяжесть возможных последствий.

Математически это можно выразить через следующее выражение:

$$P_{эб} = P_{происшествия} \times V_{потери}\ , \qquad (1)$$

где $P_{происшествия}$ – вероятность происшествия,

$V_{потери}$ – тяжесть возможных последствий.

Таким образом, в данном случае риск есть математическое ожидание потерь.

Для детального расчета рисков учитывают три фактора: угроза, уязвимость, величина потери. Математически это выражается следующим выражением:

$$P_{иб} = P_{угрозы} \times P_{уязвимости} \times V_{потери,} \qquad (2)$$

где $P_{уязвимости}$ - вероятность уязвимости.

Выражения (1) и (2) используют в случае количественных оценок риска.

На основе результатов расчета и оценки рисков информационной безопасности на данном этапе определяются меры организационного характера, подбираются технические и программно-аппаратные средства защиты информации, предназначенные для снижения рассматриваемых рисков. Соответственно как мы определили риски, связанные с человеческим фактором в данный момент, превалируют над рисками, связанными с физической защитой информации. Исходя из этой зависимости видно, что если можно снизить риск человеческого фактора, то соответственно снизится риск всей информационной

безопасности предприятия. Математически это можно выразить следующим выражением:

$$Р_{эб} = Р_{угрозы} \times Р_{уязвимости} \times V_{потери,} \quad (3)$$

$$Р_{угрозы} = Р_{чф} \times Р_{апс} \times Р_{впо} \times Р_{тс}\ , \quad (4)$$

где$Р_{чф}$ – человеческий фактор,

$Р_{апс}$ – аппаратно-программные сбои,

$Р_{впо}$ – вирусное программное обеспечение,

$Р_{тс}$ – технические сбои.

Из выражения (4) видно, что $Р_{иб} \downarrow$ если $\downarrow Р_{чф}$.

Таким образом, выходом, позволяющим снизить риски информационной безопасности, является применение современной системы, решающей любой степени сложности задачи, связанные с вопросами надежности и предсказуемости человека, определения его истинных мотивов, прогнозирование поведения и оценки отношения к тому или иному деянию, явлению или персоне, или автоматизированная система оценки лояльности персонала.

Существующие способы анализа надежности человека, прогноза его поведения уже не полностью удовлетворяют современным требованиям. Психологические тесты, полиграфные проверки весьма трудозатратны, требуют высокого профессионализма сотрудника их проводящего. Их результаты подчас находятся в прямой зависимости от опыта и субъективных качеств специалиста, а не от личных качеств тестируемого. Также можно утверждать, что перечисленные методы обеспечения экономической безопасности являются очень дорогими.

Использование данной системы существенно сократит инсайдерские угрозы в различных формах предприятий. Разработка автоматизированной системы выявления инсайдеров при обеспечении информационной безопасности является актуальной задачей, т.к. в настоящее время организации различных форм собственности, особенно коммерческие и административные, не имеют в штате квалифицированных сотрудников, способных вести работу по оценке лояльности персонала. Это вызвано, как правило, сложностью в использовании существующих методик, а также достаточно высокой оплатой труда подобных специалистов. Данная система позволит руководителю или работнику кадровой службы достаточно быстро и без значительных затрат оценивать деловые и личностные качества кандидата в сотрудники организации, а также производить периодический мониторинг лояльности персонала.

Система выявления инсайдеров должна быть полностью автоматизированной системой, которая повышала бы качество проектных работ, решала все перечисленные задачи и была лишена недостатков традиционно применяющихся методик, а также позволяющая значительно сократить затраты на мероприятия, связанные с подбором и оценкой лояльности персонала.

Материал поступил в редколлегию 23.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.056

Макеев Сергей Михайлович, *к.т.н., сотрудник*
Грушевая Екатерина Васильевна, *сотрудник*
Мысин Олег Денисович, *сотрудник*
Академия ФСО России, Орёл, Россия
e-mail: maksm57@yandex.ru

ВОЗМОЖНОСТЬ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО КОМПЛЕКСА "БРЕСТ" В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

Рассмотрена возможность применения защищенной программной платформы на основе отечественного комплексного средства виртуализации для хранения и обработки больших данных.

Одно из направлений эффективного и безопасного использования ресурсов аппаратных платформ – применение защищенных технологий виртуализации. На текущий момент наиболее актуальной является проблема защищенной аппаратной виртуализации, в частности проброс вычислительной мощности видеоадаптера в виртуальную среду. Данная задача решается с помощью платформ или сред виртуализации [1]. В сфере разработки отечественных информационных систем выступает реализация мероприятий по импортозамещению, регламентированных в Постановлении Правительства РФ от 14 января 2017 г. N 9 "Об установлении запрета на допуск товаров, происходящих из иностранных государств, работ (услуг), выполняемых (оказываемых) иностранными лицами, для целей осуществления закупок товаров, работ (услуг) для нужд обороны страны и безопасности государства" [2].

Одним из разработчиков таких систем на отечественном рынке выступает фирма "РусБИТех". Для информационных систем, где происходит обработка информации ограниченного доступа, в качестве среды виртуализации возможно использование программного комплекса средств виртуализации "Брест" (далее - ПК СВ "Брест") [3]. ПК СВ "Брест" имеет некоторые преимущества перед программным комплексом виртуализации и управления (ПК "ВИУ"), предыдущей разработкой фирмы "РусБИТех" в этой области. На рисунке 1 представлена подробная таблица сравнительных возможностей данных систем.

ПК СВ "Брест" разработан для работы на базе операционной системы Astra Linux Special Edition версии 1.5 (далее − ОС СН) в условиях мандатного и дискретного разграничения доступа. Данный программный комплекс предназначен для защищенного дополнения ОС СН средствами: обеспечения отказоустойчивости и масштабирования; защищенной виртуализации для ПЭВМ; построения защищенных облачных решений; защищенной виртуализации сетей. С помощью данного комплекса решаются функциональные задачи: эмуляция аппаратного обеспечения с использованием аппаратных возможностей архи-

тектуры x86-64 по виртуализации процессов на основе модуля KVM; создание виртуальных машин; мандатное и дискреционное управление доступом к функциям ПК; обеспечение создание тонких клиентов с использованием технологии VDI; автоматическое распределение сервером виртуализации ресурсов между работающими виртуальными машинами; возможностями регистрации событий с использованием средств централизованного протоколирования из состава ОС СН.

Возможности	ПК «ВИУ»	ПК СВ «БРЕСТ»
использование аппаратных возможностей архитектуры x86-64 по виртуализации на основе модуля KVM и средств эмуляции аппаратного обеспечения QEMU	✔	✔
создание изолированных от хоста виртуальных машин с помощью графической и консольных утилит	✔	✔
запуск изолированной виртуальной машины в виде процесса операционной системы от имени учетной записи пользователя с его мандатными атрибутами безопасности	✔	✔
предоставление пользователям удаленного доступа к виртуальным машинам в соответствии с дискреционными и мандатными правилами разграничения доступа	✔	✔
доступ к виртуальным машинам по протоколам VNC и SPICE	✔	✔
проброс звука с виртуальной машины по протоколу SPICE	✖	✔
использование нескольких мониторов при подключении к виртуальной машине по протоколу SPICE	✖	✔
организация терминального сервера на базе SPICE протокола	✖	✔
взаимодействие между виртуальными машинами, а так же между процессами пользователей и виртуальными машинами по протоколам стека IPv4 в условиях мандатного разграничения доступа	✔	✔
возможность защиты файлов-образов виртуальных машин от модификации в процессе функционирования виртуальных машин	✔	✔
создание терминальных клиентов с использованием технологии VDI	✔	✔
обеспечение масштабируемости	✔	✔
организация сетевого RAID	✔	✔
организация и управление кластером серверов с помощью веб-интерфейса	✖	✔
создание виртуального частного облако и управление им с помощью веб-интерфейса	✖	✔
организация систем хранения данных	✖	✔
построение кластерных систем высокой доступности	✖	✔
использование и организация блочных устройств на базе технологии ISCSI	✖	✔
поддержка защищенных распределенных параллельных файловых систем	✖	✔
создание многоуровневых программных сетевых коммутаторов с поддержкой VLAN (IEEE 802.1q)	✖	✔

Рис. 1. Сравнение возможностей ПК "ВИУ" и ПК СВ "Брест"

Исключительной особенностью ПК СВ "Брест" является использование облачной платформы OpenNebula [4]. Обеспечение виртуализации, реализуемой в центре обработке и хранения данных (далее − ЦОХД), заключается в организации облачных вычислений корпоративного уровня. Платформа OpenNebula является простым, но гибким решением с богатым набором средств, обеспечивающим построение и управление облаками корпоративного уровня и виртуализованными ЦОХД, которое совмещает в себе существующие технологии виртуализации с расширенными функциональными возможностями для обеспечения работы в режиме и способности быстрой адаптации. OpenNebula обеспечивает работу по восходящему принципу, определяемому на основании фактических потребностей системных администраторов, специалистов по интеграции разработки и эксплуатации и пользователей.

OpenNebula состоит из нескольких компонентов:

– Front-end − сервис OpenNebula (требует Ruby);

– Hosts − узлы содержащие гипервизоры (требует ssh и настроенный гипервизор);

– База данных − используется для хранения параметров OpenNebula (поддерживается MySQL или SQLite).

Каждый компонент OpenNebula содержит определенные требования, все они достаточно хорошо расписаны в документации к ПК СВ "Брест".

Для удобного управления виртуальными ресурсами и учетными записями используются несколько уровней абстракции. Так, разные физические серверы объединяются в кластеры, позволяющие распределять и балансировать нагрузку. Несколько установок OpenNebula объединяют в зоны (oZones). Доступ к зонам организован через абстрактный дата-центр, который содержит собственный набор ресурсов (VM, виртуальные сети, образы и шаблоны VM) и учетные записи. Как кластеры, так и зоны могут охватывать один или несколько дата-центров. Кроме того, используется концепция групп, каждая из которых может иметь индивидуальные установки и набор доступных ресурсов, не пересекающихся с остальными. На рис. 2 представлена начальная страница управления сервиса OpenNebula.

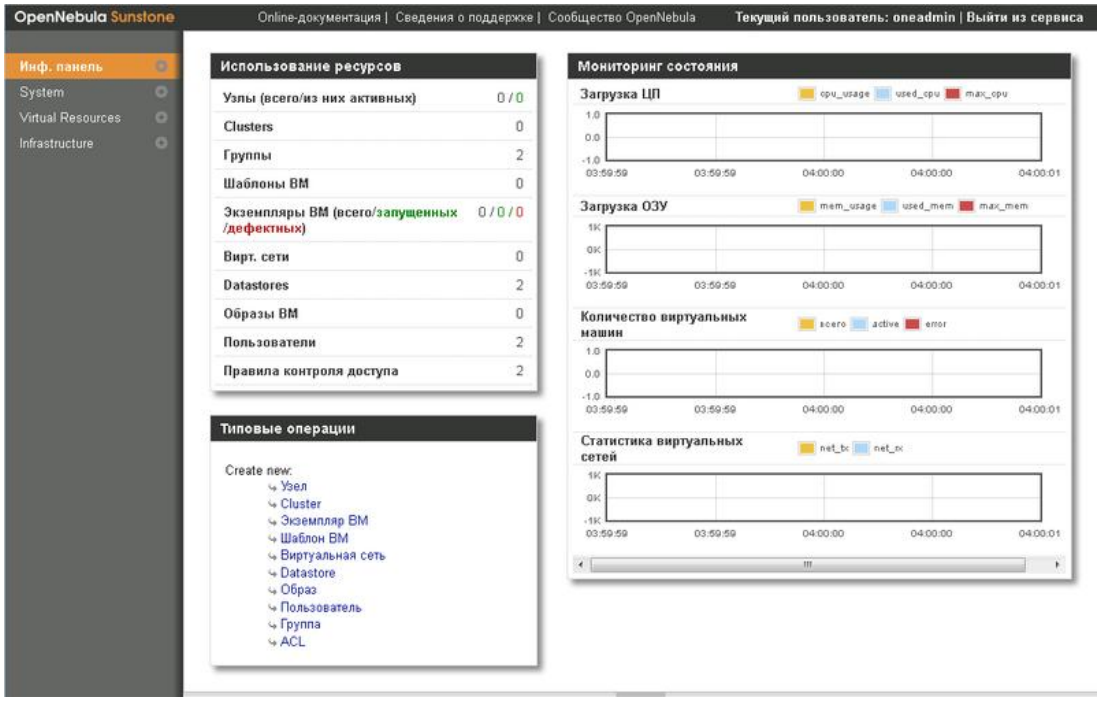

Рис. 2. Начальный экран управления виртуальными машинами в OpenNebula

В итоге мы получаем безопасную отечественную облачную платформу для решения различного рода задач [5]. На данный момент компания "РусБИТех" планирует сертификацию ПК СВ «Брест» в Минобороны России и ФСТЭК России.

Таким образом, использование платформы ПК СВ «Брест» с установленным OpenNebula дает безопасную платформу для хранения и обработки больших данных.

Список литературы

1. Оптимизация вычислительных ресурсов на базе ПК СВ «БРЕСТ». [Электронный ресурс]. -URL: http://irsural.ru/poleznaya-informaciya/optimizaciya-vychislitelnyh-resursov-na-baze-pk-sv-brest.html

2. Постановление Правительства РФ от 14 января 2017 г. № 9 "Об установлении запрета на допуск товаров, происходящих из иностранных государств, работ (услуг), выполняемых (оказываемых) иностранными лицами, для целей осуществления закупок товаров, работ (услуг) для нужд обороны страны и безопасности государства".

3. Программные комплексы виртуализации. [Электронный ресурс]. - URL: http://astra-linux.com/products/virt.html.

4. OpenNebula project website. URL: http://opennebula.org.

5. Терехов, И. Не рано ли Cloud Computing в массы? / И. Терехов. – М.: Компьютерра, 2009.

Материал поступил в редколлегию 20.04.18..

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.056

Маркин Дмитрий Олегович, *сотрудник*
Биркун Николай Иванович, *к. п. н., сотрудник*
Анисимова Елена Юрьевна, *сотрудник*
Академия ФСО России, Орёл, Россия
e-mail: admin@nikitka.net

ОПРЕДЕЛЕНИЕ МЕСТОПОЛОЖЕНИЯ МОБИЛЬНОГО УСТРОЙСТВА ПОСРЕДСТВОМ СИГНАЛОВ СЕТЕЙ БЕСПРОВОДНОГО ДОСТУПА СТАНДАРТА LTE

Представлено исследование для определения оптимальных параметров, которые позволять достичь наилучшей точности определения местоположения мобильного устройства в помещениях и в условиях городской застройки. Для этого исследуются алгоритмы определения местоположения с помощью метода k-ближайших соседей и на основе скрытой марковской модели.

В настоящее время многие приложения требуют точного определения местоположения как в помещении, так и в условиях городских застроек. В таких ситуациях позиционирование с помощью глобальных навигационных спутниковых систем демонстрирует слабую производительность из-за низкой мощности принимаемого сигнала, а также многолучевого распространения [1].

В противоположность этому сотовые сети радиосвязи, такие как LTE, обеспечивают превосходное покрытие в городских застройках, и это делает их интересными для позиционирования. Стандарт LTE вводит такие технологии позиционирования, как вспомогательная глобальная навигационная спутниковая система (Assisted GNSS – A-GNSS); методы, базирующиеся на Cell-ID; наблюдаемая разница по времени прибытия (Observed Time Difference of Arrival – OTDOA). Стандарт также предусматривает дополнительные ресурсы связи для определения местоположения в сети LTE, так называемые опорные сигналы позиционирования (Positioning Reference Signals – PRSs). PRSs разделены во времени или частоте для соседних базовых станций. Для PRSs стандарт LTE определяет полосу пропускания нисходящей линии связи от 1,4 МГц до 20 МГц.

В данной работе исследуется возможность использования LTE сигнала с ограниченной полосой до 20 МГц. Цель состоит в том, чтобы определить оптимальные параметры, которые позволят достичь максимальной точности определения местоположения мобильного устройства в помещениях и в условиях городской застройки. Для этого необходимо исследовать известные алгоритмы определения местоположения.

Метод и алгоритм. В качестве исходных данных используются идентификатор точки доступа и уровень принимаемого сигнала (received signal strength indicator – RSSI) стандарта LTE, а также GPS/ГЛОНАСС координаты мобильного пользователя. Для сбора данных реализовано программное

обеспечение для мобильного устройства с операционной системой Android [2]. На рис. 1, 2 представлены результаты измерений, проведенных с помощью этого программного обеспечения в помещении и в условиях городской застройки.

rowid	signal_typ	signal_str	log_time	cell_mcc	cell_mnc	cell_lac	cell_cid	lat	lon
1418	4G	-122	1489934811	250	99	57157	147059205	52,99281	36,04185
1419	4G	-122	1489934811	250	99	57157	147059205	52,99281	36,04185
1420	4G	-122	1489934811	250	99	57157	147059205	52,99281	36,04185
1421	4G	-122	1489934811	250	99	57157	147059205	52,99281	36,04185
1426	4G	-122	1489934812	250	99	57157	147059205	52,99281	36,04185
1427	4G	-122	1489934812	250	99	57157	147059205	52,99281	36,04185
1550	4G	-121	1489934859	250	99	57157	147059205	52,99351	36,03981
1551	4G	-121	1489934859	250	99	57157	147059205	52,99351	36,03981
1552	4G	-121	1489934859	250	99	57157	147059205	52,99351	36,03981
1553	4G	-121	1489934860	250	99	57157	147059205	52,99351	36,03981
1720	4G	-122	1489934945	250	99	57157	147059205	52,99319	36,04144
1721	4G	-122	1489934945	250	99	57157	147059205	52,99319	36,04144
1722	4G	-119	1489934949	250	99	57157	147059205	52,99319	36,04144
1723	4G	-119	1489934949	250	99	57157	147059205	52,99319	36,04144
1724	4G	-119	1489934949	250	99	57157	147059205	52,99319	36,04144
1798	4G	-121	1489935020	250	99	57157	147059205	52,99319	36,04144
1799	4G	-121	1489935021	250	99	57157	147059205	52,99319	36,04144
1800	4G	-121	1489935021	250	99	57157	147059205	52,99319	36,04144
1801	4G	-121	1489935021	250	99	57157	147059205	52,99319	36,04144
1802	4G	-120	1489935025	250	99	57157	147059205	52,99319	36,04144
1803	4G	-120	1489935025	250	99	57157	147059205	52,99319	36,04144
1804	4G	-120	1489935025	250	99	57157	147059205	52,99319	36,04144

Рис. 1. Фрагмент результатов измерений, проведенных в помещении с помощью программного обеспечения для мобильного устройства с ОС Android

2596	4G	-120	1490542264	250	99	57357	146803716	52,97098	36,05865
2597	4G	-120	1490542264	250	99	57357	146803716	52,97098	36,05865
2598	4G	-120	1490542264	250	99	57357	146803716	52,97098	36,05865
2599	4G	-120	1490542265	250	99	57357	146803716	52,97098	36,05865
2600	4G	-120	1490542265	250	99	57357	146803716	52,97098	36,05865
2601	4G	-120	1490542265	250	99	57357	146803716	52,97098	36,05865
2602	4G	-120	1490542265	250	99	57357	146803716	52,97098	36,05865
2603	4G	-120	1490542265	250	99	57357	146803716	52,97098	36,05865
2604	4G	-117	1490542268	250	99	57357	146803716	52,97098	36,05865
2605	4G	-117	1490542268	250	99	57357	146803716	52,97098	36,05865
2606	4G	-117	1490542269	250	99	57357	146803716	52,97098	36,05865
2607	4G	-117	1490542269	250	99	57357	146803716	52,97098	36,05865
2608	4G	-117	1490542269	250	99	57357	146803716	52,97098	36,05865
2609	4G	-121	1490542272	250	99	57357	146803716	52,97098	36,05865
2610	4G	-121	1490542272	250	99	57357	146803716	52,97098	36,05865
2611	4G	-121	1490542272	250	99	57357	146803716	52,97098	36,05865
2612	4G	-121	1490542272	250	99	57357	146803716	52,97098	36,05865
2613	4G	-121	1490542272	250	99	57357	146803716	52,97098	36,05865
2614	4G	-121	1490542274	250	99	57357	146803716	52,97098	36,05865
2615	4G	-121	1490542274	250	99	57357	146803716	52,97098	36,05865
2616	4G	-121	1490542274	250	99	57357	146803716	52,97098	36,05865
2617	4G	-120	1490542277	250	99	57357	146803716	52,97098	36,05865
2618	4G	-120	1490542277	250	99	57357	146803716	52,97098	36,05865

Рис. 2. Фрагмент результатов измерений, проведенных в условиях городской застройки с помощью программного обеспечения для мобильного устройства с ОС Android

После сбора измерений необходимо обработать экспериментальные данные с применением интеллектуальных методов. В данном случае анализируются статистические свойства выборки по уровням принимаемого сигнала (рис. 3).

В результате анализа статистических свойств получены закон распределения уровня принимаемого сигнала и его параметры, а зная эти данные, становится возможным проведение анализа методов определения местоположения [3,4].

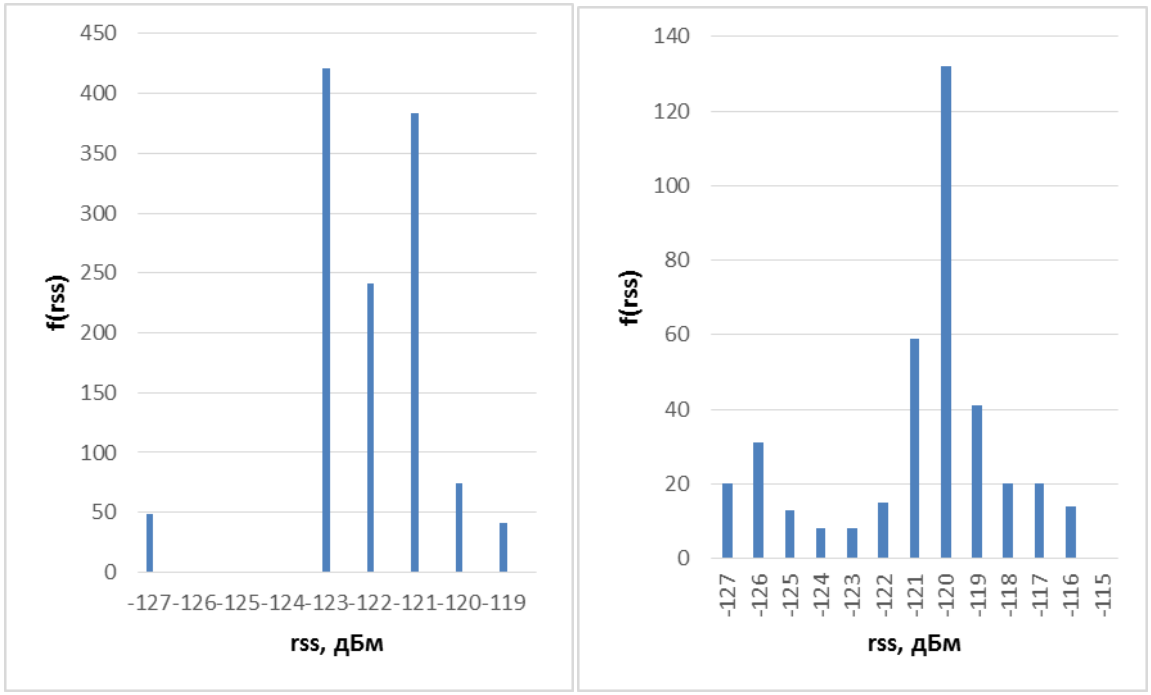

Рис. 3. Статистика уровней принимаемых сигналов в помещении и в условиях городской застройки

В данном случае анализируются такие методы, как метод k-ближайших соседей, скрытая марковская модель. Построив имитационную модель, можно оценить погрешность определения местоположения [3].

Метод k-ближайших соседей [4,5] является одним из методов интеллектуального анализа, с помощью которого можно определить местоположение. Для использования этого метода необходим предварительный сбор измерений уровней принимаемого сигнала в разных точках здания с известными координатами, а также, возможно, известной ориентацией передающего устройства, поэтому выборка исходных данных будет иметь следующий вид:

$$X^{N_{kNN}} = \left\langle \left\{ (x_i, y_i), \upsilon_i \right\}, P_{r_i}^{RSS} \right\rangle, \qquad (1)$$

где (x_i, y_i) – координаты i-й точки карты сигнального пространства; υ_i – угол ориентации в пространстве мобильного устройства; $P_{r_i}^{RSS}$ – уровень мощно-

сти принимаемого сигнала от мобильного устройства; $i=\overline{1,N_{kNN}}$ – индекс точки измерений уровней сигнала, а N_{kNN} – их количество.

В качестве метрики для вычисления расстояния между текущими измерениями уровня сигнала и значениями, хранящимися в набранных в качестве исходных данных измерениях целесообразно использовать метрику Евклида:

$$d_{Evkl}\left(P_r^{RSS},P_{r_i}^{RSS}\right)=\sqrt{\sum_{j=1}^{N_{AP}}\left(P_{r_j}^{RSS}-P_{r_{i,j}}^{RSS}\right)^2}, \quad (2)$$

где $P_r^{RSS}=\left\{P_{r_j}^{RSS}\right\}, j=\overline{1,N_{AP}}$ – текущие измерения уровня сигнала N_{AP} точками доступа; $P_{r_i}^{RSS}=\left\{P_{r_{i,j}}^{RSS}\right\}, j=\overline{1,N_{AP}}, i=\overline{1,N_{kNN}}$ – измерения уровня сигнала в i-й точке N_{AP} точками доступа; N_{kNN} – количество точек сигнального пространства.

Таким образом, каждый набор измерений P_r^{RSS} порождает свою нумерацию выборки. Тогда в общем виде метод k-ближайших соседей можно представить в виде

$$\begin{aligned}&a_{kNN}(u=P_r^{RSS})=\\&=\arg\min_{x_i,y_i}\sum_{i=1}^{N_{kNN}}\left[d_{Evkl_i}\left(P_r^{RSS},P_{r_i}^{RSS}\right)\right]\cdot\omega(i,u)\end{aligned}, \quad (3)$$

где $\omega(i,u)=\left[i\le k\right]$ – весовая функция, оценивающая степень важности i-го соседа. Тогда координаты $\left(x_{kNN},y_{kNN}\right)$ местоположения мобильного устройства будут определяться выражением

$$x_{kNN}=\frac{1}{k}\cdot\sum_{i=1}^{k}x_i,\ y_{kNN}=\frac{1}{k}\cdot\sum_{i=1}^{k}y_i. \quad (4)$$

Для определения местоположения с помощью скрытой марковской модели, как и для метода k-ближайших соседей, необходимы исходные измерения уровней сигнала. Однако отличие заключается в том, что в каждой точке с известными координатами хранятся не данные об измерениях уровня сигнала, а статистика измерений уровней сигналов. Необходимо провести исследование статистики измерений уровня сигнала. Для сети LTE исследования показывают, что уровень сигнала является случайной величиной, зависящей от множества факторов, поэтому необходимо определить закон распределения уровня сигнала и его параметры, это позволит более точно определить местоположение мобильного устройства.

Выборка для данного метода имеет вид:

$$X^{N_{HMM}}=\left\langle\left(x_i,y_i\right),P_{r_i}\left[\lambda_i/\left(x_i,y_i\right)\right]\right\rangle, i=\overline{1,N_{HMM}} \quad (5)$$

где $\left(x_i,y_i\right)$ – координаты i-й точки исходных измерений; $P_{r_i}\left[\lambda_i/\left(x_i,y_i\right)\right]$ – условная вероятность получения измерений сигнала мобильным устройством со статистическим распределением λ_i в точке с координатами (x_i,y_i); N_{HMM} – количество точек выборки.

Процесс определения местоположения представляется в следующем виде:

$$\lambda=\left\{A,B,\pi\right\}, \quad (6)$$

где $A=\{a_{ij}\}$ – матрица переходных вероятностей для "скрытых" состояний $s_i, i=\overline{1,N}_{HMM}$, где a_{ij} – вероятность перехода из i-го в j-е состояние, $i,j=\overline{1,N}_{HMM}$; $S=\{s_i\}$ – множество состояний скрытой Марковской модели; $s_i=(x_i,y_i)$ – i-е состояние скрытой Марковской модели; (x_i,y_i) – координаты точки в здании; N_{HMM} – количество точек выборки с известными координатами; $B=\{P_r(o_j/s_i)=P_r[\lambda_j/(x_i,y_i)]\}$ – матрица функций условных распределений вероятностей наблюдения символов o_j при условии нахождения в состоянии s_i, где $i=\overline{1,N}_{HMM}$, $j=\overline{1,m}$, m – количество допустимых наблюдений; $o_j=\{(b_1,P_{r_1}^{RSS}),(b_2,P_{r_2}^{RSS}),...,(b_k,P_{r_k}^{RSS})\}$ – j-е допустимое наблюдение; b_k – номер k-й точки доступа, осуществляющей измерение уровня сигнала; $P_{r_k}^{RSS}$ –уровень сигнала k-й точкой доступа беспроводной сети; $\pi=\{\pi_i\}$, $i=\overline{1,N}_{HMM}$ – начальное распределение вероятностей состояний скрытой Марковской модели.

Для определения местоположения мобильного устройства – наиболее вероятного состояния скрытой Марковской модели используют выражение

$$\pi_i'=\frac{\pi_i P_r(o_j/s_i)}{\sum_{k=1}^{N_{HMM}}\pi_k\cdot P_r(o_j/s_k)}. \qquad (7)$$

Тогда координаты наиболее вероятного местоположения мобильного устройства можно получить, используя выражение

$$(x_i,y_i)=\arg\max(\pi_i'). \qquad (8)$$

Проведенные исследования показали, что точность определения местоположения можно повысить, используя для определения местоположения мобильных устройств k значений наиболее вероятных состояний, фактически используя для вычисления координат первые k значений вектора вероятностей состояний скрытой Марковской модели. Тогда координаты $(\%_{HMM},\%_{HMM})$ местоположения мобильных устройств будут определяться выражением

$$\begin{aligned}\%_{HMM}&=\frac{1}{k}\sum_{i=1}^{k}\arg\max_{x_i}(\pi_i'),\\ \%_{HMM}&=\frac{1}{k}\sum_{i=1}^{k}\arg\max_{y_i}(\pi_i')\end{aligned}, \qquad (9)$$

Таким образом, в данной работе обосновано использование оптимальных параметров для алгоритмов определения местоположения, с помощью имитационного моделирования исследована эффективность алгоритмов. Наиболее точным методом определения местоположения является метод на основе скрытой марковской модели. ошибка позиционирования для этого метода, как правило, меньше одного метра, а в худшем случае она не превышает трех метров [1, 4]].

Список литературы

1. ITU-R P.1238-7 Propagation data and prediction methods for the planning of indoor radio communication systems and the radio local area networks in the frequency range 900 MHz to 100 GHz. Geneva: ITU-R Recommendations, 2001.

2. Автоматизированная система определения местоположения пользователей мобильных устройств внутри здания на основе сигналов беспроводной сети: свидетельство о государственной регистрации программы для ЭВМ № 2015615631 Российская Федерация / Д. О. Маркин, Н. И. Биркун, А. О. Зозуля ; заявл. 24.03.2015; зарегистрировано в Реестре программ для ЭВМ 21.05.2015 г.

3. Маркин, Д. О. Имитационное моделирование определения местоположения пользователей мобильных устройств внутри помещений / Д. О. Маркин, В. В. Комашинский // Информационная безопасность и защита персональных данных. Проблемы и пути их решения [Текст]+[Электронный ресурс]: материалы VII Межрегиональной научно-практическая конференция / под ред. О. М. Голембиовской. – Брянск: БГТУ, 2015. – С. 109–115.

4. Маркин, Д. О. Исследование эффективности алгоритмов определения местоположения мобильных устройств внутри помещений / Д. О. Маркин // Вестник РГРТУ. – 2015. – № 54-1. – С. 32–39.

5. Маркин Д. О., Макеев С. М. Модель системы определения местоположения мобильного устройства на основе метода статистических испытаний. // Известия Тульского государственного университета. Технические науки. – 2016. – № 2. – С. 150–165.

Материал поступил в редколлегию 09.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.056

Маркин Дмитрий Олегович, *сотрудник*
Макеев Сергей Михайлович, *к.т.н., сотрудник*
Голенков Родион Олегович, *сотрудник*
Академия ФСО России, Орёл, Россия
e-mail: admin@nikitka.net

СИСТЕМА ИДЕНТИФИКАЦИИ ИСТОЧНИКОВ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЕБ-РЕСУРСОВ НА ОСНОВЕ ОТКРЫТЫХ ДАННЫХ СЕТИ ИНТЕРНЕТ

Рассмотрена концепция построения системы идентификации источников угроз информационной безопасности веб-ресурсов на основе открытых данных сети интернет, типовой алгоритм извлечения данных из открытых источников, логическая схема базы данных для хранения идентифицирующей информации.

Успешное функционирование органов государственной власти (ОГВ) и государственных организаций в значительной степени зависит от эффективности и качества государственных информационных систем (ГИС). Стабильная и надежная работа ГИС невозможна без эффективной системы информационной безопасности (ИБ), нарушение работоспособности которой может оказывать прямое или косвенное негативное воздействие на деятельность ОГВ и спровоцировать различные инциденты ИБ. Недостаточная способность системы управления инцидентами и событиями (СУИС) к обработке таких инцидентов делает практическую реакцию на них малоэффективной, что потенциально увеличивает степень негативного воздействия на ГИС.

Успешное функционирование ГИС проявляется в правильном и эффективном реагировании на потенциально опасные с точки зрения ИБ события [5], что позволяет минимизировать ущерб и не допустить повторение инцидентов.

Одним из компонентов существующих систем защиты информации (СЗИ) по отношению к СУИС являются средства идентификации источников угроз ИБ [8]. В рамках данной работы предлагается для решения данной задачи использовать автоматизированные средства, позволяющие получать идентификационные данные об источниках угроз ИБ из общедоступных открытых источников сети Интернет, предоставляющих, в том числе, услуги определения местоположения. Концептуальная схема такого взаимодействия представлена на рис. 1.

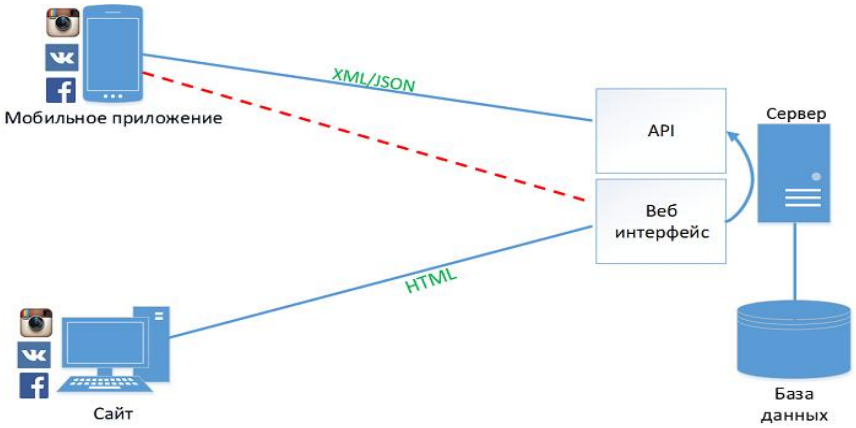

Рис. 1. Общая схема взаимодействия веб-сервисов с API

В основе ее функционирования лежит возможность взаимодействия с доступными API-функциями открытых систем.

Согласно данным всероссийского центра изучения общественного мнения (ВЦОМ), наиболее популярной за последние годы является социальная сеть "Вконтакте", которая, кроме того, обладает удобным API и предоставляет и исчерпывающую идентификационную информацию. Следовательно, ее целесообразно использовать в качестве поставщика информации для повышения эффективности функционирования СУИС.

Потенциальную ценность для идентификации источников угроз ИБ представляют следующие данные (полученные из "Вконтакте", используя открытые API-функции):

- имя и фамилия пользователя;
- геоинформацию, указанную пользователем на своей странице при регистрации, указанную на страницах друзей пользователя, указанную в группах, где он состоит;
- геолокационные метки, прикрепленные к записям на странице пользователя.

Сбор и анализ указанной совокупности данных, извлеченных из открытой базы данных социального сервиса, позволяет повысить полноту идентификационных данных и эффективность геопозиционирования потенциальных источников угроз ИБ для ГИС.

На рис. 2 представлена обобщенная структурная схема предлагаемой системы идентификации источников угроз ИБ ГИС.

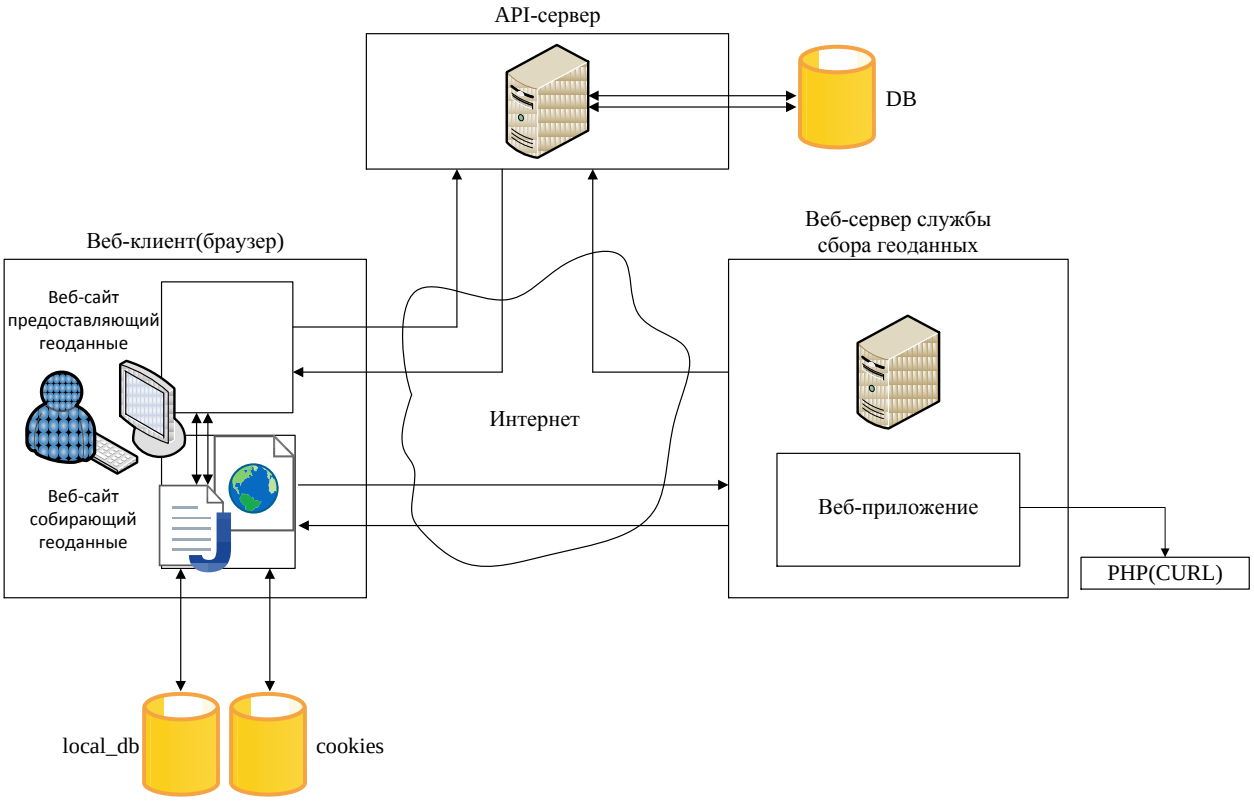

Рис. 2. Обобщенная структурная схема системы идентификации источников угроз ИБ ГИС

Организационно система идентификации источников угроз ИБ состоит из нескольких программных модулей:

1) модуль расширения для веб-клиентов (браузеров) пользователей ГИС;

2) веб-приложение, в состав которого входят:

- модуль веб-приложения СУИС, обеспечивающий взаимодействие с API-серверами служб, представляющих доступ к открытым данным;
- модуль веб-приложения СУИС, обеспечивающий взаимодействие с локальной БД, хранящей идентификационные данные об источниках угроз;
- модуль веб-приложения СУИС, обеспечивающий функционирование аналитической подсистемы.

Исходная идентификационная информация поставляется в СУИС благодаря модулю расширения веб-клиентов пользователей ГИС. Данное JavaScript-расширение получает доступ к ID-пользователя, хранящиеся в cookies-файлах веб-клиента, в случае если при обращении к ГИС одновременно он является авторизованным и в заданной социальной сети.

Используя ID-пользователя, модуль веб-приложения СУИС, обеспечивающий взаимодействие с API-серверами служб, извлекает идентификационные данные об источнике угрозы. Сбор таких сведений дает нам возможность получить о пользователе дополнительную информацию, которая может быть полезной и помочь при расследовании инцидентов, связанных с нарушением ИБ ГИС. Все данные, извлекаемые с помощью данного модуля, помещаются в базу

данных СУИС. Структурно-логическая схема прототипа такой базы данных представлена на рис. 3.

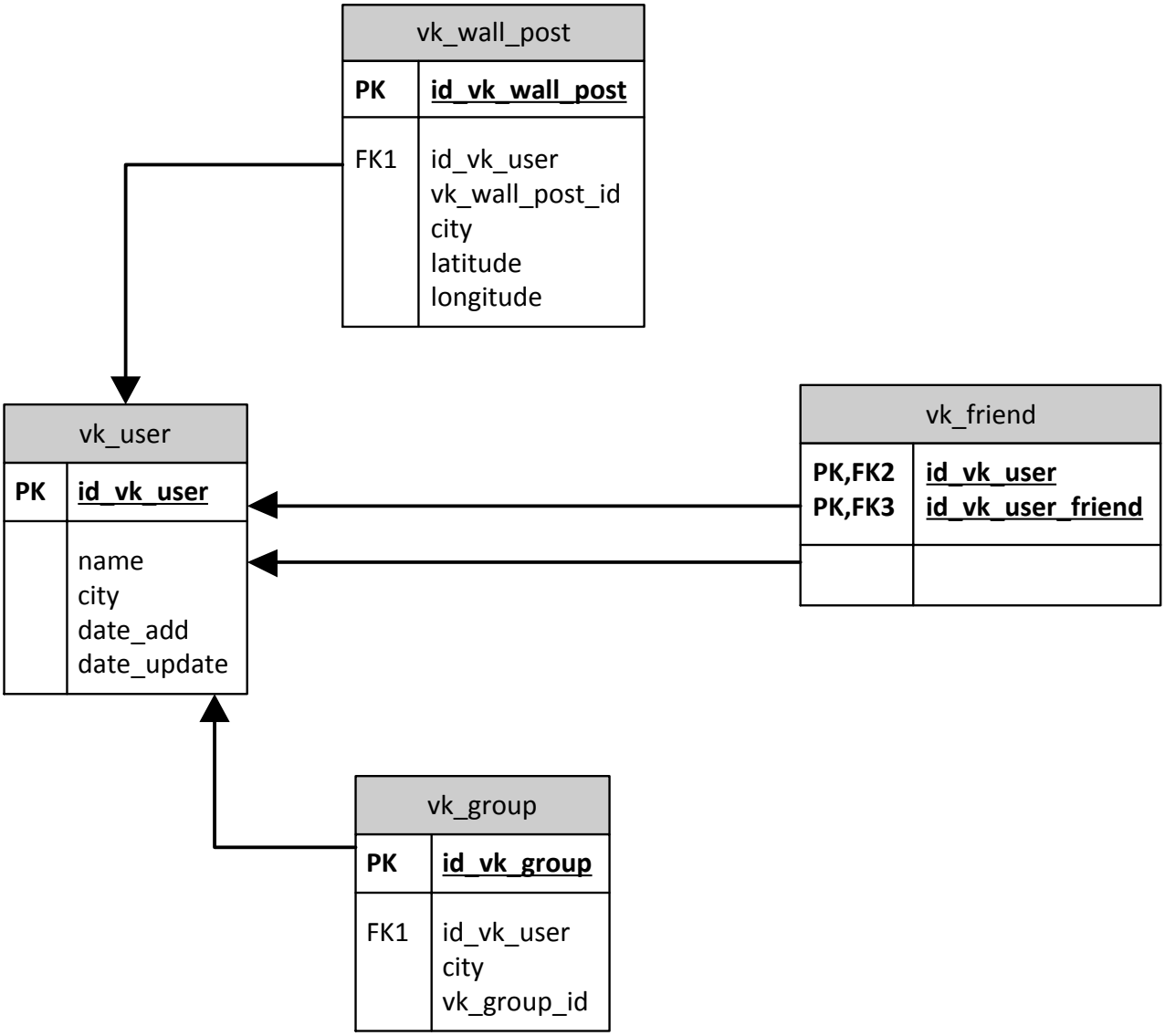

Рис. 3. Структурно-логическая схема базы идентификационных данных источников угроз ИБ ГИС

На рис. 4 представлен алгоритм функционирования веб-приложения системы идентификации источников угроз ИБ ГИС, на котором наглядно представлен порядок выполнения процедуры взаимодействия приложения с сервером API веб-ресурса "Вконтакте".

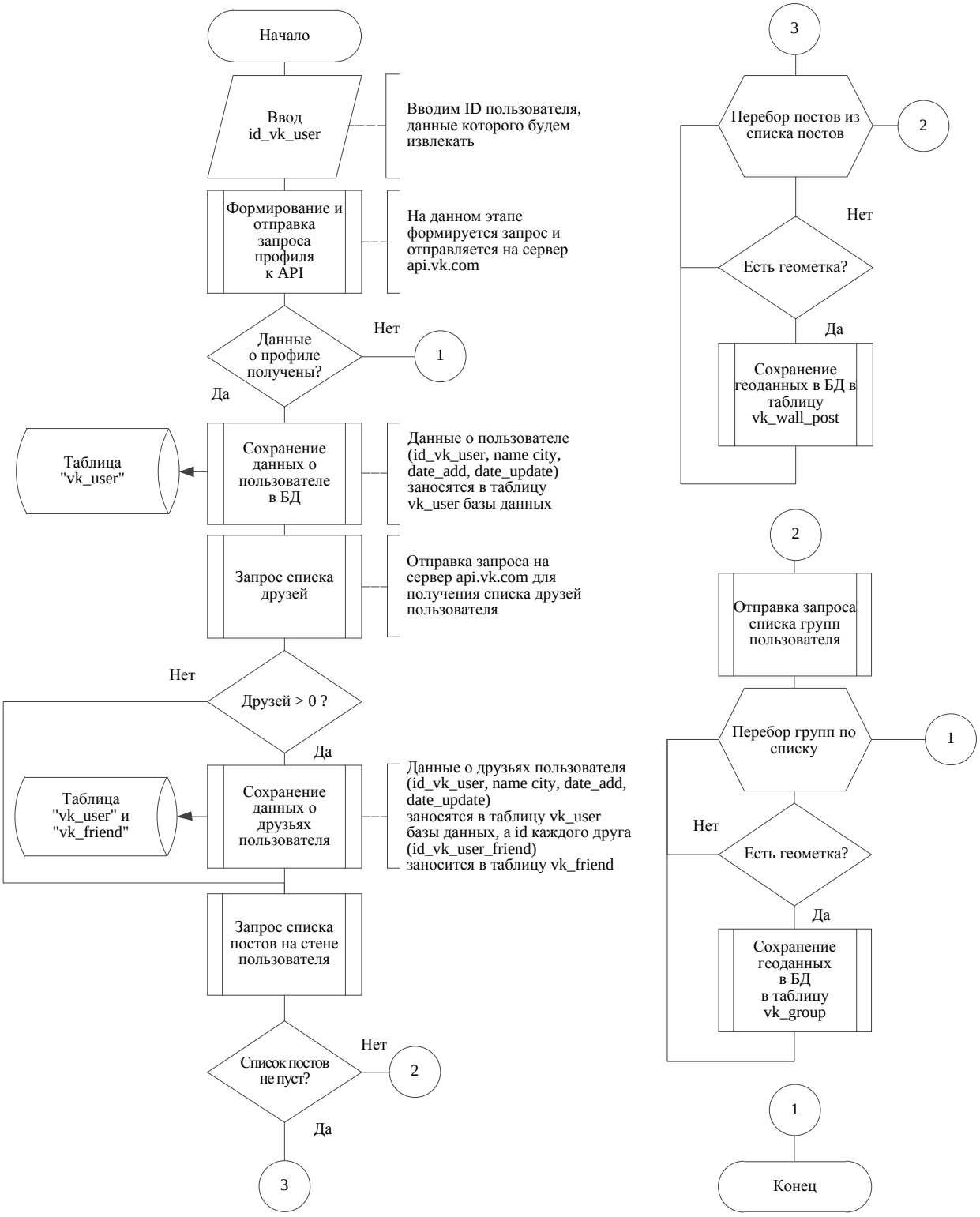

Рис. 4. Блок-схема алгоритма функционирования веб-приложение системы идентификации источников угроз ИБ ГИС

Извлеченная информация сохраняется в базу данных, представленную выше. С помощью аналитической подсистемы можно проанализировать собранную статистику и просмотреть аналитический отчет о потенциально возможном местоположении источников угроз ИБ ГИС.

Сбор статистических данных о местоположении пользователя по геолокационным меткам, размещенным на его странице, а также анализ динамики их изменения позволит с определённой вероятностью установить его фактическое местоположение с точностью до города, при наличии более подробной информации – до улицы.

Список литературы

6. Рыженкова, А. Управление инцидентами информационной безопасности: о чем говорят стандарты / А. Рыженкова // Connect. Мир информационных технологий. – 2014. – № 7–8. – С. 62–65.

7. Анализ угроз веб-приложений [Электронный ресурс] / InfoSecurity // www.infosecurity.ru. – Электрон. дан. – 2005–2011. – Режим доступа: http://www.infosecurity.ru/page_info_web. – Дата обращения: 22.05.2017.

8. Котенко, И. В. SIEM-системы для управления информацией и событиями безопасности / И. В. Котенко, И. Б. Саенко // Защита информации. Инсайд. – 2012. – № 5. – С. 54–65 : ил.

Материал поступил в редколлегию 09.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.056.5

***Маркин Дмитрий Олегович,**, сотрудник*
***Санников Иван Алексеевич,** сотрудник*
***Хомякова Анна Андреевна,** сотрудник*
Академия ФСО России, Орёл, Россия
e-mail: admin@nikitka.net

ИССЛЕДОВАНИЕ ЗАЩИЩЕННОСТИ СИСТЕМНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СЕТЕВОГО ОБОРУДОВАНИЯ СЕМЕЙСТВА CISCO

Описана методика исследования защищенности системного программного обеспечения сетевого оборудования семейства Cisco Systems. Описан порядок дизассемблирования системного программного обеспечения с учетом архитектуры процессоров, методика поиска критических с точки зрения реализации процедур аутентификации и авторизации маршрутов потоков управления.

В настоящее время значительная часть сетевого оборудования, обеспечивающего инфокоммуникационное взаимодействие как в отрытых информационно-телекоммуникационных сетях, так и в защищенных корпоративных, построена на базе программно-аппаратных комплексов иностранного производства, в частности на телекоммуникационном оборудовании компании Cisco Systems [1]. В связи с этим при возникновении острых конфликтов возможны внешние воздействия на данное оборудования с целью эксплуатирования скрытых возможностей данного оборудования и нанесения ущерба экономике страны. Основной для функционирования любого телекоммуникационного оборудования является его программно-аппаратная составляющая и, в частности, системное программное обеспечение (СПО). Таким образом, одной из актуальных задач по обеспечению информационной безопасности в инфокоммуникационных сетях является исследование защищенности СПО телекоммуникационного оборудования [2] иностранного производства на предмет наличия уязвимостей (недекларированных возможностей – НДВ и/или программных закладок), способных нанести ущерб информационной безопасности в виде нарушения конфиденциальности, целостности или доступности защищаемой информации.

Обеспечение защищенного доступа к коммуникационному оборудованию в значительной степени зависит от СПО, установленного на нем. Удаленное подключение к телекоммуникационному оборудованию компании Cisco Systems. как правило, осуществляется с использованием протоколов Telnet и SSH. При этом принципиальное значение при получении авторизованного удаленного доступа к оборудованию имеют процедуры аутентификации и авторизации, за которые отвечает соответствующие подсистемы и модули СПО.

Для исследования особенностей функционирования СПО сетевого оборудования компании Cisco Systems могут применяться такие классы инструментальных средств анализа программного обеспечения (ПО), как диззассемблеры, отладчики и эмуляторы.

Особенностью СПО сетевого оборудования компании Cisco Systems является архитектура микропроцессоров – PowerPC, на основе которых оно разработано, что накладывает специфические ограничения на применения указанных средств анализа ПО.

В качестве инструментов исследования использовались программы:

– IDA Pro 6.8 + Hex-Rays Decompiler [3];

– HT Text Editor;

– Dynamips + GDB Stub.

Начальная настройка телекоммуникационно**го** оборудовани**я** Cisco Systems осуществляется через консольный кабель и заключается в установке основных настроек аппаратуры. После подключения к действующей сети к данному оборудованию можно получить удаленный доступ по протоколам Telnet или SSH. Очевидно, что при наличии уязвимостей в СПО некоторые разрушающие программные воздействия способны привести к преодолению подсистем аутентификации и авторизации и получению доступа к передаваемой информации, изменению сетевых настроек оборудования.

Объектом исследования защищенности СПО являются его двоичные скомпилированные образы. В данной работе проводился анализ защищенности образа c2600-bino3s3-mz.123-22.bin. Этапы анализа представлены на рис. 1.

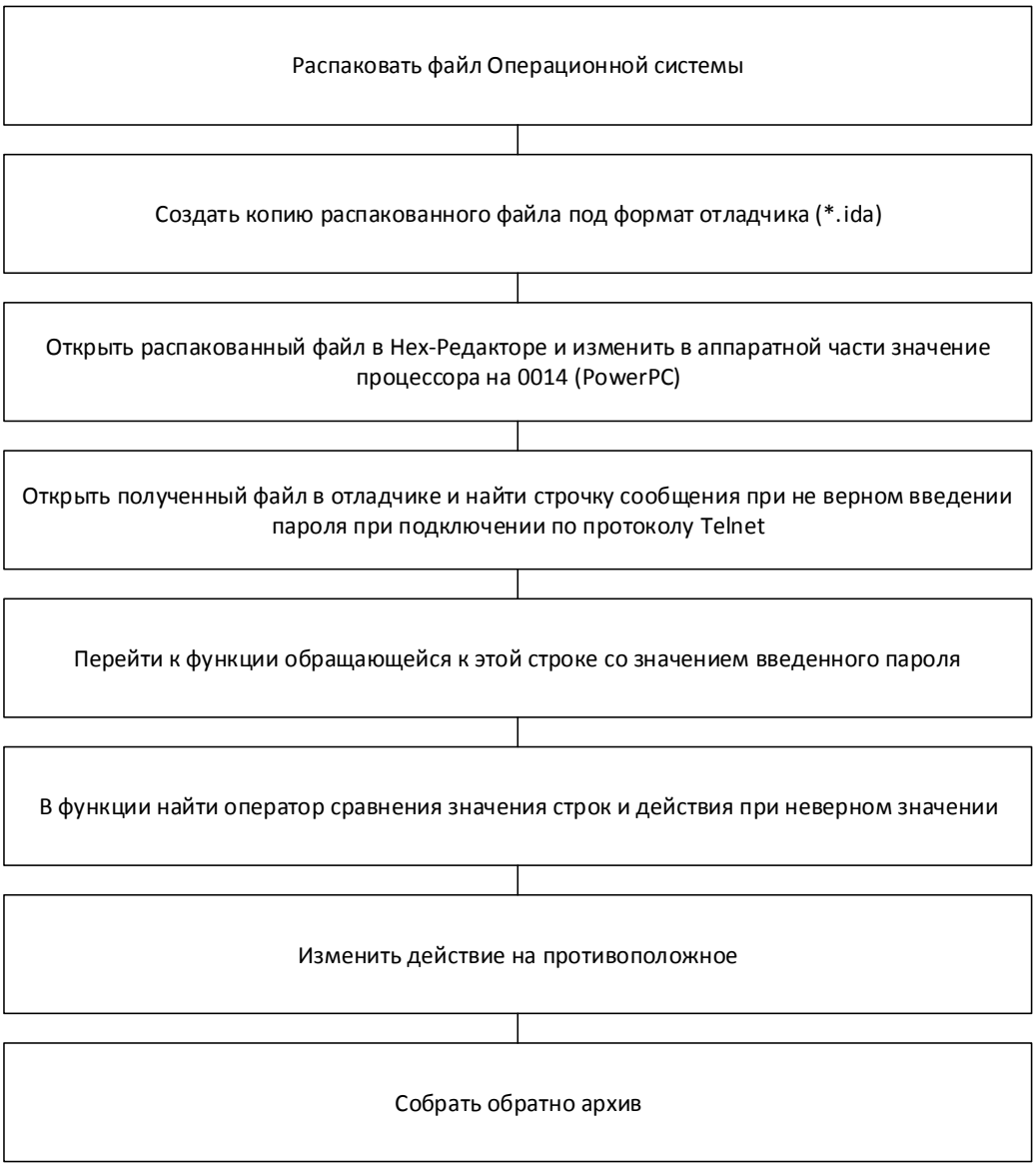

Рис. 1. Этапы анализ защищенности СПО телекоммуникационного оборудования Cisco Systems

Образ может быть распакован с помощью любой UNIX-системы. В работе для распаковки была использована операционная система (ОС) Debian 9.2.0.

Далее полученный образ необходимо подготовить для дизассемблирования. В качестве диззассемблера использовалось ПО IDA Pro 6.8. с форматом образа "*.ida". Для этого с помощью HEX-редактора в файле образа необходимо установить значение, идентифицирующее тип процессора, на 0x0014 (процессор с архитектурой PowerPC). Иллюстрация данного этапа представлена на рисунке 2.

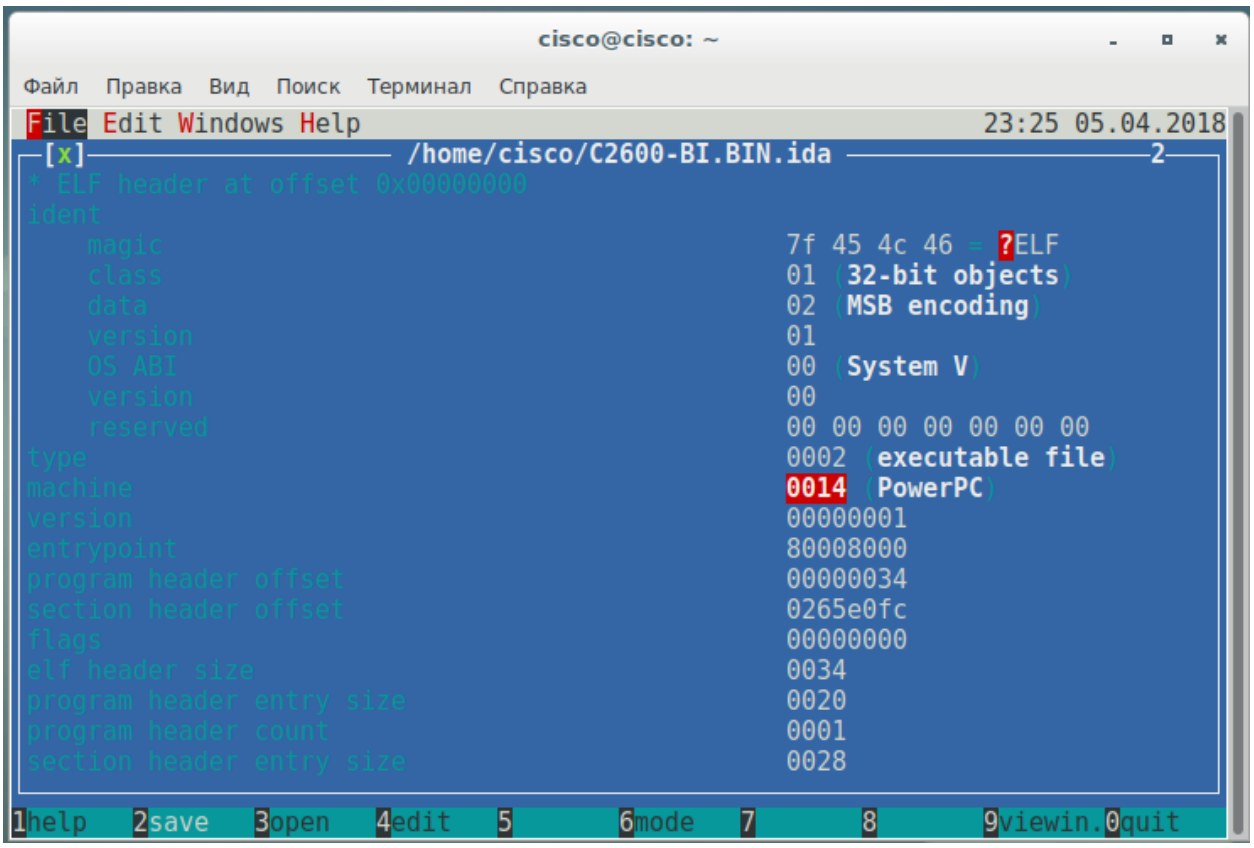

Рис. 2. Редактирование значения процессора

После этого отредактированный файл образа дизассемблируется с помощью ПО IDA Pro 6.8, в результате чего появляется возможность провести статический анализ полученного текста исходного кода СПО.

В исходном коде СПО с использованием функции поиска строк необходимо найти сообщение с текстом, выдаваемым программой при введении некорректного пароля при подключении по протоколу Telnet. Иллюстрация данного этапа представлена на рисунке 3.

Рис. 3. Строка с текстом ошибки пароля

После обнаружения данной строки непосредственно перед ней будет находиться оператор сравнения и оператор условного перехода, которые используются фактически для принятия решения о правильности введенного пароля. Иллюстрация данного этапа представлена на рис. 4.

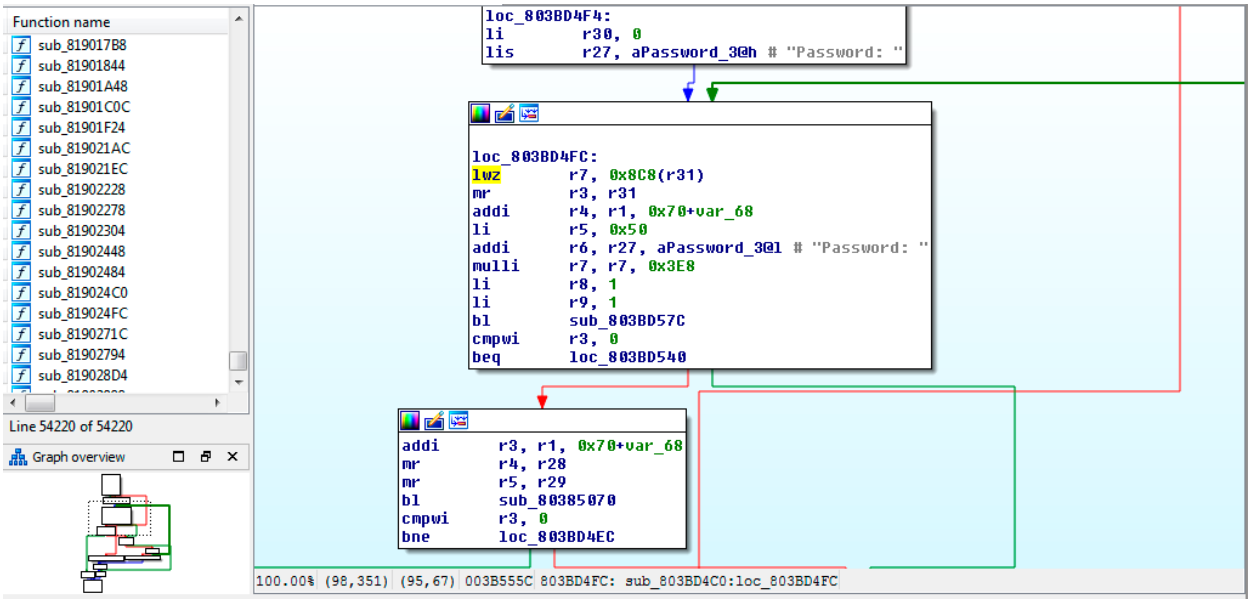

Рис. 4. Функция проверка верности пароля

Для нейтрализации подсистемы аутентификации в СПО достаточно осуществить оператора сравнения на противоположное условие либо на безусловный переход, после чего сохранить изменения в новом образе СПО. Установка данного образа СПО в оборудование и осуществление начальных настроек приведет к тому, что доступ к данному оборудованию по протоколу Telnet можно будет получить без ввода пароля.

Таким образом, в результате исследования было установлено, что программный код СПО телекоммуникационного оборудования Cisco Systems не содержит механизмов противодействия анализу подсистем аутентификации, что позволяет сравнительно легко нейтрализовать систему защиты СПО и получить удаленный доступ к данному оборудованию.

Список литературы

1. CISCO: Сетевое программное обеспечение [Электронный ресурс] : [сайт]. – Режим доступа: http://www.cisco.com. – Дата обращения: 30.11.2017.

2. Whitepaper: Writing Cisco IOS Rootkits [Электронный ресурс] : [сайт] / Grid32 Security. – Newark, 2015 г. – Режим доступа: https://grid32.com/cisco_ios_rootkits.pdf. – Дата обращения: 06.04.18..

3. IDA: About [Электронный ресурс] : [сайт] / Hex-Rays SA. – Rue Rennequin Sualem, 2016– . – Режим доступа: https://www.hex-rays.com/products/ida/. – Дата обращения: 06.04.18..

Материал поступил в редколлегию 09.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.056:004.272

Маркин Дмитрий Олегович, *сотрудник*
Трохачёв Максим Александрович, *сотрудник*
Земцов Артемий Эдуардович, *сотрудник*
Академия ФСО России, Орёл, Россия
e-mail: admin@nikitka.net

СИСТЕМА РАСПРЕДЕЛЕННЫХ ЗАЩИЩЕННЫХ ВЫЧИСЛЕНИЙ НА ОСНОВЕ СЕТИ МОБИЛЬНЫХ УСТРОЙСТВ И ТЕХНОЛОГИИ АКТИВНЫХ ДАННЫХ

Описаны состав, структура и алгоритмы функционирования элементов системы распределенных защищенных вычислений, основанной на объединении в вычислительную сеть мобильных устройств под управлением операционных систем, поддерживающих приложения-интерпретаторы скриптовых языков программирования, и концепции активных данных, позволяющих реализовать адаптируемые распределенные вычисления на абонентских устройствах.

Мобильные устройства в настоящее время занимают преобладающую позицию по количеству и распространенности среди прочих вычислительных устройств. В среднем производительность мобильных устройств "отстает" от настольных ПЭВМ примерно на 10-15 лет, однако их количество уже сейчас заметно выше. Желание использовать вычислительные возможности мобильных устройств привело к появлению технологий "туманных вычислений" (fog computing) [9]. Термин был введен сравнительно недавно компанией Cisco Systems, и определяет технологии использования сети мобильных устройств для решения вычислительно сложных задач. "Туманные вычисления" являются логическим продолжением облачных вычислений и развитием инфокоммуникационных технологий, сотовых сетей новых поколений (5G) и "интернета вещей" (IoT – "Internet of Things"). "Туманная" вычислительная сеть состоит из множества устройств с невысокой производительностью, но объединённых в единый инфокоммуникационный ресурс. К таким устройствам относятся мобильные вычислительные устройства (смартфоны, планшетные компьютеры, "умные" часы и браслеты), бортовые ЭВМ транспортных средств, "умная" бытовая техника, камеры, датчики и многое другое.

В данной работе предлагается прототип системы защищенных туманных вычислений на основе технологии активных данных [10]. Описана типовая инфраструктура, необходимая для управления распределенными вычислениями. Предложен технологический подход на основе реализации концепции активных данных, позволяющий более эффективно использовать производительность мобильных устройств по сравнению со статичными клиентскими приложениями за счет внедрения возможности универсализировать вычисления независимо от программной реализации клиентского приложения.

Технология туманных вычислений позволяет использовать вычислительные возможности объединенных в сеть мобильных устройств. Наиболее распространенными мобильными устройствами, пригодными для использования в туманных вычислениях, являются мобильные абонентские устройства (далее – МАУ) под управлением операционных систем (ОС) Android, iOS и других.

Инструмент туманных вычислений может эффективно применяться для решения следующих задач:

1) построение распределенного защищенного вычислительного кластера (интеллектуальной обработки данных);

2) решение задачи активной (интеллектуальной) маршрутизации;

3) распределенного тестирования (анализа защищенности, например, фаззинга);

4) построения анонимной сети;

5) распределенных конфиденциальных вычислений;

6) криптографического анализа;

7) сбора и анализа данных, фильтрации;

8) мониторинга состояния объектов (социальных сетей, "Интернета вещей", датчиков).

Одной из задач, необходимых для объединения МАУ в сеть является задача "преодоления" службы трансляции адресов NAT провайдеров сотовой связи. В настоящее время известны 4 вариант построения NAT: Full Cone NAT, Symmetric NAT, Address Resctriced NAT, Port Resctricted NAT.

Известно стандартизованное решение данной задачи – клиент-серверный протокол STUN (Session Traversal Utilities for NAT). Данный протокол активно применяется в области IP-телефонии и основывается на использовании сервера с "белым" сетевым адресом, задача которого – определение внешнего сетевого адреса МАУ. Протокол описан в рекомендации RFC 3489 и способен эффективно решать данную задачу для всех типов NAT за исключением Symmetric NAT ("двойной" NAT).

Для реализации защищенных туманных вычислений предлагается использовать типовую структурную схему инфраструктуры сети МАУ, представленную на рис. 1, которая может быть применена для реализации туманных вычислений.

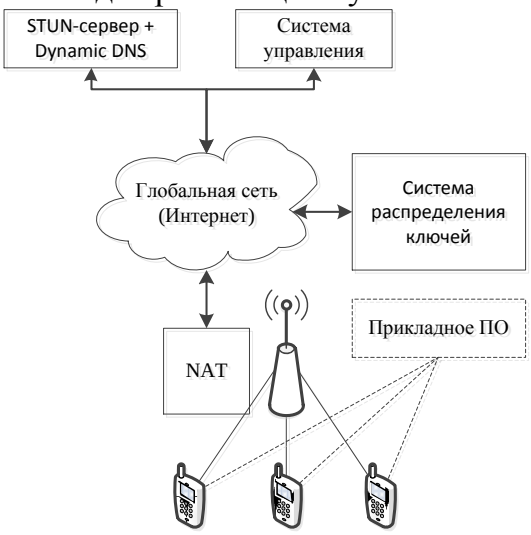

Рис. 1. Типовая структурная схема инфраструктуры сети мобильных устройств

В состав такой инфраструктуры должны входить:

1) **приложение для мобильного устройства**, содержащее: STUN-клиент, вычислительный модуль, модуль обеспечения защиты информации;

2) **сервер поддержки сети МАУ** (например, веб-приложение), содержащий: STUN-сервер; сервер службы динамического DNS;

3) **сервер системы управления сетью МАУ**, выполняющий задачи по управления вычислительными задачами и управлению доступом;

4) **сервер системы распределения ключей** (веб-приложение или служба).

Реализация концепции активных данных базируется на применении скриптовых языков программирования, таких как PHP, Perl, Python, Ruby, JavaScript и других, а также способности приложений, выполняющих роль интерпретатора, обрабатывать содержание данных (например, тела HTTP(s)-запросов) как программный код [11,12]. Иллюстрация такого применения скриптовых языков в контексте реализации концепции активных данных представлена на рис. 2.

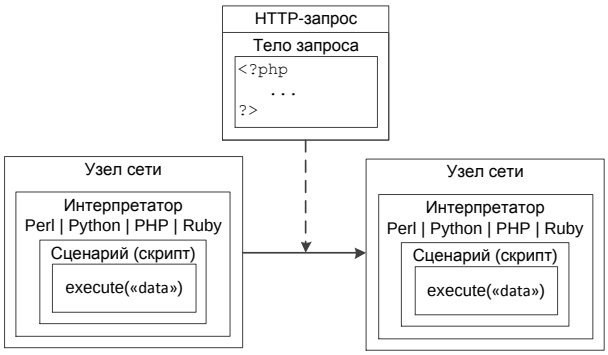

Рис. 2. Реализация концепции активных данных на основе применения скриптовых языков

Типовой алгоритм обработки активных данных представлен на рис. 3.

Рис. 3. Алгоритм обработки активных данных

Для реализации подобного алгоритма требуется поддержка скриптового языка программирования и возможность его вызова из приложения для МАУ с ОС Android, iOS или другой системы.

Разработка алгоритма клиентского приложения для мобильных устройств

Клиентское приложение для мобильных устройств под управлением ОС Android, iOS и других должно решать следующие задачи:

1) периодически отправлять запросы к STUN-серверу для идентификации текущего внешнего сетевого адреса и порта;

2) периодически обращаться к системе управления для получения данных о наличии вычислительных задач, их загрузки, выполнения и отправки отчета;

3) осуществлять аутентификацию системы управления, а также предоставлять собственные аутентифицирующие данные.

Был проведен анализ сред разработки для ОС Android, позволяющих создать приложение для МАУ с возможностью обработки активных данных на скриптовых языках программирования. Кроме основной среды Android Studio и приложения для МАУ – AIDE, известны следующие инструменты:

1) без поддержки скриптовых языков: Android Studio, Xamarin, Basic4Android, Theappbuilder, Ionic, Junior, Intel XDK, C4droid;

2) с поддержкой Lua: Corona SDK;

3) с поддержкой Python: Kivy, QPython3;

4) с поддержкой Javascript: Phonegap, Sencha Touch, Appacelerator, JQuery Mobile, Dojo Mobile, DHTML Touch, MoSync SDK, Ext JS, jQTouch, Lungo, Ratchet.

Некоторые из представленных инструментов содержат поддержку создания apk-приложений.

На рис. 4 представлен типовой алгоритм функционирования клиентского приложения для МАУ, решающий задачу по исполнению активных данных.

Рис. 4. Алгоритм функционирования клиентского приложения для МАУ

Выводы

Представленные алгоритмы позволяют реализовать высокопроизводительную систему обработки данных построенную на основе следующих принципов:

- асинхронность вычислительного процесса;
- естественный параллелизм независимых задач;
- мультипроцессорную архитектуру;
- универсальность системы (система общего назначения);
- надежность информационного обмена (за счет использования протокола TCP);
- распределенная память;
- централизованность управления задачами.

Частота выполнения операций в современных многоядерных процессорах для МАУ колеблется в диапазоне 2200 ГГц – 3000 ГГц. При этом МАУ, как правило, содержат от 2 до 8 ядер.

Если провести грубое оценивание без учета реализации многопоточности, временных издержек на передачу данных и обработку запросов системой управления, а также ряда других факторов, то для достижения производительности 10^{20} операций в секунду при условии использования МАУ с 2-х ядерным процессором и частотой 2500 ГГц потребуется создать сеть МАУ из $2 \cdot 10^7$ устройств. При этом по некоторым оценкам в настоящее время в мире уже существует и активно используется порядка $5{,}1 \cdot 10^9$ устройств, и это количество постоянно растет, как и их производительность.

Список литературы

9. Финогенов, А. А. Технология конвергентной обработки данных в защищенной сети системы мониторинга / А. А. Финогеев, А. Г. Финогеев, И. С. Неведова // Фундаментальные исследования. – 2015. – № 11. – С. 923–927.

10. Кулешов, С. В. Активные данные в цифровых программно-определяемых системах/ С.В. Кулешов, О.В. Цветков// Информационно-измерительные и управляющие системы. 2014. Т. 12. № 6. С. 12-19.

11. Маркин, Д. О. Исследование устойчивости анонимной сети на основе технологий веб-прокси / Д. О. Маркин, П. А. Архипов, А. С. Галкин // Вопросы кибербезопасности. – 2016. – № 2 (15). – С. 21–28.

12. Маркин, Д. О. Алгоритм распределенного тестирования веб-приложений на основе технологий веб-прокси и активных данных / Д. О. Маркин, А. С. Галкин, П. А. Архипов // Информационные системы и технологии. – 2018. – № 1. (105). – С. 93–101.

Материал поступил в редколлегию 09.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.056.53

***Масалыгин Кирилл Константинович,** студент*
Орловский государственный университет им. И.С.Тургенева, Орёл, Россия,
e-mail:ironpet@yandex.ru

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ЛАЗЕРНЫХ МИКРОФОНОВ, КАК СКРЫТЫХ СРЕДСТВ АКУСТИЧЕСКОГО НАБЛЮДЕНИЯ

На основе изучения современных технических и организационных методов борьбы с прослушивающими устройствами приведены минусы использования лазерного микрофона в качестве устройства скрытого акустического наблюдения и современные проблемы рынка лазерных микрофонов.

1. Актуальность. В последние годы вопрос о методах ведения разведки данных стоит очень остро не только в масштабах государства, но и предприятий. Благодаря научному прогрессу появляется все больше способов получения конфиденциальных данных. Но вместе с новыми возможностями появляются новые методы борьбы с кражей информации. Кража информации наказывается по закону, но для успешного ведения борьбы против шпионажа необходимо подходить к вопросу со всех сторон. Именно поэтому стоит рассмотреть вопрос защиты данных с точки зрения их возможного похитителя. Только зная, с какими проблемами столкнется нарушитель, можно понять, какие методы для их обхода он будет использовать. Это позволит подготовиться к возможному хищению конфиденциальной информации, подготовить персонал и оборудовать контролируемое помещение.

2. Особенность использования лазерных микрофон как средства акустического наблюдения. Лазерные микрофоны, как средство акустического наблюдения, применяются на дальних расстояниях и являются сложными аппаратными решениями для записи и передачи акустической информации. В основе таких устройств лежит модуляция отраженных невидимых инфракрасных лазерных лучей от стекла. В лазерных микрофонах можно выделить три вида модуляции излучений: частотная, амплитудная и фазовая.

С помощью лазерных микрофонов происходит прослушивание разговоров в помещении, подверженном акустическому наблюдению. Можно утверждать, что применение лазерных микрофонов представляет собой один из самых эффективных способов для удаленного прослушивания. Применение подобной техники делает возможным недетектируемое прослушивание акустической информации и сигналов. Главным условием является лишь наличие хотя бы одного окна в целевом помещении. По расстоянию, на котором можно совершать съем информации, можно видеть очень внушительные цифры, что позволяет осуществлять подобную деятельность без обнаружения. Для примера

приведена дальности работы популярных моделей, которые можно найти и приобрести в интернете (табл.1).

Таблица 1

Дальность прослушивания доступных на рынке лазерных микрофонов

Модель	**Производитель**	**Дальность**
SIM-LAMIC	SIM Security & Electronic System	500 м.
Laser-3000	PKI Electronic Intellegence	500 м.
AA79106	Argo-A Security	500 м.
MR-7800	Jarvis International Intellegence	400 м.
HP-150	Hewlett-Packard	1000 м.

3. Схема установки и режимы работы лазерных микрофонов. Помимо дальности действия, подобные устройства можно разделить по схеме их установки и режиму работы. Так, есть режим гетеродинного приема и режим прямого фотодетектирования.

Лазерные микрофоны, которые работают в первом режиме, имеют следующую схему установки:

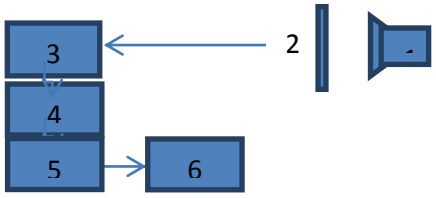

Рис. 1 Схема установки в режиме гетеродинного приема:
1 – Источник сигнала, 2 – Стекло, 3 – Приемное устройство,
4 – Блок регистрации и обработки речевой информации,
5 – Специальное ПО для обработки информации,
6 – Акустическая приставка

Лазерные микрофоны, которые работают во втором режиме, имеют следующую схему установки:

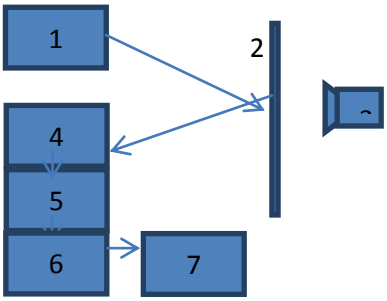

Рис. 2 Схема установки в режиме прямого фотодетектирования:
1 – Лазерный излучатель, 2 – Стекло, 3 – Источник сигнала,
4 – Фотоприемное устройство, 5 – Блок регистрации и обработки речевой информации, 6 – Специальное ПО, 7 – Акустическая приставка

В плюсы применения лазерных микрофонов можно отнести трудность обнаружения подобного оборудования. Это связано с тем, что инфракрасный луч лазера является невидимым для невооруженного глаза человека. Вкупе с удаленностью оператора подслушивающего устройства и самого микрофона от объекта, можно говорить о невозможности визуального контакта объекта съема информации и тех, кто пытается украсть информацию.

Однако этот метод все еще остается не идеальным и можно заранее обезопасить помещение от подобного рода устройств до проведения переговоров. К организации защиты относятся не только технические средства, но и организационные меры. Помимо подготовки помещения на предмет прослушивания, на успех операции по акустическому наблюдению также влияют другие внешние факторы.

4. Качество полученной информации. Для устранения возможных проблем перед использованием подобной аппаратуры можно провести исследования по определению качества информации, которую можно снять лазерным микрофоном. Эффективность канала можно измерить по следующей формуле

$$\eta = \frac{J_0}{J_1},$$

где η – эффективность, J_0 – кол-во поступившей информации, а J_1 – кол-во информации на выходе.

Также стоит провести оценку разборчивости речи

$$W = \frac{N_0}{N_1},$$

где W – разборчивость, N_0 – число разборчивых принятых слов, а N_1 – общее кол-во слов.

Таким образом, видно, что чем больше величина W, тем лучше полученная запись. Однако эту величину можно изменить с помощью специализированного ПО по обработке речевых сигналов.

5. Основные недостатки лазерных микрофонов как средств снятия акустической информации. К существенным недостаткам лазерных микрофонов можно отнести достаточную дешевизну и простоту защиты от лазерного прослушивания. Достаточно лишь установить правила касаемо переговоров и передачи устно конфиденциальной информации. Переговоры можно вести в помещении, не имеющем внешних стен и окон, либо окна должны выходить на контролируемую территорию. Однако этот способ легко нивелируется человеческим фактором. Известно, что одним из наиболее распространенных каналов утечки информации является халатность или ошибки персонала.

Еще одним минусом применения лазерных микрофонов является его зависимость от внешних факторов, таких как параметры атмосферы (сюда можно включить яркость солнца, температуру, осадки); материал из которого сделаны окна (неровности и шероховатости); фоновые акустические шумы; громкость источника сигнала и др.

К одним и самых важных минусов использования лазерных микрофонов можно отнести все способы технической защиты от такого рода устройств, так

как они являются достаточно доступными, простыми и дешевыми. К ним относятся системы вибрационной защиты и акустического зашумления; тройные стекла в оконной раме и расположение их под разными углами; отражающие пленки на окнах; использование разных материалов вместо стекла, которые хуже подвержены вибрациям; отсутствие в помещении зеркал, люстр и других предметов, которые можно использовать для снятия информации лазером.

Также не стоит забывать и о том, что действительно качественная аппаратура стоит весьма дорого. Этот минус способен отпугнуть очень многих от использования такого метода снятия информации. Помимо самой цены, необходимо еще знать и уметь пользоваться лазерными микрофонами. Для их работы требуется высококвалифицированные настройщики, а иначе есть риск не записать вообще никакую информацию. Все это ведет к большим тратам, что зачастую может быть не соизмеримо с выгодой от полученной информации.

Последним важным минусом является сложность разверстки такой системы для каждого отдельного случая. Необходимо найти место для такого оборудования, подобрать правильный угол расположения (если лазерный микрофон не работает в режиме гетеродинного приема) и дальность от места съема информации. К тому же это место не должно контролироваться и нельзя, что бы видели, что проводятся такие операции. Зачастую это совершенно невозможно либо велик риск обнаружения, что может также привести к нецелесообразности использования лазерных микрофонов для “прослушки”.

6. Выводы. Таким образом, лазерный микрофон не является панацеей в вопросах скрытого прослушивания и снятия акустической информации. Он все так же имеет свои минусы и плюсы. Поэтому при необходимости скрытого получения информации необходимо рассматривать все возможные и доступные методы или вовсе использовать их комплекс. При всем богатстве технических средств самым легким способом хищения информации до сих пор остается нечестность сотрудников организации или их халатность.

Список литературы

1. Каторин, Ю.Ф. Большая энциклопедия промышленного шпионажа / Ю.Ф. Каторин, Е. В. Куренков, А. В. Лысов, А. Н. Остапенко. – СПб.: Полигон, 2000.

2. Каторин, Ю.Ф. Защита информации техническими средствами. Учебное пособие / Ю. Ф. Каторин, А.В. Разумовский, А. И. Спивак. – СПб.: Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, 2012.

3. Лазерные микрофоны-универсальное средство разведки или очередное поветрие моды? [Электронный ресурс]. – Режим доступа: http://kiev-security.org.ua/box/8/13.shtml

4. Лазерные микрофоны [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/blog/personal/aguryanov/30026.php

5. Средства акустической разведки: направленные микрофоны и лазерные акустические системы разведки [Электронный ресурс]. – Режим доступа:

http://docplayer.ru/35043005-Sredstva-akusticheskoy-razvedki-napravlennye-mikrofony-i-lazernye-akusticheskie-sistemy-razvedki.html

6. Лазерные микрофоны [Электронный ресурс]. – Режим доступа: http://www.laser-portal.ru/content_935

Материал поступил в редколлегию 23.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.75

***Мишин Дмитрий Станиславович**, к.ю.н., доцент кафедры информационных технологий в деятельности ОВД ОрЮИ имени В.В. Лукьянова*
Орловский юридический институт МВД России имени В.В. Лукьянова, г. Орел, Россия
e-mail:mishinds@mail.ru

СПОСОБЫ И ПРИЕМЫ ФОРМИРОВАНИЯ РЕАКЦИЙ НА ДЕСТРУКТИВНЫЕ ИНФОРМАЦИОННЫЕ АТАКИ

Эффективное обнаружение атак на информационные ресурсы требует понимания ожидаемого поведения контролируемого объекта системы и знания всех возможных способов воздействия и их модификаций. Использование нейросетевых методов анализа позволяет производить анализ файлов отчета о работе сети и определять аномальное поведение пользователя.

Научно-техническая революция, начавшаяся во второй половине XX века, не только вызвала существенные изменения в общественной жизни, но и инициировало разработку и внедрение в повседневную жизнь новых технологий. Современное общество предъявляет все более возрастающие требования к оперативности протекания информационных процессов во всех областях повседневной деятельности в связи с тем, что оперативность и достоверность информации играет ключевую роль в функционировании общественных и государственных институтов, но и в жизни каждого человека. Все эти процессы стали побудительным мотивом для создания и, в последующем, постоянного совершенствования программных и технических средств распределенных систем обработки данных, которые получили название информационно-телекоммуникационные сети. В Федеральном законодательстве Российской Федерации дается следующее определение: «Информационно-телекоммуникационная сеть (ИТС) - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники»[1].

Следствием создания, построения и развития информационно-телекоммуникационной инфраструктуры стало существенное повышение важности и роли информации и, как следствие, разработка процедур нарушения безопасности информации с целью получения противоправного доступа для совершения деструктивных действий. Немаловажную роль данная проблема играет и в повседневной деятельности органов внутренних тела, особенно остро встала после введения в эксплуатацию единой информационно-телекоммуникационной системы МВД России.

Как показывает практика, любой попытке совершения неправомерного доступа необходимо противопоставить быстрый и продуманный ответ, с целью недопущения потери информации, а также эффективное использование специ-

альных процедур для последующей идентификации злоумышленника. То есть в этом случае целесообразно формирование доказательной базы подобного инцидента специально подготовленным специалистом, иначе высока вероятность программной модификации или ошибочной идентификации следов при анализе процесса совершения инцидента.

Выработка эффективной процедуры реагирования на инцидент является достаточно сложной задачей. Признаки совершения неправомерного доступа к компьютерной информации представляют собой следы, оставленные злоумышленником. Чаще всего злоумышленник использует не один метод неправомерного доступа, а их совокупность для достижения поставленной цели. Построение эффективной модели системы защиты информации требует ее соответствия специальным нормативным документам по обеспечению информационной безопасности, принятым в Российской Федерации, международному стандарту ISO/IEC 15408 «Информационная технология - методы защиты - критерии оценки информационной безопасности», стандарту ISO/IEC 17799 «Управление информационной безопасностью» и учитывает тенденции развития отечественной нормативной базы (в частности, ФСТЭК РФ) по вопросам защиты информации.

Обнаружение атак требует или понимания ожидаемого поведения контролируемого объекта системы или знания всех возможных атак и их модификаций.

В первом случае используется технология обнаружения аномального поведения, а во втором случае - технология обнаружения злоумышленного поведения или злоупотреблений. Вторая технология заключается в описании атаки в виде шаблона или сигнатуры и поиска данного шаблона в контролируемом пространстве (например, сетевом трафике или журнале регистрации).[2] Эта технология очень похожа на обнаружение вирусов (антивирусные системы являются ярким примером системы обнаружения атак), т.е. система может обнаружить все известные атаки, но она мало приспособлена для обнаружения новых, еще неизвестных, атак. Подход, реализованный в таких системах, очень прост и именно на нем основаны практически все предлагаемые сегодня на рынке системы обнаружения атак, которые основаны на сигнатурном подходе.

Поведение взломщиков, вторгающихся в работу сети, значительно отличается от действий зарегистрированных пользователей. При этом производится анализ отчетов о функционировании операционной системы, приложений и сравнение системных событий с заранее известной базой процедур нарушений безопасности. Располагающиеся на сетевых рабочих станциях компоненты системы обнаружения атак следят за различными аспектами безопасности, и в случае взлома или отклонений от нормального режима функционирования реагируют на это[2]. Системой регистрируется факт произошедшего инцидента, предупреждается администратор, а в отдельных случаях производится полная остановка рабочих станций, изменение настроек межсетевых экранов или маршрутизаторов.

Использование на элементах компьютерной сети специального программного обеспечения позволяющего производить анализ файлов отчета о работе сети и определять:

- компьютер, с которого был произведен неправомерный доступ;
- время и продолжительность соединения одной рабочей станции с другой;
- протокол информационного обмена компьютерной сети, который автоматически ведется на каждом компьютера имеющем доступ к сети и информация остается в лог-файлах;
- данные о пользователе, определяемые по адресу его электронной почты, назначенном системным администратором;
- содержание разговоров через компьютерную сеть, информация о которых автоматически сохраняется во временных файлах, которые даже после стирания могут быть частично восстановлены.

Обеспечение адекватного реагирования на производимые атаки невозможно без использования системы поддержки и принятия решений, накопления знаний и опыта в области расследования правонарушений и преступлений в сфере компьютерной информации целесообразно использовать нейросетевые методы анализа, что позволит обеспечивать информационную безопасность на должном уровне.

Экспериментальная оценка реальных данных показывает, что нейронная сеть может обучаться с целью идентификации пользователей просто по тем командам, которые они используют и по частоте их использования, и такая идентификация может быть использована для обнаружения атак в компьютерной сети против информации. Нет необходимости принимать во внимание порядок команд. Нейросетевые методы позволяют легко обучаться, не требуют значительных затрат работая в автономном режиме позволяют ежедневно создавать регистрационные записи.

Учитывая рассмотренное, можно предложить обобщенную методику реакции на инцидент, связанный с неправомерным доступом к компьютерной информации.

На первом этапе целесообразны разработка и формирование алгоритма реагирования на инцидент с учетом его возможных процедур и используемого, в вычислительной системе, программного обеспечения. Как нам кажется, к наиболее эффективным программно-техническим средствам обеспечения информационной безопасности, с целью противодействия или предотвращения неправомерного доступа к информации, можно отнести систему обнаружения атак и брандмауэры (firewall), формирующие сообщения об опасных ситуациях в файлах отчета (журналах регистрации). В течение этого процесса происходит фиксирование даты и времени, природы инцидента, оборудования и программного обеспечения, участвующего в нем, а в конечном итоге, формируется файл отчета.

На следующем этапе: на основе сформированного алгоритма осуществляется реакция на инцидент или внештатную ситуацию, заключающаяся в реализации мероприятий по реагированию на нарушение информационной безопасности, изоляция попытки неправомерного доступа, фиксировании и формировании доказательной базы.

Четкое выполнение всех рассмотренных этапов позволяет создать достаточно полный набор документов о попытке неправомерного доступа, начиная с начальной фазы вторжения.

Использование предлагаемой методики реагирования на инцидент, связанный с неправомерным доступом к компьютерной информации, позволит получить достаточно полную картину происшествия и, следовательно, разработать более эффективную политику предупреждения, противодействия и самое главное профилактики.

Остановимся на данном вопросе более подробно. Существует традиционный способ профилактики неправомерного доступа к компьютерной информации, который заключается в усилении защищенности компьютерных систем от вмешательства в их деятельность. В этом случае применяются программно-технические средства обеспечения информационной безопасности, а также ограничение физического доступа к компьютерам.

Помимо этого, можно предложить ряд способов, применение которых позволит снизить количество случаев неправомерного доступа к компьютерной информации.

В первую очередь, кажется необходимым осуществление пропаганды правовых знаний и широкая огласка ответственности за рассматриваемое нами деяние, что позволит ограничить круг лиц, совершающих их из любопытства или хулиганских побуждений.

Также кажется необходимым проведение работы по официальной блокировке и закрытии сайтов, размещенных в сети Интернет, на которых осуществляется пропаганда хакерства и крэкерства, а также свободно распространяются способы совершения и программы, позволяющие осуществлять неправомерный доступ к компьютерной информации.

Кроме того, следует осуществлять рассылку предупреждений в издательства и типографии страны о недопустимости издания книг, газет и журналов, содержащих пропаганду хакерства и крэкерства.

Постоянное совершенствование процедур неправомерного доступа к компьютерной информации приводит к адекватному улучшению средств обеспечения и информационной безопасности в телекоммуникационных сетях с целью построения эффективной политики безопасности.

Практика показывает, что следы деструктивных последствий практически любого случая неправомерного доступа остаются на жестком диске рабочей станции, и корректное проведение с помощью специальных программно-аппаратных средств, последующего анализа позволяет более полно оценить

действия правонарушителя, а также принять необходимые меры для предотвращения подобных деяний и их профилактики.

Как представляется, применение рассматриваемых в данной статье методов позволит в дальнейшем принимать достаточно эффективные меры для профилактики нарушений, совершаемых в сфере компьютерной информации в телекоммуникационных системах вообще и в органах внутренних дел в частности.

Список литературы

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Хогланд Грег, Мак-Гроу Гари Взлом программного обеспечения: анализ и использование кода.: Пер. с англ. – М.: Издательский дом «Вильямс», 2005.

3. Уголовный кодекс Российской Федерации. Принят Государственной Думой РФ 24 мая 1996 г. Одобрен Советом Федерации 5 июня 1996 г. (с последующими изменениями и дополнениями) — М.: ТК Велби, 2005.

4. Мишин, Д.С. Методы и системы обнаружения атак в компьютерных сетях / Д.С. Мишин, А.В. Еременко // Вестник информационных и компьютерных технологий. – 2006. – № 10. – С.35-41.

5. Усов, А.И. Судебно-экспертное исследование компьютерных средств и систем: учебное пособие/А.И. Усов. – М: Экзамен, 2003.

6. Шурухнов, Н.Г. Криминалистика: учебник/Н.Г. Шурухнов. – М.: Изд-во Эксмо, 2005.

Материал поступил в редколлегию 23.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.4

***Можин С. В.**, сотрудник*
Академия ФСО, Орел, Россия
e-mail: kattz74@mail.ru

НЕКОТОРЫЕ ПОДХОДЫ К ОБФУСКАЦИИ ИСПОЛНЯЕМОГО КОДА ДЛЯ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ К СТАТИЧЕСКОМУ АНАЛИЗУ

Возможность реверс-инжениринга программного кода дает возможность для хищения интеллектуальной собственности через программное пиратство, а также для нарушения безопасности, позволяя злоумышленникам обнаруживать уязвимости в приложении. Работа направлена усложнение начальной стадии дизассемблирования. Наша цель - нарушить процесс статического дизассемблирования, чтобы код было сложнее правильно дизассемблировать. Экспериментальные результаты показывают высокую эффективность предложенных методов обфускации.

Реверс-инженеринг – процесс восстановления структуры и семантики более высокого уровня из машинного кода. В широком смысле мы можем разделить реверс-инженеринг на две части: дизассемблирование, которое производит машинный код в ассемблерный; и декомпиляции, которая реконструирует из ассемблерного кода семантическую структуру более высокого уровня. Наша цель – увеличить сложность статического дизассемблирования программы. Таким образом, наш подход не зависит, а дополняет существующие подходы к обфускации кода.

Дизассемблирование является процессом восстановления последовательности ассемблерных инструкции из такого файла, например, в текстовый формат, читаемый человеком. Вообще говоря, существует два подхода к дизассемблированию: статическое дизассемблирование, когда файл дизассемблируется дизассемблером, но сам не выполняется во время дизассемблирования; а также динамическое дизассемблирование, когда файл выполняется под отладчиком для идентификации выполняющихся инструкций. Преимущество статического дизассемблирования - возможность обработки всего файла сразу, в то время как динамическое дизассемблирование дает только «срез» программы, т. е. инструкции, которые были выполнены для конкретных исходных данных, которые были использованы. Другим преимуществом статического дизассемблирования является то, что требуется время, пропорциональное размеру программы, а время, затраченное на динамическое дизассемблирование, как правило, пропорционально количеству команд, выполняемых программой во время выполнения. Как правило, первое значительно меньше последних (часто на несколько порядков), делая статическое дизассемблирование более эффективным, чем динамическое.

Алгоритм линейной развертки начинает дизассемблирование с точки входа в программу и просто дизассемблирует каждую встречающуюся инструкцию. Основная слабость этого алгоритма заключается в том, что он подвержен ошибкам дизассемблирования, возникающим в результате неправильного толкования данных, встроенных в поток инструкций. Только при особых обстоятельствах, например когда появляется недопустимый код операции, дизассемблер может узнать о таких ошибках.

Проблема с алгоритмом линейной развертки заключается в том, что он не учитывает поведение потока управления программой, он не может «обходить» данные (например, байты выравнивания, таблицы перехода и.т.д.), встроенные в поток команд, и ошибочно интерпретирует их как исполняемый код. Вариацией этого базового подхода к дизассемблированию является рекурсивный обход. Достоинством этого алгоритма является то, что, следуя поведению потока управления обрабатываемой программы, он способен «обойти» и таким образом избежать дизассемблирования данных, встроенных в сегмент кода. Его основная слабость заключается в том, что предположение о возможности точно идентифицировать набор адресов переходов потока управления может не всегда выполняться при косвенной передаче управления. Неточность определения множества возможных адресов такого перехода приведет либо к неспособности дизассемблировать некоторый достижимый код (если недооценивается набор адресов перехода), либо ошибочное дизассемблирование данных (если набор адресов избыточен).

Чтобы помешать дизассемблеру, мы должны изменить его представление о том, где находятся границы инструкций в коде. В архитектуре Intel IA-32, структура команд такова, что очень часто процесс дизассемблирования самовосстанавливается: даже когда ошибка дизассемблирования (например, из-за дизассемблирования данных), дизассемблер ресинхронизируется и в конечном итоге заканчивает с правильным потоком команд. Другими словами, с такими наборами команд ошибка дизассемблирования приводит к отличной от нуля разности между начальными адресами команд, идентифицированными дизассемблером и «фактическими» адресами инструкций, но эта разница обычно стремится к нулю по мере продолжения дизассемблирования, и через некоторое время начальные адреса команд, идентифицированные дизассемблером, начинают совпадать с фактическими адресами инструкций.

Когда точка дизассемблирования смещена на один байт, дизассемблер создает две ошибочные инструкции, но возвращается к правильному дизассемблированию после второй инструкции. Подобное явление возникает, когда дизассемблирование изначально смещено на два байта: он ресинхронизируется, начиная со второй инструкции в фактическом коде, после создания одной неправильно дизассемблированной инструкции. Если дизассемблер изначально смещен на три байта, он генерирует три неправильно дизассемблированные команды, но после третьей инструкции продолжает работать правильно.

Очевидно, что фактическое поведение ресинхронизации для конкретной программы будет зависеть от конкретного распределения инструкций в ней. На практике ошибки дизассемблирования обычно ресинхронизируются довольно быстро: часто в пределах одной или двух команд за пределами точки, в которой произошла ошибка дизассемблирования. Усилия по запутыванию дизассемблирования должны учитывать это самовосстанавливающееся свойство дизассемблирования.

Мы можем ввести ошибки дизассемблирования, вставив «мусорные» байты в выбранных местах в потоке команд, где дизассемблер, скорее всего, ожидает код. Любые такие «мусорные» байты должны удовлетворять двум свойствам. Во-первых, для того, чтобы реально сбивать дизассемблер, «мусорные» байты должны быть частичными инструкциями, а не полными инструкциями. Во-вторых, чтобы сохранить семантику программы, такие частичные инструкции должны быть вставлены таким образом, чтобы они были недоступны во время выполнения. С этой целью определяется базовый блок в качестве блока-кандидата, если он может иметь такие «мусорные» байты, вставленные перед ним. Чтобы гарантировать, что какой-либо «мусор», который был вставлен, недоступен во время выполнения, базовый блок-кандидат не может выполнить его. Другими словами, базовый блок непосредственно перед блоком-кандидатом должен завершиться безусловным переносом управления, например безусловным переходом или возвратом функции. Блоки кандидатов могут быть идентифицированы простым способом, сканируя основные блоки программы после того, как была определена окончательная схема распределения памяти.

Процесс статического дизассемблирования очень часто удается «повторно синхронизировать» после ошибки дизассемблирования. После того, как был идентифицирован блок-кандидат *B*, мы должны определить, какие «мусорные» байты должны быть вставлены перед ним, чтобы как можно больше путать дизассемблер, т. е. задержать эту повторную синхронизацию как можно дольше. Для этого мы берем конкретную *n*-байтную инструкцию *I* и определить, как далеко может произойти повторная синхронизация, если первые *k* байтов *I* будут вставлены непосредственно перед блоком-кандидатом *B*, для каждого *k*, $0 < k < n$. Чтобы определить точку повторной синхронизации, для каждого такого *k* моделируется дизассемблирование для блока-кандидата, предполагая, что дизассемблер встречает первые *k* байтов команды *I* в начале *B*, а затем продолжит последовательность байтов, содержащую фактический машинный код инструкций в блоке *B*. При использовании этого подхода, определяется значение k_{max}, для которого расстояние повторной синхронизации максимизируется, и вставляются первые k_{max} байт *I* непосредственно перед блоком *B*.

Дизассемблирование линейной разверткой, как правило, не может отличить данные, встроенные в секцию кода. Можно использовать эту слабость, вставив «мусорные» байты в выбранные места в потоке команд, как описано выше. Здесь следует отметить, что, поскольку симуляция дизассемблирования

проверяется от каждого блока-кандидата, чтобы определить количество «мусорных» байт, которые должны быть там вставлены, важно обеспечить, чтобы такие решения, принятые для одного кандидата, впоследствии не были аннулированы введением «мусора» к последующим кандидатам. Чтобы избежать такого эффекта, блоки кандидатов при вставке «мусора» рассматриваются в обратном порядке.

Мы обычно можем достичь «коэффициента ошибки» в среднем примерно 26-30%, то есть 26-30% инструкций в программе неправильно дизассемблированы. Причина, по которой коэффициент не может быть выше, заключается в том, что кандидаты на вставку «мусорных» байт не должны выполнять их: предыдущий блок должен завершиться безусловной передачей управления. В коде, полученном из обычного оптимизирующего компилятора, блоки-кандидаты, как правило, составляют в среднем около 30 инструкций. Это расстояние в сочетании с самовосстанавливающимся характером дизассемблирования означает, что при сбое дизассемблирования после вставки «мусора» перед кандидатом, дизассемблеру обычно удается ресинхронизироваться до того, как встретится следующий кандидат. Увеличить количество кандидатов можно путем преобразования, направленного на увеличение ветвистости. При таком преобразовании расстояние между блоками-кандидатами в среднем падает примерно до 12 инструкций, а коэффициент ошибки возрастает примерно до 70%.

Основная сила алгоритма рекурсивного дизассемблирования - его способность разумно обрабатывать поток управления и тем самым дизассемблировать вокруг данных встроенных в сегмент кода - также оказывается слабостью, которую можно использовать, чтобы запутать процесс дизассемблирования. Есть два (связанных) аспекта рекурсивного обхода, которые можно использовать. Во-первых, когда дизассемблер сталкивается с передачей управления, дизассемблирование продолжается в тех местах, которые считаются возможными точками передачи управления. В этом контексте дизассемблеры обычно предполагают, что типовые команды передачи управления, такие как условные переходы и вызовы функций, ведут себя «разумно». Так, предполагается, что условный переход имеет две возможные точки: переход при выполнении условия и переход к следующей инструкции при невыполнении условия. Аналогичным образом предполагается, что функция возвращает управление к следующей инструкции после своего выполнения.

Предположение о том, что функция возвращает управление инструкции, следующей за инструкцией вызова функции, может быть проэксплуатирована с использованием термина «функции ветвления». Дано конечное отображение φ над участками памяти в программе $\varphi=\{a_1 \rightarrow b_1, \ldots, a_n \rightarrow b_n\}$, функция ветвления f_φ является такой функцией, что всякий раз, когда она вызывается из одного из участка a_i, заставляет управление передается в соответствующее местоположение b_i, $1 \leq i \leq n$. Учитывая такую функцию ветвления f_φ, мы можем заменить n безусловных переходов в программе:

a_1: jmp b_1
…
a_2: jmp b_2
…
a_n: jmp b_n
На вызовы функции ветвления:
a_1: call f_φ
…
a_2: call f_φ
…
a_n: call f_φ

Код для функции ветвления отвечает за определение целевого местоположения b_i на основе местоположения a_i, из которого он был вызван, затем выполняет переход на соответствующий b_i. Более того, он должен делать это таким образом, чтобы программным состоянием было то, что было бы встречено в местоположении b_i в исходном коде с безусловным переходом. Обратите внимание, что функция ветвления не ведет себя как «нормальные» функции, поскольку она обычно не возвращает управление к инструкции, следующей за инструкцией вызова, а вместо этого переходит в другое место в программе, которое зависит в общем от того, откуда оно было вызвано.

Функции ветвления выполняют две различные цели. Первая заключается в том, чтобы запутать поток управления в программе: значительно затрудняя вычисление целевого адреса b_i внутри функции ветвления, мы можем затруднить попытку злоумышленника восстановить исходную карту φ, которую она реализует. Во-вторых, создание возможностей для введения в заблуждение дизассемблера: поскольку дизассемблер обычно продолжит дизассемблирование с инструкции, следующей за инструкцией вызова функции, мы можем ввести ошибки в дизассемблировании, вставляя «мусорные» байты в точке сразу после каждой команды «call f_φ».

Функции ветвления могут быть реализованы несколькими способами. Тривиальные реализации включают поиск по таблице с использованием адреса возврата, переданного функции ветвления, для определения целевого адреса. Такие реализации имеют недостаток, заключающийся в относительно простом реверс-инжиниринге. Более сложный подход может использовать хеширование или другие схемы, которые трудно обратить. Сложность реализации функции ветвления и способ ее доступа дают возможность выбирать между скоростью выполнения, с одной стороны, и сложностью реверс-инжиниринга, с другой. Так, мы можем выбрать различные реализации функций ветвления для команд перехода в зависимости от частоты их выполнения: часто исполняемые инструкции перехода могут быть направлены на облегченную функцию ветвления, реже выполняемые на более сложную функцию ветвления, и так далее. Более того, определенная команда перехода в программе может быть сделана частью отображения ветвления для нескольких различных функций ветвления,

причем одна из них выбирается произвольным (и динамически изменяемом) образом во время выполнения.

Описанные методы применимы к широкому спектру архитектур. Вставка частичных инструкций для ошибок дизассемблирования применима к наборам инструкций переменной длины, например, к широко используемым Intel Pentium и Motorola 680x0, а также к архитектурам смешанного типа, таких как MIPS32/MIPS16. Функции ветвления и спуфинг таблицы переходов могут использоваться для любой архитектуры.

Материал поступил в редколлегию 23.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.056

Можин Сергей Владимирович, *сотрудник*
Бондарева Наталья Вячеславовна, *сотрудник*
Академия ФСО России, Орёл, Россия
e-mail: natalibond.ru@gmail.com

РАЗРАБОТКА АВТОМАТИЗИРОВАННОГО УЧЕБНО-ТРЕНИРОВОЧНОГО КОМПЛЕКСА ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО НАСТРОЙКЕ ОБОРУДОВАНИЯ КОММУТАЦИИ ПАКЕТОВ МОБИЛЬНОГО УЗЛА СВЯЗИ

Представлены требования и подходы к построению автоматизированного учебно-тренировочного комплекса, позволяющего повысить эффективность подготовки экипажа мобильного узла связи, а также разработаны его состав и структура.

Процесс приобретения новых знаний, навыков и умений неразрывно связан с обучением. Благодаря современным информационным технологиям обществу предоставляются практические неограниченные возможности для освоения различных программ обучения. В то же время, несмотря на доступность огромного количества информационных ресурсов конкретному человеку, актуальной остается проблема обучения больших и малых групп людей. При детальном рассмотрении данной проблемы оказывается, что существует большое количество факторов, влияющих на качество обучения, и наиболее важные из них – недостаточная техническая оснащенность для организации обучения и бессодержательность обучающего материала. Критически важными эти факторы являются для таких специфичных направлений обучения, где требуется наличие большого количества дорогостоящего оборудования – в данном случае это мультипротокольное коммутационное оборудование мобильного узла связи. Новинки образовательной деятельности позволяют решать эти проблемы.

Непрекращающийся процесс совершенствования обучающих технологий привел к появлению программных продуктов, позволяющих эффективно управлять образовательный процессом. К таким продуктам можно отнести автоматизированные обучающие комплексы, к которым относятся:

- электронные учебные материалы;
- обучающие сайты;
- специализированные среды обучения;
- лабораторные комплексы;
- обучающие программы.

При грамотном комбинировании перечисленных программных продуктов в едином автоматизированном учебно-тренировочном комплексе (АУТК) становится возможным достичь большей эффективности обучения. АУТК направ-

лены на поддержку процесса обучения и построены на базе компьютерных и информационных технологий.

Техническое обеспечение разработанного АУТК включает в себя автоматизированные рабочие места (АРМ) обучающихся, объединенные в локальную вычислительную сеть (ЛВС), и аппаратный стенд. Цель этих технических и программных средств состоит в обеспечении учащихся средствами решения, справочным материалом и средствами регистрации ответов [1].

Таким образом, АУТК должен объединить в себе три основных компонента, обеспечивающих современные технологии обучения: информационное, техническое и программное обеспечение образовательного процесса. Такой комплексный подход позволит обеспечить обучающегося всеми условиями для успешного
освоения учебного материала, свободным графиком изучения, а также индивидуальным маршрутом обучения за счет использования различной глубины представленного
материала [2].

Для наполнения АУТК предметным материалом первоначально должна быть разработана структура всего курса, и при его оформлении необходимо следовать единому стандарту компоновки и оформления. Предметный материал для обучения должен иметь не только теорию, но и полный набор всего дидактического материала (схемы, рисунки, таблицы, графики, упражнения и пояснения к их выполнению, вопросы текущего контроля и правильные ответы) [3].

Электронные интерактивные учебно-методические материалы в рамках разработанного АУТК представляют собой набор взаимосвязанных вебдокументов, объединенных в единую логическую структуру и включающих в себя элементы текста, статических и динамических изображений, элементы меню и навигации, а также средства тестирования и самоконтроля [4]. Кроме того, в конце изучения каждого раздела предусмотрен итоговый контроль по пройденному материалу.

Проблема недостаточной технической оснащенности решается с помощью программ (сред) эмуляции сетевого оборудования. Эти программы используются при подготовке лабораторных работ, направленных на практическую отработку вопросов, связанных с настройкой оборудования коммутации пакетов, которую невозможно осуществить на реальном оборудовании по причине его отсутствия.

Безопасность разработанного комплекса обеспечивается системой аутентификации и идентификации, реализованными в сайте с обучающими материалами, а также криптографической надстройкой веб-сервера Apache с помощью протокола SSL/TLS.

Все технологии, реализованные в единой информационно-образовательной среде, и представленные в виде АУТК, направлены на качественное повышение уровня образования и позволяют обеспечить создание условий профессионального роста обучаемых и преподавателей.

В ходе исследования предметной области были сформированы требования к функциональным возможностям АУТК, которые позволяют определить его
компоненты:

1. Обучающий комплекс, состоящий из следующих модулей:

– модуль теоретической подготовки, предназначенный для самостоятельного изучения теоретической части курса, имеющий наполнение в виде материала теоретической направленности по настройке оборудования коммутации пакетов. Материал курса имеет последовательное изложение: от общих сведений об используемом на мобильном узле оборудовании, его начальной конфигурации до вопросов обеспечения защиты информации, циркулирующей в организуемой сети, удаленного доступа и скрытия структуры сети;

– модуль практической подготовки, для формирования навыков и умений работы с используемыми видами мультипротокольного оборудования, содержащий учебно-тренировочные карты для отработки практических вопросов настройки и эксплуатации оборудования коммутации пакетов, а также практические задания для самостоятельного выполнения. Порядок изложения практических заданий в рамках курса подготовки также упорядочен по степени усложнения ставящихся перед обучающимися задач;

– тестовый модуль, предназначенный для создания базы тестовых вопросов, оценки и закрепления полученных знаний в виде промежуточного и итогового тестирования, а также обработки и вывода результата тестирования. Представляет собой тестовый диалог с выбором одного из вариантов ответа.

2. Аппаратно-программный стенд, представляющий собой совокупность аппаратных и программных средств, предназначенных для овладения умениями и навыками работы с реальной техникой и программным обеспечением.

Структура разрабатываемого автоматизированного учебно-тренировочного комплекса представлена на рис. 1.

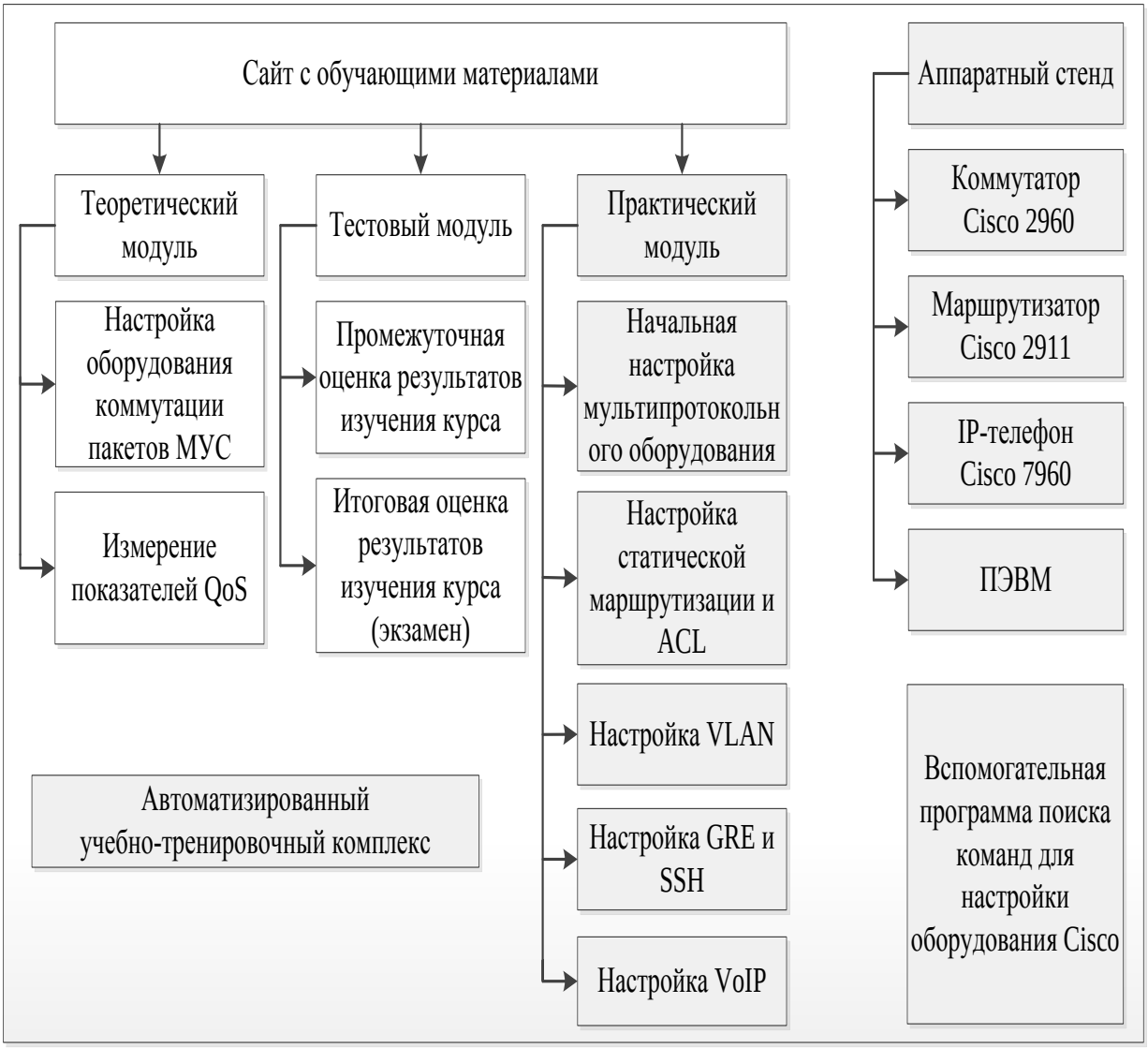

Рис. 1. Структура автоматизированного учебно-тренировочного комплекса

Разработанный автоматизированный учебно-тренировочный комплекс ориентирован на изучение принципов построения и функционирования мобильного
узла связи и отработке практических вопросов по его настройке.

Основные задачи, решаемые посредством АУТК:

– индивидуализация и интенсификация процесса обучения;

– активизация познавательной деятельности обучающихся по вопросам применения мультипротокольного оборудования для настройки мобильного узла связи;

– закрепления обучающимися своих знаний и умений;

– структурирование и визуализация содержания учебного материала с целью более эффективного его восприятия обучающимися;

– получение специальных профессионально-ориентированных знаний и навыков из области будущей профессиональной деятельности.

При реализации АУТК использованы следующие инновационные технологии:

– реализация в процессе обучения профессионально-ориентированной технологии обучения;

– применение личностно-ориентированного подхода к процессу обучения;

– использование программ автоматизированного контроля знаний обучающихся;

– организация обучения на основе полноценной реализации мультимедиа технологий представления информации;

– использование проблемных заданий, связанных с применением мобильного узла связи, для развития творческих способностей и повышения мотивации изучения вопросов настройки мультипротокольного оборудования.

В состав АУТК входят:

– комплект документации для изучения принципов построения и функционирования мобильного узла связи;

– учебно-методические материалы, в которых приведены описания тем занятий, его целей, отрабатываемые учебные вопросы, литература, а также подробное описание выполняемых практических вопросов: настройка маршрутизаторов, коммутаторов, абонентских пунктов и др.;

– учебно-тренировочный стенд для отработки практических вопросов по настройке мобильного узла связи;

– вспомогательная программа поиска команд для настройки оборудования Cisco.

Применяемые технологии обучения позволят получить положительный развивающий и воспитательный эффект. Решение в процессе обучения практических задач способствуют лучшему усвоению знаний и развитию творческих способностей обучающихся, формируют у будущих специалистов информационной безопасности четкое представление об условиях функционирования и необходимых требованиях по применению мобильного узла связи [5].

Список литературы

1. ГОСТ Р ИСО/МЭК 12207. Информационная технология. Процессы жизненного цикла программных средств.

2. Жукова, Г.С., Технологии профессионально-ориентированного обучения: учеб. пособие/ Г.С. Жукова, Н.И. Никитина, Е.В. Комарова. – М.: Издательство РГСУ, 2012. – 165 с.

3. Линевич, Л.А. Электронный учебно-методический комплекс как средство развития комплексных умений студентов / Л. А. Линевич, Барнаул, 2009.

4. Селевко, Г.К. Современные образовательные технологии: учебное пособие/Г.К. Селевко. – М.: Народное образование, 2015. – 78 с.

5. Вербицкий, А. А. Активное обучение в высшей школе: контекстный подход/А.А. Вербицкий [Текст] – М.: Высшая школа, 1991. – 208 с.

Материал поступил в редколлегию 18.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 006.4

***Мусиенко Никита Олегович**, студент каф. «Системы информационной безопасности» БГТУ*

***Шинаков Кирилл Евгеньевич,** асс. каф. «Системы информационной безопасности»*

***Банников Артур Игоревич,** студент каф. «Системы информационной безопасности»*

Брянский государственный технический университет, Брянск, Россия.

Email:musienkono@yandex.ru

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПОСТРОЕНИЯ МОДЕЛИ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ КОМБИНИРОВАННОЙ МЕТОДИКОЙ ФСТЭК И ФСБ

Описана автоматизированная система построения модели нарушителя, основанная на комбинированной методике построения модели нарушителя ФСТЭК и ФСБ.

При построении модели угроз и модели нарушителя ИС специалист сталкивается с множеством проблем: неясность в выборе методической рекомендации, отсутствие доступных и быстро действенных решений для разработки и необходимость постоянной актуализации разработанной модели.

Решить данную проблему универсальным решением невозможно, так как ИС и требования, выдвигаемые к ним. очень разнообразны, а ресурсы, которыми располагает специалист, зачастую минимальны. Поэтому оптимальным решением является декомпозиция задачи на отдельные универсальные решения. Одним из таких решений может стать новый подход к построению модели нарушителя, использующий методику построения удовлетворяющую требования ФСТЭК и ФСБ России, а также доступный интерфейс и актуальную обновляемую базу угроз.

Результатом такого решения стала разработанная автоматизированная система построения модели нарушителя безопасности на основе комбинирования методики ФСТЭК и ФСБ, представляющая собой веб-инструмент, позволяющий пользователю построить модель нарушителя на основании нормативно-правовых документов РФ в данной сфере.

На старте работы системы происходит формирование информационной базы исходных данных о системе, её физических и логических границах, компонентах и свойствах (рис.1(а)). Именно такой процесс происходит на этапе ввода сведений и условий, при которых будет строится модель нарушителя. Пользователю необходимо выбрать актуальные параметры информационной системы, для которой разрабатывается текущая модель, и обозначить условия, при которых данная модель будет эксплуатироваться. Список параметров представляет собой обобщенный перечень мер, затрудняющих реализацию атак на информационные системы, согласно методическим документам ФСТЭК и ФСБ.

Данные обоснования вкупе с выбранным потенциалом нарушителя представляют широкий анализ портрета нарушителя.

Также пользователю предстоит сделать выбор о предполагаемых возможностях нарушителя в следующей анкетной форме (рис.1(б)). Данная анкета представляет собой перечень обобщенных возможностей нарушителя, основанный на методических документах ФСТЭК и ФСБ. Такой список соответствует представлению ФСБ о возможностях нарушителя, но при разработке методики было определено, что представления ФСЭК о потенциале нарушителя смежные по значению. Таким образом, происходит сбор данных о возможностях нарушителя, анализ которых в дальнейшем помогает при построении модели нарушителя.

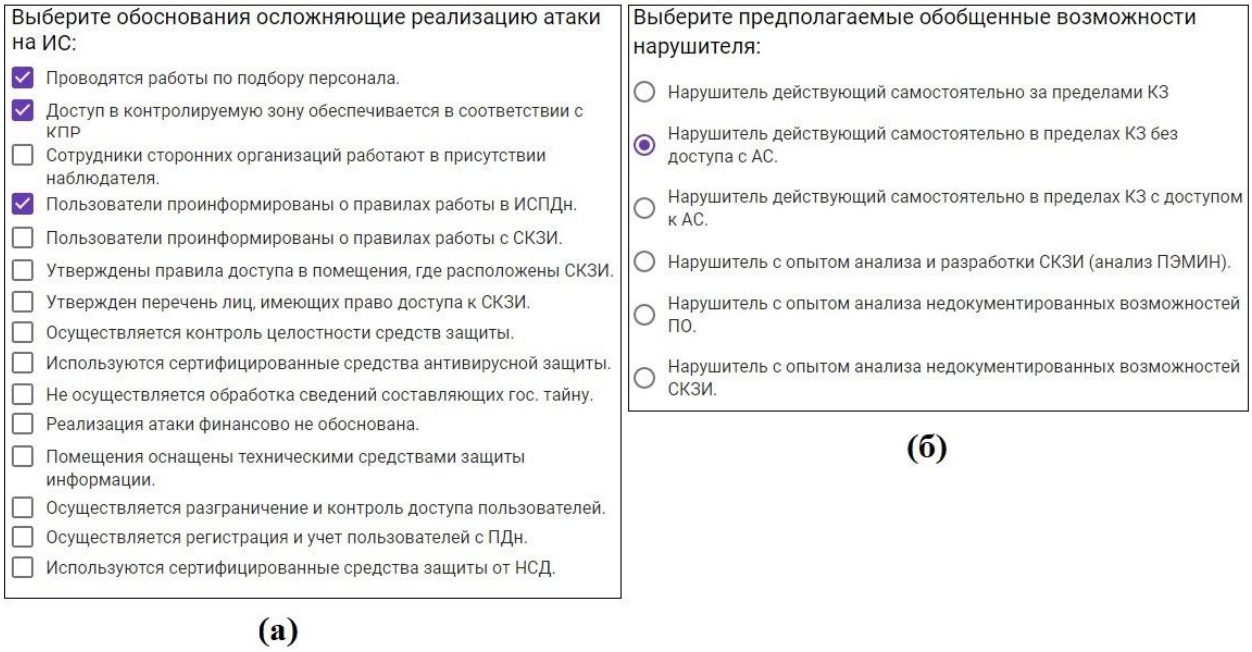

Рис. 1. Анкета о предполагаемых возможностях нарушителя

После определения возможностей нарушителя пользователю предлагается заполнить следующую анкетную форму (рис.2(а)), в которой рассматривается предположение о возможности сговора среди предполагаемых нарушителей информационной безопасности. Пользователю необходимо подтвердить или отклонить такое предположение. В зависимости от результата выбора автоматизированная система производит построение предполагаемых связей между потенциальными нарушителями и анализирует возможные схемы сговора, затем вводит полученные данные в общую модель нарушителя.

Последним этапом ввода данных для построения модели нарушителя станет анкетная форма (рис.2(б)), в которой пользователю предлагают определить аппаратно-технический состав обеспечительных мер безопасности в информационной системе.

Пользователь принимает решение о необходимости применения криптографических средств защиты информации в информационной системе. В зави-

симости от результата автоматизированная система построения модели нарушителя, на основе собранных данных подготовляет пакет документов, в котором в виде таблиц представлена соответствующая информационной системе модель нарушителя информационной безопасности.

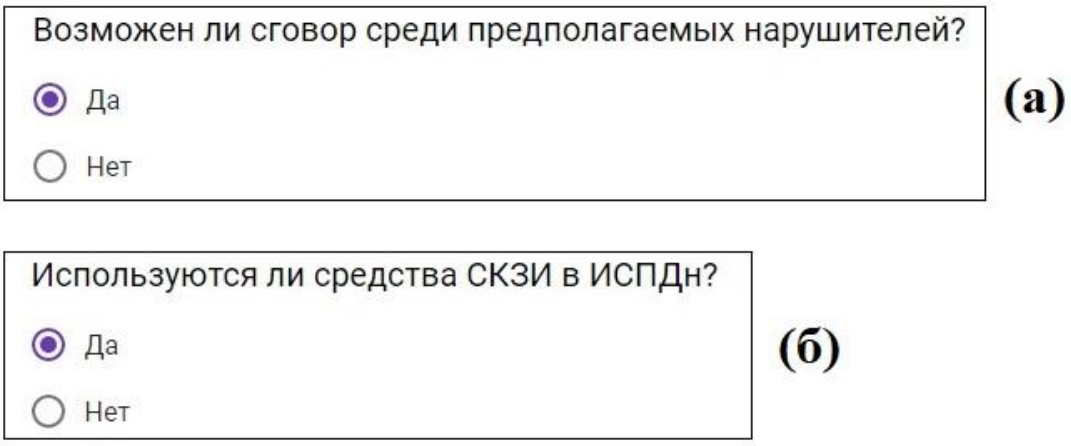

Рис. 2. Анкета

После заполнения всех анкетных форм для получения готовой модели нарушителя пользователю предоставляется возможность скачать готовую модель.Скачанный пакет документов представляет собой файл в формате XML (рис.3), в котором в виде таблиц представлена разработанная модель нарушителя информационной безопасности.

	A	B	C	D	E	F
1	Модель нарушителя информационной безопасности					
2	№	Тип нарушителя	Вид нарушителя	Потенциал нарушителя	Цели нарушителя	Возможные способы реализации угрозы
3	1	Внешний	Террористические, экстремистские группировки;	Средний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Совершение террористических актов. Идеологические или политические мотивы. Дестабилизация деятельности органов государственной власти, организаций.	• Воздействия на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия).
4	2	Внешний	Преступные группы (криминальные структуры);	Средний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды.	• Несанкционированного физического доступа и (или) воздействия на линии, (каналы) связи, технические средства, машинные носители информации;
5	3	Внешний	Конкурирующие организации;	Низкий	Идеологические или политические мотивы. Причинение имущественного ущерба путем мошенничества или иным преступным путем.	• Воздействия на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал.
6	4	Внешний	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ;	Средний	Получение конкурентных преимуществ. Причинение имущественного ущерба путем обмана или злоупотребления доверием.	• Воздействия на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия).

Рис. 3. Модель нарушителя информационной безопасности

В итоге пользователю предоставляется персонализированная модель нарушителя информационной безопасности, представляющая собой пакет таблиц,

в которые записываются характеристики, полученные при построении модели нарушителя. Состав пакета варьируется в зависимости от условий, которые были выдвинуты пользователем на этапе ввода исходных данных об информационной системе.

Модель разработана с учетом всех необходимых требований со стороны ФСТЭК и ФСБ и в дальнейшем может быть использована как часть общей модели угроз.

Материал поступил в редколлегию 11.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 681.324

***Мысютин Алексей Петрович**, к.т.н., доцент*
каф. «Высшая математика» БГТУ
ФГБОУ ВО «Брянский государственный технический университет», Брянск, Россия
e-mail: map@tu-bryansk.ru

ИМИТАЦИОННЫЙ ПОДХОД К МОДЕЛИРОВАНИЮ ПРОЦЕССА ЗАЩИТЫ ИНФОРМАЦИИ

Рассмотрена имитационная модель системы защиты информации от несанкционированного доступа, представляющая собой систему массового обслуживания. Для ее описания использована система имитационного моделирования общего назначения GPSS. Приведены результаты численных экспериментов с моделью.

Основным методом изучения систем защиты информации является моделирование. Оно предусматривает разработку модели и ее анализ. В модели учитываются существенные для решаемой задачи компоненты, взаимосвязи и свойства исследуемого объекта. Различают вербальные, физические и математические модели и соответствующее моделирование.

По мере развития вычислительной математики и техники расширяется сфера применения математического моделирования. Математическое моделирование предусматривает создание и исследование математических моделей реальных объектов и процессов. Математические модели могут разрабатываться в виде аналитических зависимостей выходных параметров системы от входных, уравнений для моделирования динамических процессов в системе, статистических характеристик реакций системы на воздействия случайных факторов. Математическое моделирование позволяет наиболее экономно и глубоко исследовать сложные объекты, чего нельзя добиться с помощью вербального моделирования или что чрезмерно дорого при физическом моделировании. Возможности математического моделирования ограничиваются уровнем формализации описания объекта и степенью адекватности.

Для моделирования сложных систем все шире и шире применяется метод математического моделирования, называемый имитационным моделированием [1-2]. Оно предполагает определение реакции модели системы на внешние воздействия, которые генерирует ЭВМ в виде случайных чисел. Статистические характеристики этих случайных чисел должны с приемлемой точностью соответствовать характеристикам реальных воздействий. Функционирование системы при случайных внешних воздействиях описывается в виде алгоритма действий системы и их характеристик в ответ на каждое воздействие на входе. Таким образом, имитируется работа сложной системы в реальных условиях. Путем статистической обработки выходных результатов при достаточно большой

выборке входных воздействий получаются достоверные оценки работы системы. Так, достаточно объективная оценка эффективности системы защиты информации при многообразии действий злоумышленников, которые с точки зрения службы безопасности носят случайный характер, возможна на основе имитационного моделирования системы защиты.

В статье система защиты информации представлена n-канальной системой массового обслуживания, на вход которой подается m потоков угроз. Угрозы j-го потока распределяются между каналами с вероятностями q_{ii} (i=1,2,…,n; j=1,2. …, m). Канал i обслуживания обеспечивает с вероятностью p_{ij} защиту от угрозы j-го типа, используя соответствующий защитный механизм. Поток угроз j-го типа характеризуется интенсивностью λ_j или средним значением τ_j времени между моментами поступления угроз. Время θ_j нейтрализации угрозы j-го типа рассматривается как случайная величина, распределенная по некоторому закону. На выходе системы защиты информации образуются два выходных потока (нейтрализованных и активных угроз), являющиеся объединением выходных потоков n каналов обслуживания. Выходной поток активных угроз направляется на повторное обслуживание, которое осуществляется наименее загруженными каналами.

Для описания моделей систем массового обслуживания разработаны специальные языки и системы имитационного моделирования. Существуют общецелевые языки, ориентированные на описание широкого класса систем массового обслуживания в различных предметных областях, и специализированные языки, предназначенные для анализа систем определенного типа. Примером общецелевых языков служит широко распространенный язык GPSS World (General purpose simulation system).

Имитационная модель, построенная при помощи подобных систем, состоит из набора операторов (блоков), выполняющих необходимые действия или задержки динамических элементов (транзактов), которые последовательно проходят через блоки. Так, блок GENERATE в системе GPSS World создает новые транзакты, генерируя поток заявок (требований на обслуживание) с заданным распределением интервалов между ними. Система GPSS World имеет с своем арсенале ряд блоков, позволяющих имитировать работу каналов обслуживания , собирать информацию об очередях, создавать и уничтожать транзакты, организовывать условные ветвления и изменять маршруты движения транзактов в модели. Транзакты перемещаются в модельных времени и пространстве, двигаясь от одного блока модели к другому. Транзакты могут расщепляться, объединяться и синхронизировать свое движение в модели. Входя в блок, транзакт оказывает на блок и испытывает со стороны блока определенное воздействие в зависимости от подпрограммы, которую выполняет этот блок. Движение тракзакта в модели продолжается до тех пор, пока блок TERMINATE не удалит его из модели.

Имитационная модель системы массового обслуживания представляет собой программу, отражающую поведение системы во времени при заданных

потоках заявок, поступающих на вход системы. Входные потоки заявок определяют внешние параметры системы массового обслуживания. Характеристики выходных потоков отражают свойства функционирования системы и являются ее выходными параметрами. В качестве выходных параметров можно рассматривать производительность системы массового обслуживания, коэффициенты загрузки каналов, среднее время обслуживания заявок, среднюю длину очередей и т.д.

Имитационное моделирование позволяет исследовать системы массового обслуживания при различных типах входных потоков и интенсивностях поступления заявок и варьировании параметров обслуживающих каналов. В моделях систем массового обслуживания заявки, приходящие на вход занятого канала, образуют очереди. При освобождении канала на обслуживание принимается заявка из непустой очереди. Для построения имитационной модели системы защиты информации при помощи имитационного моделирования необходимо соотнести структурные элементы исходной модели с заменяющими их блоками GPSS World.

В предложенной модели для определения вероятности направления угрозы j-го типа на i-й канал обслуживания, времени нейтрализации угрозы j-го типа i-м каналом и вероятности защиты от угрозы j-го типа с помощью i-го канала используются дискретные функции, аргументами которых являются либо встроенные датчики случайных чисел с равномерным распределением в интервале (0;1), либо параметры транзактов, реальными аналогами которых выступают угрозы. Подобная функция применяется и для организации повторного обслуживания угроз, которые не удалось нейтрализовать на первом этапе. Для определения наименее загруженного канала пронумеровываются с помощью команды EQU все каналы обслуживания.

Появление угроз моделируется с помощью m блоков GENERATE. Время между моментами появления угроз в каждом из m потоков есть непрерывная случайная величина. Выбор закона распределения случайной величины остается за пользователем. Отметим только, что система GPSS World обладает большим набором встроенных вероятностных распределений. Для определенности в модели реализован экспоненциальный закон.

Обслуживание (нейтрализация) угроз моделируется n блоками ADVANCE. Время обслуживания является операндом этого блока и может представлять собой положительное число или ссылку на встроенное вероятностное распределение с соответствующими параметрами. После обслуживания выполняется с помощью блока TRANSFER, работающем в статистическом режиме, розыгрыш ситуации, связанной с проверкой эффективности защиты. В модели также использовались блоки TRANSFER, работающие в безусловном и функциональном режимах.

С каждой угрозой (транзактом) связаны два параметра. В первом содержится указатель типа угрозы, во втором – число попыток нейтрализовать угрозу. Если второй параметр транзакта равен единице и этот транзакт

имитирует угрозу, которую не удалось нейтрализовать, он будет направлен с помощью блока SELECT на повторное обслуживание каналом с наименьшим коэффициентом использования.

По модели был выполнен ряд прогонов с конкретными числовыми значениями входных параметров. Число каналов равнялось 4, число потоков угроз – 5. Для равномерной загрузки каналов было принято, что для всех i $\sum_{j=1}^{5} q_{ij} = 1{,}25$. Из условия задачи следовало, что для всех j $\sum_{i=1}^{4} q_{ij} = 1$. Все вероятности p_{ij} взяты из отрезка [0,91;0,99], причем для всех i $(1/5)\sum_{j=1}^{5} p_{ij} = 0{,}95$ и для всех j $(1/4)\sum_{i=1}^{4} p_{ij} = 0{,}95$. В расчетах было принято, что время θ_j нейтрализации угрозы j-го типа есть случайная величина, распределенная по равномерному закону в интервале (k; τ_i–k), где k – положительное число, меньшее половины любого из τ_i. Моделирование проводилось по времени (как вариант можно рассмотреть случай моделирования по числу угроз, прошедших через систему защиты информации), поэтому в модели присутствовал сегмент таймера.

Расчеты показали, что при различных k процент угроз, которые не удалось нейтрализовать не превосходит 0,3. После первого этапа обслуживания остаются активными примерно 5% угроз. Из-за высокой скорости нейтрализации угроз (в среднем она в два раза выше интенсивности потока угроз того или иного типа) коэффициент использования каналов обслуживания – доля времени моделирования, в течение которого канал был занят – находится в пределах 63-69%.

Список литературы

1.Бабаш, А.В. Актуальные вопросы защиты информации: монография / А.В. Бабаш, Е.К. Баранова. – М.: РИОР ИНФРА-М, 2017. – 111 с.

2.Григорьев, В.А. Имитационная модель системы защиты информации / В.А. Григорьев, А.В. Карпов // Программные продукты и системы. – 2005. – №2. – С. 26-30.

Материал поступил в редколлегию 20.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 005.007

***Проничева Екатерина Александровна**, магистрант каф. «Системы информационной безопасности»*
***Лузик Сергей Викторович**, студент каф. «Системы информационной безопасности»*
ФГБОУ ВО «Брянский Государственный Технический Университет», Брянск, Россия
e-mail: katya.pronicheva@mail.ru

РАЗРАБОТКА МЕТОДИКИ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Описана методика реагирования на инциденты информационной безопасности, а также разработан алгоритм работы по обозначенной методике.

В ходе выполнения работы был проведен анализ руководящих документов ФСТЭК России, а также изучен «Банк данных угроз безопасности информации», на основании которых необходимо формировать методы реагирования на инциденты ИБ. Также был проведен анализ существующих методов реагирования и существующих программных продуктов по формированию рекомендация по защите информации. Были разработаны методики реагирования на инциденты информационный безопасности, а также предложены меры и средства защиты в соответствии с руководящими документами ФСТЭК России.

Основные этапы методики реагирования на инциденты ИБ:

1. Подготовка. Для эффективного реагирования необходима предварительная подготовка. Сотрудники, ответственные за ИБ, должны обеспечить защиту ИС и проинформировать пользователей, а также ИТ-персонал, о важности мер по обеспечению ИБ.
2. Обнаружение. Сотрудники, занимающиеся реагированием на инциденты, должны определить, является ли обнаруженное ими с помощью различных систем обеспечения ИБ событие инцидентом ИБ. Для этого могут использоваться публичные отчеты, потоки данных об угрозах, средства статического и динамического анализа образцов ПО.
3. Сдерживание. Сотрудники, ответственные за ИБ, должны идентифицировать скомпрометированные компьютеры и настроить правила безопасности таким образом, чтобы заражение не распространилось дальше по сети. Кроме того, на этом этапе необходимо перенастроить сеть таким образом, чтобы ИС могла продолжать работать без зараженных машин.
4. Удаление. Цель этого этапа – привести скомпрометированную ИС в состояние, в котором она была до заражения. Сотрудники, ответственные за ИБ, удаляют вредоносное ПО, а также все артефакты, которые оно могло оставить на зараженных компьютерах в ИС.
5. Восстановление. Ранее скомпрометированные компьютеры вводятся обратно в сеть. При этом сотрудники, ответственные за ИБ, некоторое время

продолжают наблюдать за состоянием этих машин и ИС в целом, чтобы убедиться в полном устранении угрозы.

6. Выводы. Сотрудники, ответственные за ИБ, анализируют произошедший инцидент, вносят необходимые изменения в конфигурацию ПО и оборудования, обеспечивающего ИБ, и формируют рекомендации для того, чтобы в будущем предотвратить подобные инциденты.

На основании описанных этапов сформируем алгоритм методики реагирования на инциденты информационной безопасности (рис.1).

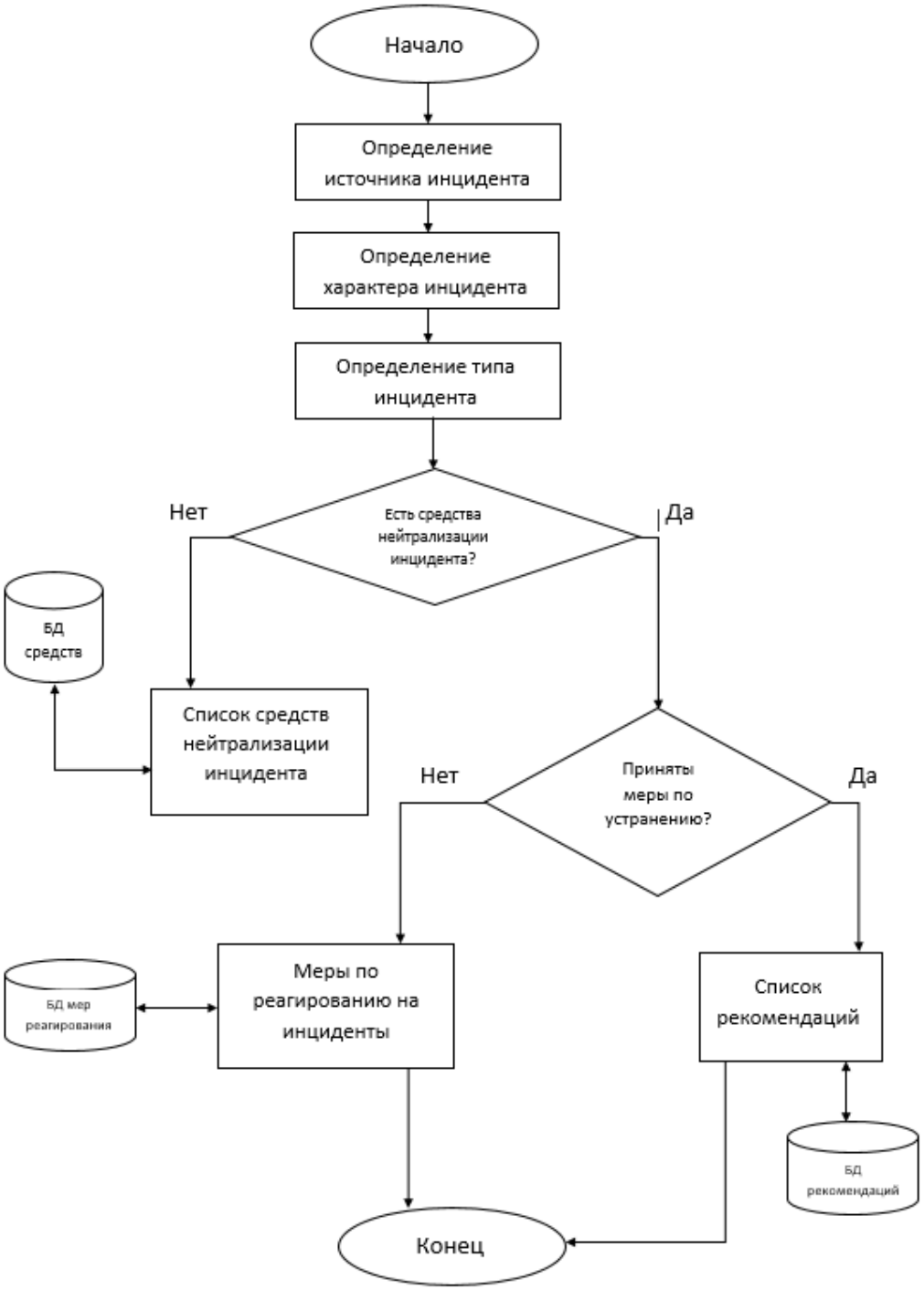

Рис.1. Алгоритм методики реагирования на инциденты ИБ

Результатом работы стал рабочий алгоритм методики реагирования на инциденты ИБ, позволяющий подобрать необходимые средства для устранения и/или предотвращения инцидентов ИБ на предприятии.

Материал поступил в редколлегию 22.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.56

***Рытов Михаил Юрьевич**, к.т.н., доцент, зав. каф. «Системы информационной безопасности» БГТУ*
***Горлов Алексей Петрович**, к.т.н., доцент кафедры «Системы информационной безопасности» БГТУ*
***Воронин Владимир Александрович**, старший преподаватель кафедры «Системы информационной безопасности» БГТУ*
***Лысов Дмитрий Андреевич**, студент кафедры «Системы информационной безопасности» БГТУ*
ФГБОУ ВО «Брянский государственный технический университет», Брянск, Россия
e-mail: lysovdmitriia@gmail.com

ОЦЕНКА УРОВНЯ ИСХОДНОЙ ЗАЩИЩЕННОСТИ КОММЕРЧЕСКИХ ОРГАНИЗАЦИЙ

Поднимается вопрос оценки уровня исходной защищенности объектов защищенности коммерческих организаций. Предложен подход к оценке уровня исходной защищенности.

В современных условиях развития информационных технологий и их глубокой интеграции в жизнь людей информация стала товаром, который можно не только приобрести, продать, обменять, но и получить к ней несанкционированный доступ, внести изменения и даже удалить. В связи с этим стоимость информации зачастую в десятки раз превосходит стоимость аппаратной части, на которой она хранится. От степени безопасности информационных систем, в наше время, зависит благополучие, а порой и жизнь многих людей.

Проектирование и внедрение программно-аппаратной защиты информации на объекте является достаточно ресурсозатратной процедурой. К тому же, в нормативно-правовых документах по созданию систем защиты указывается только необходимость наличия определенных средств защиты, но не предусматривается динамическое изменение воздействия угроз. Дополнительно усложняет задачу отсутствие хорошо зарекомендовавших себя критериев оценки эффективности систем защиты информации.

Программно-аппаратная защита применяется для защиты программного обеспечения от несанкционированного доступа и использования. Структура программно-аппаратной защиты информации представлена на рисунке 1.

Некоторые компоненты программно-аппаратной защиты информации могут быть представлены как в аппаратном, так и в программном виде.

Опыт создания таких систем показывает, что на выбор конкретных решений влияют, в первую очередь, такие факторы как стоимость и шаблонность мышления отдельных разработчиков. При этом не проводится оценка эффективности принимаемых проектных решений.

Дополнительно усложняет задачу разработки ПАЗИ возможная несовместимость аппаратных продуктов, или конфликт отдельных программных и аппаратных решений на разных уровнях.

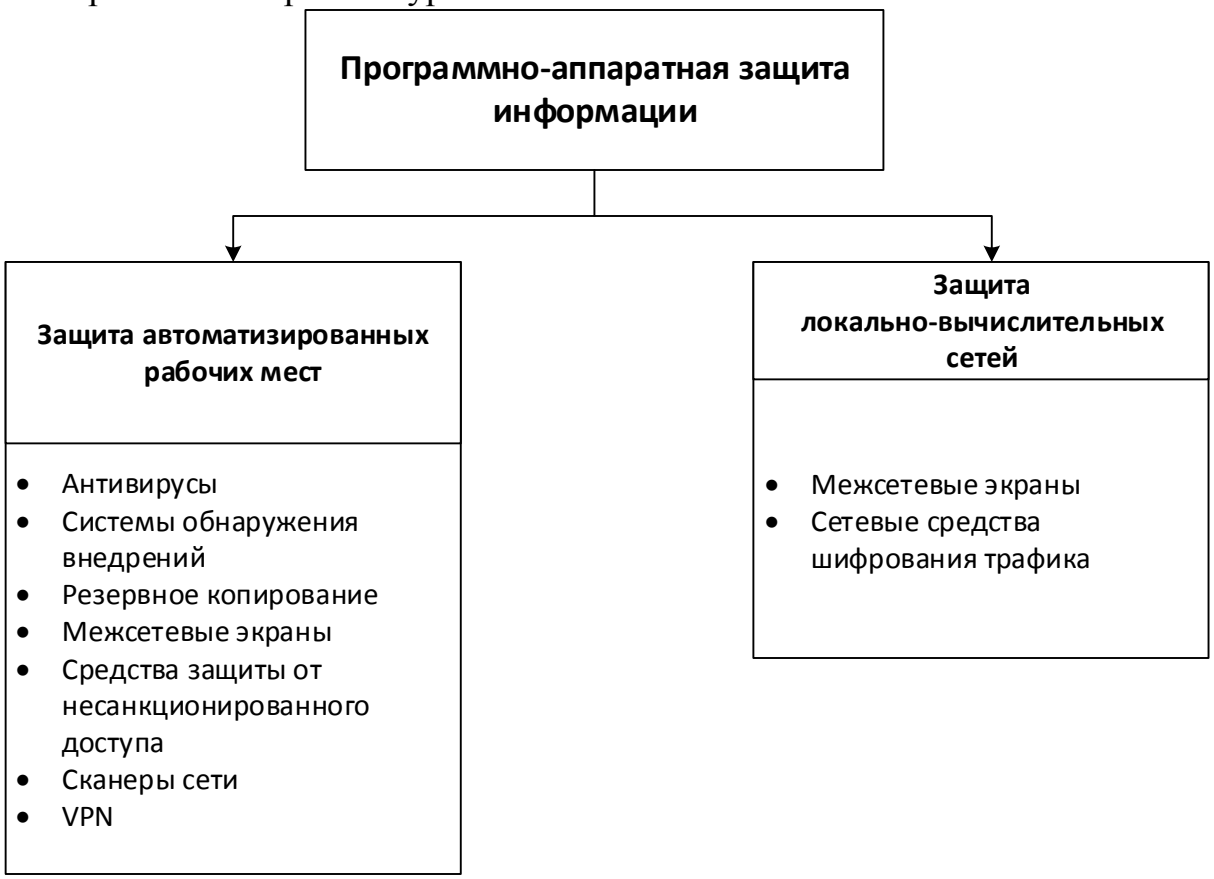

Рис. 1.Структура программно-аппаратной защиты информации

Таким образом, основные проблемы проектирования ПАЗИ:

1. Высокая стоимость и продолжительность процесса разработки
2. Высокая трудоемкость, связанная с выработкой конкретных проектных решений
3. Практический подход не подразумевает оценки эффективности и анализа возможной несовместимости продуктов

Для решения поставленных задач целесообразно разработать автоматизированную систему выбора средств ПАЗИ.

На первом этапе разработки новых систем защиты информации производится оценка уровня исходной защищенности объекта. Основной задачей данного этапа является выявление имеющихся на объекте программно-аппаратных решений, обеспечивающих безопасную обработку информации. Алгоритм оценки уровня исходной защищенности представлен на рис. 2.

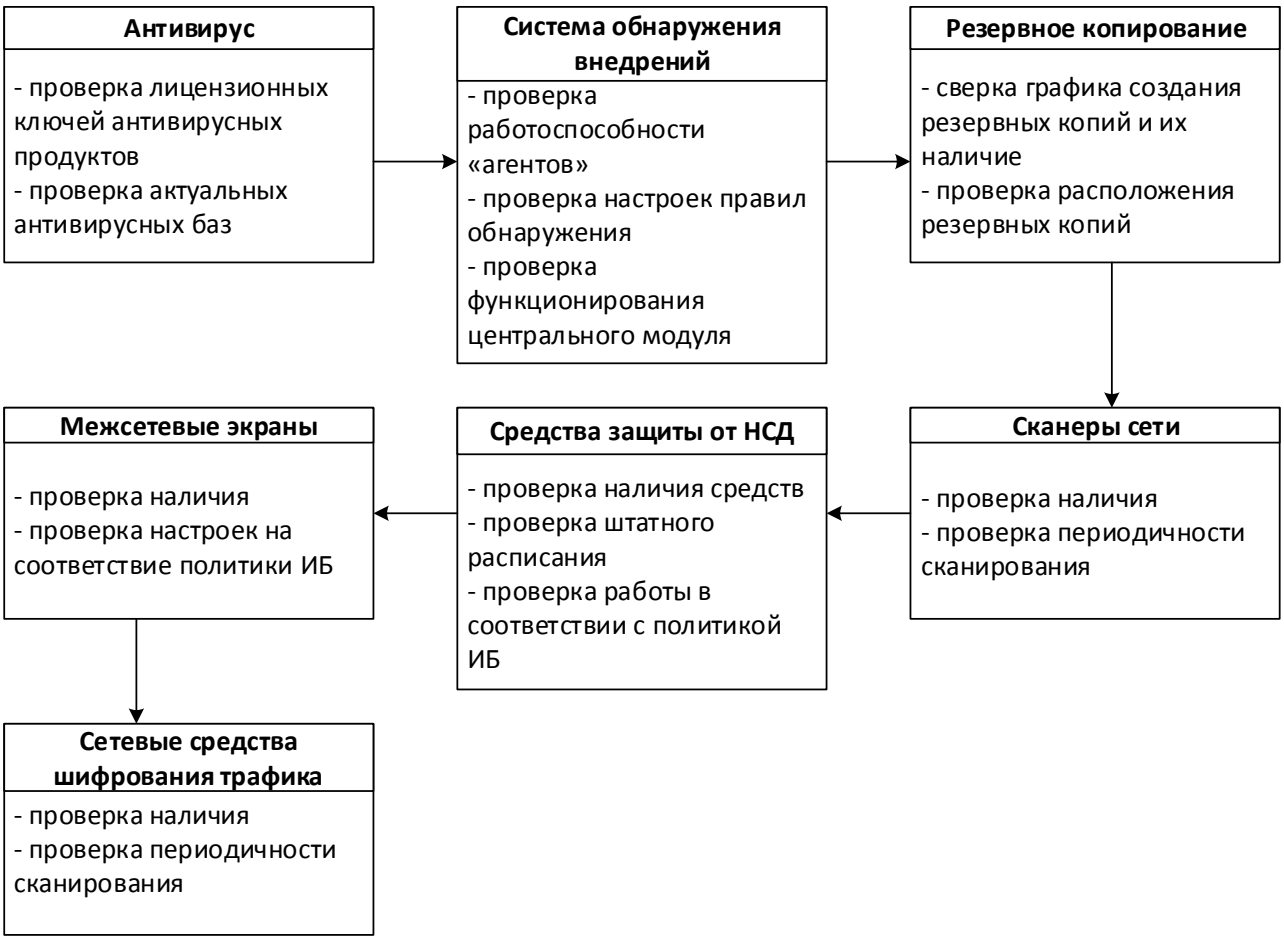

Рис.2. Алгоритм оценки уровня исходной защищенности

Предлагаемый подход к оценке уровня исходной защищенности позволяет выявить имеющиеся актуальные решения по защите информации, определить режимы их работы и возможность дальнейшего использования вследствие чего становится возможным сокращение временных и материальных затрат на доработку программно-аппаратной системы защиты информации.

Материал поступил в редколлегию 17.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 006.4

Рытов Михаил Юрьевич, *к.т.н., доцент, зав. каф. «Системы информационной безопасности» БГТУ*

Аверченков Владимир Иванович, *д.т.н.. профессор каф. «Системы информационной безопасности» БГТУ*

Брянский государственный технический университет, Брянск, Россия

e-mail: rmy@tu-bryansk.ru

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В БРЯНСКОЙ ОБЛАСТИ

Рассмотрены нормативно-правовые акты, регламентирующие защиту персональных данных, и определены основные проблемы, возникающие при обеспечении их защиты в Брянской области.

В настоящий момент правовая основа механизма защиты персональных данных стала приобретать ясные очертания, формируясь по двум направлениям: специализированное законодательство и иное смежное законодательство, которое лишь частично содержит правовые нормы, гарантирующие неприкосновенность частной жизни и регулирующие сферу защиты персональных данных. К специализированному законодательству относятся такие правовые акты, как Федеральный закон № 152-ФЗ «О персональных данных» от 27 июля 2006 г., Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и защите информации» от 27 июля 2006 г., закрепляющий принцип неприкосновенности частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия (статья 3), Указ Президента РФ от 6 марта 1997 г. №188, утверждающий «Перечень сведений конфиденциального характера», и другие.

Правовые нормы, регулирующие работу с персональными данными, содержатся в Законе N 125-ФЗ «Об архивном деле в Российской Федерации» от 22 октября 2004 г. (ст.25), в Законе № 144- ФЗ «Об оперативно-розыскной деятельности» (ст. 3, 5, 9, 10, 12, 21) от 12 августа 1995 г., в Законе № 2124-I «О средствах массовой информации» от 27 декабря 1991 г. (ст. 41, 43, 46, 51, 57), Законе № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе государственного пенсионного страхования» от 1 апреля 1996 г., в соответствии с которым персональные данные содержатся в индивидуальном лицевом счете застрахованного лица, нормы о защите сведений, полученных в ходе всероссийской переписи населения (персональные данные), содержатся в Законе № 8-ФЗ «О всероссийской переписи населения» от 25 января 2002 г. В соответствии со статьей 84 Налогового кодекса РФ при постановке на учет физических лиц в состав сведений об указанных лицах включаются также их персональные данные.

Обеспечение технической защиты персональных данных регламентируется следующими основными документами: Федеральным законом №128-ФЗ от 08.08.01 г, «О лицензировании отдельных видов деятельности»; Постановлением Правительства РФ №45 от 26.01.06 г. «Об организации лицензирования отдельных видов деятельности»; Постановлением Правительства РФ №504 от 15.08.06 г. «О лицензировании деятельности по технической защите конфиденциальной информации»; «Положением о государственном лицензировании деятельности в области защиты информации», решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации №10 от 27.04.94 г.; «Положением по аттестации объектов информатизации по требованиям безопасности информации», утвержденным председателем Государственной технической комиссии при Президенте РФ 25.11.94 г., документами ФСБ и ФСТЭК России по обеспечению безопасности конфиденциальной информации.

Несмотря на достаточное количество специализированных законодательных актов в области защиты персональных данных, в России создана достаточно проработанная смежная нормативно-правовая база. К таким документам можно отнести:

- Федеральный закон №5341-1 от 07.07.93 г. «Об архивном фонде Российской Федерации и архивах»;
- Федеральный закон №25-ФЗ от 02.03.07 г. «О муниципальной службе в Российской Федерации»;
- Материалы Минэкономразвития России «О создании системы персонального учета населения Российской Федерации»;
- Распоряжение Правительства Российской Федерации №748-р от 09.06.05 г. «Концепция создания системы персонального учета населения Российской Федерации»;
- Указ Президента Российской Федерации №320 от 12.03.07 г. «О Федеральной службе по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия»;
- Постановление Правительства Российской Федерации №419 от 02.06.08 г. «Об утверждении положения о Федеральной службе по надзору в сфере связи и массовых коммуникаций».

Среди многообразия задач обеспечения информационной безопасности Российской Федерации и нашего региона, в частности, острой проблемой, требующей безотлагательного решения, является обеспечение защиты персональных данных в соответствии с требованиями ФЗ № 152 «О персональных данных». В силу неподготовленности организаций нашей страны к защите персональных данных действия ФЗ № 152 перенесено на год. В соответствии с требованиями ФЗ № 152 «О персональных данных» защита персональных данных должна осуществляться путем создания специализированных систем защиты ИСПДн. Система защиты ИСПДн включает ряд направлений организационного

и организационно-технического характера. Реализация этих направлений достаточно подробно регламентируется нормативно-правовыми документами Российской Федерации, требованиями ФСТЭК России и рядом документов ведомственной принадлежности. Однако, реализация закона ФЗ № 152 «О персональных данных» в организациях нашего региона проходит не достаточно активно и массово.

Анализируя опыт работы, полученный сотрудниками кафедры «СИБ» при проведении научно-исследовательских работ по информационной безопасности в интересах Брянской области и защиты персональных данных в организациях региона, необходимо заметить, что основными проблемами реализации требований ФЗ № 152 «О персональных данных» в Брянской области, по нашему мнению, являются:

1. Низкая правовая грамотность как собственников, так и операторов персональных данных.
2. Халатное отношение собственников к своим персональным данным и документам в частности.
3. Неподготовленность правовой базы по защите персональных данных к реализации её на практике
4. Непонимание важности защиты персональных данных рядом операторов и отсутствие финансирования работ по защите персональных данных в таких организациях
5. Недостаток специалистов и организаций, способных грамотно решать задачи защиты персональных данных.

Очевидно, что только комплексное решение данных проблем позволит точно в срок обеспечить защиту персональных данных в нашем регионе.

Материал поступил в редколлегию 23.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.7

***Рытов Михаил Юрьевич**, к.т.н., заведующий каф. «Системы информационной безопасности» БГТУ*

***Калашников Руслан Юрьевич**, аспирант каф. «Системы информационной безопасности» БГТУ*

Брянский государственный технический университет, Брянск, Россия

e-mail: human033@gmail.com

ПРОБЛЕМЫ ВНЕДРЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТАХ АСУ ТП КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ

Рассмотрены уязвимости и угрозы ИБ, характерные для критически важной инфраструктуры. Определены направления развития систем защиты информации промышленного объекта.

Термин АСУ ТП включает в себя группу технологий автоматизации процессов, таких как системы диспетчерского контроля и сбора данных (SCADA) и распределенные системы управления (DCS), которые, к сожалению, подвергаются все большему числу атак в последние годы. Поскольку они обеспечивают жизненно важные услуги для критической инфраструктуры, такие как связь, производство и энергетика, инциденты ИБ на таких объектах представляют собой серьезную угрозу для национальной безопасности государства.

АСУ ТП обладают повышенными требованиями к производительности и надежности и, как правило, используют специфичные операционные системы и протоколы. Эти требования, прежде всего, отдают приоритет доступности и целостности, а лишь потом конфиденциальности.

Недоступность критической инфраструктуры (например, электроэнергии, транспорта) может иметь экономические последствия, многократно превышающие прямой и физический ущерб. Эти последствия могут негативно повлиять на местную, региональную, национальную или даже глобальную экономику.

Несмотря на очевидный риск для критической инфраструктуры, безопасность АСУ ТП не является приоритетной областью для инвестиций в структуру предприятия. Зачастую затраты, связанные с безопасностью АСУ ТП, являются запретительными, особенно в критических системах, когда воспринимаемые риски для организации или инфраструктуры не могут быть адекватно оценены. Как правило, следствием этого являются недостаточные возможности для своевременного реагирования на инциденты в развернутой операционной системе АСУ ТП. Ещё одним фактором, усложняющим разработку СЗИ для АСУ ТП, является то, что эта система сочетает в себе крупномасштабные, географически распределенные, устаревшие и запатентованные системные компоненты.

Раньше АСУ ТП функционировали как изолированные сети, не связанные с инфраструктурой связи общего пользования, но по мере того, как предприятия внедряли в эксплуатацию сервисы и данные, предоставляемые через Интернет, такая изоляция уменьшилась. Преимущества, обеспечиваемые мониторингом в реальном времени, P2P соединениями и резервированием, позволили повысить качество услуг, предоставляемых потребителям. Такая взаимосвязь только возрастает с развитием интеллектуальных сетей электроснабжения и интернета вещей. Следовательно, ранее изолированные системы становятся все более подверженными целому ряду угроз.

В связи с большой зависимостью сетей АСУ ТП от внешних соединений, безопасность стоит на повестке дня. Более того, коммуникация внутри них через общую инфраструктуру IP порождает ряд проблем, связанных с внедрением систем защиты в АСУ ТП, таких как:

- требование к повышенной надежности системы регулярно превалирует над угрозами безопасности и может привести к уязвимостям.
- отсутствие шифрования в ранних промышленных протоколах связи (часто используется открытый текст).
- общедоступные и повсеместно используемые протоколы и аппаратные средства могут быть целью для эксплуатации уязвимостей нулевого дня. Хотя использование открытых решений не является брешью в безопасности, атаки на них могут быть проще в реализации.
- работа АСУ ТП зачастую должна быть непрерывна, что затрудняет установку обновлений, исправление или изменение компонентов системы.
- срок жизни современных систем АСУ ТП больше, чем в прошлом, а это означает, что аппаратное и программное обеспечение работают за дольше, чем длится их поддержка.

Эти ограничения в отношении АСУ ТП означают, что проектирование системы безопасности должно основываться на знаниях конкретной системы автоматизации и предполагаемой операционной среде, то есть на знаниях промышленных производственных процессов.

Не рекомендуется использовать встроенные механизмы безопасности или инструменты безопасности на уровне хоста (например, антивирус) из-за возможного воздействия на задержку или появления отдельных точек отказа вдоль пути связи. Кроме того, учитывая растущую сложность атак, средства защиты сети больше не могут зависеть от алгоритмов обнаружения на основе шаблонов. Требуется использование механизмов, которые отслеживают скрытые угрозы и обеспечивают подходящий баланс между уровнем обслуживания и обнаружения.

Как пример, распространение червя STUXNET прекрасно отражает слабость систем регулирования, предназначенных для управления критическими инфраструктурами. STUXNET, впервые выделенный в середине июня 2010 года, был компьютерным вирусом, специально разработанным для атаки на промышленные компьютеры под управлением Windows и управляющим програм-

мируемым логическим контроллером (ПЛК), влияющим на поведение удаленных приводов. Парадокс заключается в том, что критические инфраструктуры широко используют новейшие взаимосвязанные (и уязвимые) технологии информационно-коммуникационных технологий, в то время как оборудование управления, как правило, является старым, устаревшим программным и аппаратным обеспечением. Такое сочетание факторов может привести к опасным ситуациям, подвергая системы воздействию самых разных атак.

Применяемые сегодня средства защиты АСУ ТП, как правило, не учитывают, что злоумышленники в конечном итоге могут получить доступ к тому, что защищено периметром. В связи с этим одной из основных задач современных решений в области безопасности промышленного объекта является разработка методов, которые могли бы выявлять и пресекать деятельность злоумышленников после того, как они получили доступ в системе. Важно, при этом, уделять внимание внедрению новых стратегий, которые могут выявлять, предотвращать и смягчать атаки на фильтрацию данных, поскольку стратегии обнаружения/предотвращения вторжений в настоящее время считаются неадекватными для защиты данных.

Таким образом, синергия информационных и программных технологий с классическими промышленными процессами породила новые проблемы безопасности. Основные направления по разработке средств защиты АСУ ТП в первую очередь должны сосредоточиться на балансе подходов, которые могут предотвратить широкий спектр атак, идентификации злоумышленников в режиме реального времени с высокой точностью и решений, которые налагают небольшие накладные расходы на связь и производительность АСУ ТП.

Материал поступил в редколлегию 23.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 006.4

Рытов Михаил Юрьевич, *к.т.н., доц., зав. каф. «Системы информационной безопасности» БГТУ*

Луценко Игорь Владимирович*, аспирант каф. «Системы информационной безопасности» БГТУ*

Брянский государственный технический университет, Брянск, Россия

e-mail: eropa@live.ru

РЕАЛИЗАЦИЯ СИСТЕМЫ ПРОЕКТИРОВАНИЯ ЗАЩИТЫ ДАННЫХ ДЛЯ МАЛОГО ПРЕДПРИЯТИЯ

Рассматривается проблемы проектирования системы защиты данных для малого предприятия. Чтобы проектировать быстро и качественно, используют различные программы и сервисы. Для вычисления используют различные модели. В статье рассматривается система на основе модели «Полного перекрытия».

Согласно данным учебно-методических объединений, у которых основная задача – подготовка специалистов по информационной безопасности, в настоящее время специалистов «Информационная безопасность» готовят более 150 вузов, примерно суммарное количество выпускников 5000 абитуриентов, которые заканчивают обучение каждый год. Приблизительная потребность специалистов около 7000 человек в год. Как показывает статистика, что большая половина выпускников остается работать в отрасли. Из этого следует, что компании не могут перекрыть свою потребность [3].

Чтобы как-то исключить кадровый голод, приходится искать специалистов из смежных специальностей. Если брать специалистов с технических специальностей, для таких специалистов появляется проблема в работе с нормативными документами. Если брать специалистов из силовых структур, проблема – в технологии и в технической части. Предприятия находят другой выход из такой ситуации: не создавая собственное подразделение по защите информации, прибегают к услугам специализированных компаний, которые проводят аудит и аутсорсинг.

Такие компании используют специализированные программные средства, которые могут моделировать процессы. Из моделированных процессов можно проводить анализ защищенности системы против различных угроз. Такие программы ограничены в общем доступе из-за нескольких причин (угрозы часто модифицируются, компании разрабатывают свои и не хотят делиться разработками и другие). Поэтому есть необходимость создать сервис, который будет доступен каждому, с помощью вычислений можно будет проанализировать комплексную системы защиты данных на основе математической модели «Полного перекрытия». С помощью модели «Полного перекрытия» можно про-

анализировать, перебрать различные варианты и выбрать оптимальный вариант (максимальная защита при определенных затратах).

Сегодня в любой работе используют различные технические устройства для автоматизации бизнес процесса. Чаще всего это является компьютеры, которые имеет доступ к сети Интернет. Компьютеры помогают в реализации продажи товара, в ведении учета товара, аналитики продаж. Компьютеры проникли в повседневную жизнь человека, с их помощью быстрее передается большой объем информации, чем бумажный источник. Это упростило труд человека. Есть обратная сторона использования компьютеров различные компьютерные вирусы, сетевые атаки и т.д.

Для необходимой защиты от различных атак нужно использовать комплексную систему защиты данных. Комплексная система защиты данных представляет собой ряд различных мер и специализированных программ, которые направлены на предотвращения, мониторинг и выявление угроз на ранней стадии угроз [2].

Если лет 20 назад, чтобы реализовать угрозу, нужно было иметь специализированные знания и навыки, то сейчас в сети Интернет в открытом доступе есть программы, с помощью которых без всяких трудностей можно не санкционированно получить информацию. Так как методы защиты данных всегда модернизируются, злоумышленники пытаются найти новые уязвимости в системе защиты данных. Из перечисленного следует, что процесс защиты является динамическим.

В крупных компаниях для своевременной защиты данных создаются отделы, которые направлены на защиту данных. В отделе находятся люди, которые специализированы не только в технической области знаний, но и в правовой. При создании комплексной защиты данных, защита должна соответствовать как техническим нормам, так и ГОСТу.

В крупных компаниях есть возможность создать такие отделы. Но для малого предприятия, где бюджет ограничен, создание такого отдела невозможно. Но ущерб от различных атак на информационную систему малого предприятия может привести к печальным последствиям. Ущерб может превышать несколько раз от суммарного оборота малого предприятия. Чтобы не ждать, когда уже пройдет атака на информационную систему малого предприятия, руководство предприятия используют услуги специализированных организаций.

Компании, которые специализируются на защите информационной системы, используют различные программы. Благодаря таким программам можно быстро и качественно провести анализ существующей системы защиты, найти слабые места в защите данных и предложить правила политики безопасности. Большинство таких программ используют различные математические модели. Среди всех моделей можно выделить модель «Полного перекрытия».

Модель «Полного перекрытия» позволяет рассчитать необходимые затраты для проектирования системы защиты данных, определить оптимальный вариант построения системы защиты данных. В модели используются теория гра-

фов (для представления взаимосвязей между элементами системы защиты данных), теория нечетких множеств (для представления системы защиты), теория вероятностей (для расчета вероятности стойкости барьеров защиты от различных угроз). В модели описываются взаимодействие «угрозы», «информационные ресурсы», «барьеры защиты». Рассматривают три множества для описания системы защиты данных [2]:

- множество угроз или атак $U = \{u_i\}, i = \overline{1,m}$;
- множество барьеров защиты $O = \{o_j\}, j = \overline{1,n}$;
- множество информационных ресурсов $M = \{m_k\}, k = \overline{1,r}$.

Для усовершенствования предлагается ввести еще два элемента:

- V - набор уязвимых мест в защите данных, с помощью которых можно осуществлять угрозы u_i в отношение объектов o_j.
- B - набор барьеров в системе защиты данных, который представляет собой пути осуществления угроз безопасности, перекрытые средствами защиты.

Таким образом, после добавления двух элементов, модель будет представлена как на рис. 1.

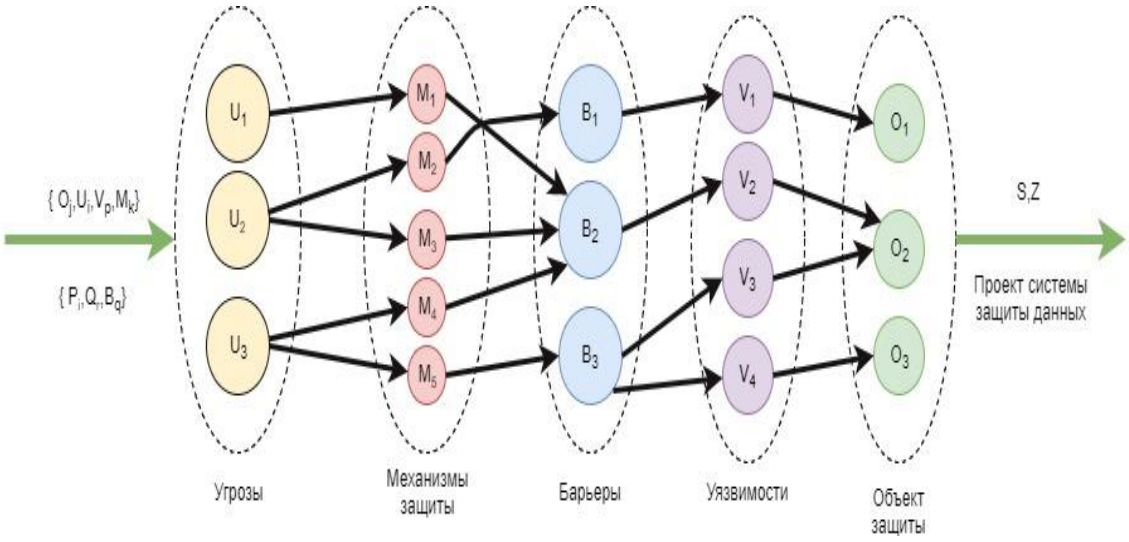

Рис. 1. Модель «Полного перекрытия»

Таким образом, процесс защиты данных представляет собой кортеж:

$S = \{O, U, M, V, B\}$, (1)

Где O - множество защищаемых объектов;

U - множество возможных угроз;

M - множество средств защиты;

V - множество уязвимых мест в системе защиты данных;

B - множество барьеров.

Чтобы получить доступ, злоумышленнику необходимо выполнить ряд этапов и процессов, которые можно свести к трем условиям разведывательного контакта злоумышленника с источником данных:

- поиск ценных данных ($P_{пр}$ - пространственный фактор);
- размещение программно-аппаратных средств для получения данных на удалении от источника, при котором гарантируется приемлемое отношение сигнал/шум на входе средства ($P_{эн}$ - энергетический фактор);
- совпадение времени проявления демаскирующих признаков объекта защиты или передачи данных, и работы средства добывания ($P_{вр}$ - временный фактор).

Угрозы выполняются одновременно при трех условиях, а общая вероятность равна произведению

$$P = P_{пр} \cdot P_{эн} \cdot P_{вр}, \quad (2)$$

Прочность барьера системы защиты данных характеризуется величиной остаточного риска $Risk_i$, связанного с возможностью осуществления угрозы u_i в отношении объекта o_j, при использовании барьера b_q. Определяется по формуле

$$\begin{aligned} &Risk_i = P_i \cdot Q_j \cdot (1 - B_q), \\ &i = \overline{1,m},\ j = \overline{1,n}, q = \overline{1,m \times n};, \end{aligned} \quad (3)$$

где P_i - вероятность появления угрозы u_i,

Q_j - величина ущерба при удачном осуществлении угрозы u_i в отношении защищаемого объекта o_j; величина ущерба рассчитывается в условных единицах,

B_q - степень сопротивления барьера, величина характеризует вероятность его преодоления.

Защищенность всей системы определяется по формуле

$$S = \frac{1}{\sum_{(\forall b_q \in B)} (P_i \cdot Q_j \cdot (1 - B_q))}, \quad (4)$$

$$P_i \in (0,1), B_q \in [0,1).$$

На основе предложенной модели была разработана функциональная схема системы проектирования комплексной защиты данных, а также создан алгоритм программно-методических модулей, входящих в состав системы. Структурная схема представлена на рис. 2.

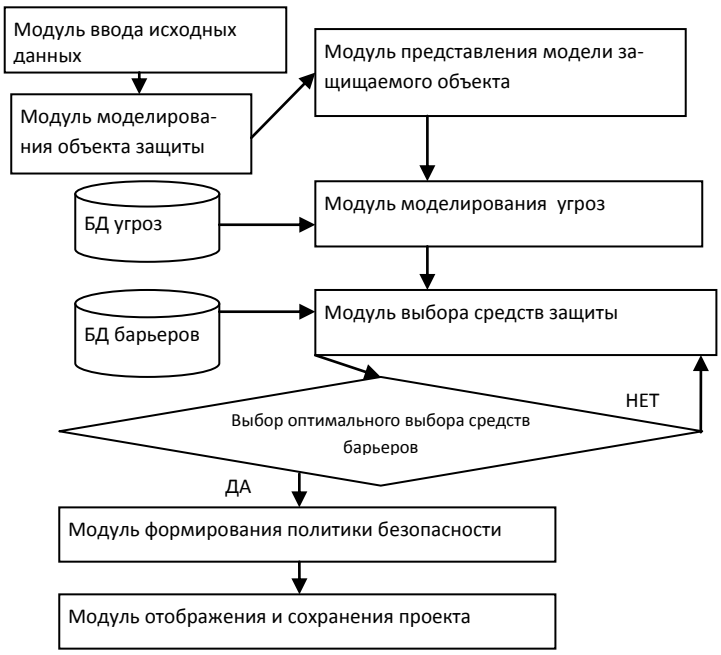

Рис. 2. Структурная схема разработанной системы

Начало проектирования системы защиты данных начинается с ввода исходных данных об защищаемых объектах. Защищаемые объекты (файлы, персональные данные, данные аутификации) должны быть представлены в системе, в виде некоторой структуры данных. Свойства защищаемого объекта должны иметь важные характеристика объекта.

После создания модели защищаемого объекта происходит проектирование системы защиты. На основе системного подхода каждый элемент в программном комплексе проектируется отдельным модулем, что позволяет динамически менять один модуль, и это не будет отражаться на работе других модулей.

В системе защиты данных основой является программно-аппаратная защита (рис.3). Разработанный модуль позволяет оценить и выбрать оптимальный вариант защиты. Данные меры защиты существенно увеличивают время, необходимое для проникновения через барьеры защиты, что увеличивает время реагирования для специализированных подразделений для выявления угрозы и принять меры против злоумышленника.

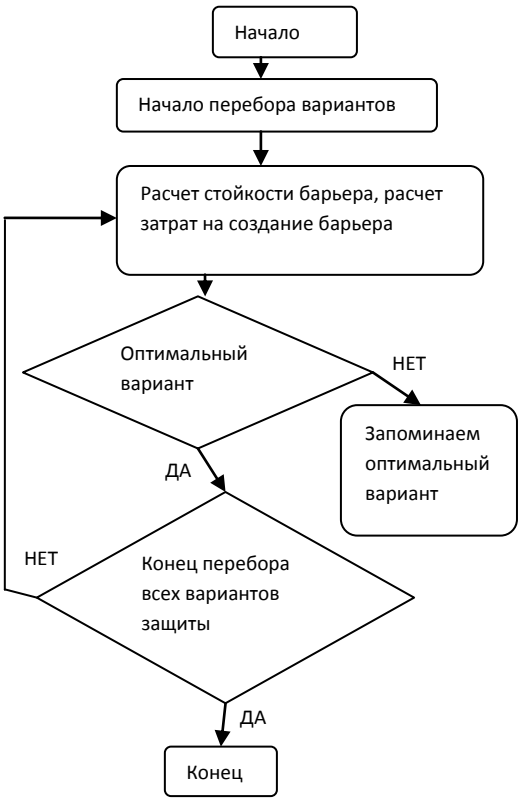

Рис.3. Алгоритм выбора оптимальных средств защиты данных

Основной задачей разработанной системы является моделирование объектов барьеров от различных угроз на информационную систему и анализ комплексной системы защиты данных. Важным моментом можно отметить, что в системе уже имеется набор угроз, взятых с «базы данных ФСТЭК», также есть возможность добавлять свои данные в базу (будет доступна тому пользователю, которые добавляют эти данные). Таким образом, разработанная система является универсальной.

Результатом работы является автоматизирование разработки системы комплексной защиты данных для малых предприятий. Так как система представлена в виде сайта, нет явной привязки к характеристикам компьютера, главное, чтобы был установлен веб-браузер и подключение к сети интернет.

Список литературы

1. Аверченков, В.И. Организационная защита информации/ В. И. Аверченков, М.Ю. Рытов. – Брянск: Изд-во БГТУ, 2005. – 184 с.

2. Аверченков, В.И. Рытов, М.Ю. Гайнулин, Т.Р. Автоматизация выбора состава технических средств системы физической защиты/ В. И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин// Весник БГТУ. Брянск 2008г.

3. Агарунов Д. «Информзащита». Интервью с заместителем генерального директора по сервисным проектам Максимом Темновым [Электронный ресурс]. – Режим доступа: ttps://xakep.ru/2018/02/26/infosec-interview/l (дата обращения: 01.03.2018).

Материал поступил в редколлегию 18.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.056:004.272

Свечников Дмитрий Александрович, *к.т.н., сотрудник*
Филоненко Сергей Станиславович, *сотрудник*
Секач Никита Олегович, *сотрудник*
Академия ФСО России, Орёл, Россия
e-mail: sda33@academ.msk.rsnet.ru

ПРЕДЛОЖЕНИЯ ПО ПОСТРОЕНИЮ КОМПЛЕКСНОЙ МЕТОДИКИ АНАЛИЗА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ВЕБ-ПОРТАЛОВ

Описаны предложения по построению комплексной методики анализа защищенности информационных ресурсов веб-порталов, разработанной в соответствии с требованиями руководящих документов ФСТЭК России и учитывающей рекомендации по обеспечению информационной безопасности организаций банковской системы Российской Федерации.

Возрастающая популярность применения веб-технологий для организации доступа к информационным ресурсам обусловливает необходимость решения вопросов обеспечения их безопасности. Одной из основных задач в процессе обеспечения безопасности информационных ресурсов общедоступных веб-порталов является реализация функции контроля их защищенности в соответствии с установленными требованиями к обеспечению защиты информации.

При разработке комплексной методики контроля защищенности информационных ресурсов веб-порталов учитывались требования руководящих документов ФСТЭК России [1, 2, 3], рекомендации по обеспечению информационной безопасности организаций банковской системы Российской Федерации [4] и перечень основных рекомендаций по тестированию безопасности веб-приложений, направленных на выявление способности веб-приложения противостоять угрозам, представленных в открытом проекте обеспечения безопасности веб-приложений [5].

В соответствии с [2] выделяют три класса защищенности информационных систем. Для каждого класса защищенности определен состав мер защиты информации и их базовые наборы. Положения по контролю (анализу) защищенности информации (АНЗ) включают:

– АНЗ.1 выявление, анализ и устранение уязвимостей информационной системы;

– АНЗ.2 контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации;

– АНЗ.3 контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;

– АНЗ.4 контроль состава технических средств, программного обеспечения и средств защиты информации;

– АНЗ.5 контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе.

Меры защиты информации АНЗ.1 включены в обязательный базовый набор мер для всех трех классов защищенности информационных систем. Помимо этого, для всех классов защищенности информационных систем определены требования к усилению базовой меры АНЗ.1.

В соответствии с основными положениями руководящих документов [1, 2, 3, 4] разрабатываемая комплексная методика контроля защищенности информационных ресурсов веб-порталов должна быть ориентирована:

- на выявление (поиск) дефектов безопасности программного обеспечения (Common Weakness Enumeration, CWE) на этапе разработки и в случае его обновления (инспекционный контроль). Дефекты безопасности ПО – дефекты, сбои, ошибки, уязвимости и прочие проблемы реализации, кода, проектирования или архитектуры ПО, которые могут сделать веб-портал уязвимым к атакам злоумышленников;
- выявление (поиск) уязвимостей программного обеспечения (Common Vulnerabilities and Exposures, CVE), общесистемного, веб-сервера, прикладного, средств защиты информации. Уязвимости – ошибки программы, которые могут быть непосредственно использованы злоумышленником;
- выявление (поиск) неразрешенного программного обеспечения (компонентов программного обеспечения);
- выявление уязвимостей «нулевого дня», о которых стало известно, но информация о которых не включена в сканеры уязвимостей;
- выявление новых уязвимостей, информация о которых не опубликована в общедоступных источниках;
- проверку правильности установки и настройки средств защиты информации, технических средств и программного обеспечения;
- проверку корректности работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;
- проверку своевременности обновлений программного обеспечения средств защиты информации, общесистемного и прикладного программного обеспечения;
- выявление (поиск) уязвимостей в информационной системе с использованием учетных записей на сканируемых ресурсах;
- тестирование информационной системы на проникновение.

При проведении контроля защищенности информационных ресурсов ведомственных веб-порталов в соответствии с основными положениями руководящих документов ФСТЭК России [1, 2, 3] должны выполняться следующие требования:

- выявление (поиск) уязвимостей веб-порталов должно осуществляться администраторами безопасности посредством применения сертифицированных средств анализа (контроля) защищенности (сканеров безопасности), имеющих стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ;
- обнаружение в информационной системе неразрешенного программного обеспечения должно осуществляться посредством автоматизированных средств;
- анализ журналов регистрации событий безопасности (журнала аудита) в целях определения, были ли выявленные уязвимости ранее использованы в информационной системе для нарушения безопасности информации.

По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик информационной системы, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Для сравнения результатов сканирования уязвимостей в разные периоды времени и анализа изменения количества и классов (типов) уязвимостей в информационной системе должны применяться автоматизированные средства.

Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и эксплуатации информационной системы.

На этапе эксплуатации поиск и анализ уязвимостей проводится с периодичностью, установленной оператором информационной системы.

Обеспечение защиты информации в ходе эксплуатации осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации и организационно-распорядительными документами по защите информации и включает:

- управление (администрирование) системой защиты информации информационной системы;
- выявление инцидентов и реагирование на них;
- управление конфигурацией аттестованной информационной системы и ее системы защиты информации;
- контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе.

Выявление уязвимостей «нулевого дня», о которых стало известно, но информация, о которых еще не включена в сканеры уязвимостей, должно проводится немедленно.

Периодичность проведения исследований на предмет выявления новых уязвимостей, информация о которых не опубликована в общедоступных источниках, устанавливается оператором. При этом в обязательном порядке для критических уязвимостей проводится поиск и анализ уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемом в информационной системе.

Для анализа изменения количества и классов (типов) уязвимостей в информационной системе должно выполняться сравнение результатов сканирования уязвимостей в разные периоды времени посредством автоматизированных средств.

Контроль проведения исследований проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации, и фиксируется в соответствующих журналах.

Список литературы

1. Приказ ФСТЭК России от 11.2.2013 г. № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".

2. Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России от 11.02.2014 г.).

3. Изменения, которые вносятся в "Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах", утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17 (утв. ФСТЭК России от 15.2 2017 г. № 27).

4. Рекомендации в области стандартизации Банка России РС БР ИББС-2.6-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации.

5. The Open Web Application Security Project (OWASP) [Электронный ресурс]. – Режим доступа https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29. pdf.

Материал поступил в редколлегию 23.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 34.342

Фисун Александр Павлович, *д.т.н., профессор, профессор кафедры информационной безопасности*
Белевская Юлия Александровна, *к.ю.н., доцент, доцент кафедры конституционного и муниципального права*
Орловский государственный университет имени И.С. Тургенева
Россия, 302026, г. Орёл, пл. Комсомольская, 95
E-mail: fisun11@yandex.ru
Среднерусский институт управления – филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации
Россия, 302028, Орёл, бульвар Победы, д. 5А
E-mail: belevskaya.ua@gmail.com

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ОДИН ИЗ ВАЖНЕЙШИХ ПОЛИТИЧЕСКИХ МЕХАНИЗМОВ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Рассматриваются вопросы информационной безопасности информационного общества как одного из приоритетных политических механизмов развития информационного общества. Анализируются основные направления деятельности органов государственной власти, связанные с обеспечением информационной безопасности.

Актуальность постановки и решения проблемы обеспечения информационной безопасности информационного общества, определяется следующими факторами:

– устойчивой тенденцией внедрения практически во все материально-энергетические сферы и виды деятельности личности, общества и государства современных информационных технологий, в том числе глобальных, национальных, региональных и локальных информационных систем;

– динамичным развитием рынка и производимых ими информационных продуктов и услуг, лежащих в основе развития материально-энергетического мирового и национального производств, социально-политического, экономического, научного развития мирового сообщества;

– формированием и динамичным развитием международного информационного пространства и его составляющих национальных информационных сфер;

– повышением требований обеспечения информационной безопасности личности, общества, государства и используемых ими в условиях лавинообразного возрастания объемов информационных потоков циркулирующих в информационном обществе, состоящих как из полезной, обеспечивающей созидательное развитие личности, общества и государства, так и с вредной, разру-

шающей информации, обусловливающей негативные изменения личности, общества и государства;

– качественным и количественным изменениями объемов и содержания задач управления органов публичной власти, вызванными переходом к информационному обществу и обусловившими необходимость повышения эффективности деятельности органов публичной власти и соответствующего совершенствования их информационного обеспечения;

– усложнением внутринациональных и межнациональных социальных, экономический, политических, научно-технических и иных процессов, видов и сфер деятельности личности, общества и государства в основе которых лежат производство и потребление интеллекта, знаний, и, в целом информационные процессы, обусловливающие возникновение новых, информационных общественных отношений;

– широким использованием во всех сферах и видах деятельности личности, общества и государства современных информационных технологий, обусловливающих формирование новых, устойчивых закономерностей развития информационного общества, и соответствующих общественных отношений, требующих эффективного регулирования;

– повышением роли информации как объекта правоотношений во всех сферах и видах материально-энергетической деятельности личности, общества, государства и сложностью, неопределенностью объективной оценки ее свойств;

– возрастанием угроз информации, и, в целом, информационной сфере, обусловленных лавинообразным развитием и широким использованием самих во всех сферах и видах деятельности современного общества, развивающихся национальных и международного информационных пространств;

– необходимостью предоставления и обеспечения достоверной, полной, своевременной и безопасной информации, как основы эффективной деятельности личности, общества, государства, используемых и обеспечения их информационной безопасности;

– недостаточным динамичным развитием современного научно-методологического инструментария для решения проблем повышения качества информационного обеспечения существующих материально-энергетических и вновь появляющихся информационных сфер и видов деятельности развивающегося информационного общества;

– закономерностями формирования, развития фундаментальной, прикладной информационной и юридических наук, их интеграцией в части исследования и использования общих и единых объектов общественных отношений – информации;

– другими факторами.

Рассмотренные факторы обуславливают и определяют:

– особенности, видоизменение, сложности возникновения, существования и эффективность развития общественных отношений в материально-энергетической и информационной сферах современного общества и государ-

ства, его институтов, а также их целостность, устойчивость функционирования и безопасное развитие;

– формирование новых общественных отношений, являющихся по содержанию информационными, представляющих, правоотношения, связанные с реализацией информационных процессов сбора, накопления, обработки, анализа, переработки, хранения, передачи (распространения) информации, направленных и осуществляемых с конечной целью предоставления субъектам информации, информационных продуктов и услуг заданного качества (своевременности, достоверности, безопасности, релевантности, пертинентности и других), обеспечивающих эффективное решение задач в искомых материально-энергетических и информационной сферах.

При этом обеспечение указанных качеств информации, а равно информационных ресурсов, информационных продуктов, услуг, и, прежде всего такого важного качества как безопасность, должно реализовываться в едином неразрывном процессе с комплексным обеспечением информационной безопасности субъектов правоотношений.

Не менее важными и наиболее характерными направлениями государственной политики и ее практической деятельности по защите интересов общества в сфере обеспечения информационной безопасности, его сфер и видов деятельности, как известно [1,2], являются защита имеющих информационную природу национальных, духовных ценностей, защита норм морали и общественной нравственности, которые реализуются в рамках таких общенациональных направлений, как:

– обеспечение конституционных прав и свобод личности, личной безопасности во всех материально-энергетических и информационной сферах;

– повышение качества и уровня жизни, физического, духовного и интеллектуального развития человека и гражданина;

– разработка соответствующей нормативной правовой базы по защите национальных ценностей интересов государства.

Кроме названных направлений, Стратегия национальной безопасности Российской Федерации [2] определяет и интересы самого государства, которое является основным субъектом правового регулирования и обеспечения прав и свобод личности и общества в информационной сфере, реализуемых в рамках этих интересов, состоящих:

– в незыблемости конституционного строя, суверенитета и территориальной целостности России;

– политической, экономической, социальной стабильности;

– безусловном обеспечении законности и поддержании правопорядка;

– развитии равноправного и взаимовыгодного сотрудничества.

Необходимо отметить, что обеспечение прав и свобод личности и общества в сфере информационной безопасности в рамках реализации этих законных интересов субъектов правоотношений, возможно только на основе устойчивого развития экономики, что позволяет выделить в качестве ключевого на-

правления государственной политики, являющегося материально-энергетической основой развития информационной сферы – направление реализации национальных экономических интересов России.

Не менее важным является тот факт, что, реализуя рассмотренные выше направления обеспечения интересов личности и государства в информационной сфере и сфере обеспечения их информационной безопасности, государство само начинает выступать в качестве субъекта информационных отношений, который также требует обеспечения информационной безопасности, в том числе защиты от внешних и внутренних угроз, охраны государственной тайны, защиты от иностранных разведок, шпионажа, в том числе промышленного, банковского и других его видов. А учитывая широкое глобальное использование информационных технологий, в том числе ЭВМ, систем и сетей ЭВМ во всех видах и сферах деятельности, повлекшее увеличение компьютерных правонарушений во всех сферах деятельности, в том числе экономической, политической, военной и научной сфере, на первое место выходят такие направления деятельности государства по обеспечению его информационной безопасности, как:

– защита персональных данных, циркулирующих в органах публичной власти;

– борьба с компьютерной преступностью, в первую очередь в финансовой сфере, как исключительной сфере ведения государства;

– защита коммерческой тайны, секретов производства, особенно в сфере оборонных отраслей промышленности и обеспечение благоприятных условий для предпринимательской деятельности;

– защита государственных секретов;

– создание системы взаимных финансовых расчетов в электронной форме с на основе электронной цифровой подписи;

– обеспечение безопасности автоматизированных систем обработки информации и управления, и прежде всего используемых в системе органов государственной власти, системе национальной безопасности, правоохранительных органах, в оборонных отраслях промышленности и в потенциально опасных производствах, в том числе критически опасных объектах;

– страхование информации и информационных систем;

– сертификация и лицензирование в области защиты информации, безопасности информации, информационной безопасности, других социотехнических систем, контроля безопасности и информационной безопасности этих систем;

– организация взаимодействия в сфере защиты информации при международном информационном обмене, в том числе со странами–членами СНГ, другими иностранными государствами и международными организациями.

Перечисленные направления деятельности государства в сфере обеспечения информационной безопасности тесно связаны с другими направлениями и реализуются в рамках обеспечения национальной безопасности России в целом, включающего:

– защиту конституционного строя;
– защиту экологической среды;
– защиту государственных границ;
– обеспечение национальной безопасности страны при сотрудничестве с другими государствами.

На сегодняшний день наиболее содержательным отражением деятельности государства по обеспечению информационной безопасности во взаимосвязи с рассмотренными направлениями национальной безопасности России, является существующая Доктрина информационной безопасности Российской Федерации, которая, как известно [1], представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации и служит основой:
– для формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
– подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации в целом и ее сфер;
– разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Анализ содержания Доктрины с учетом исследуемой проблемы позволил констатировать следующее:

1. Достаточно полно определено содержание основного, базового понятия – «информационная безопасность России», отражающего сущность важнейшего свойства государства, определяющего его национального интересы.

2. Уточнены, по сравнению с раннее декларированными в известных концепциях национальной безопасности, информационные интересы личности, общества и государства, где на первое место ставятся интересы личности в информационной сфере, которые, прежде всего, заключаются в реализации конституционных прав человека и гражданина на доступ к информации, использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность. В свою очередь, реализация интересов личности осуществляется также через реализацию интересов общества в информационной сфере, которые, в свою очередь обеспечивают практическую реализацию информационных интересов личности, упрочение демократии, создание правового социального, открытого государства, достижение и поддержание общественного согласия, в духовном обновлении России, а также через реализацию интересов государства в информационной сфере, направленную на создание условий для гармоничного развития российской информационной инфраструктуры, реализацию конституционных прав и свобод человека и гражданина в области получения информации и пользования ее в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной

стабильности, в безусловном обеспечении законности и правопорядка, развития равноправного и взаимовыгодного международного сотрудничества.

3. На основе перечисленных выше интересов в информационной сфере достаточно полно сформированы стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности России.

4. Относительно полно уточнены виды внешних и внутренних угроз информационной безопасности России и их источники.

5. С учетом указных в предыдущем пункте угроз и их источников системно выделены общие методы и особенности обеспечения информационной безопасности России, в том числе и при международном сотрудничестве, что характеризует учет глобальности проблемы информационной безопасности развивающегося информационного общества и его интеграции в мировое информационное пространство.

6. Однозначно и полно сформированы принципы обеспечения государственной политики в сфере обеспечения информационной безопасности страны, определены первоочередные мероприятия по ее реализации и выделены основные функции системы обеспечения информационной безопасности страны, направленные на приоритетную реализацию прав человека и гражданина в информационной сфере и сфере обеспечения информационной безопасности.

Таким образом, проведенный анализ состояния и основных направлений обеспечения информационной безопасности акцентировал внимание на дальнейшую работу в сфере обеспечения информационной безопасности как важнейшего политического механизма развития информационного общества и позволил сделать следующие важные выводы:

– ни один вид и сфера деятельности современного общества не может существовать, формироваться, функционировать и развиваться без развитой информационной структуры, обладающей одним из важных свойств – информационной безопасности, что, в свою очередь обусловливает необходимость обеспечения информационной безопасности Российской Федерации и используемых информационных технологий, как основной и неотъемлемой составляющей обеспечения национальной безопасности страны, а защита информации всегда является одной из приоритетных государственных задач;

– современные информационные технологии, обрабатываемая в них информация и национальный информационный ресурс являются в настоящее время одним из главных источников формирования и развития материально-энергетического базиса, общества и государства, и, прежде всего его социально-экономической, научно-технической, оборонной и других сфер, определяющих мощь и лидирующую роль, место национального государства в мировом сообществе;

– лежащая в основе, определяющая эффективность и являющаяся результатом всех, без исключения, сфер и видов деятельности личности, общества и государства информация приобретает и обусловливает формирование кон

кретной политической, социальной, духовной, материальной и стоимостной ценности этих субъектов;

– реализация прав и свобод в информационной сфере возможна только путем создания оптимальных условий (факторов) для эффективного обеспечения информационной безопасности.

Список литература

1. Доктрина информационной безопасности РФ, утв. Президентом РФ от 9 сентября 2000г. // Российская газета. 2000. 28 сентября.

2. Стратегия национальной безопасности Российской Федерации [Электронный ресурс]: [Утверждена Президентом Российской Федерации 31 декабря 2015г. № Пр.-683.]. - URL: https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html.

Материал поступил в редколлегию 27.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.942

Хаматнуров Ильдар Ильнатович, *студент кафедры «Системы информационной безопасности» КНИТУ-КАИ*
Мухаматханов Ренат Маратович, *студент кафедры «Системы информационной безопасности» КНИТУ-КАИ*
Баянов Булат Ильмирович, *студент кафедры «Системы информационной безопасности» КНИТУ-КАИ*
Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ, Казань, Россия
e-mail: ildarka96@mail.ru

СОЗДАНИЕ МОДЕЛИ ЗАЩИТЫ WEB-РЕСУРСОВ

Рассмотрена модель защиты web-ресурсов. Проанализированы существующие методики, направленные на обеспечение защиты информации от различных видов угроз.

В настоящее время множество web-ресурсов используют конфиденциальную информацию пользователей сети интернет. Любой web-ресурс имеет множество уязвимостей, поэтому каждый из них требует особый уровень защиты. Обеспечение безопасности web-ресурсов предполагает использование методов защиты от всевозможных видов угроз, направленных на дестабилизацию функционирования web-ресурсов, а также на хищение и модификацию конфиденциальной информации [2].

Перечислим основные направления защиты от конкретных видов угроз. Одним из самых доступных методов хакерской атаки на web-ресурс является DDoS-атака, которая позволяет злоумышленникам ограничить доступ пользователей к ресурсу [4]. Помимо доступности, ресурс также должен обеспечивать собственную целостность. Поэтому необходимо позаботиться об устранении уязвимостей баз данных web-ресурсов, в которых содержится конфиденциальная информация пользователей. Такая информация хранится на каждом web-ресурсе, предполагающем регистрацию, а также прохождение аутентификации зарегистрированного пользователя. Соответственно следует позаботиться о защите от bruteforce-атак [1].

Рассмотрим предложенную нами методику. Ее основой являются существующие методики других авторов. Пусть имеется web-ресурс, в котором реализован функционал регистрации и аутентификации, почтовый сервис и мгновенный обмен сообщениями. Для того, чтобы обеспечить защиту данного web-ресурса, мы предлагаем выполнить шаги, представленные ниже.

Для разработчиков web-ресурсов рекомендуется строить систему защиты при проектировании самой системы, поэтому система защиты выдвигает ряд требований по созданию системы, следовательно, для начала необходимо выделить два компонента задач структурного проектирования web-ресурса на яд-

ро и интерфейс, где ядро выполняет обработку данных, а интерфейс устанавливает правило взаимоотношений пользователей системы [3]. Затем при разработке web-ресурса важным является формирования задач, выполняемых web-ресурсом.

Любой web-ресурс хранит информацию в базе данных (БД), поэтому БД можно отнести к объекту защиты. Процесс защиты БД можно разбить на следующие этапы: фильтрация строковых параметров, усечение входных параметров, использование параметризованных команд, использование хранимых процедур, использование функции блокировки, создание менее привилегированного пользователя, создание четкой матрицы доступа или применение политик безопасности к системам распределения доступа, контроль сообщений об ошибках.

Одним из популярных методов хакерской атаки на web-ресурс является внедрение вредоносных программ, поэтому обязательным является установка и конфигурация антивирусных программ.

Для скрытия конфиденциальной информации, такой как пароли пользователей, удобным и эффективным является шифрование данной информации [5]. Обычно процесс шифрования в web-ресурсах подразделяют на хэширование паролей, введенных пользователем web-ресурса, использование «соли» при хэшировании пароля, BCrypt алгоритма, локальных параметров, вшитых в конфигурационные файлы. Также пользователям web-ресурса рекомендуется использовать плагин web-браузера Google Chrome «LastPass», который позволяет обезопасить хранение паролей от учетных записей пользователя.

После установки всех необходимых компонентов защиты web-ресурса предполагается провести предварительное тестирование этих компонентов. Для автоматизации тестирования предлагается использовать предварительно обученную нейронную сеть. Данный этап включает в себя формирование тестовой выборки, выбор основных параметров для тестирования, применение политик безопасности, определяющих состояние пользователя, расчет статистических данных и обучение нейронной сети, процесс тестирования созданных моделей. При успешном прохождении тестирования переходят к следующему пункту обобщенной методики, в противном случае производится прохождение повторного тестирования: повторное обучение нейронной сети с учетом коррекции ошибок, выделение важных параметров сетевого трафика применение политик безопасности, определяющих состояние пользователя.

Успешным результатом внедрения обобщенной методики является запуск web-ресурса и его стабильное функционирование с учетом возможной реализации сетевых атак на web-ресурс. Данная методика была разработана для оптимизации системы защиты web-ресурса.

Список литературы

1. Родичев, Ю.А. Нормативная база и стандарты в области информационной безопасности/Ю.А. Родичев. – СПб.: Питер, 2017, – С. 256.

2. Власенко, А.В. Разработка и системный анализ математической модели угроз, модели нарушителя, процедур защиты Web-приложений на всех этапах функционирования/А.В. Власенко, П.И. Дзъбан // Политематический сетевой электронный научный журнал КубГАУ = Scientific Journal of KubSAU. 2014. № 101. С. 11. URL: http://ej.kubagro.ru/2014/07/pdf/143.pdf. Дата обращения (12.04.18.);

3. Власенко, А.В. Разработка алгоритмов и программ выбора оптимального набора компонент нейтрализации актуальных угроз на основе описания модели и интеграции их в Web-приложение /А.В. Власенко, П.И. Дзъбан // Вестник Адыгейского государственного университета. Сер. Естественно-математические и технические науки. – 2014. – Вып. 3 (142). – С. 189–193. URL: http://vestnik.adygnet.ru. Дата обращения (12.04.18.);

4. Частикова, В.А. Нейросетевой метод защиты информации от DDOS-атак /В.А. Частикова, Д.А. Картамышев, К.А. Власов// Журнал Современные проблемы науки и образования. 2015. URL: https://www.science-education.ru/pdf/2015/1/974.pdf. Дата обращения (13.04.18.);

5. Журавленко, Н. И. Использование методов шифрования для предотвращения киберугроз/ Н.И. Журавленко, О.В. Олюшкевич // I региональная научно-практическая конференция «Векторы развития информационных технологий: перспективы и направления». – 2017. – С. 86-88.

Материал поступил в редколлегию 23.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.056

Цибуля Алексей Николаевич, *сотрудник*
Чиженькова Виталия Александровна, *сотрудник*
Академия ФСО России, Орёл, Россия
e-mail: tsibul@mail.ru

АЛГОРИТМ ПОИСКА АДРЕСОВ ФИШИНГОВЫХ САЙТОВ С ИСПОЛЬЗОВАНИЕМ МЕТОДА ВАГНЕРА-ФИШЕРА

Представлены результаты исследования способов синтеза близких по виду названий сайтов с целью поиска и выявления имен фишинговых сайтов в сети Интернет

Фишинг – это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего. После того, как пользователь попадает на поддельную страницу, мошенники пытаются различными приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определенному сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам [1, 2].

Интернет-сообщество ведет активную борьбу с фишингом. Для этого используются различные механизмы. Одним из важных признаков фишингового сайта является визуально близкое соответствие его адреса адресу реального сайта, от имени которого производятся мошеннические действия. Для выявления таких адресов необходимо произвести генерацию и последующую проверку наличия в сети Интернет адресов, наиболее близких по виду реальному.

Разработанный алгоритм (см. рис. 1) позволяет найти в сети Интернет существующие сайты, визуально схожие с заданным сайтом или убедиться, что таких сайтов нет.

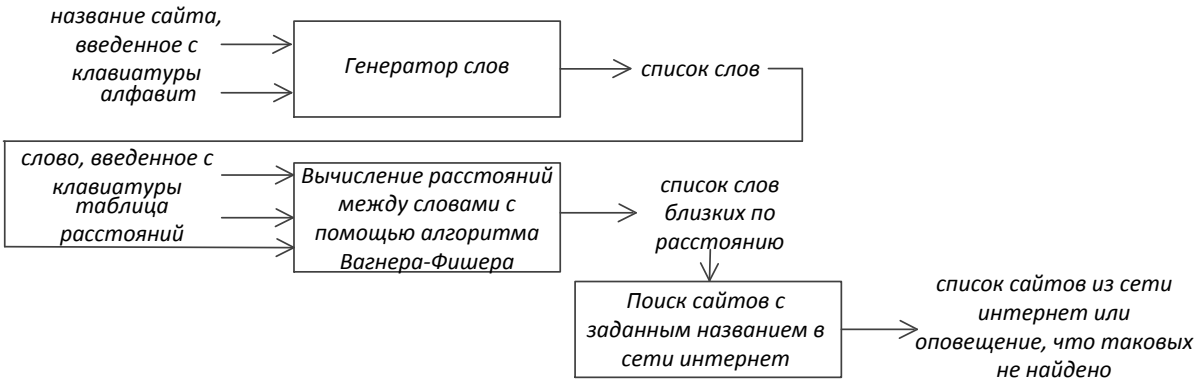

Рис. 1. Обобщенная схема алгоритма выявления адресов фишинговых сайтов

Алгоритм работает следующим образом:

- пользователь вводит с клавиатуры название сайта;
- название сайта вместе с алфавитом (заранее определенные допустимые значения символов, биграмм и триграмм) попадает на вход генератора слов, в котором каждый символ заданного слова последовательно заменяется символом из алфавита;
- на выходе генератора получается список всевозможных комбинаций, полученных из данного слова;
- слова из этого списка с таблицей расстояний и заданным словом поочередно поступают на вход элемента для вычисления расстояний между словами с помощью алгоритма Вагнера-Фишера;
- на выходе получаем список слов близких по расстоянию с данным (количество этих слов либо вводится с клавиатуры, либо определяется предельным значением близости, которое определяет пользователь);
- далее все слова, схожие с названием данного сайта, проверяются на наличие в сети Интернет;
- на выходе получаем список сайтов, найденных в сети Интернет, либо уведомление, что таковые найдены не были.

В основе структурной схемы лежит алгоритм нахождения визуально близкого соответствия между словами. С этой целью требуется ввести метрику близости двух текстовых строк, содержащих адреса. Понятие функции, измеряющей расстояние, или метрики, используется в самых разных областях и часто используется для оценки сходства двух векторов. Такие функции применяют для определения силы связи двух признаков, или, например, в распознавании образов при сопоставлении шаблонов с различными частями изображений.

Введем обозначения:

d – метрика;

$x_1x_2 \dots x_m$ – строка x длины $|x| = m$, где x_i представляет $i-$ й символ x;

$x_R(i,j)$ – подстрока $x_ix_{i+1} \dots x_j$ строки x, где $i \le j \le$ □ .

Требуется для двух данных строк адресов x и y, где $|x|, |y| > 0$, и метрики d, задающей расстояния между строками, вычислить $d(x,y)$. С этой целью может быть использована одна из метрик, предложенных Левенштейном [3]. Согласно данной метрике, расстояние между строками равно минимальному количеству операций редактирования (замена, вставка и удаление символов), преобразующих одну строку в другую. Однако при этом предполагается, что вес (цена) каждой из операций равен 1. В то же время, цена замены, например, одного символа на другой, может отличаться в зависимости от их визуальной схожести. Поэтому имеет смысл воспользоваться методом динамического программирования Вагнера–Фишера [4].

Пусть $d_{i,j}$ есть расстояние между префиксами строк адресов x и y, длины которых равны, соответственно, i и j, то есть

$$d_{i,j} = d(x(1,i), y(1,j))$$

Цену преобразования символа a в символ b обозначим через $w(a,b)$. Таким образом, $w(a,b)$ – это цена замены одного символа на другой, когда $a \neq b, w(a,\varepsilon)$ – цена удаления a, а $w(\varepsilon,b)$ – цена вставки b. Заметим, что в случае, когда выполнены нижеследующие условия, d является расстоянием Левенштейна:

$w(a,\varepsilon) = 1$

$w(\varepsilon,b) = 1$

$w(a,b) = 1$, если $a \neq b$

$w(a,b) = 0$, если $a = b$

В процессе вычислений значения $\square_{i,j}$ записываются в массив $(m+1) * (n+1)$. При этом вычисляются они с помощью следующего рекуррентного соотношения:

$$d_{i,j} = min\{d_{i-1,j} + w(x_{i,\varepsilon}), d_{i,j-1} + w(\varepsilon, y_j), d_{i-1,j-1} + w(x_i, y_i)\}$$

Оно выводится следующим образом. Если предположить, что известна цена преобразования $x(1,i-1)$ в $y(1,j)$, то цену преобразования $x(1,i)$ в $y(1,j)$ мы получим, добавив к ней цену удаления x_i. Аналогично, цену преобразования $x(1,i)$ в $y(1,j)$ можно получить, прибавив цену вставки y_j к цене преобразования $x(1,i)$ в $y(1,j-1)$. Наконец, зная цену преобразования $x(1,i-1)$ в $y(1,j-1)$, цену преобразования $x(1,i)$ в $y(1,j)$ мы получим, прибавив к ней цену замены xi на yj. Вспомним, что расстояние $d_{\square,j}$ является минимальной ценой преобразования $x(1,j)$ в $y(1,j)$, поэтому из трех указанных выше операций надо выбрать самую дешевую.

Перед тем, как начать вычислять $d_{i,j}$ надо установить граничные значения массива. Что касается первого столбца массива, то значение $d_{i,0}$ равно сумме цен удаления первых i символов x. Аналогично, значения $d_{0,j}$ первой строки задаются суммой цен вставки первых j символов y. Итак, имеем следующее:

$d_{0,0} = 0$

$d_{i,0} = \sum_{k=1}^{i} w(x_i, \varepsilon)$, для $1 < i < m$

$d_{0,j} = \sum_{k=1}^{j} w(\varepsilon, j_k)$, для $1 < j < n$

Для расстояния Левенштейна $d_{i,0} = i$ и $d_{0,j} = j$.

Алгоритм вычисления массива расстояний, разработанный Вагнером и Фишером:

-инициализация границ массива

$d_{0,0} = 0$

for i = 1 to m

$d_{i,0} = d_{i-1,0} + w(x_i, \varepsilon)$

for j = 1 to n

$d_{0,j} = d_{0,j-1} + w(\varepsilon, y_j)$- вычисление $d_{i,j}$

for i = 1 to m

for j = 1 to n

$$d_{i,j} = min\{d_{i-1,j} + w(x_{i,\varepsilon}), d_{i,j-1} + w(\varepsilon, y_j), d_{i-1,j-1} + w(x_i, y_i)\}$$

Можно видеть, что стадия инициализации границ включает $1 + m + n$ операций, а основной цикл повторяется mn раз. Таким образом, временная сложность этого алгоритма составляет $O(mn)$.

Последовательность операций редактирования для преобразования x в y можно получить с помощью структуры, называемой *след*. След из x в y можно описать как соединение символов строки x с символами помещенной под ней строки y ребрами, причем каждый из символов соприкасается не больше чем с одним ребром, и никакие два ребра не пересекаются. Представляя ребро из x_i в y_j как упорядоченную пару целых чисел (i, j), след из x в y можно формально определить как множество упорядоченных пар, удовлетворяющих следующим условиям:

(a) $1 < i < m, 1 < j < n$

(b) для разных ребер $(i_1, j_1), (i_2, j_2)$

$i_1 \neq i_2,\ j_2 \neq j_2, i_1 < i_2 <=>\ j_2 < j_2$

Последовательность операций редактирования можно получить из следа следующим образом. Все не касающиеся ребер символы x надо удалить, а аналогичные символы y вставить. Для каждого ребра (i, j) в следе, x_i заменить на y_j, если $x_i \neq y_j$, если же $x_i = y_j$, то редактирование не требуется. След с наименьшей ценой от sberbank к zeirobnak:

```
i     1 2 3 4 5 6 7 8
xi    s b e r b a n k
      | / | \ | \
yj    z e i r o b n a k
j     1 2 3 4 5 6 7 8 9
```

В связи с целями проводимого исследования необходимо отметить, что цены замены $w(a, b)$, удаления $w(a, \varepsilon)$ и вставки $w(\varepsilon, b)$ должны отличаться в зависимости от визуальной близости символов в адресной строке. Они могут формироваться следующим образом:

1. Цена операции замены $w(a, b)$ равна значению функции близости символов a и b, которое стремится к 0 при их максимальной "похожести" (о и 0, 1 и l). Для оценки близости могут быть использованы различные методы, применяемые при распознавании символов в оптических системах распознавания: сопоставления с шаблоном, статистические, на базе интегральных преобразований (методы, использующие Фурье-дескрипторы символов или частотные дескрипторы границ), структурные, а также классификации.

2. Цена операции вставки символа $w(\varepsilon, b)$ зависит от его окружения (символов, находящихся слева и справа от него), то есть если $y_j = b$, то надо учитывать символы y_{j-1} и y_{j+1}. В этом случае необходимо оценивать близость изображения биграммы (y_{j-1}, y_{j+1}) и триграммы (y_{j-1}, y_j, y_{j+1}).

3. Операция удаления символа $w(a, \varepsilon)$ в этом смысле обратна операции вставки и поэтому также необходимо оценивать близость триграммы (y_{j-1}, y_j, y_{j+1}) и биграммы (y_{j-1}, y_{j+1}) при $y_j = a$.

4. В ряде случаев происходит замена одного символа на два (например, m на rn, d на cl). Метод Вагнера-Фишера данную замену рассматривает как две последовательные операции редактирования (одна замена и одна вставка), что не позволяет выявить визуальную близость адресных строк. В дальнейших исследованиях необходимо предусмотреть данную ситуацию посредством модификации алгоритма.

Предложенный метод позволяет оценивать степень близости адресов фишинговых и реальных страниц (сайтов). Он использован в качестве ядра алгоритма поиска и выявления имен фишинговых сайтов в сети Интернет, а также может применяться для проверки качества работы средств защиты от фишинговых атак

Список литературы

1. Джеймс, Л. Фишинг: Техника компьютерных преступлений / пер. с англ. Р.В. Гадицкого. - М.: НТ Пресс, 2008. – 314 с.

2. Хачатурова, С.С. Осторожно, фишинг! /С.С. Хачатурова, Ю.П. Жихарева// Международный журнал прикладных и фундаментальных исследований. – 2016. – № 4-4. – С. 793-795.

3. Левенштейн, В.И. Двоичные коды с исправлением выпадений, вставок и замещений символов / В.И. Ливенштейн// Доклады Академий Наук СССР. – 1965. – С. 845–848.

4. Бобылева, О.В. Математические аспекты метода Вагнера-Фишера / О.В. Бобылева// Молодой ученый. – 2014. – №13. – С. 1-4.

Материал поступил в редколлегию 23.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.414.23

***Шугуров Дмитрий Евгеньевич**, сотрудник*
***Анисенкова Алина Олеговна**, сотрудник*
Академия ФСО России, Орел, Россия
e-mail: shdevg@mail.ru

БЕЗОПАСНОСТЬ МАРШРУТИЗАЦИИ В ОТКРЫТЫХ СЕТЯХ

Описаны уязвимости ИТКС, приведен вариант топологии сети, в котором возможна реализации различных атак на передаваемы данные и проведена их классификация, определены способы определения маршрута передачи данных.

В настоящее время большинство пользователей, используя открытые сети, передают некоторые свои персональные данные, считая, что это достаточно безопасно. При этом достоверно уверенные, что передаваемые ими данные не могут быть использованы в корыстных целях третьими лицами или же привести к их финансовым потерям. Отсюда возникает вопрос, на сколько уязвима система и какие способы защиты могут применяться для исключения перехвата данных и изменения маршрута.

Рассмотрим характерные уязвимости информационно-телекоммуникационной сети используемые нарушителем для атаки, направленной на ПЭВМ жертвы посредством специальных программ, реализованных через сеть, цель которых завладеть, модифицировать или уничтожить важную для пользователя информацию. В качестве примера можно выделить следующие уязвимости информационно-телекоммуникационной сети (ИТКС) представленные на рис. 1.

Рис. 1. Уязвимости ИТКС

Рассмотрим одну из основных причин более детально, на примере отсутствия в ИТКС возможности контроля маршрута передачи сообщений.

В ИТКС в качестве начальной фазы соединения между источником и приемником служит идентифицирующий адрес. Под адресом объекта понимается определенная системой уникальная информация, которой он наделяется при внесении в систему. Все сообщения от других взаимодействующих объектов ИТКС, отправленные на этот адрес, поступят на данный объект. Путь или маршрут сообщения определяется топологией ИТКС и проходит через совокупность узлов-маршрутизаторов, задачей которых является проанализировать адрес назначения и выбрать оптимальный путь для переправки объекта пользователю. На рис. 2 представлен вариант топологии сети и возможного внешнего нарушителя, который имеет возможность перенаправления трафика.

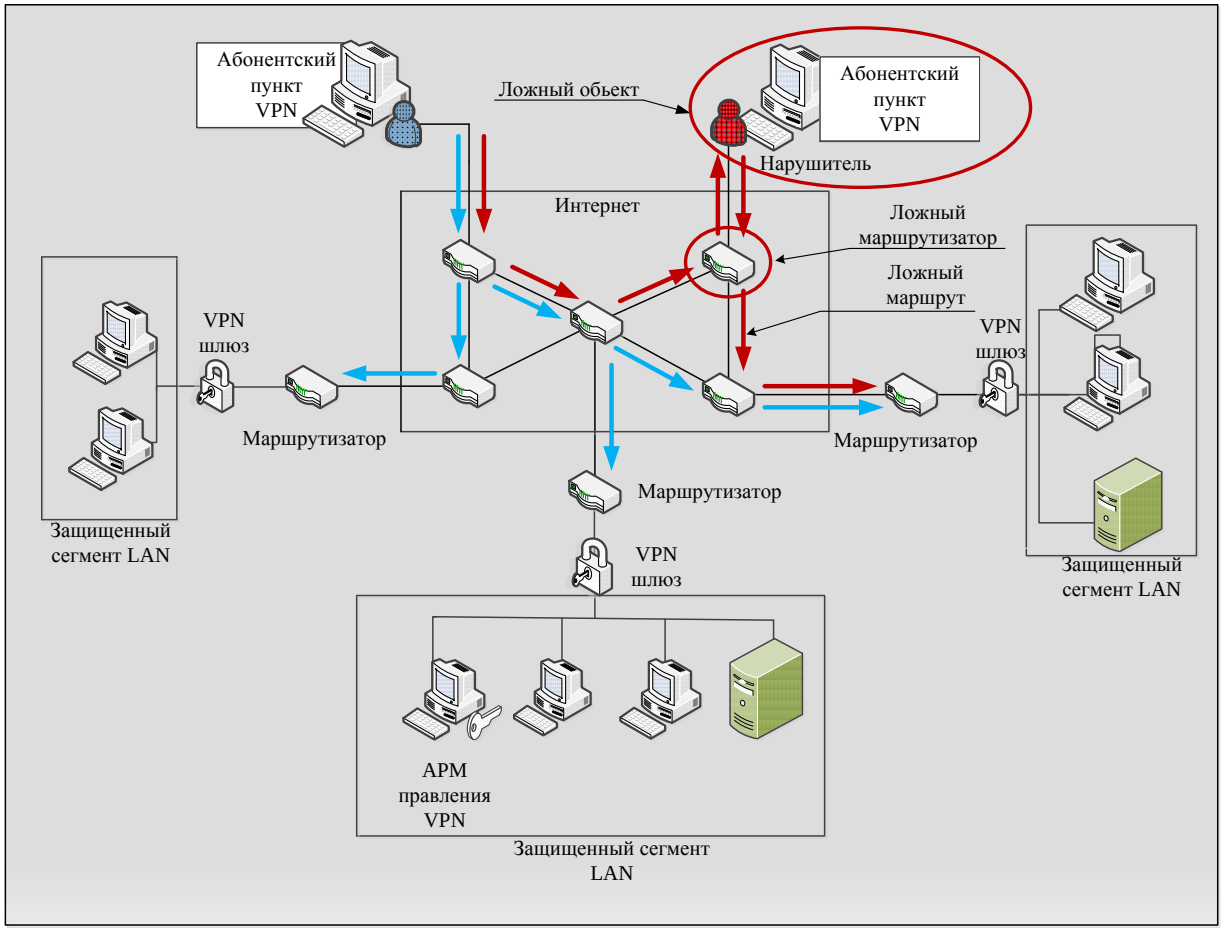

Рис. 2. Вариант топологии сети

Если в сети не предусмотрен контроль за маршрутом передвижения, то адрес полученного сообщения окажется ничем не подтвержден [1]. Это значит, что существует возможность отправки сообщения от чужого имени, путем указания в заголовке чужого адреса. Еще одним недостатком таких сетей будет невозможность отследить подлинный адрес откуда пришло сообщение, а следовательно, нельзя точно определить координаты нарушителя.

Используя эту уязвимость, нарушитель может реализовать свои атаки различными способами, например внедрить ложный объект на основе навязывания ложного маршрута. В настоящее время данная ситуация может возникнуть в открытой сети Интернет. Ввиду того, что для обеспечения эффективной и оптимальной маршрутизации в сети применяются специальные управляющие протоколы, RIP (Routing internet Protocol), OSPF – (Open Shortest Path First), но при этом отсутствует контроль прохождения трафика, где задачей нарушителя является изменение первоначальной маршрутизации на объекте ИТКС так, чтобы новый маршрут проходил через ложный объект-хост нарушителя. Для этого необходимо изменить исходные таблицы маршрутизации, значит, нужно отправить определенные протоколы управления сетью служебные сообщения, позволяющие изменить маршрут следования сообщений и получить контроль над потоком информации между объектами. На рис. 3 представлен этап реализации подложных ICMP–ответов [2].

Рис.3. Этапы реализации атак путем отправки ложных ICMP-ответов

Также существует еще одна реализация удаленной атаки на основе вышеуказанной уязвимости это внедрение ложного объекта на основе использования недостатков удаленного поиска. Зачастую оказывается, что в сети удаленные объекты не имеют достаточно информации для адресации сообщения, например аппаратные и логические адреса объектов. Для получения нужной информации используется множество алгоритмов удаленного поиска, заключающиеся в передаче по сети различных видов запросов и ожидания ответов на них, что впоследствии предоставит нарушителю необходимую информацию. После нарушитель использует ее для адресации ложного сообщения. Также существует возможность перехвата запроса и отправки на него ответа, в котором будут содержаться данные для создания канала между пользователем и хостом нарушителя.

Подмена доверенного объекта также может иметь место в перехвате персональных данных. Она заключается в передаче по каналу связи сообщений от имени произвольного объекта сети, и также меняет маршрут сообщений. Если есть установленное визуальное соединение, то суть данного способа будет заключаться в присвоении прав доверенного объекта, который подключился к данной сети, и использовании его имени в дальнейших целях. Также данный способ может быть представлен, как подменна доверенного объекта с обратной

связью, что даст возможность нарушителю управлять объектами с двух концов соединения [3].

Таким образом, можно сделать вывод, что маршрут от отправителя до получателя будет определяться цепочкой узлов, которые пройдет сообщение. Для предупреждения удаленной сетевой атаки можно предложить следующие варианты решения:

Предусмотреть в маршрутизаторе функцию проверки подлинности адреса отправителя с адресом откуда пришло данное сообщение. В случае подтверждения подлинности сообщение должно быть отправлено получателю, в ином случае – отфильтровано.

Создание отдельного поля в заголовке, в которое будет заноситься маршрутная информация, т. е. каждый маршрутизатор, через который будет проходить сообщение, последовательно оставит в этом поле метку, которая будет указывать на данное устройство. Это поможет точно определить полный маршрут следования сообщения от отправителя до получателя, тем самым убедиться в достоверности маршрута.

Список литературы

1. Хорев,П.Б. Программно-аппаратная защита информации :учебное пособие/П.Б. Хорев – М.: ФОРУМ, 2009. – 352 с.

2. Михайлов, С.Ф. Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции: учеб. пособие/ С.Ф. Михайлов, В.А. Петров, Ю.А. Тимофеев. – М.: МИФИ, 1995. – 112 с.

3. Юркин, А.А. Системы анализа защищенности : практическое пособие / А. А. Юркин, Д.Е. Шугуров [и др.] ; под общ. ред. А. А. Юркина. – Орёл : Академия ФСО России, 2017. – 140 с.

Материал поступил в редколлегию 18.04.18.

ISBN 978-5-906967-92-3 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2018

УДК 004.414.23

***Шугуров Дмитрий Евгеньевич**, сотрудник*
***Скородумов Александр Сергеевич**, сотрудник*
Академия ФСО России, Орел, Россия
e-mail: shdevg@mail.ru

НЕОБХОДИМОСТЬ ПРИМЕНЕНИЯ БИОМЕТРИЧЕСКИХ СИСТЕМ АУТЕНТИФИКАЦИИ

Описана структура обобщенной компьютерной сети, приведены сервисы безопасности, проведена классификация угроз для обобщенной автоматизированной системы и проведено теоретическое обоснование необходимости применения биометрических систем аутентификации.

В настоящее время компьютерные сети предназначены для реализации обработки, хранения и передачи информации, именно поэтому важной задачей при организации подобных систем является обеспечение безопасного процесса взаимодействия с информацией посредством организации защищенного доступа пользователей к автоматизированным рабочим местах [1].

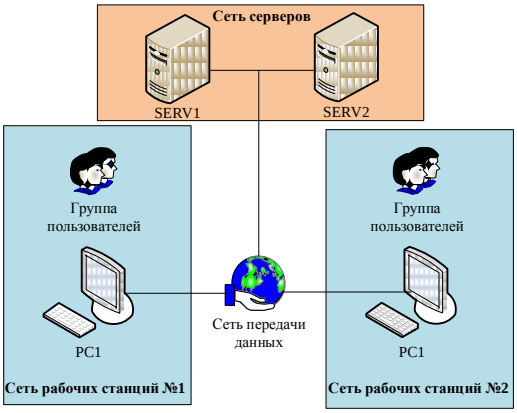

Рис. 1. Обобщенная схема компьютерной сети

Из рассматриваемых подсистем компьютерной сети выделена сеть рабочих станций, а именно составляющие процесса доступа пользователей к АРМ. Для защиты сети от несанкционированных действий разработаны сервисы безопасности, каждый из которых отвечает за определенные функции защиты. Организация функционирования отдельного сервиса безопасности в рамках компьютерной сети повышает уровень безопасности сети в целом. На рисунке 2 представлены основные сервисы безопасности которые напрямую влияют на защищённость компьютерной сети [2].

Из представленных сервисов рассмотрим сервис разграничения доступа, который определяет порядок предоставления доступа пользователям системы, а также уровень прав этого пользователя на получение доступа к определённой

информации. Также рассмотрим сервис идентификации и аутентификации, который определяет непосредственный алгоритм предоставления пользователями данных, необходимых для входа в систему и алгоритм проверки соответствия предоставленных данных с лицом, их предоставившим. Отсюда становится очевидным, что процесс аутентификации является основным процессом в эксплуатации защищенной компьютерной сети. Компьютерная сеть с реализованными в ней сервисами безопасности может выполнять функции автоматизированной системы обработки данных (АСОД).

Рис.2. Сервисы безопасности в соответствии с ГОСТ Р ИСО/МЭК 15408-2003

В случае рассмотрения государственных информационных систем тип рассматриваемой системы обработки данных определяется типом обрабатываемой, хранимой на АРМ информации, которая носит ограниченный (конфиденциальный) характер. Классификация АСОД определяется типом информации, обрабатываемой в системе, количеством пользователей с разными уровнями прав на доступ к информации. Для информационной системы, в которой организуется защищенный доступ пользователей к АРМ существует ряд угроз безопасности информации, которые могут быть реализованы нарушителем в том числе и на подсистему аутентификации (рис.3).

Угрозы аутентификации
Сбои, отказы оборудования и программного обеспечения
Непреднамеренное разглашение парольной информации лицами, имеющими права доступа
Несанкционированное изменение аутентификационной информации, несанкционированное копирование защищаемой информации
Несанкционированный доступ к защищаемой информации, несанкционированное уничтожение защищаемой информации
Несанкционированное подключение к техническим средствам и системам, физическая подмена технических средств или их отдельных узлов
Несанкционированные действия со стороны лиц, имеющих права доступа к защищаемой информации
Использование дефектов программного обеспечения средств защиты
Подмена легитимного пользователя

Рис. 3. Возможные угрозы для подсистемы аутентификации

Из рассмотренного перечня наиболее актуальной является "подмена легитимного пользователя". Реализация этой угрозы может привести не только к несанкционированному доступу, но и к модификации и другим изменениям информации. Следовательно, для повышения эффективности защиты от угрозы подмены легитимного пользователя необходимо совершенствовать систему аутентификации пользователя. Наиболее общий подход для создания системы аутентификации предполагает наличие у пользователя следующих информационных и вещественных данных [3]:

А. Персональная информация. (пароль, графический ключ).

Б. Уникальный предмет. (смарт-карта, RU-токен).

В. Ассоциированная с пользователем информация (координаты местоположения).

Г. Биометрическая информация пользователя (отпечаток пальца, геометрия руки и другие виды биометрической аутентификации).

Для угрозы подмены пользователя предлагается использовать биометрические данные, которые в совокупности с другими факторами однозначно повысят защищённость доступа. При этом биометрические методы распознавания пользователя различны и предоставляют пользователям огромный выбор технологий и средств, в зависимости от требуемой точности и конкретных биометрических характеристик.

Основные достоинства использования биометрических систем распознавания пользователя представлены на рис. 4.

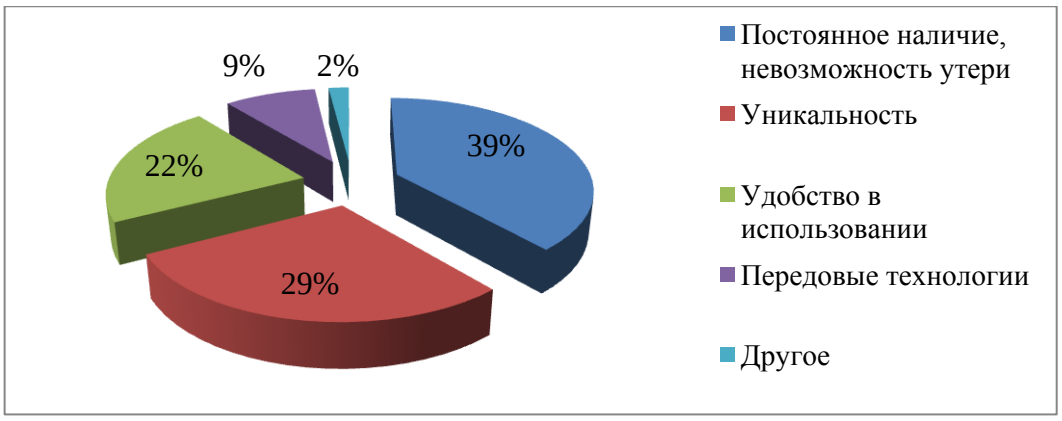

Рис. 4. Достоинства биометрической аутентификации

Учитывая достоинства биометрических методов, можно предположить их несомненное преимущество в использовании для упреждения угрозы подмены пользователя, а именно:

– присутствие признака непосредственно у лица, а так же возможности комбинации нескольких признаков;

– уникальность признакового пространства, достаточно большое их количество, но не безразмерное;

– достаточное удобство, позволяет пользователю не запоминать сложные комбинации паролей;

– передовые технологии, рынок биометрических средств на базе высокопроизводительных систем в достаточно малое время способен распознать пользователя;

– неявное (скрытое) использование методов аутентификации.

Перспективы биометрических методов аутентификации очевидны. Повсеместное и устойчивое развитие технологий и разработка инновационных продуктов делают биометрические методы все более доступными для конечного пользователя как в плане наличия готовых решений, так и в плане стоимости, а также увеличивают точность средств, реализующих биометрические методы.

При использовании системы распознавания доступ пользователей к АРМ может быть реализован в защищенных условиях, тогда достоверность данных субъекта может иметь достаточно высокий уровень. Однако необходимо ввести дополнительные средства защиты при доступе к АРМ. Этим средством является система распознавания пользователей на основе использования биометрических методов аутентификации, которые будут проверять легитимность пользователя.

Список литературы

1. ГОСТ Р ИСО/МЭК 15408 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий" (три части).

2. Афанасьев, А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: учебное пособие для вузов / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др.; под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. – М.: Горячая линия – Телеком, 2016. – 552 с.

3. Галатенко, В. А. Идентификация и аутентификация, управление доступом. Лекция из курса "Основы информационной безопасности" / В. А. Галатенко. – Интернет Университет Информационных Технологий, 2016.

Материал поступил в редколлегию 18.04.18.

СОДЕРЖАНИЕ