МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Брянский государственный технический университет

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

Материалы XI Межрегиональной научно-практической конференции

30 апреля 2019 г.
г. Брянск

БРЯНСК
ИЗДАТЕЛЬСТВО БГТУ
2019

ББК 75.7

Информационная безопасность и защита персональных данных. Проблемы и пути их решения: материалы XI Межрегиональной научно-практической конференции [Электронный ресурс]/ под ред. О.М. Голембиовской, М.Ю.Рытова. – Брянск: БГТУ, 2019. – 224с.

ISBN 978-5-907111-88-2

Приведены материалы докладов участников XI Межрегиональной научно-практической конференции «Информационная безопасность и защита персональных данных. Проблемы и пути их решения», состоявшейся 30 апреля 2019 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. Пестракова

Темплан 2019 г., п.28

Подписано в печать 13.05.19 Формат 60x84 1/16. Бумага офсетная. Офсетная печать. Печ.л. 13,8 Уч.-изд.л. 13,8

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

ISBN 978-5-907111-88-2

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

Анисимов Константин Сергеевич, *сотрудник*
Горбачев Павел Николаевич, *сотрудник*
Академия ФСО России
Россия, г. Орёл
e-mail: pavel.gorbachev@list.ru

ПРОТОТИП ПРОГРАММНОГО СРЕДСТВА ТРАССИРОВКИ ПРИЛОЖЕНИЙ НА БАЗЕ PIN

Описаны подходы к трассировке приложений в процессе поиска ошибок, некорректных реализаций алгоритмов с использованием динамической бинарной инструментации.

В настоящее время существует множество средств динамической бинарной инструментации и многие из них созданы при помощи фреймворка PIN для платформы Windows. Так как это очень удобное средство для тестирования приложений и сбора данных о его работе, то весьма актуальным вопросом является создание такого программного средства, которое будет объединять в себе все необходимое для анализа приложений. Структурно это приложение будет представлять собой программное средство с включенными в него модулями (рис. 1).

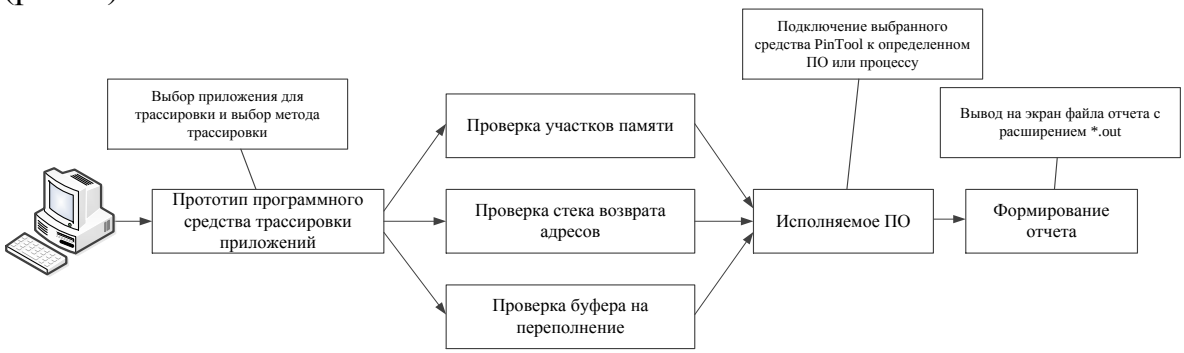


Рис. 1. Функциональная схема прототипа программного средства трассировки приложений

ПЭВМ предназначена для организации взаимодействия пользователя с программным средством трассировки приложений. А именно: установка параметров, запуск и получение результатов тестирования. Данный элемент взаимодействует с модулями динамической бинарной инструментации PIN. ПЭВМ может функционировать только на ОС семейства Windows. Для взаимодействия с данным приложением требуется .NET Framework 4.5.2 или новее.

На ПЭВМ запускается приложение PinTool и отображается форма выбора средства трассировки приложений, выбор приложения или выбор запущенного процесса, для подключения к данному ПО выбранного средства трассировки.

Сам прототип программного средства трассировки приложений является важной составляющей, потому что предоставляет пользователю интуитивно

понятный интерфейс для тестирования исполняемого ПО, а также помогает пользователю взаимодействовать со средствами трассировки приложений и по окончанию тестирования формировать отчет о возможных уязвимостях, найденных в исполняемом ПО.

Данные, собранные в ходе трассировки, хранятся в файлах с расширением *.out (trace.out и т. д.), после их формирования они выводятся на экран пользователя для ознакомления с ними.

Главным компонентом данного программного средства являются его модули, которые представляют собой отдельные средства, созданные при помощи фреймворка PIN. Первым модулем является средство проверки работы с памятью (алгоритм его работы приведен на рис. 2). Данное средство собирает информацию об участках памяти, где по одному и тому же адресу производится: двойное освобождение памяти; освобождение памяти, ранее не выделенной; вторичное выделение памяти, которая уже была выделена по данному адресу. Сбор происходит посредством записи в контейнер всех вызовов функций free() и malloc() и последующее их сравнение и нахождение ошибок памяти по вышеприведенным критериям.

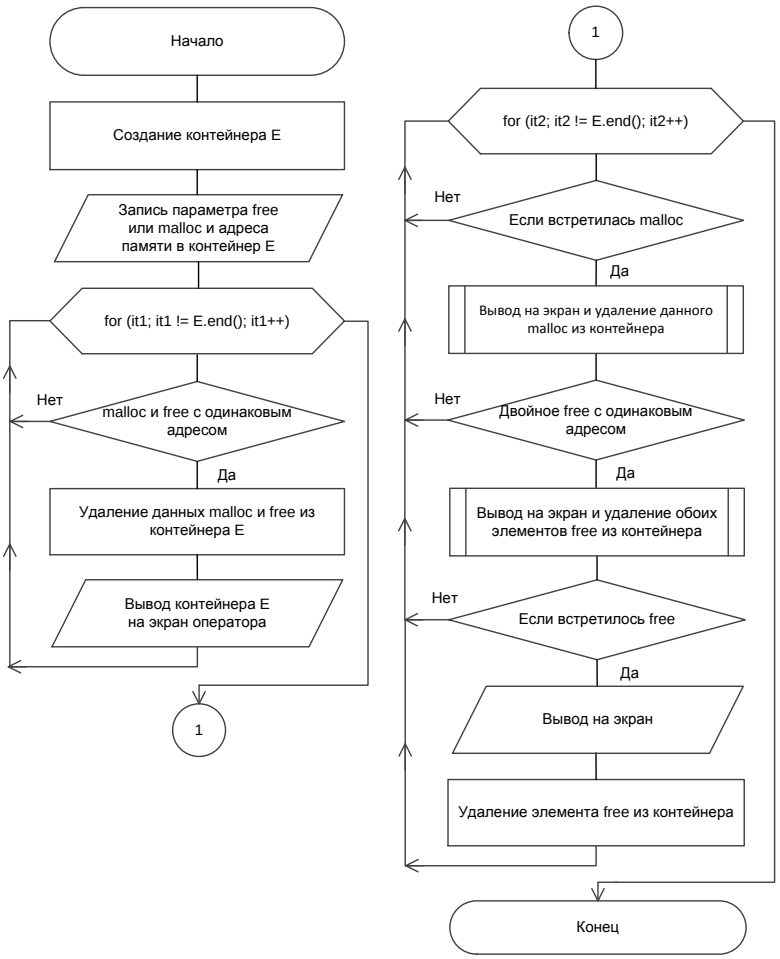
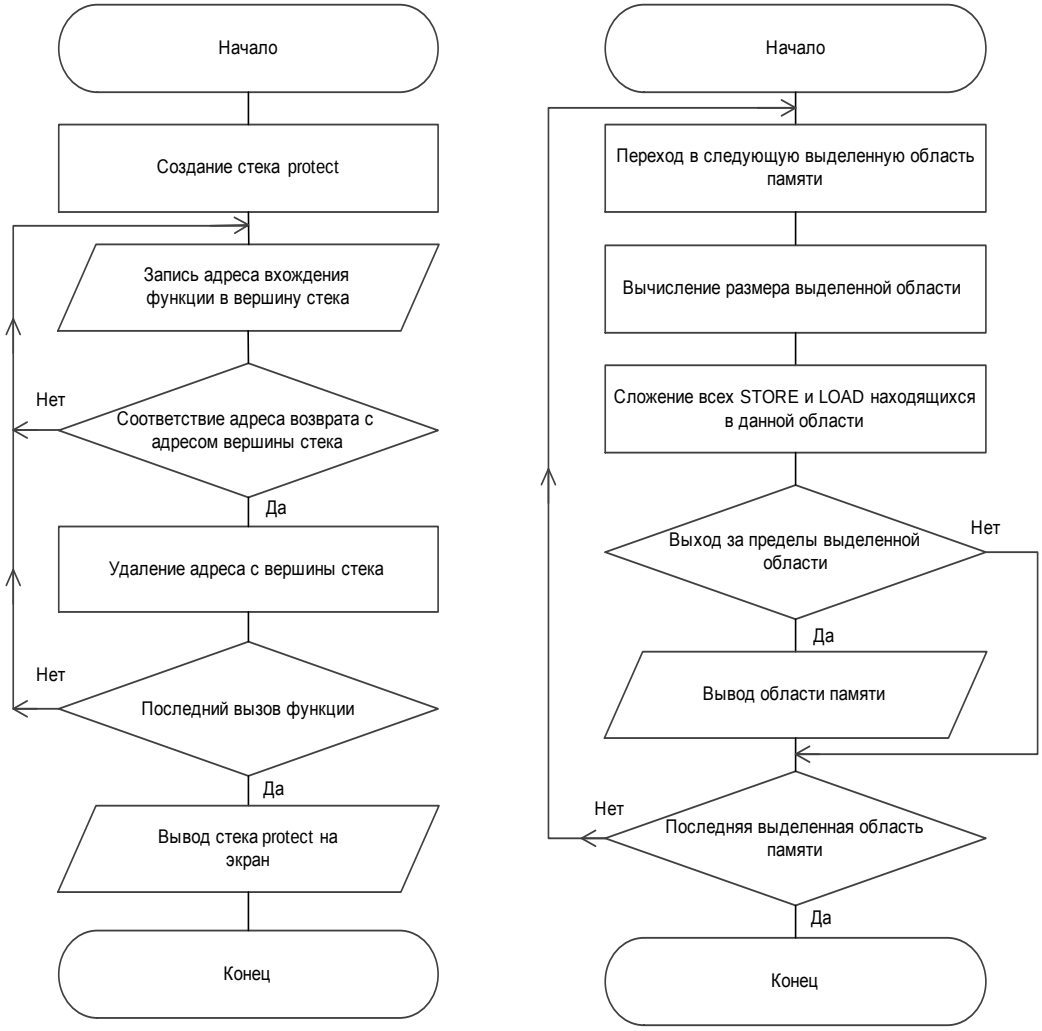


Рис. 2. Алгоритм функционирования средства анализа участков памяти

Вторым модулем является средство проверки стека возврата адресов памятью (алгоритм его работы приведен на рис. 3а). Данное средство создает “теневой” стек возврата адресов для того, чтобы отслеживать изменения в “основном” стеке возврата адресов. То есть при вхождении в функцию, происходит запись адреса этой функции в вершину стека, а при выходе сверка адреса этой функции с адресом, занесенным на вершину стека. Если эти адреса соответствуют друг другу, то происходит “выталкивание” последнего внесенного элемента на вершину стека, если совпадения не имеется, то работа программы продолжается дальше. В конце все оставшиеся адреса в стеке выводятся пользователю и помечаются как адреса, в которых происходила подмена адреса во время работы ПО, а также выводится наименование функции для облегчения поиска и работы по устранению данной неисправности.



а) б)

Рис. 3. а – алгоритм функционирования средства проверки стека возврата адресов;
б – алгоритм функционирования средства проверки буфера на переполнение

Последним модулем является средство проверки буфера на переполнение (алгоритм работы приведен на рис. 3б). Когда в буфере выделяется область па-

мяти под определенные данные, обычно распределитель памяти устанавливает заголовки в начале или в конце (или в обоих местах) области памяти. Эти заголовки могут содержать некоторую информацию, такую как: размер; использована память или нет и прочее. Выделенная область имеет определенный размер, значение которого находится в заголовке и, соответственно, добавление данных, превышающих размер заголовка, приводит к переполнению буфера. Каждый заголовок зависит от распределителя и его версии. В общих чертах, память выглядит так (рис. 4):

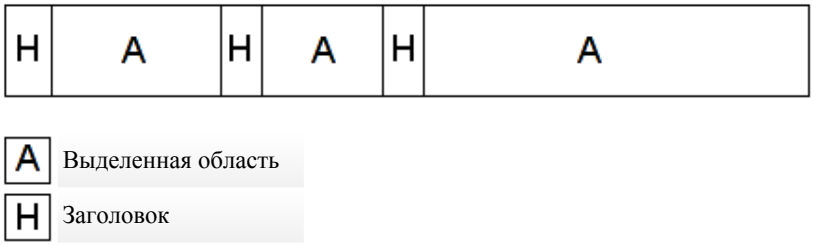


Рис. 4. Разделение памяти на выделенную и заголовки

Если происходит контроль распределителя памяти, то можно определить базовый адрес и размер областей выделения. Затем, если проверять все доступы STORE и LOAD в памяти, можно определить, какой из них находится за пределами выделенной области. Следующая диаграмма представляет, как выглядит загрузка в память и хранение в ней, а также красным отмечен выход за пределы памяти (рис. 5).

Рис. 5. Выход за пределы выделенной области

Алгоритм программы простой: при встрече заголовка выделенной области памяти происходит считывание размера выделенной области и далее идет сложение всех STORE и LOAD, находящихся в данной области. Если сумма этих данных превышает размеры выделенной области, то произошло переполнение буфера на данном участке памяти, о чем информируется пользователь и процесс проверки идет дальше до тех пор, пока не будут пройдены все участки памяти.

Список литературы

1. Инструментация — эволюция анализа – [Электронный ресурс] – https://xakep.ru/2013/09/11/61232/.

2. Application Instrumentation: Application Analysis with Pin – [Электронный ресурс] – https://msdn.microsoft.com/en-us//magazine/dn818497.aspx.

3. Pin: Pin 3.2 User Guide – [Электронный ресурс] – https://software.intel.com/sites/landingpage/pintool/docs/81205/Pin/html/

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

Н.М. Аршинов
Научный руководитель: доц. кафедры «Системы информационной безопасности», к.т.н., О.М. Голембиовская
ФГБОУ ВО «Брянский государственный технический университет»
Россия, г. Брянск
Mehanik32rus@ya.ru

РАЗРАБОТКА МЕТОДИКИ МИНИМИЗАЦИИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ

Рассматриваются этапы формирования методики по минимизации рисков информационной безопасности коммерческой организации.

В ходе анализа нормативно-правовой базы, а также учебников и статей по данной проблематике, было решено разработать методику минимизации рисков коммерческой организации, позволяющую в отличие от известных методик проводить более быстрый анализ рисков информационной безопасности коммерческой организации.

Методика минимизации рисков информационной безопасности коммерческой организации состоит из следующих этапов:

1. Идентификация активов.
2. Определение основных угроз и уязвимостей.
3. Определение средств защиты информации (СЗИ) организации с помощью базы данных (БД) СЗИ.
4. Оценка ущерба.
5. Определение рисков.
6. Выбор мер и средств по снижению рисков.

1. Идентификация активов.

На первом этапе необходимо определить активы коммерческой организации, подлежащие защите, к которым относятся: электронные документы, базы данных, бизнес-процессы и т.д. Фрагмент определения ценного актива для организации представлен в табл.1.

Таблица 1

Активы коммерческой организации

№ п/п	Актив	Какой инцидент может произойти	Нарушение свойства безопасности	Оценка нанесенного ущерба
1	Электронные документы	Неправомерный доступ	Доступность Целостность Конфиденциальность	Создание новых документов 35 тыс. руб. Восстановление электронных документов 30 тыс. руб. Потери 15 тыс. руб.

2. Определение основных угроз и уязвимостей.

На втором этапе необходимо сформулировать список актуальных угроз для выявленных активов. Данный список угроз сформирован на основании анализа угроз из банка данных угроз информационной безопасности ФСТЭК (Федеральная служба по техническому и экспортному контролю) России. В табл.2. приведен фрагмент таблицы угроз и уязвимостей.

Таблица 2

Угрозы и уязвимости ИБ для актива организации

№ п/п	Наименование угрозы	Соответствующие ей уязвимости
1	НСД	Открытый доступ к БД
		Отсутствие пароля
		Отсутствие разграничения доступа к документам
		Отсутствие видеонаблюдения
		Отсутствие сигнализации
2	Воздействие вирусов	Несвоевременное обновление средств АВЗ
		Отсутствие средств АВЗ
		Нестойкость ПО к вирусам

3. Определение СЗИ организации с помощью БД СЗИ.

На третьем этапе нужно провести идентификацию СЗИ (средств защиты информации) коммерческой организации для получения сведений о вероятности угроз, которым подвержены активы. Средства занесены в базу данных СЗИ. Сравнение средств между собой было проведено по методу анализа иерархий. И определена вероятность угрозы в соответствии с концепцией определения угроз ПДн (персональных данных) (табл.3).

Таблица 3

Вероятность реализации угроз ИБ

№ п/п	Формулировка вопроса	Наименование средств и мер нейтрализации	Вероятность угрозы	Наличие на объекте средства нейтрализации
1	Какие средства борются с угрозой НСД?	SecretNet 7	0	Блокхост-сеть 2.0
		DallasLock 8.0-C	2	
		Блокхост-сеть 2.0	5	
		Страж NT 4.0	5	
		Нет	10	
2	Какие средства борются с угрозой воздействия вирусов?	Dr.Web	0	ESET NOD32
		Kaspersky	2	
		ESET NOD32	2	
		Нет	10	

4. Оценка ущерба.

На четвертом этапе необходимо провести оценку ущерба. Ценность активов можно рассматривать с точки зрения ущерба, который может быть причи-

нен в результате разглашения, удаления или изменения информации. Для оценки активов по балльной системе необходимо знать ежемесячную прибыль организации. В табл. 4 представлены единицы ущерба и соответствующий им балл.

Таблица 4

Баллы ущерба коммерческой организации

№ п/п	Балл	Ущерб (руб.)	Ежемесячная прибыль
1	**2**	**3**	**4**
1	1	до 20 тыс. руб.	100 тыс. руб.
2	2	20 – 40 тыс. руб.	
3	3	40 – 60 тыс. руб.	
4	4	60 – 80 тыс. руб.	
5	5	более 80 тыс. руб.	

5. Определение рисков.

На пятом этапе необходимо провести оценку рисков информационной безопасности для каждого актива. Риск складывается из произведения ценности актива и вероятности реализации угрозы (табл. 5).Данная оценка позволяет получить качественную оценку риска «Низкий», «Средний», «Высокий».

Таблица 5

Пример оценки рисков ИБ для коммерческой организации

№ п/п	Актив	Угроза	Риск
1	Личные дела (бумажный вид)	НСД	Н
		Нарушение целостности личных дел	Н
2	База данных	НСД	С
		Потеря данных при сбое техники	С
		DDOS атаки	Н
		Случайное или преднамеренное удаление сотрудником файлов БД	С
		Утечка информации по каналам передачи данных	Н

Нужно определить варианты по реагированию на риски: снизить, принять или перенести. В случае если по каким-то причинам не удается снизить риски, выполняется перенос на компетентные организации. Если риски устраивают, то их необходимо принять. Снижение рисков выполняется на следующем этапе.

6. Выбор мер и средств по снижению рисков.

На шестом этапе необходимо осуществить подбор необходимых средств и мер из базы данных СЗИ и базы данных мер ЗИ соответственно. Подбор средств и мер защиты нужно осуществлять до тех пор, пока остаточный риск не станет низким (табл. 6).

Таблица 6

Остаточные риски

№ п/п	Актив	Угроза	Средства и меры минимизации	Остаточный риск
1	База данных	НСД	DallasLock 8.0-C	Н
		Потеря данных при сбое техники	Полное копирование	Н
		Случайное или преднамеренное удаление сотрудником файлов БД	DallasLock 8.0-C	Н
		Физическое выведение из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Электронный пропуск	Н

Остаточный риск имеет качественную оценку «Низкий», поэтому его можно принять.

Таким образом, данная методика позволит оператору, работающему с персональными данными и коммерческой тайной, эффективно решать проблему минимизации рисков коммерческой организации, но так как эта методика трудоемка, целесообразно провести ее автоматизацию.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 303.64

Н.М. Аршинов
Научный руководитель: доц. кафедры «Системы информационной безопасности», к.т.н., О.М. Голембиовская
ФГБОУ ВО «Брянский государственный технический университет»
Россия, г. Брянск
Mehanik32rus@ya.ru

АНАЛИЗ НАУЧНОЙ ЛИТЕРАТУРЫ В ОБЛАСТИ МИНИМИЗАЦИИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ

Рассмотрены международные стандарты, законодательные акты РФ, книги и статьи, направленные на анализ информации по тематике «Минимизации рисков информационной безопасности».

Так, в рамках анализа международного стандарта ISO/IEC 27001 были сформулированы основные тезисы требований к системе менеджмента информационной безопасности в организациях различных форм собственности. Пункт 6.1 данного стандарта затрагивает вопросы действий по обработке рисков, который включает методы оценки и обработки рисков информационной безопасности.

Необходимым к рассмотрению и формированию общего подхода к оценке риска информационной безопасности на объекте является ГОСТ 27005-2010 Менеджмент риска ИБ (информационной безопасности). Приведенные в данном стандарте формулировки послужили основной для разработки методики оценки рисков ИБ, которая должна включать в себя следующие этапы:

1. Идентификация активов;
2. Определение угроз;
3. Оценка ущерба;
4. Определение риска.

Относительно нормативно-правовой базы Российской Федерации, ни один из НПА не регламентирует вопросы оценки рисков ИБ. Однако они позволяют получить общую классификацию конфиденциальной информации.

Одним из важнейших законодательных актов в РФ, положившим начало формированию общей системы нормативно-правовых актов, регулирующих процессы информатизации общества, явился Федеральный закон «Об информации, информатизации и защите информации» 1995г.

В целом Федеральный закон создал основу для упорядочения отношений в информационной сфере, а также послужил основой для последующего развития информационного законодательства. Этот закон действовал на протяжении более десяти лет и был заменен Федеральным законом от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и защите информации».

В законе сформулированы такие понятия в сфере информационной безопасности, как «информационная система» и «конфиденциальность информации» (статья 2).

Статья 6 определяет права обладателя информации, которым может быть, в том числе, и юридическое лицо (коммерческая организация):

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами.

Указанная статья также возлагает обязанности на обладателя информации по:

- принятию мер по защите информации;
- ограничению доступа к информации, если такая обязанность установлена федеральными законами.

Законодательно определено, что федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение (статья 9).

В коммерческих организациях информационная безопасность должна учитываться в первую очередь в отношении коммерческой тайны.

Основные понятия, непосредственно связанные с термином коммерческая тайна, наиболее полно приведены в Федеральном законе от 29.07.2004г. №98-ФЗ «О коммерческой тайне».

Коммерческая тайна – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. Коммерческая тайна представляет собой не разновидность информации, а ее определенное состояние – конфиденциальность, которая позволяет обладателю информации получить исключительно коммерческую выгоду в виде: увеличения доходов, избегания неоправданных расходов, сохранения положения на рынке либо получения иной коммерческой выгоды.

Помимо коммерческой тайны любая организация обязана обеспечить защиту персональных данных своих работников. Эти правила регламентирует Федеральный Закон от 27 июля 2006г. № 152-ФЗ «О персональных данных», действие которого направлено на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных.

В ходе анализа данных нормативно-правовых актов к рассматриваемой конфиденциальной информации в рамках данной научной работы решено отнести персональные данные и коммерческую тайну, ввиду их наибольшей регламентированости относительно обеспечении защиты с точки зрения законодательных норм.

Следующим этапом явилось рассмотрение возможных угроз для данных видов коммерческой информации. За основу были взяты такие документы, как базовая модель угроз, методика определения актуальных угроз, банк данных ФСТЭК (Федеральная служба по техническому и экспортному контролю) России включает в себя базу данных уязвимостей, а также список и описание киберугроз, наиболее характерных для государственных информационных систем, систем персональных данных и автоматизированных систем управления производственными и технологическими процессами на критически важных объектах. Используя данный банк угроз, можно создать основу для формирования перечня угроз. Кроме этого была изучена методика определения угроз ПДн (персональных данных), и взята за основу система, выявляющая вероятность угроз.

Немаловажной задачей в рамках анализа стал обзор учебников и статей по рассматриваемой тематике. Для формирования собственной методики целесообразно рассмотреть опыт предшественников.

Были рассмотрены научные статьи, касающиеся данной проблематики.

Авторы Малюков Ч.Ч., Трещев И.А. в статье «Исследование методики расчета рисков информационной безопасности» описывают основные этапы оценки рисков ИБ, которые можно использовать в данной работе, а именно:

1. Интервью, которое проводят эксперты для выяснения, какие именно активы используются.
2. Определение соответствия требованиям законодательства в области ИБ.
3. Разработка модели угроз. Для того чтобы максимально точно определить риск ИБ, необходимо разработать частную модель угроз ИБ предприятия.
4. Количественная оценка рисков ИБ.

В статье «Организация управления риском безопасности информационных банковских систем в кредитной организации» автора Корнейчука В.И. излагается об организации управления риском в банковских системах. Отсюда можно позаимствовать способы минимизации операционного риска безопасности ИБС:

1. Анализ состояния индикатора риска.
2. Выявления их наиболее худших значений.
3. Выработка рекомендаций для устранения недостатков.

Данные статьи позволили узнать о методиках расчетов рисков информационной безопасности, которые могут помочь в разработке методики минимизации рисков информационной безопасности в коммерческой организации.

Также был проведен обзор учебной литературы по данной теме.

Анисимов А.А. в учебнике «Менеджмент в сфере информационной безопасности» описывает основные направления управления работы в сфере информационной безопасности на уровне отдельного предприятия, раскрывает общую структуру политики информационной безопасности предприятия. Данный подход целесообразно использовать для разработки методики минимизации рисков информационной безопасности коммерческой организации.

Аверченков В.И. в учебном пособии «Методы и средства инженерно-технической защиты информации» уделяет внимание уязвимостям ИБ. Там описываются угрозы ИБ, которые имеют множество возможностей к реализации через уязвимости. Данная информация позволяет выбрать актуальные угрозы для дальнейшей работы.

В учебнике Галатенко В.А. «Основы информационной безопасности» представлены программные и технические меры защиты информации, направленные на контроль оборудования, программ и/или данных. Также рассматривается управление доступом. Достаточно хорошо здесь представлены программные и технические меры защиты информации, которые можно использовать для разработки методики. Управление доступом описано достаточно грамотно, поэтому данный аспект целесообразно добавить в разрабатываемую методику.

Данная учебная литература позволила получить сведения, которые будут использованы для разработки методики минимизации рисков информационной безопасности в коммерческой организации.

Таким образом, проанализированные международные стандарты, законы РФ, научные статьи и учебники будут применяться для разработки методики минимизации рисков коммерческой организации.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

Астапкович Дмитрий Сергеевич, *сотрудник*
Горбачев Павел Николаевич, *сотрудник*
Академия ФСО России
Россия, г. Орёл
e-mail: pavel.gorbachev@list.ru

ФАЗЗИНГ ФУНКЦИОНАЛЬНЫХ ОБЪЕКТОВ ПРИЛОЖЕНИЙ

Описана сущность фаззинга как методики тестирования приложений. Описан подход к тестированию приложений через тестирование их функциональных объектов, рассмотрена возможность использования динамической бинарной инструментации в процессе такого тестирования.

Активное развитие информационных технологий, автоматизация всех процессов сбора, обработки, распределения информации, автоматизация процессов управления приводит к увеличению числа программных продуктов. Помимо этого, происходит непрерывное усложнение используемых в этих программных продуктах алгоритмов, что в свою очередь приводит к увеличению объемов исходных текстов и полученных из них машинных кодов. Эти процессы характерны как для прикладного программного обеспечения, так и для системного (в том числе и системного программного обеспечения сетевого оборудования и пользовательской электроники). На фоне роста объема и сложности приложений все большую актуальность приобретают вопросы корректности работы и безопасности программного обеспечения.

Среди многих методов обнаружения уязвимостей программного обеспечения, доступных сегодня, фаззинг остается очень популярным благодаря своей концептуальной простоте, легкой реализации и огромному количеству эмпирических данных для обнаружения реальных уязвимостей программного обеспечения. Отличием тестирования методом фаззинга от остальных является то, что есть определенная цель, направленная на поиск ошибок, связанных с безопасностью, которые включают в себя программные сбои.

Фаззинг тестируемого объекта

Фаззинг — метод выполнения операций над тестируемым объектом, используя входные данные, отобранные из определенного хранилища входных параметров, который могли быть как случайными, так и детерминированными значениями. Есть три важных замечания к подходу тестирования методом фаззинга. Во-первых, входные данные для тестирования могут быть выбраны из хранилища с ожидаемыми параметрами, а значит, не гарантирован тот факт, что при первой итерации тестирования будет выявлено непредсказуемое поведение тестируемого объекта. Во-вторых, на практике процесс фаззинга почти всегда работает на протяжении многих итераций. Таким образом, необходимо написать «сценарий фаззинга», который будут значительно сокращать количество итера-

ций фаззинга и не уменьшать точность тестирования. В-третьих, процесс выбора параметров тестирования не обязательно должен быть рандомизирован.

Целью такого тестирования является проверить политику безопасности тестируемого объекта.

В рамках автоматизации процесса тестирования существует среда, которая выполняет тестирование объекта методом фаззинга и она называется фаззером. Ее задачей является проверить политику безопасности тестируемого объекта по определенному алгоритму фаззинга, который содержит значение параметров, которые передаются среде тестирования.

Общий алгоритм фаззинга тестируемого объекта.

Вход. Сценарий фаззинга тестируемого объекта, предел времени ожидания выполнения сценария тестируемым объектом.

Выход. Множество обнаруженных ошибок в тестируемом объекте.

Метод:

1. Присвоение множеству обнаруженных ошибок пустого значения.

2. Предварительная обработка сценария фаззинга. Сценарий фаззинга модифицируется в потенциально-модифицированный набор команд, предназначенных для выполнения объектом тестирования.

3. Пока время выполнения не превышает предела времени ожидания и пока не конец сценария тестирования, выполнять следующие действия.

3.1. В текущий момент выбирается набор данных из сценария тестирования, которые будут использоваться для текущей итерации тестирования

3.2. Выбранная итерация приводится к виду, пригодному для исполнения тестируемым объектом

3.3. Сконфигурированная итерация передается на исполнение тестируемому объекту. Контроль исполнения записывает информацию о результате выполнения текущей итерации, и если во время выполнения происходят нарушения политики безопасности, производится запись во множество обнаруженных ошибках исполнения.

3.4. На основе информации, полученной в результате исполнения, производится сокращение сценария тестирования.

4. Результатом фаззинга является отчет об обнаруженных ошибках в тестируемом объекте.

Фаззинг исполняемого приложения

В роли объекта тестирования, как правило, выступает исполняемое приложение. В таком случае подходы к фаззингу разделяют на:

- фаззинг по принципу белого ящика;
- фаззинг по принципу черного ящика.

Принцип «белого» заключается в том, что об исполняемом приложении известна исчерпывающая информация, имеется документация, исходные тексты, описание алгоритмов функционирования. Под «черным» ящиком подразумевается отсутствие какой-либо информации о тестируемом приложении, возможно только оказание на него некоторых воздействий и анализ реакции на них. Одной из проблем тестирования приложений является проблема формиро-

вания набора входных данных, которые обеспечат выполнение приложения по всем возможным маршрутам. Одним из вариантов решения этой проблемы является переход от тестирования самого исполняемого приложения к тестированию входящих в его состав функциональных объектов. Тестирование функциональных объектов требует совершения дополнительных действий в отношении тестируемого приложения, направленных на предоставление возможности вызова функциональных объектов с произвольными параметрами. Для обеспечения этой возможности необходимо получить информацию о порядке вызова тестируемых функциональных объектов (список параметров, тип возвращаемого значения и т.д.). В случае наличия исходных текстов приложения это не является проблемой, а задача сводится к написанию модульных тестов для соответствующих функциональных объектов. Гораздо сложнее обстоит дело в случае необходимости осуществить вызов с целью тестирования функционального объекта приложения без исходных текстов. Для этого необходимо определить:

- адрес в памяти, по которому размещается соответствующий функциональный объект;
- число его параметров;
- тип каждого параметра
- тип возвращаемого значения;
- соглашение о вызове, указывающее на порядок передачи параметров функциональному объекту и распределение обязанностей по очистке выделяемой памяти между вызывающим и вызываемым кодом.

Одним из отличий фаззинга функциональных объектов от традиционного тестирования программного обеспечения, где есть только две основные категории (тестирование черного и белого ящиков), является наличие тестирования методом серого ящика. Фаззинг функциональных объектов и является методом тестирования серого ящика так, как для реализации тестирования необходимо выполнить статический анализ исполняемого приложения, с целью выявления вышеперечисленных сигнатур.

Инструментация, как инструмент фаззинга

Автоматизировать процесс сбора вышеперечисленной информации можно, используя интерактивные средства дизассемблирования, которые предоставляют свои API. Дизассемблирование обеспечивает эффективное и правильное разделение функциональных объектов, восстанавливает поведение исполняемого приложения в ассемблерном виде, позволяя приступить к следующему этапу – передача параметров функциональным объектам. Чтобы осуществить контроль параметров, передаваемых функциональным объектам, возвращаемых ими значений и информации о корректности работы необходимо выполнять дополнительный код в момент вызова функционального объекта, в момент передачи управления вызывающему коду, а также контролировать корректность работы. Такое внедрение кода для решения описанных выше задач носит название инструментация. При инструментации бинарного кода существует два подхода:

- статическая инструментация бинарного кода;

- динамическая инструментация бинарного кода.

Основной подход при статической бинарной инструментации заключается в предварительном анализе бинарного файла, непосредственной инструментации кода и компиляции тестируемого приложения. Преимущество этого подхода заключается в относительно высокой скорости выполнения исполняемого файла.

Недостатками статической инструментации являются:

1) отличие инструментированного приложения от оригинального;
2) разделяемые библиотеки необходимо инструментировать отдельно;
3) меньшая гибкость за счет постоянного хранения инструментирующего кода.

Этих недостатков лишена динамическая инструментация. Её достоинствами являются:

1) неизменность приложения при хранении;
2) инструментируется приложение со всеми зависимостями;
3) гибкое управление инструментирующим кодом;
4) отсутствие потребности в перекомпиляции и перелинковке приложения;
5) возможность обнаружения кода во время выполнения приложения;
6) возможность работы с кодом, генерируемым на этапе исполнения (в том числе полиморфным).

В результате передачи различных параметров на вход тестируемой функции, появляется возможность отследить результаты ее исполнения и по итогам тестирования составляется отчет о каждом функциональном объекте и возможных ошибок исполнения.

Основной проблемой предложенного решения является невозможность автоматического определения неочевидных параметров тестируемых функциональных объектов. Если вопрос определения числа, типов параметров решается относительно просто, то выявление зависимостей фактических маршрутов выполнения функциональных объектов от глобальных переменных, переменных окружения и т.д. является сложноразрешимой задачей, на выполнение которой и предполагается направить основные усилия.

Список литературы

1. Майкл Дж.Д. Саттон. Fuzzing. Исследование уязвимостей методом грубой силы / Майкл Дж.Д. Саттон, Адам Грин, Педрам Амини.
2. Frida. Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers / Электронный ресурс: https://www.frida.re/docs/home/.
3. DBI (2017) / Электронный ресурс: http://uninformed. org/index.cgi?v=7&a=1&p=3..
4. Инструментация — эволюция анализа / Электронный ресурс: https://xakep.ru/2013/09/11/61232.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.932.2

***Белим Сергей Викторович**, д.ф.-м.н., профессор, заведующий каф.информационной безопасности ОмГУ им. Ф.М. Достоевского*
***Вильховский Данил Эдуардович**, аспирант каф.информационной безопасности ОмГУ им. Ф.М. Достоевского*
Омский государственный университет им. Ф.М. Достоевского
Омск, Россия
e-mail: sbelim@mail.ru, vilkhovskiy@gmail.com

СТЕГОАНАЛИЗ АЛГОРИТМА КОХА-ЖАО

Предложен алгоритм выявления стеганографических вставок в изображении, встраиваемых с помощью метода Коха-Жао. В качестве объекта исследования рассмотрено цифровое изображение, о котором отсутствует информации о наличии или отсутствии встроенного сообщения.

Стеганографический метод Коха-Жао[1] основывается на двумерном дискретном косинусном преобразовании (ДКП). Анализ алгоритмов встраивания и извлечения показывает, что для осуществления успешной атаки на стеганографический метод Коха-Жао необходимо определить блоки, в которые производилось встраивание сообщения, индексы изменяемых коэффициентов ДКП и пороговое значение M_0.

Для корректного извлечения сообщения отправляющая и принимающая стороны должны иметь общую секретную информацию о параметрах встраивания. Будем исходить из того, что информация о параметрах имеет минимальный размер. В этом случае можно сформулировать три предположения, используемые в дальнейшем. Во-первых, встраивание производится в непрерывную последовательность блоков. Во-вторых, для всех блоков используются одни и те же пары коэффициентов ДКП. В-третьих, для всех блоков используется одинаковое значение M_0. Любые отклонения от этих предположений увеличивают объем секретной информации.

Для определения параметров стеганографической вставки будем использовать тот факт, что параметр M_0 должен иметь большое значение, позволяющее принимающей стороне извлекать скрытое сообщение без потерь из любого изображения. Если M_0 выбрать недостаточно большим, то в извлекаемом сообщении могут возникать ошибки, обусловленные особенностями изображения-контейнера.

Прежде всего, определим коэффициенты ДКП, в которые производилось встраивание. Для этого, как и в алгоритме встраивания, разобьем изображение на блоки B_i $(i = 1, \dots, N)$ размером 8×8 пикселей. К каждому блоку B_i $(i = 1, \dots, N)$ применим ДКП. В результате получим набор матриц коэффициентов D_i $(i = 1, \dots, N)$ размером 8×8. Проанализируем среднечастотные элементы матриц D_i $(i = 1, \dots, N)$. Введем три последовательности величин $(i = 1, \dots, N)$:

$$C_i^{(1)} = ||D_i[3,4]| - |D_i[4,3]|,$$
$$C_i^{(2)} = ||D_i[3,5]| - |D_i[5,3]|,$$
$$C_i^{(3)} = ||D_i[4,5]| - |D_i[5,4]|.$$

Встраивание сообщения приводит к изменениям в одной из этих последовательностей. Построим гистограммы зависимости $C_i^{(j)}$ $(j = 1,2,3;\ i = 1, \dots, N)$ от номера блока i. Встраивание сообщения приводит к изменению одной из последовательностей в виде появления «ступени» высотой M_0.

Проблема обнаружения стеганографической вставки сводится к анализу зависимостей $C_i^{(j)}$ $(j = 1,2,3;\ i = 1, \dots, N)$ от номера блока i и поиску ступенчатых изменений. Границы ступеней на гистограмме могут быть выявлены с помощью численного дифференцирования на основе разностных схем. Выполним численное дифференцирование зависимости $C_i^{(j)}$ $(j = 1,2,3;\ i = 1, \dots, N)$ по i:

$$dC_i^{(j)} = C_i^{(j)} - C_{i-1}^{(j)}.$$

В результате этой операции ступенчатые изменения дадут высокие пики, которые позволят определить границы встроенного сообщения. Чтобы автоматически определить границы встроенного сообщения для каждого массива $d\mathrm{C}^{(j)}$, вычислим следующие величины: M_j - максимальное значение элементов массива $d\mathrm{C}^{(j)}$, N_j - среднее значение элементов массива $d\mathrm{C}^{(j)}$, O_j - среднеквадратичное отклонение для элементов массива $d\mathrm{C}^{(j)}$. Найдем величины $R_j = N_j + O_j$. Введем величину Y_j, которая будет изменяться в интервале значений от R_j до M_j. Выберем значение Y_j таким, чтобы существовало ровно два значения $C_{i1}^{(j)} > Y_j$ и $C_{i2}^{(j)} > Y_j$. Значения i_1 и i_2 будут служить границами встроенного сообщения. Для определения значения M_0 необходимо найти минимальное значение $C_i^{(j)}$ на интервале от i_1 до i_2.

Чтобы автоматически определить границы встроенного сообщения для каждого массива $d\mathrm{C}^{(j)}$, вычислим следующие величины: M_j - максимальное значение элементов массива $d\mathrm{C}^{(j)}$, N_j - среднее значение элементов массива $d\mathrm{C}^{(j)}$, O_j - среднеквадратичное отклонение для элементов массива $d\mathrm{C}^{(j)}$. Найдем величины $R_j = N_j + O_j$. Введем величину Y_j, которая будет изменяться в интервале значений от R_j до M_j. Выберем значение Y_j таким, чтобы существовало ровно два значения $C_{i1}^{(j)} > Y_j$ и $C_{i2}^{(j)} > Y_j$. Значения i_1 и i_2 будут служить границами встроенного сообщения. Для определения значения M_0 необходимо найти минимальное значение $C_i^{(j)}$ на интервале от i_1 до i_2.

Формально алгоритм можно записать в виде последовательности следующих шагов:

1. Разбить изображение на блоки B_i размером 8×8 пикселей.

2. К каждому блоку B_i применить дискретное косинусное преобразование. В результате получаются матрицы коэффициентов ДКП D_i размером 8×8.

3. Построить три последовательности величин ($i = 1, \dots, N$):

$$C_i^{(1)} = ||D_i[3,4]| - |D_i[4,3]|,$$
$$C_i^{(2)} = ||D_i[3,5]| - |D_i[5,3]|,$$
$$C_i^{(3)} = ||D_i[4,5]| - |D_i[5,4]|.$$

4. Выполнить численное дифференцирование $C_i^{(j)}$ ($j = 1,2,3;\ i = 1, \dots, N$) по i:

$$dC_i^{(j)} = C_i^{(j)} - C_{i-1}^{(j)}.$$

5. Вычислить: M_j - максимальное значение элементов массива $d\mathrm{C}^{(j)}$, N_j - среднее значение элементов массива $d\mathrm{C}^{(j)}$, O_j - среднеквадратичное отклонение для элементов массива $d\mathrm{C}^{(j)}$. Найти величины $R_j = N_j + O_j$.

6. Осуществить перебор величины Y_j в интервале от R_j до M_j с шагом dY. Определить значение Y_j такое, что существует ровно два значения $C_{i_1}^{(j)} > Y_j$ и $C_{i_2}^{(j)} > Y_j$. Если такое значения определить невозможно, то уменьшить шаг dY. Определить i_1 и i_2.

7. Найти минимальное значение $C_i^{(j)}$ на интервале от i_1 до i_2. Присвоить M_0 найденное значение.

8. Извлечь сообщение, используя найденные параметры.

Для определения эффективности работы предложенного в данной главе алгоритма протестируем его результаты на основе библиотеки изображений Беркли (Berkeley Segmentation Data Set and Benchmarks 500, BSDS500[2]. Данная коллекция предназначена для проверки алгоритмов кластеризации и на текущий момент содержит набор из 500 изображений в формате JPEG. Эта коллекция была выбрана для тестирования предложенного метода, так как содержит изображения с различными типами областей заливки и различным содержимым. Кроме того, формат JPEG так же, как и метод Коха-Жао[3], основан на дискретном косинусном преобразовании, что исключает дополнительные ошибки при изменении формата файла изображения.

При тестировании на вход алгоритма подавалось каждое изображение сначала без встроенных данных (пустой стегоконтейнер), а затем с встроенным сообщением (заполненный стегоконтейнер). Следует отметить, что предложенный алгоритм эффективен при $M_0 > 54$. Однако следует отметить, что при более низких значениях порога M_0 использование алгоритма Коха-Жао сталкивается с существенными трудностями при извлечении встроенных данных. Кроме этого, если алгоритм обнаруживает встроенное сообщение, то он может его однозначно извлечь.

В рамках компьютерного эксперимента на основе обработки 500 изображений коллекции BSDS500 определялись следующие параметры:

TP - процент истинно-положительных результатов, для которых непустой стегоконтейнер был корректно определен и сообщение верно извлечено.

FN – процент ложно-негативных результатов, для которых непустой стегоконтейнер был определен как контейнер, не содержащий встроенного сообщения.

TN – процент истинно-негативных результатов, для которых пустой контейнер был корректно определен.

FP - процент ложно-позитивных результатов, при которых пустой контейнер был некорректно определен как стегоконтейнер.

Для предложенного алгоритма были получены следующие результаты:

$$TP = 85{,}5\%,\ FN = 14{,}5\%,\ TN = 77\%,\ FP = 23\%.$$

Как видим из статистических данных, предложенный алгоритм с достаточно высокой эффективностью определяет наличие встроенного сообщения. Ошибки в работе алгоритма связаны со структурой изображения. В пустом изображении стегоконтейнере возможно наличие пиков в последовательности коэффициентов дискретного косинусного преобразования, которые ошибочно принимаются за границу встроенного сообщения. Наличие двух ложных границ приводит к ложно-позитивным результатам. Присутствие больше двух ложных границ приводит к невозможности определить истинные границы встроенного сообщения.

С точки зрения защиты информации интерес представляют изображения, для которых стегоанализ не позволяет выявить факт встраивания.

Список литературы

1. Provos N and Honeyman P 2001 Detecting steganographic content on the internet *CITI Technical Report 01–11* (Ann Arbor: University of Michigan)

2. Барсуков, В.С. Оценка уровня скрытности мультимедийных стеганографических каналов хранения и передачи информации / В.С. Барсуков, А.П. Романцов // Специальная Техника. – 2000. – № 1.

3. Koch E. Towards robust and hidden image copyright labeling / E. Koch, J. Zhao// IEEE Workshop on Nonlinear Signal and Image Processing. – 1995. – pp 452-455

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.932.2

***Белим Сергей Викторович**, д.ф.-м.н., профессор, заведующий каф.информационной безопасности ОмГУ им. Ф.М. Достоевского*
***Вильховский Данил Эдуардович**, аспирант каф.информационной безопасности ОмГУ им. Ф.М. Достоевского*
Омский государственный университет им. Ф.М. Достоевского
Омск, Россия
e-mail: sbelim@mail.ru, vilkhovskiy@gmail.com

ВЫЯВЛЕНИЕ LSB-ВСТАВОК НА ОСНОВЕ АНАЛИЗА МЛАДШЕГО СЛОЯ

Предложен алгоритм выявления пикселей изображения, в которых произведена подмена наименее значащего бита при стеганографическом встраивании сообщения, на основе автоматического анализа нулевого слоя.

Наличие встроенного сообщения может быть обнаружено визуально из анализа нулевого слоя. Причем визуально можно определить только наличие встроенного сообщения, но не его расположение и размер. Поставим себе целью автоматическое определение наличия, размеров и положения области встраивания.

Для построения алгоритма обнаружения и автоматического выделения области встраивания сообщения в нулевой слой сделаем некоторые предположения:

1) Прямоугольная область встраивания имеет пересечение с областью равномерной заливки изображения стегоконтейнера не менее чем на 25%.
2) Стороны прямоугольной области встраивания параллельны сторонам изображения стегоконтейнера.
3) Встраиваемое сообщение представляет собой поток битов с распределением нулей и единиц, близким к равномерному.

Из визуального анализа нулевого слоя зафиксируем некоторые особенности изменения распределения нулевых и единичных битов:

1) Встроенное сообщение создает прямоугольную область с равномерным распределением единичных битов.
2) Область равномерной заливки на исходном изображении не совпадает с областью равномерной заливки на нулевом слое.

Таким образом, для выделения области встраивания необходимо провести анализ нулевого слоя и выделить те области, которые соответствуют одинаковому значению плотности единичных значений битов. Данная задача, по своей постановке, совпадает с задачей таксономии точек на плоскости. Однако классические алгоритмы таксономии выделяют области, ограниченные окружностями. В нашем случае необходима модификация алгоритмов таксономии с

учетом априорной информации о прямоугольной геометрической форме области встраивания. Построим алгоритм таксономии с помощью метода последовательных приближений.

Для того чтобы локализовать область встраивания, применим алгоритм, основанный на алгоритме таксономии FOREL[4]. В своей классическом реализации FOREL группирует точки в таксоны, находящиеся в самой окружности. Сделаем модификацию алгоритма: будем считать, что таксоны должны иметь прямоугольную форму. Введем показатель плотности единичных значений p. Если в некоторой области изображения содержится N пикселей и N_1 из них имеет единичное значение, показатель плотности единичных значений $p = N_1/N$.

В качестве областей, в которые может быть встроено сообщение, выбираем таксоны, размер которых не меньше, чем 10% размеров исходного изображения.

Разбиение исходного прямоугольника на группу прямоугольников обусловлено распределением единичных и нулевых битов внутри самого сообщения. Однако уже для искусственных изображений с градиентной заливкой возникают сложности, так как непрерывное изменение цвета изображения в целом проявляется как полосы одинаковых значений на нулевом слое. Появление данных полос связано с равномерным изменением цвета, которое проявляется как дискретное изменение младшего бита. Данные полосы могут быть устранены с помощью предварительной обработки изображения.

Результаты работы алгоритма зависят от выбора параметров R_0 и p. Первый параметр определяет начальный размер таксона. Как показывает компьютерный эксперимент, окончательный размер таксона незначительно отличается от первоначального.

Экспериментально было определено, что наилучших результатов удается добиться при значениях p в интервале от 0.50 до 0.60. Конкретное значение p зависит от структуры изображения. Для искусственных изображений наиболее приемлемые результаты получаются при более низких значениях p, тогда как для фотографических изображений лучше выбирать значение p ближе к 0.60, так как это позволяет отсечь лишние детали.

Алгоритм таксономии не позволяет выделить область встраивания стеганографического сообщения в виде одной прямоугольной области. За счет внутренних особенностей распределения битов происходит разбиение области на прямоугольные области меньшего размера. Для определения одной области встраивания было применено два различных подхода.

Первый подход состоит в том, что строится минимальный прямоугольник, включающий в себя выделенные небольшие прямоугольные области. Причем таких прямоугольников может быть на изображении несколько. Данный подход позволяет выделить на изображении наиболее вероятные области встраивания.

Второй подход состоит в том, что кроме нулевого слоя рассматривается также ближайший к нему первый слой. Для точек первого слоя, так же как для нулевого, выполняется алгоритм поиска таксонов с теми же параметрами, что и

в нулевом слое. В большинстве чистых изображений первый слой по своей структуре близок к нулевому слою. Поэтому таксоны, образующиеся вследствие особенностей самого изображения, с большой вероятностью будут присутствовать как в нулевом, так и в первом битовом слое. Тогда как стеганографически встроенное сообщение будет присутствовать только в нулевом слое. Поэтому, вычитая таксоны, выделенные в первом слое из таксонов, найденных в нулевом слое, мы уберем большинство особенностей, присутствующих в изображении и никак не связанных со стеганографией.

Значительное влияние на результаты оказывают области небольшого размера с резким изменением цвета, обусловленным наличием четких границ. Эксперимент на большом количестве изображений показал, что, в среднем, правильно идентифицируется 88% пикселей, в которые производилось встраивание. Ложные срабатывания составляют в среднем 34% от выделенных пикселей.

Предложенный в данной статье алгоритм анализа нулевого слоя стегоконтейнера позволяет выявлять наличие стеганографического встраивания методом LSB-вставок, при этом:

1. Алгоритм позволяет обнаруживать стеганографические вставки при низком относительном заполнении контейнера.

2. Использование алгоритма таксономии позволяет локализовать область встраивания в автоматическом режиме.

3. Предложенный алгоритм позволяет определять размеры и положение области встраивания, если она пересекается с областью равномерной или градиентной заливки изображения-стегоконтейнера.

Список литературы

1. Abreu E., Lightstone M., Mitra S.K., Arakawa S.K. A new efficient approach for the removal of impulse noise from highly corrupted images. // IEEE Transactions on Image Processing, IEEE Transactions on. 1996. – V.5, – P. 1012-1025

2. Сорокин, С.В. Реализация SD-ROM фильтра на основе концепции нечеткой логики / С.В. Сорокин, М.А. Щербаков //Известия высших учебных заведений. Поволжский регион. – 2007. – №3. – С.56-65

3. Garnett R., Huegerich T., Chui C., He W. A Universal Noise Removal Algorithm with an Impulse Detector. // IEEE Trans Image Process. – 2005. – № 14(11). – P. 1747-54.

4. Загоруйко, Н.Г. Прикладные методы анализа данных и знаний // Новосибирск: ИМ СО РАН. – 1999. – 270 с.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 003.26

А.Г. Белоусов
ФГБОУ ВО «Брянский государственный технический университет»
Россия, г. Брянск
belousov-ag@yandex.ru

ПРИНЦИПЫ ПОСТРОЕНИЯ КРИПТОГРАФИЧЕСКИ СТОЙКИХ ПСЕВДОСЛУЧАЙНЫХ ГЕНЕРАТОРОВ И ИХ ПРИМЕНЕНИЯ

Рассматриваются требования к криптографически стойким псевдослучайным генераторам и особенности данных генераторов. Указываются некоторые стратегии построения криптостойких псевдослучайных генераторов.

Прежде, чем рассматривать, что такое псевдослучайные числа и зачем они нужны в криптографии, рассмотрим, в чём принципиальная разница между случайными и псевдослучайными числами. Число является *истинно случайным*, если оно может принимать значение на некотором множестве, и до измерения нельзя предсказать, какое именно это значение. Классические примеры случайных величин – сторона, которой выпадет монета при броске, или число очков на верхней грани подброшенной кости. В принципе, броски монеты или кости подчинены законам физики, однако на практике бросающий не может это учесть в достаточной мере, чтобы наперёд знать результат [2].

Псевдослучайные числа основаны на детерминированных математических алгоритмах, хотя человеку, не знающему о таких алгоритмах, последовательность чисел будет казаться случайной. Между числами такой последовательности есть зависимость – член последовательности можно восстановить, зная алгоритм и некоторые данные, какие именно данные – зависит от конкретного генератора псевдослучайных чисел. Так, иногда достаточно знать несколько предыдущих членов для восстановления следующего.

Приведём пример. Для человека, не знающего о псевдослучайных числах, ряд 52, 18, 94, 89, 68, 98, 109, 41, 86, 49 выглядит похожим на случайный ряд. Пусть теперь $X_i = (5X_{i-1} + 3) \bmod 128, i = 1, 2, 3, \ldots$. Каждое псевдослучайное число получаем как результат циклического сдвига 7-битного представления X_i на 2 бита влево. При $X_0 = 2$ получим: $X_1 = 13_{10} = 0001101_2$. После циклического сдвига: $0110100_2 = 52_{10}$. Аналогично, $X_2 = 68_{10} = 1000100_2$. После циклического сдвига: $0010010_2 = 18_{10}$. Аналогично получаем следующие числа последовательности. Как мы показали, наш ряд не случайный, хотя внешне похож на случайный.

Псевдослучайные датчики получили широкое распространение, поскольку получение случайных чисел с помощью различных физических процессов, как правило, выполняется слишком медленно. В криптографии псевдослучайные

датчики получили применение, поскольку здесь нельзя рассчитывать на волю случая.

Далеко не всякий псевдослучайный генератор может быть применён в криптографии. Рассмотрим особенности построения криптографических псевдослучайных генераторов.

Ориентация на биты. Как правило, криптографические псевдослучайные генераторы оперируют не с десятичными числами, а с последовательностями бит, одна из причин этого – особенности современных ЭВМ. Некоторые генераторы, как например, *регистры сдвига с обратной связью*, генерируют на каждой итерации по одному биту последовательности. Другие, как например, *генератор BBS*, могут на каждой итерации выдавать несколько выходных бит последовательности. Если же некоторый генератор оперирует с десятичными числами, при использовании в криптографических целях, как правило, требуется рассматривать генерируемые числа в двоичном виде.

Прохождение статистических тестов. Статистические тесты псевдослучайных последовательностей позволяют оценить, насколько близки такие последовательности к случайным по статистическим свойствам. Существует весьма много различных статистических тестов. Некоторые из них основываются на критерии «хи-квадрат», другие – на анализе серий идущих подряд бит, третьи – на установлении соответствия между числовыми последовательностями и различными геометрическими объектами и т.д. [1] Однако центральным в криптографии является *тест на следующий бит*: если есть полиномиальный алгоритм, который по первым k битам псевдослучайной последовательности предсказывает k+1-ый бит с вероятностью существенно выше 0,5, генератор последовательности не является криптостойким. Такой тест имеет следующее практическое значение: если часть последовательности, созданной генератором, становится известной криптоаналитику, в идеале это не должно помочь ему восстановить, какие члены последовательности идут дальше.

Большой период. Необходимым условием высокой криптостойкости генератора псевдослучайных чисел является высокая *информационная длина периода*, т.е. мы должны иметь возможность сгенерировать много чисел, прежде чем они начнут повторяться или станут легко предсказуемыми. Следует при этом учитывать, что период может существенно зависеть от подбора параметров генератора. Непригодный для криптографии генератор, но хорошо демонстрирующий влияние параметров на период, - *линейный конгруэнтный генератор*. Если его модуль равен 2^n, где n-натуральное число, то период может достигать 2^n, но будет в разы меньше при неудачном подборе множителя и приращения. Также обратим внимание, что сам по себе большой период ещё не гарантирует криптостойкость. *Вихрь Мерсенна* имеет огромный период, но ненадёжен с точки зрения криптографии: знание криптоаналитиком достаточно длинной подпоследовательности скомпрометирует всю последовательность.

Использование трудноразрешимых математических задач. Чтобы криптосистему, использующую псевдослучайный генератор, было сложно взломать, использование генератора должно основываться на математических задачах,

для которых нет вычислительно эффективных решений. *Генератор BBS* основывается на вычислительно сложной задаче *факторизации больших чисел*. *Алгоритм Блюма-Микали* использует *проблему дискретного логарифмирования*. *Криптографические хеш-функции* при условии, что они хорошо спроектированы, также могут быть использованы в качестве генераторов псевдослучайных чисел, и здесь значительную роль играет сложность *восстановления прообразов по хеш-значениям*. Фактически, все описанные примеры основываются на понятии *односторонних функций* – некоторая операция выполняется относительно легко, но нет вычислительно эффективных алгоритмов выполнения обратной операции.

Существуют различные стратегии, позволяющие построить псевдослучайные генераторы, имеющие высокую криптографическую стойкость. Опишем некоторые из них.

1. Использование *хеш-функций* или *блочных шифров*. Псевдослучайный генератор в этом случае строится на основе некоторого криптографического алгоритма, изначально предназначенного для других целей. *Криптографические хеш-функции* при их использовании для случайных входных строк дают распределение хешей, близкое к равномерному. Кроме того, хорошо спроектированная хеш-функция обладает лавинным эффектом и вследствие этого низкой предсказуемостью. Возможно также использование *режима счётчика для блочных шифров*. Тогда блоки шифртекста образуют псевдослучайную последовательность с хорошими статистическими свойствами. Криптоаналитику требуется определить ключ шифрования, что весьма сложно для современных блочных шифров.

2. Использование *специализированных псевдослучайных генераторов*, изначально предназначенных именно для задачи генерации псевдослучайной последовательности. *Регистры сдвига с обратной связью*, *алгоритм BBS* – примеры именно таких генераторов.

3. Усиление *некриптографических псевдослучайных генераторов*. Существуют довольно простые и быстрые псевдослучайные генераторы, изначально не предназначенные для криптографии, например, *линейный конгруэнтный генератор*, *полиномиальный конгруэнтный генератор*. Возможно пытаться модифицировать их так, чтобы повысить их криптостойкость, но сохранить простоту реализации и высокую скорость. В частности, если для линейного конгруэнтного генератора с модулем 2^n на выход подавать не порождаемые им значения, а результат их циклического сдвига на r бит вправо, то работа криптоаналитика несколько усложнится. В n раз повысится мощность множества возможных комбинаций параметров (r может быть от 0 до n-1). Для восстановления параметров генератора потребуется знать более длинную подпоследовательность, чем раньше. Кроме того, улучшатся статистические свойства. В частности, в исходной версии при нечётных множителе и приращении в последовательности есть чередование чётных и нечётных чисел, а теперь его не будет. Такого рода усиления полезны, например, когда достаточно, чтобы криптоаналитик не смог вскрыть защищаемую информацию быстро, поскольку ин-

формация быстро становится неактуальной. Также рассматриваемая стратегия полезна, если в приоритете высокое быстродействие – например, требуется гаммировать большой объём данных невысокой степени секретности при передаче их по сети.

4. *Комбинирование* – применяется несколько взаимосвязанных алгоритмов или стратегий. В частности, в *алгоритме Ярроу* используется криптографическая хеш-функция и блочный шифр. *Фибоначчиев генератор* требует на вход достаточно длинную серию чисел, длина которой определяется так называемыми *лагами*. Эта серия, необходимая для работы фибоначчиева генератора, обычно порождается с помощью некоторого более простого генератора псевдослучайных чисел, т.е. на практике мы получаем комбинацию двух генераторов псевдослучайных чисел, один из которых использует выход другого.

Выбор стратегии для конкретного случая зависит от особенностей применения в конкретной задаче – один и тот же генератор не может показать одинаковую эффективность, например, для задачи *генерации сеансовых ключей* и для *гаммирования*. Кроме того, важно, насколько высокие надёжность и быстродействие требуется обеспечить. Значимость последнего и, как следствие, интерес к криптостойким, но одновременно быстрым генераторам псевдослучайных чисел, растёт в связи с активным развитием сетевых систем, в частности, сервисов, в которых к серверу подключается одновременно большое число пользователей. Некоторые генераторы позволяют балансировать между скоростью и надёжностью. Так, в *генераторе BBS*, увеличив подаваемое на каждой итерации на выход число младших бит при неизменном целом числе Блюма и требуемом числе бит в псевдослучайной последовательности, мы уменьшим требуемое число итераций генератора, и как следствие – дорогостоящих операций возведения большого числа в квадрат и взятия остатка от деления на большое число. Однако при чрезмерном увеличении числа выходных бит мы рискуем испортить статистические свойства выходной последовательности, хотя именно ради них и создавался BBS.

Список литературы

1. Григорьев, А.Ю. Методы тестирования генераторов случайных и псевдослучайных последовательностей / А.Ю. Григорьев // Учёные записки УлГУ. Сер. Математика и информационные технологии. – 2017. – №1. – С. 22-28.

2. Ллойд, Д. Вторая Книга всеобщих заблуждений / Д. Ллойд, Д. Митчинсон. – М.: Фантом Пресс, 2012. – 175 с.

Материал поступил в редколлегию 25.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

Беляев Дмитрий Леонидович, *к.т.н., сотрудник*
Олейник Светлана Игоревна*, сотрудник*
Академия Федеральной службы охраны Российской Федерации
г. Орёл, Россия
e-mail: dbelyaew@mail.ru, svetunya13@mail.ru

РАЗРАБОТКА ОБУЧАЮЩЕГО КОМПЛЕКСА ДЛЯ ВЫПОЛНЕНИЯ ЗАДАНИЙ ПО ПОИСКУ И ЭКСПЛУАТАЦИИ УЯЗВИМОСТЕЙ ВЕБ-САЙТОВ

Проанализирована проблема безопасности веб-сайтов, используемых для нужд государственных структур, обоснована актуальность применения обучающего комплекса для повышения эффективности обучения специалистов в сфере обеспечения информационной безопасности веб-сайтов.

В качестве средств обеспечения безопасности серверов используются антивирусные средства и системы обнаружения вторжений. Однако даже такие известные и широко используемые продукты, как Kaspersky и Snort не обеспечивают достаточного уровня защищённости веб-сайтов.

При разработке веб-сайтов не уделяется должного внимания вопросам обеспечения информационной безопасности, а именно поиску уязвимостей веб-сайтов и защите от атак при эксплуатации уязвимостей. Разработкой веб-сайтов должны заниматься квалифицированные специалисты, которые имеют представление о существующих уязвимостях веб-сайтов, об актуальных угрозах для веб-приложений, а также о способах предотвращения реализации различных атак.

Периодически в открытых источниках публикуется информация об уязвимостях в различных компонентах веб-приложения, а примеры реализации атак на серверные программы и исходный код веб-приложений находятся в открытом доступе в виде статей, видео, видео-уроках и т.д., что позволяет злоумышленникам получать сведения из множества источников об актуальных уязвимостях и способах проведения атак.

Существуют специальные уязвимые веб-приложения для отработки умений и навыков в сфере проведения атак на веб-сайты, которые могут быть использованы специалистами по обеспечению информационной безопасности. Однако не существует комплексного и подробного описания использования этих приложений.

Для решения приведённых проблем предлагается разработать обучающий комплекс, позволяющий осуществлять поиск и эксплуатацию уязвимостей, а также содержащий рекомендации по их устранению. По мере прохождения заданий по реализации конкретной атаки обучающийся приобретает понимание

теоретического аспекта конкретной уязвимости и практические навыки в области ее эксплуатации.

Общий алгоритм взаимодействия преподавателя, обучающегося и обучающего комплекса для отработки заданий по поиску и эксплуатации уязвимостей веб-сайтов представлена на рис. 1.

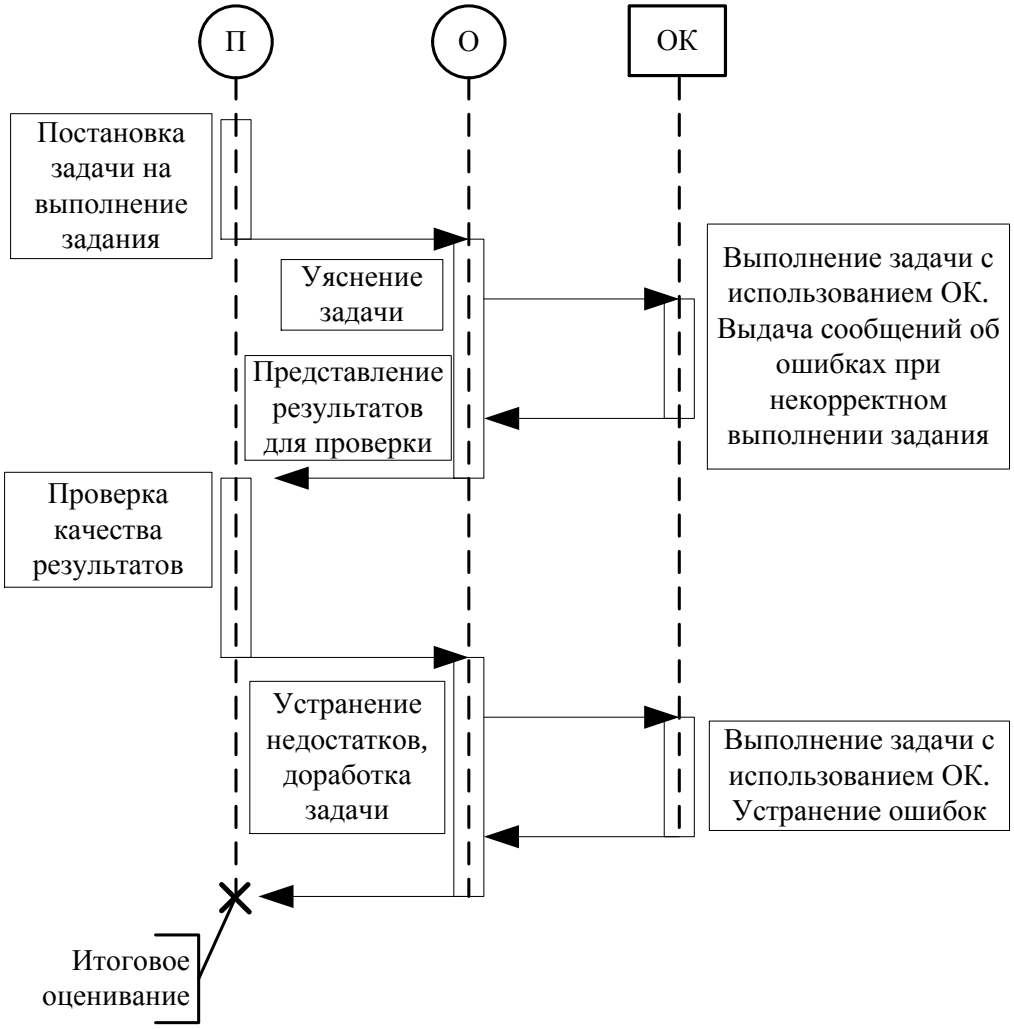


Рис. 1. Алгоритм применения обучающего комплекса

Технологически предложенный алгоритм заключается в создании обучающего комплекса на основе авторского программного приложения, отображающего текстовые и графические материалы, представленные в удобной и понятной форме с помощью приложения, разделённого на модули, посвящённые конкретной тематике, что позволяет обучающимся оперативно осуществлять поиск и находить интересующий их материал.

Общая схема проведения атак на веб-приложение с использованием обучающего комплекса представлена на рис. 2.

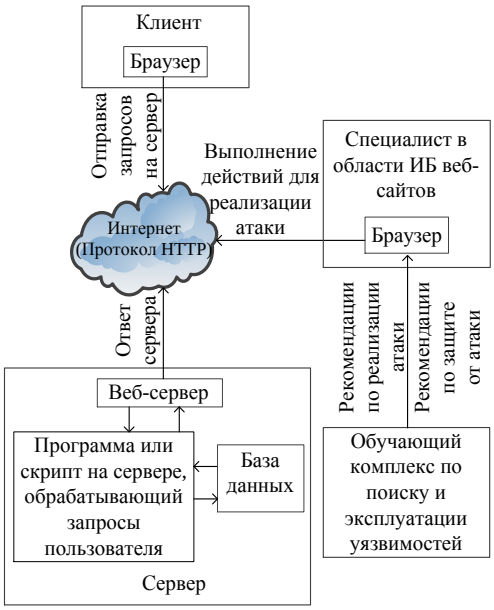


Рис. 2. Схема проведения атак на веб-приложение с использованием обучающего комплекса

При применении обучающего комплекса пользователь выбирает уязвимость веб-сайта или атаку, по которой необходимо отработать задание. Обучающий комплекс предоставляет инструкцию по реализации атаки в виде текстовой и графической информации. Обучающийся использует две виртуальные машины (клиент и сервер), на которых производит необходимые настройки и использует специальные программы для проведения атак. Страница веб-сайта отображается в браузере на клиентской машине. При неверном выполнении задания обучающий комплекс выдаёт пользователю рекомендации по устранению ошибок.

Обучающий комплекс позволяет проработать задания по следующим уязвимостям и атакам:

1) brute force (атака на сайт, реализующий подбор паролей методом перебора);

2) command execution (атака заключается во внедрении и выполнении команд, указанных злоумышленником в полях ввода, расположенных на странице веб-сайта);

3) CSRF (для реализации данной атаки необходимо, чтобы пользователь перешёл на специально подготовленную злоумышленником веб-страницу, на которую был добавлен некоторый код. При выполнении данного кода браузер пользователя-жертвы совершает некий запрос к другому серверу и выполняет нужные злоумышленнику действия);

4) upload (данная уязвимость позволяет злоумышленнику загрузить файл, содержащий внутри себя вредоносный код, который может быть выполнен на сервере);

5) XSS (для реализации данной атаки злоумышленнику необходимо внедрить скрипт, использование которого позволяет получить, например, пользовательские данные);

6) SQL-injection (атака, при которой злоумышленник, внедряя sql-запросы, может получить доступ к базе данных и возможность читать, изменять и удалять информацию, которая для него не предназначена).

В состав обучающего комплекса входят следующие модули:

– модуль «Алгоритм настройки ВМ», содержащий информацию по установке параметров виртуальных машин, их компонентов и программного обеспечения для возможности их взаимодействия для поиска уязвимостей и проведения атак;

– модуль «Теоретическая информация», содержащий данные об уязвимостях веб-сайтов, атаках на веб-сайт и способах защиты от них. Он предназначен для углубления знаний обучающихся в области информационной безопасности веб-сайтов. Теоретический материал разбит на разделы, посвящённые проведению конкретной атаки и способам защиты от неё. Это позволяет структурировать материал по каждой конкретной уязвимости**;**

– модуль «Проведение атак», содержащий информацию по поиску и эксплуатации уязвимостей веб-сайта, а также рекомендации по устранению ошибок обучающегося, допускаемых в ходе выполнения заданий, путём выдачи комментариев-подсказок. В данном блоке представлены занятия, позволяющие формировать практические навыки. В нем представлено подробное описание выполняемых практических вопросов: настройка веб-приложения, выбор соответствующего режима, настройка программного обеспечения для реализации атак, пошаговое описание действий обучающегося;

– модуль «Тестирование» содержит комплект вопросов, позволяющий производить контроль знаний обучающихся по вопросам информационной безопасности веб-сайтов.

На рис. 3 представлена структура обучающего комплекса.

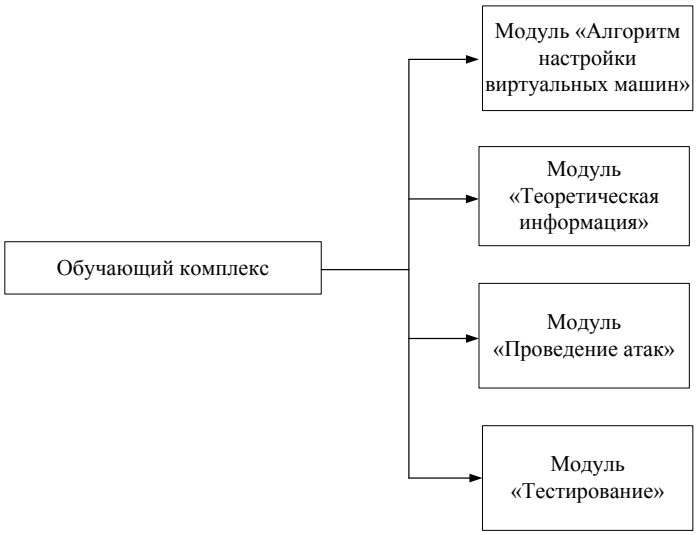


Рис. 3. Структура обучающего комплекса

Таким образом, обучающий комплекс содержит информацию по актуальным угрозам безопасности веб-сайтов. Решение проблемы качественной подго-

товки специалистов заключается в применении обучающего комплекса, позволяющего пользователю подробно и результативно освоить изучаемый материал, посвящённый поиску и эксплуатации уязвимостей веб-сайтов, а также обеспечению безопасности веб-сайтов.

Список литературы

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей / В. Ф. Шаньгин – М.: "ФОРУМ": ИНФРА-М, 2008. – 416 с.
2. Низамутдинов, М.Ф. Тактика защиты и нападения на web-приложения / М.Ф. Низамутдинов. – СПб, 2008. – 423 с.
3. Лэнс К., Фишинг, Д. Техника компьютерных преступлений / Д. Лэнс. – М.: НТ Пресс, 2008. – 320 с.
4. Линевич, Л. А. Электронный учебно-методический комплекс как средство развития комплексных умений студентов / Л. А. Линевич. – Барнаул, 2009. – 206 с.
5. Жуков, Ю. Н. Основы веб-хакинга. Нападение и защита / Ю. Жуков. – СПб, 2010. – 176 с.
6. Анализ и защита приложений с использованием решений компании Positive Technologies / Positive Technologies – учебное пособие pt08, 2015. – 179 с.

Материал поступил в редколлегию 19.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

Беляев Дмитрий Леонидович, *к.т.н., сотрудник*
Орлов Алексей Вячеславович, *сотрудник*
Академия ФСО *России*, Орёл, Россия
e-mail: AlexFullHouse@mail.ru, dbelyaew@mail.ru

РАЗРАБОТКА ПРЕДЛОЖЕНИЙ ПО МОНИТОРИНГУ И УПРАВЛЕНИЮ ФУНКЦИОНИРОВАНИЕМ ВИРТУАЛЬНЫХ УЗЛОВ

Описан метод проведения соревнований по компьютерной безопасности. Представлен способ настройки облачной платформы OpenStack. Рассмотрена функциональная схема распределённого прототипа программного средства по мониторингу виртуальных узлов и управлению ими.

Для отработки практических задач, стоящих при подготовке и совершенствовании квалификации специалистов по защите информации, а также исследования вопросов обеспечения информационной безопасности могут организовываться и проводиться соревнования по сетевому информационному противоборству. Основные информационные ресурсы, исследуемые на уязвимость с целью поиска флагов, располагаются на виртуальных машинах (серверах) в компьютерной сети организаторов соревнований. Участники получают и выполняют задания в соответствии с выбранным вариантом организации и проведения соревнований.

На рис. 1 представлен вариант проведения соревнований, в котором каждый участник команды имеет доступ к своему атакующему ресурсу, но уязвимый ресурс для всех участников одной команды является общим.

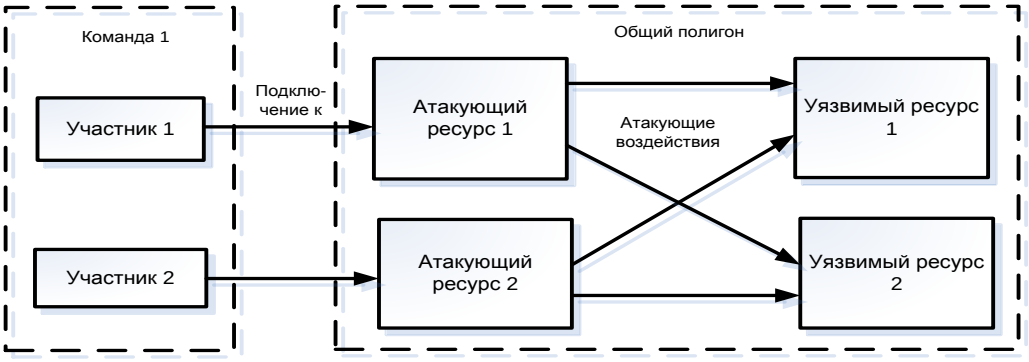


Рис. 1. Вариант проведения соревнований с общим исследуемым комплексом

Для проведения соревнований возможно использовать инфраструктуру на базе облачной платформы *OpenStack*. Применение облачных вычислений позволяет решить ряд задач:

– повысить масштабируемость сети;

– повысить отказоустойчивость серверов;

– повысить эффективность используемых ресурсов;

– обеспечить безопасность передачи данных при проведении игр.

Однако даже использование облачной платформы *OpenStack* без дополнительных средств мониторинга и управления, не отвечает достаточному уровню удобства использования полигонов, требуемых для проведения игр. В соответствии с этим важной задачей для организации соревнований является оптимизация структуры на базе *OpenStack*.

Для мониторинга и управления функционированием экземпляров виртуальных машин разрабатывается прототип программного средства, позволяющий решить ряд задач:

– автоматизировать процесс создания, управления и восстановления киберполигонов с заданиями, минимизируя при этом участие администратора;

– реализовать удобный процесс увеличения требуемого количества киберполигонов при увеличении числа участников.

Для создания лабораторного стенда потребуется развернуть три узла (рис. 2) со следующими характеристиками:

– узел 1 (управляющий): имя машины *controller*, IP адрес 10.0.0.11, объем оперативной памяти 3 Ггб, объем жесткого диска 60 Ггб;

– узел 2 (вычислительный): имя машины *compute1*, IP адрес 10.0.0.21, объем оперативной памяти 6 Ггб, объем жесткого диска 100 Ггб;

– узел 3 (вычислительный): имя машины *compute2*, IP адрес 10.0.0.31, объем оперативной памяти 6 Ггб, объем жесткого диска 100 Ггб.

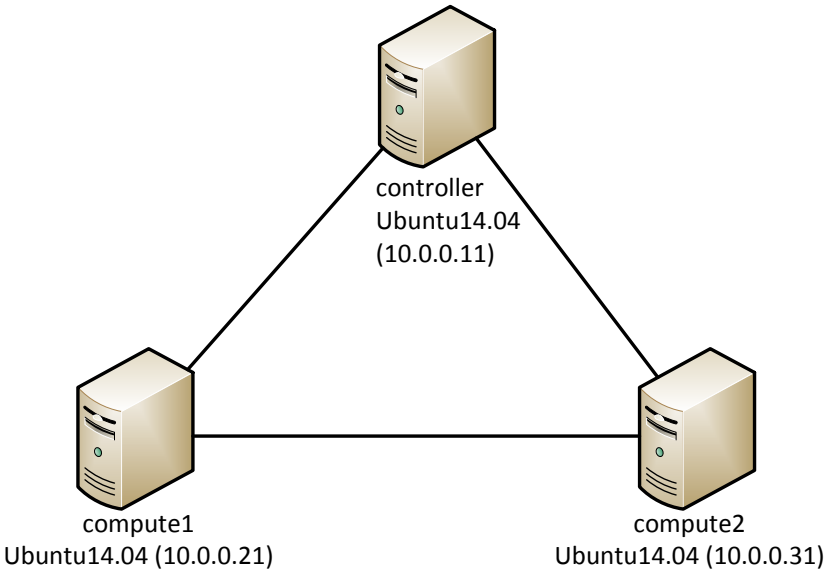


Рис. 2. Схема организации лабораторного стенда

На первом узле необходимо будет развернуть основные компоненты: *Keystone*, *Glance*, *Nova*, *Neutron* и *Horizon*, а на втором и третьем узлах компоненты *OpenStack*: *Nova* и *Neutron* [1, с. 31-88]. Первый узел будет выполнять функции

управления частным облаком, а на втором и третьем узлах будут запускаться виртуальные машины, разворачиваемые в облаке.

Структурная схема проведения соревнований по компьютерной безопасности на базе облачной инфраструктуры *OpenStack* с использованием прототипа программного средства мониторинга и управления функционированием виртуальных узлов представлена на рис. 3.

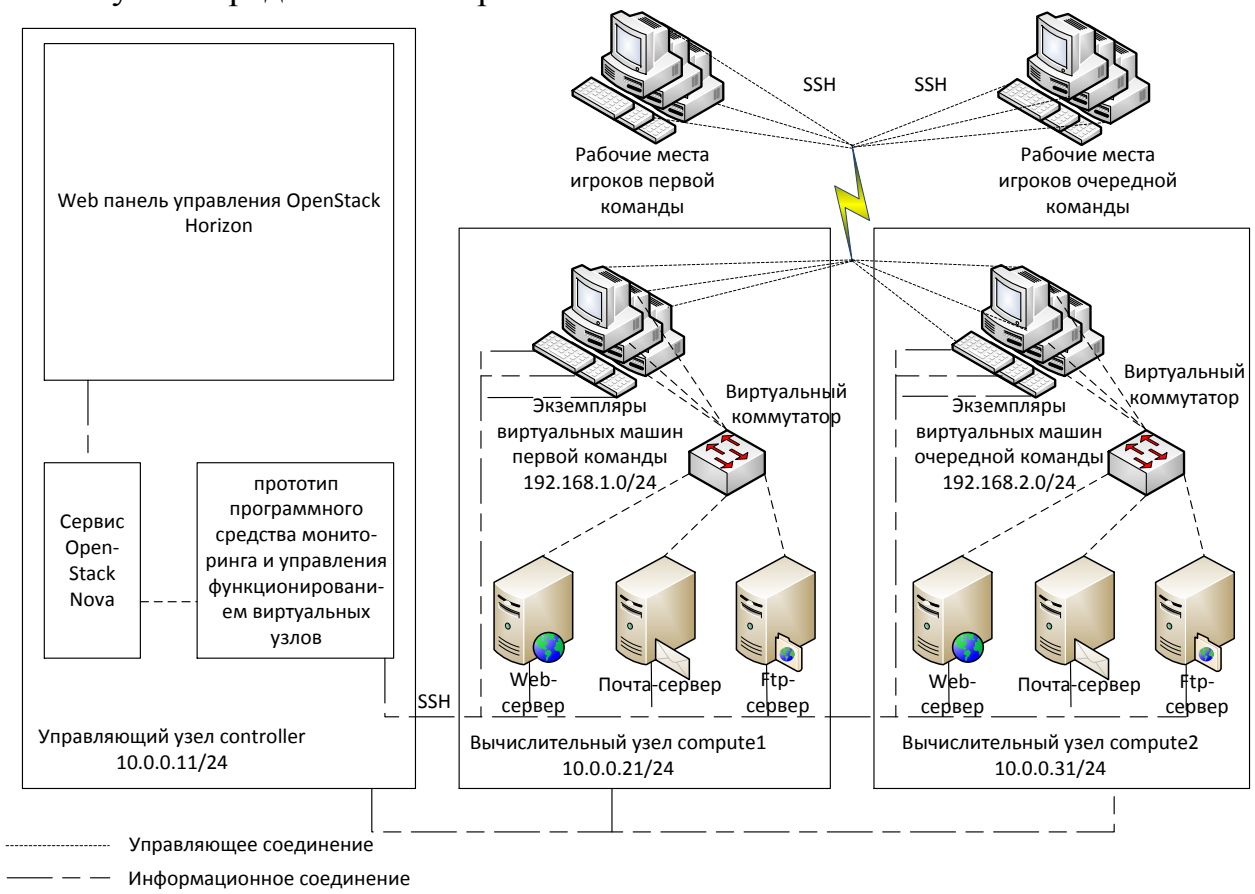


Рис. 3.Структурная схема проведения соревнований по компьютерной безопасности

С помощью *Web* панели управления *OpenStack Horizon*, расположенной на управляющем узле *controller*, создаются экземпляры виртуальных машин (инстансы), выполняющихся на вычислительном узле *compute1*. Минимальный набор параметров, требуемый для успешного и безопасного, с точки зрения информационной безопасности, создания экземпляра виртуальной машины:

– имя хоста экземпляра;

– источник экземпляра – шаблон, используемый при создании экземпляра;

– тип инстанса, отвечающий за количество выделяемой памяти, дисков и процессорной мощности для создаваемых инстансов;

– сеть, предоставляющая канал связи между инстансами в облаке;

– ключевая пара – для вхождения в экземпляр по протоколу *SSH*;

– группа безопасности – для задания правил фильтрации *IP*, которые применяются к сетевым средствам экземпляра.

Экземпляры виртуальных машин: *web*-сервер, почта-сервер *ftp*-сервер, рассмотренные в структурной схеме проведения соревнований по компьютерной безопасности, содержат задания с флагами.

Каждый участник получает *IP*-адрес своего экземпляра виртуальной машины, к которой может подключиться по протоколу *SSH* со своего рабочего места в собственной сети с помощью команды:

$ ssh <имя хоста экземпляра>@<IP-адрес своего экземпляра>

Соединение по протоколу *SSH* обеспечивает шифрование передаваемого трафика, включая пароли, что обеспечивает защиту от реализации угроз через сетевые соединения на рабочее место участника соревнований от других участников команд.

На управляющем узле *controller* установлен прототип программного средства мониторинга и управления функционированием виртуальных узлов при проведении игр по компьютерной безопасности, функциональная схема которого представлена на рис. 4.

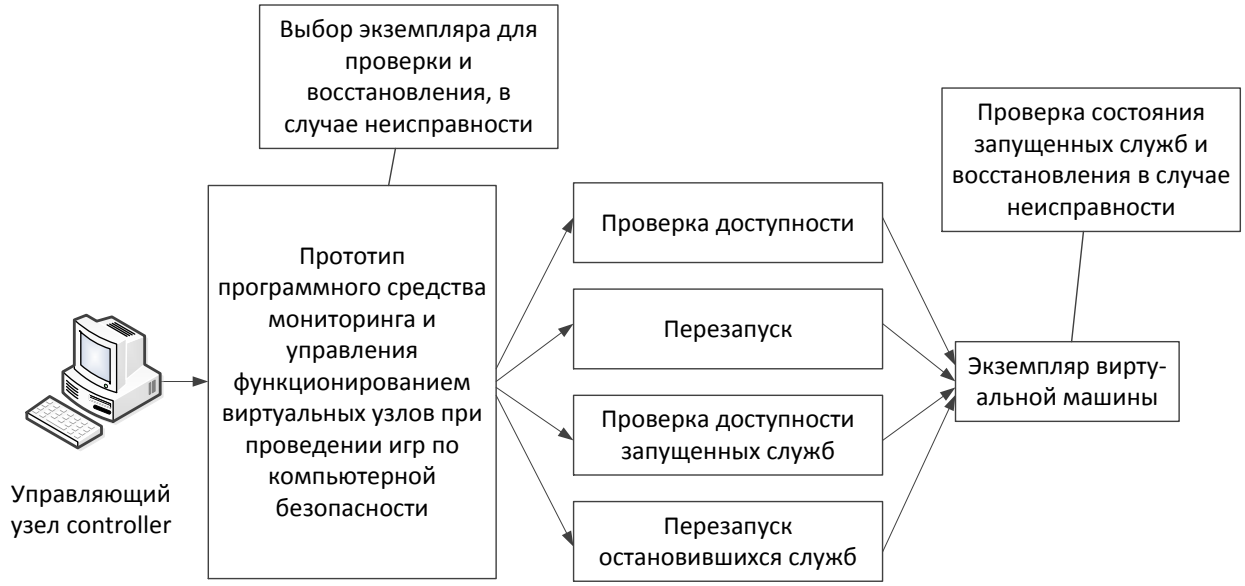


Рис. 4. Функциональная схема распределенного прототипа программного средства по мониторингу виртуальных узлов

На ПЭВМ запускается приложение *CTF-Monitoring*, в котором отображаются созданные экземпляры виртуальных машин, их состояние и состояние запущенных служб, необходимых для решения задач по компьютерной безопасности. В случае обнаружения недоступности узла или службы с помощью данной программы существует возможность оперативно восстановить работоспособность без прекращения соревнований.

Данное приложение предусматривает клонирование экземпляров виртуальных машин, что облегчает и ускоряет подготовку к соревнованиям по компьютерной безопасности. Функциональная схема по клонированию виртуальных узлов представлена на рис. 5.

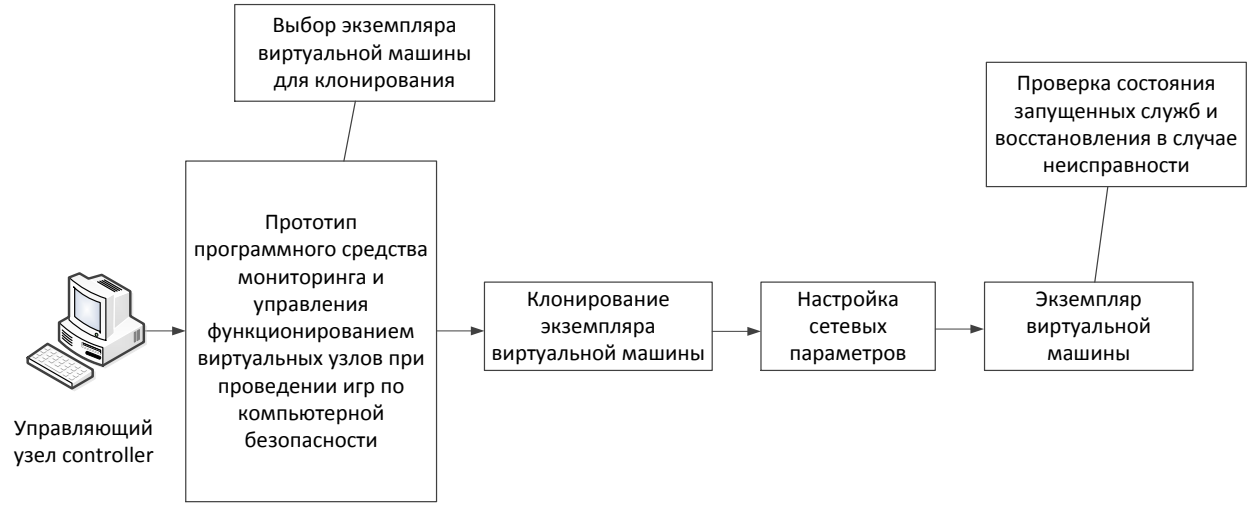


Рис. 5. Функциональная схема распределённого прототипа программного средства по клонированию и настройке виртуальных узлов

Сам прототип программного средства мониторинга и управления функционированием виртуальных узлов при проведении игр по компьютерной безопасности является важным компонентом, потому что предоставляет пользователю интуитивно понятный интерфейс для мониторинга экземпляров виртуальных машин, а также помогает администратору оперативно реагировать на неисправности, возникающие в процессе проведения игр.

Список литературы

1. Воробьев, А.А. Установка, настройка и эксплуатация частного облака на базе Openstack: пособие/ А.А. Воробьев, А.В. Потемкин, Б.И.Соловьев, А.В. Яковлев. – Орёл: Академия ФСО России, 2017. – 99 с.

2. Маркелов А., OpenStack: практическое знакомство с облачной операционной системой.: Учебное пособие ДМК Пресс, 2016 – 160 с.:ил.

3. OpenStack Documentation [Электронный ресурс] URL: https://docs.openstack.org/ocata/ (дата обращения: 29.03.19).

Материал поступил в редколлегию 19.04.19.

УДК 004.056

Богаченко Надежда Федоровна, *канд. физ.-мат. наук, доцент*
Омский государственный университет им. Ф.М. Достоевского, Омск, Россия
e-mail: nfbogachenko@mail.ru

ПРОТОКОЛ РАЗДЕЛЕНИЯ СЕКРЕТА МЕЖДУ ИЕРАРХИЧЕСКИ ОРГАНИЗОВАННЫМИ СУБЪЕКТАМИ

Предложено расширение произвольной схемы разделения секрета для иерархически организованных участников. Секрет могут восстановить только те участники, потомки которых покрывают всё множество листовых узлов иерархии. Алгоритм основан на шифровании долей секрета при помощи вычислимых ключей доступа.

Пусть на множестве субъектов S, участвующих в схеме разделения секрета, задано отношение порядка. Это отношение порождает иерархию, теоретико-графовой интерпретацией которой является ориентированный граф $G = (S, E)$ с множеством узлов S и множеством дуг E, не содержащий ориентированных циклов. Следует заметить, что каждый субъект $s \in S$ может представлять не отдельного пользователя, а целую группу пользователей или роль, как это реализовано в ролевой модели разграничения доступа [1, 2].

Требуется построить схему разделения некоторого секрета M между субъектами множества S с учётом имеющейся иерархии G: чем выше в иерархии субъекты, тем меньшее их число требуется для восстановления секрета. Традиционный подход описывается следующим требованием: чем выше субъект в иерархии, тем большее число долей он получает [3, 4]. В данной работе предлагается иное решение, использующее вычислимые ключевые материалы [5].

На первом этапе решения поставленной задачи будем считать, что иерархия, определённая на множестве S, является древовидной и описывается ориентированным деревом $T = (S, E)$. Пусть $L = \{s_{l1}, s_{l2}, \ldots, s_{lt}\} \subseteq S$ – множество листовых узлов дерева T и $t = |L|$ – мощность этого множества. Протокол разделения секрета для дерева субъектов T состоит из следующих шагов.

Шаг 1. Выбрать алгоритм разделения секрета. На его основе построить (t, t)-пороговую схему: секрет M делится на t долей $M_1, M_2, \ldots M_t$; для восстановления секрета M требуются все полученные доли.

Шаг 2. Каждому узлу s_i дерева T сопоставить уникальный идентификатор id_i – тем самым получить дерево доступа.

Шаг 3. Выбрать симметричный криптографический алгоритм для дальнейшего шифрования долей секрета (пусть E и D – функции шифрования и расшифрования). Определить секретный ключ k_1 – ключ доступа – для корня s_1 дерева доступа.

Шаг 4. Для каждого узла s_i ($s_i \neq s_1$) дерева доступа вычислить ключ доступа k_i по правилу: если дуга $(s_i, s_j) \in E$, то

$$k_j = h(k_i \circ id_j), \quad 1)$$

где h – криптографическая хеш-функция, $\circ$ – операция конкатенации ключа доступа и идентификатора.

Шаг 5. Зашифровать доли секрета $M_1, M_2, \ldots M_t$, используя ключи доступа $k_{l1}, k_{l2}, \ldots, k_{lt}$ листовых узлов, тем самым получить набор зашифрованных данных

$E(k_{l1}, M_1), E(k_{l2}, M_2), \ldots, E(k_{lt}, M_t)$.

Шаг 6. Каждому субъекту s_i выдать:

a) дерево доступа;
b) ключ доступа k_i;
c) зашифрованные доли секрета $E(k_{l1}, M_1), E(k_{l2}, M_2), \ldots, E(k_{lt}, M_t)$.

Рассмотрим процесс восстановления секрета. Множеством достижимости $R(s_i)$ узла s_i называется подмножество узлов орграфа, достижимых из узла s_i. При этом полагается, что $s_i \in R(s_i)$. Несложно понять, что восстановить секрет M может только такой набор субъектов $S_M = \{s_{i1}, s_{i2}, \ldots, s_{ik}\}$, что

$$L \subseteq R(s_{i1}) \cup R(s_{i2}) \cup \ldots \cup R(s_{ik}). \quad 2)$$

Действительно, если $S_M = L = \{s_{l1}, s_{l2}, \ldots, s_{lt}\}$, то известны ключи доступа $k_{l1}, k_{l2}, \ldots, k_{lt}$, следовательно, возможно расшифровать все доли секрета: $M_i = D(k_{li}, E(k_{li}, M_i))$ ($i = 1, \ldots, t$), и восстановить секрет M. Если $S_M = \{s_1\}$, то так как для корня дерева $R(s_1) = S$, то согласно формуле (1) возможно вычислить ключи доступа для всех узлов дерева доступа. Тем самым субъект, находящийся в вершине иерархии, может восстановить секрет. В общем случае гарантией возможности вычисления ключей доступа листовых узлов, и, как следствие, восстановления секрета M, является условие (2).

Если иерархия субъектов, определяемая орграфом G, не является древовидной, то можно воспользоваться результатами работы [6], в которой представлен алгоритм преобразования произвольной иерархии в древовидную. При этом некоторым узлам в исходном орграфе G будет сопоставлено несколько узлов эквивалентного ордерева T_G. Для каждого узла ордерева T_G следует вычислить ключ доступа, а затем получить результирующие ключи доступа для узлов орграфа G [5].

Необходимо отметить, что если рассматривать предложенный подход с точки зрения (t, n)-пороговых схем разделения секрета, то получена схема, в которой параметр t не является постоянной величиной. Количество субъектов, требующихся для восстановления секрета, зависит от местоположения этих субъектов в иерархии и изменяется в интервале от 1 до числа листовых узлов иерархии.

Если рассматривать иерархию субъектов как иерархию ролей или меток безопасности некоторой системы разграничения доступа, то представленный

подход может быть использован для организации коллективного разграничения доступа к ресурсам системы.

Список литературы

1. Ferraiolo D.F., Kuhn D.R. Role-Based Access Controls // 15th National Computer Security Conference. Baltimore MD, 1992. P. 554– 563.

2. Sandhu R.S., Coynek E.J., Feinsteink H.L., Youmank C.E. Role-Based Access Control Models // IEEE Computer. February 1996. V. 29, No. 2. P. 38–47.

3. Shamir A. How to share a secret // Communications of the ACM. 1979. Vol. 22, Iss. 11. P. 612–613.

4. Nojoumian, M., Stinson, D.R. Sequential Secret Sharing as a New Hierarchical Access Structure // J. Internet Serv. Inf. Secur. 2015. Vol. 5. P. 24–32.

5. Белим, С.В., Распределение криптографических ключей в системах с иерархией объектов / С.В. Белим, Н.Ф. Богаченко // Проблемы информационной безопасности. Компьютерные системы. 2016. № 2. С. 84–95. (Belim S.V., Bogachenko N.F. Distribution of Cryptographic Keys in Systems with a Hierarchy of Objects // Automatic Control and Computer Sciences. 2016. Vol. 50(8). P. 777–786.)

6. Bogachenko N.F. Local Optimization of the Role-Based Access Control Policy // CEUR Workshop Proceedings. 2017. Vol. 1965.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

Д.В. Винокуров
Научный руководитель: доц. кафедры «Системы информационной безопасности», к.т.н., О.М. Голембиовская
DevilKrock@gmail.com

РАЗРАБОТКА МЕТОДИКИ ОЦЕНКИ ОПРЕДЕЛЕНИЯ УЩЕРБА ОТ НАРУШЕНИЯ СВОЙСТВ БЕЗОПАСНОСТИ КОММЕРЧЕСКОЙ ТАЙНЫ

Описана разработанная методика оценки ущерба от нарушения свойств информационной безопасности относительно коммерческой тайны.

Методика оценки ущерба от нарушения свойств безопасности коммерческой тайны состоит из следующих этапов:

- Шаг 1. Определение уровней ущерба в зависимости от дохода предприятия или организации;
- Шаг 2. Определение носителей, которые содержат информацию, связанную с коммерческой тайной;
- Шаг 3. Определение существующих угроз для носителей коммерческой тайны;
- Шаг 4. Для каждой из угроз необходимо установить средства и меры защиты, имеющиеся на объекте;
- Шаг 5. После этого обратиться к базе угроз и средств защиты и определить максимальную оценку эффективности защиты на объекте, по результатом которой вынести вердикт организации;
- Шаг 6. Если уровень и сумма ущерба не удовлетворяет организацию, то необходимо дать нужные рекомендации по устранению уязвимостей в защите объектов хранения коммерческой тайны на объекте.

Определение уровней ущерба

В начале работы с методикой необходимо определить доход и ценность объекта коммерческой тайны организации, на основе которых будут установлены уровни ущерба, которые может понести организация. Корректная оценка реальных убытков или упущенной выгоды, полученных от незаконного раскрытия коммерческой тайны, предполагает объективную оценку стоимости данной информации с применением метода экспертной оценки, подтверждений факта разглашения коммерческой тайны, адекватной оценки морального ущерба. Соотношение всех образующих факторов дает возможность получить представление о наиболее полном объеме понесенного ущерба от разглашения коммерческой тайны. Уровни ущерба представлены в табл. 1.

Таблица 1

Уровень ущерба

Оценка уровня ущерба из-за нарушения свойств безопасности коммерческой тайны		
Уровень ущерба	Сумма ущерба	Доход предприятия или организации
Незначительный	до 2 млн. руб.	10 млн. руб.
Малый	2-4 млн. руб.	
Средний	4-6 млн. руб.	
Большой	6-8 млн. руб.	
Катастрофический	более 8 млн. руб.	

Определение носителей коммерческой тайны и актуальных угроз для них

На этом шаге необходимо установить все носители, которые содержат информацию, связанную с коммерческой тайной. Местом хранения коммерческой тайны могут быть бумажные носители, базы данных, жесткие диски компьютеров, съёмные носители информации и электронная почта. После того как будут установлены все носители с коммерческой тайной, необходимо для них определить все возможные угрозы. Носители коммерческой тайны и актуальные для них угрозы представлены в табл. 2.

Таблица 2

Носители коммерческой тайны и актуальные угрозы для них

Носитель коммерческой тайны	Актуальные угрозы
Бумажный носитель	Угроза несанкционированного доступа
	Угроза физического уничтожения носителя информации
	Угроза умышленного или случайного раскрытия информации
	Угроза потери или кражи носителя
Жесткий диск компьютера	Угроза вирусного заражения
	Угроза несанкционированного доступа
	Угроза физического уничтожения носителя информации
	Угроза умышленного или случайного изменения информации
	Угроза внешнего вторжения
	Угроза сбоя или отказа оборудования

Определения средств и мер защиты на объекте от актуальных угроз с определением максимальной оценки эффективности защиты на объекте

После определения угроз необходимо установить средства защиты информации (далее СЗИ) от них, имеющиеся на объекте. Для этого используется специально составленная база данных(далее БД) СЗИ. Пример такой БД представлен в табл. 3.

Таблица 3

Актуальные угрозы для носителей коммерческой тайны и оценка их эффективности.

Какие угрозы могут быть актуальны	Условия реализации угрозы	Важность СЗИ	Средства нейтрализации угрозы	Оценка эффективности средства
1. Угроза несанкционированного доступа Максимальная оценка эффективности - 4	Отсутствие пропускного пункта	0,1	Физический пропускной пункт	0,5
			Автоматическая система контроля доступа	1
			Отсутствие средств нейтрализации	0
	Отсутствие системы сигнализации	0,3	Сигнализация "Юпитер"	1
			Сигнализация "Приток"	0,7
			Сигнализация "OPERA-GSM"	0,3
			Отсутствие системы сигнализации	0
	Отсутствие защищенного места хранения бумажных носителей	0,4	Сейф	1
			Шкаф	0,5
			Отсутствие защищенного места хранения	0
	Отсутствие видеонаблюдения	0,2	Система видеонаблюдения ORIENT HVR+2+2AHD 1080p	1
			Система видеонаблюдения Ginzzu HK-443D	0,7
			Система видеонаблюдения Falcon Eye FE-104MHD KIT	0,3
			Отсутствие видеонаблюдения	0

Используя базу данных, необходимо опросить организацию на наличие СЗИ. По каждому условию реализации угрозы проводится проверка средств и мер защиты на объекте. У каждой угрозы есть своя максимальная оценка эффективности защиты от её реализации. Реализация максимальной оценки эффективности (МОЭ) зависит от весового коэффициента ответа ($кО_i$), согласно пункту оценки эффективности средства:

$$МОЭ = \sum_{i=1}^{N} кО_i$$

где N – количество вариантов реализаций угрозы.

Если $кО_i(n) \neq кО_{max}(n)$, то по данному пункту таблицы (N) будет вынесен вердикт. В вердикте описываются те условия реализации угрозы, для которых либо нет средств нейтрализации, либо эти средства не достаточно эффективны. Чем больше реализуемо условий угрозы, тем выше её актуальность. Если есть шанс угрозы, то может пострадать носитель коммерческой тайны. В зависимости от ценности коммерческой тайны назначается уровень ущерба. Если уровень и сумма ущерба не устраивают организацию, то необходимо вынести рекомендацию, которая позволит устранить условия реализации угрозы или повысит эффективность защиты от них. Пример реализации угрозы и ущерба от неё представлен в табл. 4.

Таблица 4

Реализуемые угрозы и уровни ущерба.

№	Носитель КТ	Актуальные угрозы	Возможный инцидент, связанный с угрозой, который нарушает свойства безопасности информации	Нарушаемое свойство безопасности информации	Описание инцидента	Уровень ущерба
1	Жёсткий диск компьютера	Угроза вирусного заражения; Угроза несанкционированного доступа; Угроза физического уничтожения носителя информации; Угроза умышленного или случайного изменения информации; Угроза внешнего вторжения; Угроза блокирования информации; Угроза сбоя или отказа оборудования.	Копирование.	Конфиденциальность	Была скопирована и разглашена база данных. Сотрудник скопировал БД клиентов и распространил.	Большой
			Изменение информации	Целостность	Произошла смена паролей от компьютеров. Организация потеряла свою работоспособность на несколько дней.	Малый
			Удаление информации	Доступность	Произошло удаление базы данных. Вредоносный "клон" удалил всю информацию.	Катастрофический

Данная методика позволяет эффективно определить актуальные угрозы для носителя КТ и определить уровень ущерба, если произойдёт инцидент.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 303.64

Д.В. Винокуров
Научный руководитель: доцент кафедры «Системы информационной безопасности», к.т.н., О.М. Голембиовская
DevilKrock@gmail.com

АНАЛИЗ НАУЧНОЙ ЛИТЕРАТУРЫ В ОБЛАСТИ РАЗРАБОТКИ МЕТОДИКИ ОПРЕДЕЛЕНИЯ УЩЕРБА ОТ НАРУШЕНИЯ СВОЙСТВ БЕЗОПАСНОСТИ КОММЕРЧЕСКОЙ ТАЙНЫ

Рассматривается существующая нормативно-правовая базы в области безопасности коммерческой тайны, а также формируется перечень научных задач, необходимых для разработки методики определения ущерба от нарушения свойств безопасности коммерческой тайны.

В современном мире информационной безопасности уделяется все большее внимание. На это повлияло серьёзное развитие информационных технологий и полная информатизация многих сфер в обществе.

В рамках работы были изучены следующие нормативно-правовые акты: Федеральный закон № 98 «О коммерческой тайне» от 29 июля 2004 г. и Федеральный закон № 149 «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г.

Федеральный закон «О коммерческой тайне» определил понятие «коммерческая тайна». Однако с принятием четвертой части ГК РФ закон претерпел значительные изменения. В настоящее время федеральный закон регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, составляющей секрет производства (ноу-хау).

Определение термина «коммерческая тайна» приведено в п. 1 ст. 3 ФЗ № 98 от 29 июля 2004 г. «О коммерческой тайне». Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Согласно п. 2 ст.3 упомянутого закона, можно дать определение информации, которая составляющая коммерческую тайну. Это сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у

третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

А в следующем Федеральном законе № 149 «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. использованы статьи 7 и 17. Статьи данного закона дают точное описание общедоступной информации, а так же позволяют определить ответственность за правонарушения в сфере информации.

Так же был изучен международный стандарт, применимый в рамках определения ущерба от нарушения свойств безопасности коммерческой тайны. Международный стандарт ISO/IEC 27001:2013 «Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности» позволит изучить риски информационной безопасности. Пункты 8.2 и 8.3 данного международного стандарта позволят изучить функционирование оценки и обработки рисков информационной безопасности.

По теме исследования был проведен обзор научной литературы, среди которой учебники и статьи.

Из учебника «Конфиденциальное делопроизводство и защита коммерческой тайны. Курс лекций.» под авторством Кришталюка А.Н. можно позаимствовать информацию о признаках коммерческой тайны и мерах по охране конфиденциальной информации. К ним относятся правовые, организационные, технические и иные меры, применяемые обладателем КТ для обеспечения ограниченного доступа к конфиденциальной информации, называется режимом КТ.

А со второго учебника «Стандарты информационной безопасности. Защита и обработка конфиденциальных документов. Учебное пособие.» под авторством Сычева Ю.Н. были изучены виды и способы защиты коммерческой информации взяты, а также изучены меры для установки и обеспечения безопасности режима коммерческой тайны. Так же информация из второго учебника позволила более подробно описать требования для работника и работодателя во время режима коммерческой тайны.

По теме работы была взята статья «Обеспечение безопасности конфиденциальной информации и коммерческой тайны» под авторством Гордеевой Е.В., Леонтьева А.С., Седовой Н.В. Данная статья позволяет изучить меры по защите коммерческой тайны и построить структуру разработки комплекса мер по защите информации по следующим пунктам:

- организационная защита информации;
- система контроля и управления доступом;
- инженерно-техническая защита информации;
- программно-аппаратная защита.

Из второй статьи «Оценка реальных убытков и упущенной выгоды от незаконного раскрытия коммерческой тайны» под авторством Силантьевой Н.Д. были взяты методики по оценке ущерба от разглашения информации составляющей коммерческую тайну, а так же подход к оценке убытков от её раскрытия. Методика применения доходного метода к оценке убытка, понесенного от раз-

глашения коммерческой тайны, позволяет оценить доходы, полученные злоумышленником от получения, хранения или применения информации, составляющей коммерческую тайну. Сопоставив полученные значения с аналогичными данными за период до наступления факта разглашения коммерческой тайны, учитывая возможные дополнительные расходы, можно получить значение дохода, возникшего у злоумышленника. Данная методика, по сравнению с расходным методом, даст более конкретное и близкое к истине значение, однако, зачастую возникают серьезные трудности с получением полной и достаточной информации для произведения всех соответствующих расчетов. К тому же, в случае, если в деле замешаны третьи лица, задача отслеживания реальных доходов злоумышленников значительно усложняется.

Для формирования базы угроз в рамках исследования за основу был взят банк данных угроз безопасности информации ФСТЭК.

По итогам работы была изучена нормативно-правовая база, данные методических документов, научных статей и учебников по выбранной теме, что поможет разработать методику определения ущерба от нарушения свойств безопасности коммерческой тайны.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

***Голембиовская Оксана Михайловна**, к.т.н., доцент каф. «Системы информационной безопасности»*
***Боровых Надежда Евгеньевна**, студент, каф. «Системы информационной безопасности»*
***Шинаков Кирилл Евгеньевич**, к.т.н., доцент каф. «Системы информационной безопасности»*
***Курыкин Андрей Викторович**, магистрант каф. «Системы информационной безопасности»*
ФГБОУ ВО «Брянский государственный технический университет»
Россия, г. Брянск
nirsamy-bgtu@yandex.ru

ОСОБЕННОСТИ СОДЕРЖАНИЯ МОДЕЛЕЙ УГРОЗ ДЛЯ РАЗЛИЧНОГО ВИДА ИНФОРМАЦИОННЫХ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Рассматривается построение моделей угроз для различного вида информационных и автоматизированных систем.

С развитием информационных технологий и тотальной информатизацией всех сфер общества все больше внимания уделяется информационной безопасности. Для обеспечения качественной защиты требуется определить угрозы безопасности, необходимо знать уязвимости информационной системы.

Модель угроз представляет собой физическое, математическое или описательное представление свойств или характеристик угроз безопасности информации. Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств [1].

Модель угроз для ИСПДн должна быть разработана на основании таких документов, как «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК России, 14 февраля 2008 г.) и «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК России, 15 февраля 2008 г.). Она должна включать в себя следующие угрозы (Перечень):

1. Угрозы по техническим каналам:
1.1. Угрозы утечки акустической информации.
1.2. Угрозы утечки видовой информации.
1.3. Угрозы утечки информации по каналам ПЭМИН.
2. Угрозы несанкционированного доступа к информации:
2.1. Угрозы уничтожения, хищения аппаратных средств путем физического доступа.

2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программных средств.

2.3. Угрозы непреднамеренных действий пользователей (утрата ключей, непреднамеренное отключение средств защиты, сбой системы электропитания, стихийное бедствие).

2.4. Угрозы преднамеренных действий внутренних нарушителей (доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке, разглашение информации).

2.5. Угрозы несанкционированного доступа по каналам связи (угрозы с перехватом передаваемой информации, угрозы сканирования на выявление типов ОС, открытых портов и служб, угрозы выявления паролей, удаленного запуска приложений, внедрения вредоносных программ).

Фрагмент модели угроз безопасности персональных данных при их обработке в ИСПДн представлен в табл.1

Таблица 1

Фрагмент модели угроз безопасности ПДн при их обработке в ИСПДн

2. Угрозы несанкционированного доступа к информации					
2.1. Угрозы уничтожения, хищения аппаратных средств носителей информации путем физического доступа к элементам ИСПДн					
Наименование угрозы	**Числовой коэффициент вероятности реализации угрозы (Y_2)**	**Числовой коэффициент возможности реализации угрозы (Y)**	**Опасность угрозы**	**Актуальность угрозы**	**Применяемые меры по противодействию угрозе**
					Технические
2.1.1. Кража ПЭВМ	0 (Маловероятно)	0,25 (Низкая)	Низкая	Неактуальная	1. Стальные двери оборудованы замками. 2.На объекте установлена охранная сигнализация. 3.Имеется контрольно-пропускной пункт. 4.Имеются сейфы для хранения материальных носителей конфиденциальной информации. 5.Территория огорожена забором, обеспечена физическая охрана объекта.
2.1.2. Кража носителей информации	0 (Маловероятно)	0,25 (Низкая)	Низкая	Неактуальная	
2.1.3. Кража ключей доступа	0 (Маловероятно)	0,25 (Низкая)	Низкая	Неактуальная	
2.1.4. Кражи, модификации, уничтожения информации.	0 (Маловероятно)	0,25 (Низкая)	Низкая	Неактуальная	
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0 (Маловероятно)	0,25 (Низкая)	Низкая	Неактуальная	
…	…	…	…	…	…

Государственные информационные системы – это системы для реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами

целях [2]. В соответствии с Приказом ФСТЭК №17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», модель угроз для ГИС должна описывать следующие параметры [3]: (табл.2.)

Таблица 2

Модель угроз для ГИС

Описание информационной системы	
Область использования системы	
Перечень пользователей и отделов, имеющих доступ к информационной системе	
Назначение ИС	
Цели ИС	
Задачи ИС	
Субъекты доступа ИС	
Объекты доступа ИС	
Структурно-функциональная характеристика ИС	
Структура ИС	
Состав ИС	
Физические взаимосвязи между сегментами ИС с иными ИС и информационно-телекоммуникационными сетями	
Логические взаимосвязи …	
Функциональные взаимосвязи …	
Технологические взаимосвязи …	
Режимы обработки информации в информационной системе и в ее отдельных сегментах	
Иные характеристики информационной системы	

Так как в целом процесс обработки информации в ИСПДн схож с процессом обработки в ГИС, то для ГИС целесообразно рассматривать угрозы из *Перечня*, относящиеся к модели угроз для ИСПДн, такие как 1.1. - 2.5.

АСУ ТП – автоматизированная система управления, включающая:

- уровень операторского управления;
- уровень автоматического управления;
- уровень ввода (вывода) данных исполнительных устройств [4].

Для обеспечения безопасности АСУ ТП, помимо обеспечения трех наиболее важных свойств безопасности: конфиденциальности, целостности и доступности информации, необходимо, в первую очередь, обеспечить безопасность производственного процесса. Для защиты АСУ ТП нецелесообразно использовать модели угроз ИСПДн и ГИС полностью, так как не все угрозы, касающиеся ИСПДн и ГИС, актуальны для АСУ ТП.

Для АСУ ТП будут характерны следующие угрозы из *Перечня* 2.2, 2.3, 2.5. Например, угроза утечки видовой информации не является актуальной для АСУ ТП, так как только оператор АСУ ТП при визуальном контакте с АС может понять, как функционирует автоматизированная система и где находится конфиденциальная информация. Требования к обеспечению защиты информации в АСУ ТП содержатся в Приказе ФСТЭК №31 от 14 марта 2014 г. «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процес-

сами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [4]. Согласно приказу, модель угроз для АСУ ТП должна иметь разделы, представленные в табл.3.

Таблица 3

Модель угроз для АСУ ТП

Описание АСУ ТП	
Область использования системы	
Перечень пользователей и отделов, имеющих доступ к АСУ ТП	
Назначение АСУ ТП	
Цели АСУ ТП	
Задачи АСУ ТП	
Субъекты доступа АСУ ТП	
Объекты доступа АСУ ТП	
Процессы, которыми управляет система	
Наличие уровней (сегментов) автоматизированной системы управления	
Состав АСУ	
Физические взаимосвязи в АСУ	
Логические взаимосвязи …	
Функциональные взаимосвязи …	
Технологические взаимосвязи …	
Взаимодействие с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями	
Режимы функционирования автоматизированной системы управления	
Иные особенности ее построения и функционирования	

Также для построения модели угроз следует использовать угрозы из базы данных угроз ФСТЭК. Пример оформления перечня угроз представлен в табл. 4.

Таблица 4

Пример оформления перечня угроз

УБИ	**Название угрозы**	**Описание угрозы/Описание уязвимостей/ Обоснование актуальности или неактуальности угрозы**	**Источники угрозы**	**Объект воздействия**	**Последствия реализации угрозы**
УБИ.3	Угроза анализа криптографических алгоритмов и их реализации	Угроза заключается в возможности выявления слабых мест в криптографических алгоритмах или уязвимостей в реализующем их программном обеспечении. Данная угроза обусловлена слабостями криптографических алгоритмов, а также ошибками в программном коде криптографических средств, их сопряжении с системой или параметрах их настройки. Реализация угрозы возможна в случае наличия у нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их настройки. ***Система не имеет подключения к сетям общего пользования. Угроза не актуальна.***	Внешний нарушитель со средним потенциалом	Метаданные, системное программное обеспечение	Нарушение конфиденциальности, целостности

При этом для каждой угрозы необходимо указать условия ее неактуальности.

Таким образом, рассмотрев различные подходы к наполнению моделей угроз (МУ) необходимо отметить, что главным при построении МУ является описательная часть и аргументированные доводы при присвоении угрозам значения «Неактуальная».

Список литературы

1. 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 11.04.19.).

2. Ст.4 ФЗ от 27.07.2006 № 149-ФЗ (ред. от 18.03.19.) «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/6b46c7cef112b2df9fc3d7f737c7bb1276e74225/ (Дата обращения 11.04.19.).

3. Приказ ФСТЭК №17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электронный ресурс]. Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (Дата обращения 11.04.19.).

4. Приказ ФСТЭК №31 от 14 марта 2014 г. «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [Электронный ресурс]. Режим доступа:https://fstec.ru/index?id=868:prikaz-fstek-rossii-ot-14-marta-2014-g-n-31(Дата обращения 11.04.19.).

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.04

Голембиовская Оксана Михайловна, *к.т.н., доцент каф. «Системы информационной безопасности»*
Новиков Валерий Петрович, *к.ю.н., доцент каф. «Системы информационной безопасности»*
Боровых Надежда Евгеньевна, *студент, каф. «Системы информационной безопасности»*
ФГБОУ ВО «Брянский государственный технический университет»
Россия, г. Брянск
nirsamy-bgtu@yandex.ru

ФОРМАЛИЗАЦИЯ АДЕКВАТНЫХ МЕР ЗАЩИТЫ ПРИ ТРАНСГРАНИЧНОЙ ПЕРЕДАЧЕ ПДн

Рассмотрена формализация адекватных мер защиты при трансграничной передаче ПДн.

В разных странах мира сложилась собственная практика защиты персональных данных. Так, в соответствии с Руководством по защите персональной информации в информационной системе по оказанию публичных и коммерческих услуг, которое принято в Китае, персональные данные - это любая информация о физическом лице, которая сама по себе или в комбинации с другой информацией позволяет его идентифицировать. 1 июня 2017 года в КНР вступил в силу «Закон о кибербезопасности». Этот закон является первым сводным законом, регулирующим практически все вопросы данной сферы в Китае, в том числе, и вопросы трансграничной передачи ПДн. В ст. 37 данного закона сказано, что хранение личных данных и других важных данных должно обеспечиваться исключительно на территории КНР.

В США отсутствует общее законодательство в сфере защиты персональных данных, поэтому в случае нарушения прав субъектов ПДн применяются положения Конституции и практика прецедентного права, преобладающего в США. Основные действующие документы, относящиеся к сфере обработки ПДН (регуляция деятельности органов государственной власти при обработке ПДн) являются законы о конфиденциальности: Privacy Act of 1974 и Privacy Protection Act of 1980. Также в США применяется «зонтичный» подход к защите персональных данных – обеспечение адекватной защиты ПДн в отдельных областях, где по заключению Еврокомиссии, обеспечивается адекватная защита персональных данных.

В Индии общего закона о защите ПДн нет, но в 2011 году был принят документ «Правила по практике и процедуре обеспечения безопасности особых категорий персональных данных и информации», с котором определяется формулировка персональных данных. В п.3 этого документа выделяют специальные категории:

– пароли;
– финансовая информация (включая данные о банковском счете и кредитной карте);
– данные о здоровье;
– биометрические данные.

Согласно п. 7, трансграничная передача ПДн граждан Индии может быть разрешена только тогда, когда это необходимо для выполнения договора между юридическим лицом и субъектом ПД или, когда субъект дал свое согласие на передачу данных.

Для обеспечения уважения прав и свобод граждан за границей их государства, была разработана и принята «Конвенция о защите физических лиц при автоматизированной обработке персональных данных» [1]. Документ был ратифицирован в России в 2013 году.

Существует практика, когда государство расширяет сферу применения Конвенции, для этого нужно заявление, в котором будут указаны категории файлов ПДн, перечень которых будет сдан на хранение. Если же одна Сторона исключила определенные категории ПДн из защиты, то не в праве требовать от другой Стороны защиты персональных данных ее страны, из идентичной категории.

В соответствии с ФЗ №152 «О персональных данных», трансграничная передача персональных данных может осуществляться на территории иностранных государств, если будет обеспечена их адекватная защита [2]. Так как адекватная защита может быть представлена в разных интерпретациях, то следует выделить минимум правил, на которые стоит опираться.

Организация, которая работает с персональными данными, должна обеспечить сохранность информации и запрет несанкционированного доступа к ней. Защита информации обеспечивается следующим образом:
– архивное копирование данных;
– использование средств шифрования;
– ограничением доступа к информации;
– применение антивирусных средств.

Также в организации должны быть разработаны организационно-распорядительные документы, такие, например, как:
– приказ об утверждении перечня ПДн, передаваемых трансграничным путем (в бумажном виде);
– приказ об утверждении описаний мероприятий и средств обеспечения защиты, передаваемых ПДн трансграничным путем;
– приказ об утверждении перечня круга лиц, допущенного к обработке ПДн;
– должностные инструкции по работе с ПДн;
– приказ об установлении персональной ответственности за нарушения правил обработки ПДн;

– приказ об утверждении перечня персональных данных, передаваемых организацией трансграничным путем.

Таким образом, набор предложенных мер и средств защиты можно рассматривать как адекватные меры защиты при трансграничной передаче персональных данных.

Список литературы

1. «Конвенция о защите физических лиц при автоматизированной обработке персональных данных» (Заключена в г. Страсбурге 28.01.1981) (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ N 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999) // Консультант Плюс справочная правовая система. Версия 3000.02.12. - М.: ЗАО «Консультант Плюс», 1997-2019. (Режим доступа: 19.03.19.).

2. Статья 12 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» Электронный ресурс: [принят ГД ФС РФ 08.07.2006] // Консультант Плюс справочная правовая система. Версия 3000.02.12. - М.: ЗАО «Консультант Плюс», 1997-2019. (Режим доступа: 19.03.19.).

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

Горлов А.П. *к.т.н. доц. кафедры «Системы информационной безопасности»*
Филиппова Л.Б. *к.т.н. доц. кафедры «Компьютерные технологии и системы»*
Филиппов Р.А. *к.т.н. доц. кафедры «Компьютерные технологии и системы»*
Лысов Д.А. *асс.. кафедры «Системы информационной безопасности»*
ФГБОУ ВО «Брянский государственный технический университет»
Россия, г. Брянск
lysovdmitriia@gmail.com

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕРНЕТА ВЕЩЕЙ

Рассматриваются вопросы обеспечения безопасности при подключении сенсоров и датчиков при организации процесса передачи данных между устройствами в сети Интернета вещей.

В последнее время все чаще звучит словосочетание "Интернет вещей", все больше компаний проявляют интерес к этому явлению и хотели бы начать работать в этом направлении.

Другими словами, любые устройства, системы и сервисы практически из любой отрасли могут быть автоматизированы с помощью современных технологий коммуникаций. Объекты, наделенные интеллектом, также относятся к Интернету вещей. Таким образом, Интернет вещей составляют объекты в физическом мире, способные передавать информацию о собственном состоянии, окружении, а также данные, подлежащие анализу (например, с помощью встраиваемых устройств).

К 2020 году к Интернету будет подключено 26 млрд устройств. Обилие новых приложений и встраиваемых устройств приведет к значительному увеличению генерируемых в Сети данных, что в свою очередь будет диктовать необходимость совершенствования систем хранения и обработки данных. Но что еще более важно, при этом увеличится потребность в защите данных и в обеспечении безопасности этих новых, подключенных к Интернету устройств от атак хакеров. Аспекты безопасности будут иметь особое значение для ряда отраслей, где развитие Интернета вещей способно привести к самым серьезным переменам, например, в отрасли производства – где к глобальной Сети будут подключены транспорт, устройства и производственные мощности. В этих условиях потенциальный ущерб зависит от мотивации тех лиц, кто вовлечен в процесс, но в то же время это означат, что внешние злоумышленники могут собирать частную информацию или преследовать еще более пагубные цели: например, отключить сигнализацию или вывести из строя критически важное оборудование на электростанции.

Во-первых, решение проблем безопасности следует начинать с формирования нового набора правил лицензирования программного обеспечения,

управления представлением прав доступа и защиты интеллектуальной собственности. В качестве отправной точки для Интернета вещей необходимо организовать "узел интерпретации" (Interpretation HUB) серверного типа, который будет выполнять роль базы знаний при подключении самых разнообразных опций.

Во-вторых, организациям придется воспользоваться этими средствами для предотвращения реверс-инжиниринга и внедрить с этой целью повсеместное шифрование. Для достижения максимального уровня безопасности шифрование данных должно распространяться на все каналы связи между устройствами, а коды аутентификации должны быть связаны с соответствующим аппаратным обеспечением, гарантируя безопасность учетных данных пользователей и систем.

Наконец, в-третьих, если допускать, что нарушитель способен проникнуть в систему, то следует обеспечить повсеместное шифрование. Сюда относится как шифрование данных, так и защита программного обеспечения, встроенного в сенсоры, сети и системы, которые собирают, анализируют и обмениваются данными.

Рассмотрим аспекты безопасности IoT на простом примере (рис. 1).

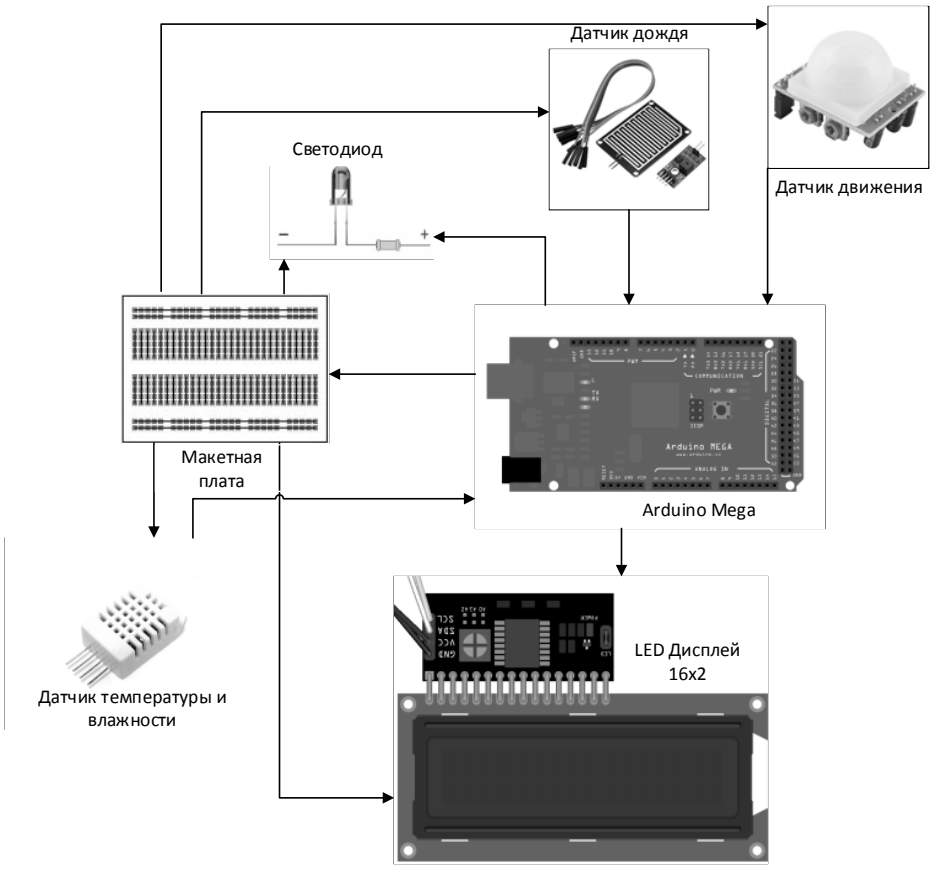


Рис. 1. Схемы коммутации датчиков.

Согласно схеме, Arduino подключается к компьютеру для загрузки ПО. После этого возможно использование батареи 9V для обеспечения питания. Затем от Arduino идёт питание (5V, “-“) на макетную плату для подключения

большого количества датчиков. После чего возможно подключение различных типов датчиков и дополнительных устройств, например:

- датчик дождя YL-83 подключается к питанию на макетной плате и входу A0 на Arduino;
- датчик температуры и влажности DHT22 подключается к питанию на макетной плате и входу D2 на Arduino;
- датчик движения HC-SR501 подключается к питанию на макетной плате и входу D3 на Arduino;
- светодиод через резистор подключается “-“к макетной плате и “+” к входу D4 на Arduino;
- LED дисплей подключается к питанию на макетной плате и ко входам D20(SDA), D21(SCL) на Arduino.

После загрузки ПО, Arduino периодически отправляет подаваемые датчиками сигналы. В зависимости от сигнала, по приоритету на LED дисплей выводится полученная информация. В данном примере приоритет следующий: движение в комнате, дождь, температура и влажность.

При обнаружении движения, на дисплей выводится сообщение «Movement!» и включается светодиод. Спустя 5 секунд после окончания движения, светодиод гаснет и приоритет экрана отдаётся другой информации. При обнаружении дождя, светодиод мигает несколько раз и на дисплей выводится сообщение раз в пять секунд в зависимости от силы дождя «Rain» или «Flood». Если ни дождя, ни движения не обнаружено, на экран выводятся показания температуры и влажности.

Вместе с тем все эти новшества создают целый ряд проблем с информационной безопасностью, которые не дают спокойно спать. В частности, беспокоит возможность попадания сети датчиков в руки злоумышленника. Такое особенно вероятно, если сеть напрямую управляет физическими устройствами с помощью коммуникаций "машина-машина" (machine-to-machine, M2M). Всякий раз, когда у вас появляются автономные или полуавтономные системы, нужно обращать внимание, под чьим управлением они находятся. Можно лишь надеяться, что все компании будут придерживаться общепринятых правил. Процветание современного общества без взаимного доверия невозможно.

В уравнении под названием "Интернет вещей" столько неизвестных, что всегда есть вероятность того, что полезные сами по себе элементы Интернета вещей могут вдруг вызвать либо ускорить катастрофический сбой. Предугадать такой сбой практически невозможно, хотя после катастрофы ее причина будет казаться совершенно очевидной. К числу таких явлений можно отнести возможное отключение сети электропередачи.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 5.007

***Горлов Алексей Петрович**, к.т.н., доцент каф. «Системы информационной безопасности» БГТУ*
***Лексиков Евгений Вячеславович**, ст. преподаватель каф. «Системы информационной безопасности» БГТУ*
***Гулак Максим Леонидович**, к.т.н., доцент каф. «Системы информационной безопасности» БГТУ*
ФГБОУ ВО «Брянский государственный технический университет»
Россия, г. Брянск
apgorlov@gmail.com

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Рассматривается методика оценки эффективности программно-аппаратных средств защиты информации, путем создания автоматизированной системы. Основными функциями предлагаемой системы являются: проведение аудита информационной безопасности, формирование модели угроз ИБ, формирование рекомендаций по созданию программно-аппаратной системы защиты информации, формирование организационно-технической документации.

На сегодняшний день проблема защиты конфиденциальной информации стоит особенно остро. Ущерб от реализации угроз компьютерным системам (КС) и обрабатываемой в них конфиденциальной информации превышает миллионы рублей.

По статистике за 2018 год на территории РФ зафиксировано около 300 тысяч преступлений в сфере информационной безопасности. К этим преступлениям относятся несанкционированный доступ к конфиденциальной информации, утечка и разглашение атрибутов доступа к подсистемам КС, создание, использование или распространение вредоносных программ для ЭВМ или машинных носителей с такими программами.

Объектом информатизации называется совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а так же средств их обеспечения, помещений или объектов, в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведений конфиденциальных переговоров.

Отсутствие на объектах информатизации программно-аппаратных систем защиты информации (ПАСЗИ) приводит к утечке конфиденциальной информации, так как разработка и внедрение таких систем является достаточно сложной и затратной процедурой. В общем случае на компьютерную систему влияет ряд факторов, который можно условно разделить на две категории: требования за-

конодательства и стандартов в области защиты информации, а также различные угрозы информационной безопасности. Автоматизированная система оценки эффективности программно-аппаратных средств защиты информации позволит привести КС в соответствие установленным требованиям, противостоять актуальным угрозам, снизить трудоемкость работ, сэкономить время и значительно сократить материальные затраты на проведение аудита и разработку ПАСЗИ.

Ввиду этого разработка системы автоматизированной оценки эффективности программно-аппаратных средств защиты представляется актуальной. На данный момент автоматизированная оценка уровня информационной безопасности производится исключительно по стандартам ISO, однако в РФ более распространена организационно-распорядительная документация.

В предлагаемом подходе в основу положена оценка защищенности объекта информатизации согласно положениям законодательной базы РФ, требованиям государственных стандартов, а так же проверка наличия организационно-технической документации регламентирующей защиту компьютерных систем.

Основной задачей разрабатываемой АС является выявление уязвимостей существующих систем обработки и защиты информации. В качестве входных данных используются данные о КС. Данные вводятся на основе специально разработанных опросных анкет.

Алгоритм работы АС

1. Ввод исходных данных.
2. Формирование информационной модели компьютерной системы, определение целей и задач по ЗИ.
3. Оценка состояния защищенности ОИ.
4. Формирование модели угроз ИБ.
5. Формирование рекомендаций по совершенствованию системы защиты информации.
6. Формирование организационно-технической документации.

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

Структурно-функциональная схема, разработанной АС представлена на рис. 1.

Ввод исходных данных представляет собой заполнение опросных анкет, которые позволят выявить вид обрабатываемой информации, существующие программно-аппаратные средства защиты информации, угрозы ИБ, уязвимости системы защиты информации, а также прочие данные позволяющие составить информационную модель объекта информатизации.

Следующим этапом является оценка состояния защищенности КС. Выделяется 3 основных направления оценки защищенности:

1. Оценка на соответствие требованиям стандартов (ГОСТ, СТР-К, ISO) .
2. Определение наличия программно-аппаратных средств защиты информации на объекте информатизации.

3. Выявление организационно-технической документации, регламентирующей защищенную обработку конфиденциальной информации.

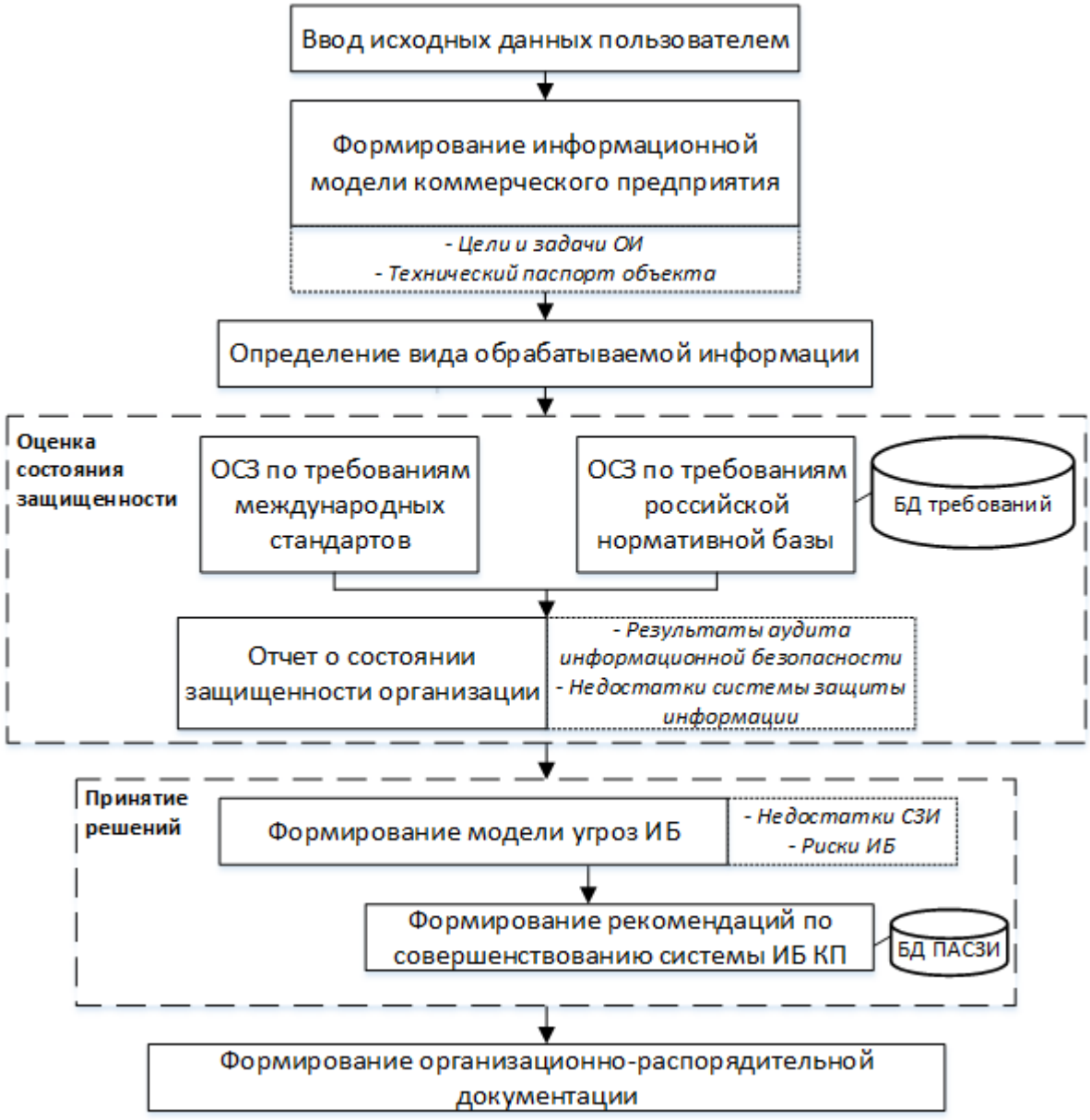


Рис. 1. Структурно-функциональная схема автоматизированной системы.

По результатам данного этапа формируется отчет о состоянии защищенности компьютерной системы.

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, режиму обработки данных и т.д.

Следующим этапом является формирование рекомендаций по совершенствованию системы защиты информации. Рекомендации разделяются на 4 основных раздела:

1. Рекомендации по антивирусной защите информации.
2. Рекомендации по защите информации от несанкционированного доступа (НСД).
3. Рекомендации по применению средств межсетевого экранирования.
4. Рекомендации по применению средств обнаружения вторжений.

По каждому разделу приводится ряд мер выполнение которых необходимо для защиты от выявленных угроз. Так же на данном этапе происходит подбор оптимальных средств программно-аппаратной защиты информации исходя из допустимой стоимости и набора необходимых характеристик.

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

На данном этапе производится оценка наличия организационно-технической документации на объекте, выявляются недостающие документы, если необходимо, производится сбор дополнительных данных необходимых для формирования дополнительных документов.

В качестве выходных данных по результатам работы данного блока является комплект организационно-технической документации регламентирующей эксплуатацию программно-аппаратных средств защиты.

Результаты работы автоматизированной системы представлены на рис.2.

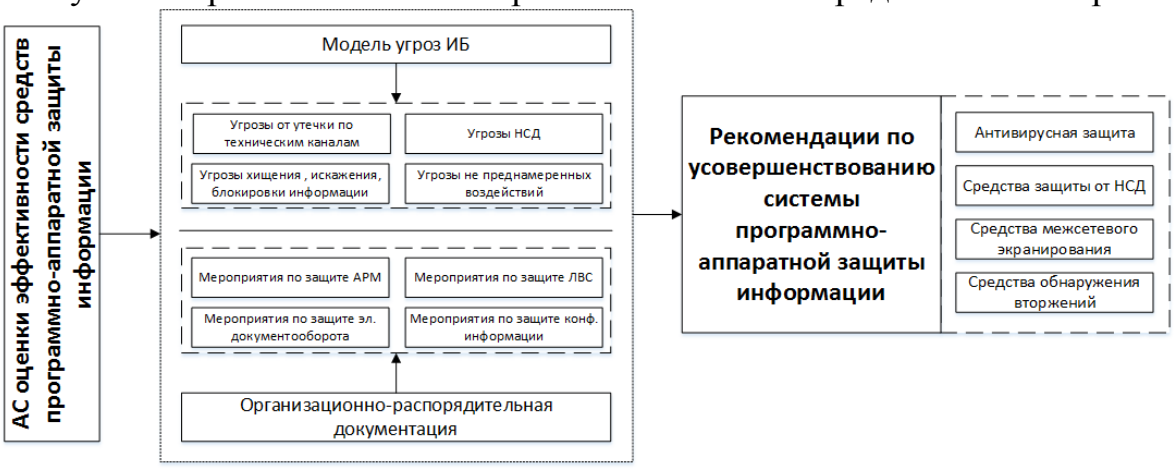


Рис. 2. Результаты работы АС.

Таким образом, разработанная автоматизированная система оценки эффективности программно-аппаратных средств защиты информации позволяет в автоматизированном режиме построить модель угроз информационной безопасности, сформировать организационно-техническую документацию регламентирующую защиту конфиденциальной информации, а так же сформировать рекомендации по усовершенствованию программно-аппаратной системы защиты информации. Применение данной системы позволит значительно сократить

временные и материальные затраты на проведение аудита информационной безопасности и разработку дополнительных мер защиты информации.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

***Гулак Максим Леонидович**, к.т.н., доцент каф. «Системы информационной безопасности» БГТУ*
***Горлов Алексей Петрович**, к.т.н., доцент каф. «Системы информационной безопасности» БГТУ*
***Лексиков Евгений Вячеславович**, ст. преподаватель каф. «Системы информационной безопасности» БГТУ*
Брянский государственный технический университет
Россия, г. Брянск
e-mail: gml13@yandex.ru

АНАЛИЗ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ

Выявлены и рассмотрены угрозы ИБ в деятельности правоохранительных органов; характеристики и уязвимости объектов, информационную безопасность которых необходимо обеспечить.

Человек XXI века, обитая в информационном обществе, не может не участвовать в информационных процессах. Информационная безопасность России является составляющей национальной безопасности страны в целом, а ее обеспечение – одной из важнейших задач государства.

Деятельность по обеспечению безопасности информационной сферы общественной жизни имеет определенные нюансы, связанные с особенностями объектов защиты. В каждой области деятельности в целях обеспечения информационной безопасности используют разнообразные методы её обеспечения, эффективные в той или иной мере. Перед специалистами, работающими в сфере обеспечения безопасности, стоят важные задачи оценки эффективности комплекса применяемых приемов, средств и методов защиты и разработки рекомендаций по улучшению используемых мер. Следовательно, выполняется анализ угроз и оценка рисков ИБ в отдельно взятой сфере общественной жизни.

Рассмотрим особенности определения угроз и оценки рисков информационной безопасности в правоохранительной сфере.

Анализ начинается с выявления и идентификации всех основных угроз, их источников, объектов и методов обеспечения ИБ.

К условиям и основным причинам возникновения угроз информационной безопасности в правоохранительной сфере можно отнести следующие факторы [1].

Расширяющиеся области применения информационных технологий наряду с развитием экономики и совершенствованием общественных и государственных институтов порождают новые информационные угрозы.

Возможности быстрого обмена информацией используются для достижения террористических, экстремистских, криминальных и иных противоправных

целей. Повсеместное внедрение информационных технологий без учета требований всестороннего обеспечения информационной безопасности существенно повышает вероятность проявления информационных угроз.

Расширяются масштабы использования криминальными структурами информационных технологий в качестве средств оказания информационно-психологического воздействия для дестабилизации социальной и криминогенной ситуации в регионах.

Использование незаконными организациями механизмов информационного воздействия на сознание в целях усиления межнациональной и социальной напряженности, разжигания религиозной или этнической ненависти, пропаганды идеологии экстремизма.

Заметно увеличивающиеся масштабы компьютерной преступности, особенно в кредитно-финансовой сфере, растущее количество преступлений, связанных с нарушением прав и свобод человека и гражданина при обработке персональных данных с использованием информационных технологий. Применяемые при этом злоумышленниками способы, методы и средства становятся все более изощренными.

Состояние информационной безопасности в области правоохранительной деятельности характеризуется постоянным повышением сложности, увеличением масштабов и скоординированности компьютерных атак на объекты информационной инфраструктуры.

Состояние информационной безопасности в правоохранительной сфере характеризуется недостаточным уровнем использования российских разработок, а также низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности. При этом мероприятия по обеспечению целостности, доступности и устойчивого функционирования информационной инфраструктуры зачастую не имеют комплексной основы.

К наиболее важным объектам обеспечения информационной безопасности в правоохранительной сфере относятся [2]:

– информационные ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;

– информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;

– информационная инфраструктура (информационно-вычислительные сети, пункты управления, узлы и линии связи).

Основываясь на Доктрине информационной безопасности Российской Федерации, можно выделить следующие основные информационные угрозы ИБ в сфере правоохранительной деятельности.

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения информационной безопасности в правоохранительной сфере, являются:

– разведывательная деятельность специальных служб иностранных государств, международных преступных сообществ, организаций и групп;

– деятельность иностранных государственных и частных коммерческих структур.

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются:

– нарушение установленного регламента сбора, обработки, хранения и передачи информации, использующейся для профилактики, раскрытия и расследования преступлений;

– недостаточность законодательного и нормативного регулирования информационного обмена;

– отсутствие единой методологии сбора, обработки и хранения информации;

– отказ технических средств и сбои программного обеспечения;

– преднамеренные действия и ошибки персонала.

В целях локализации и преодоления указанных внешних и внутренних угроз объектам обеспечения информационной безопасности в правоохранительной сфере должны использоваться традиционные методы и средства обеспечения информационной безопасности:

– систематическое выявление угроз и их источников, структурирование целей обеспечения информационной безопасности и определение соответствующих практических задач;

– проведение сертификации общего и специального программного обеспечения, и средств защиты информации в автоматизированных системах управления и системах связи;

– постоянное совершенствование средств защиты информации от НСД, развитие защищенных систем связи и управления, повышение надежности программного обеспечения;

– совершенствование структуры функциональных органов и подразделений системы обеспечения информационной безопасности в сфере правоохранительной деятельности и координация их взаимодействия;

– совершенствование приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы;

– подготовка специалистов в области обеспечения информационной безопасности в сфере обороны.

Наряду с широко применяемыми методами и средствами защиты информации применяются также достаточно специфические методы и средства обеспечения информационной безопасности в правоохранительной сфере, такие как:

– создание защищенной системы интегрированных банков данных процессуального, криминалистического, оперативно-розыскного, справочного, статистического характера;

– повышение уровня профессиональной и специальной подготовки пользователей компьютерных систем.

Выявление и оценка рисков ИБ позволяет свести к минимуму материальные и другие затраты на мероприятия по обеспечению защиты информации. Выявляются и оцениваются актуальные угрозы для активов именно правоохранительных органов, оцениваются риски, возникающие из-за возможного воздействия определенных, иногда весьма специфичных, угроз.

Все методики анализа и оценки рисков позволяют получить лишь качественную их оценку на основе экспертных методов. Для оценки рисков информационной безопасности в правоохранительной сфере может быть использована методика, разработанная на основе ISO TR 13569:2005 [3].

Методика состоит в следующем. Оценка риска проводится с помощью оценки возможности реализации угроз безопасности, связанных с уязвимостями, присущими тем или иным объектам защиты. На основе анализа воздействия угроз, им приписывается высокий, средний или низкий уровень риска по каждой зоне локализации уязвимостей.

Должны оцениваться все угрозы, уязвимости и риски для обеспечения уверенности в том, что процесс оценки рисков в правоохранительном органе является полным.

При проведении оценки рисков рассматриваются три основные категории потерь (финансовая, потеря производительности, затруднение деятельности).

Составляемая матрица оценки рисков разделяется на зоны действия конкретных уязвимостей. В рамках каждой уязвимости перечисляются потенциальные угрозы, для которых приводятся уровни возможных потерь. Матрица оценки рисков заполняется соответствующими уровнями риска – высокого (В), среднего (С) или низкого (Н).

При высоком риске предполагается возможность существенных финансовых потерь, потери работоспособности или затруднения, возникающие, вследствие реализации соответствующей уязвимости.

При среднем уровне риска возможны номинальные финансовые потери, потери работоспособности или некоторые затруднения в деятельности.

При низком уровне риска может возникнуть невысокая вероятность некоторых финансовых потерь, либо потеря работоспособности, либо затруднения в деятельности.

Таким образом, исходя из анализа угроз и оценки рисков, становится ясно основное направление совершенствования обеспечения информационной безопасности в сфере правоохранительной деятельности.

Выполнение приведенных мер является минимальным условием для снижения риска до допустимого уровня.

Список литературы

1. Указ Президента РФ от 05.12.2016 №646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

2. Петров, В.П. Информационная безопасность человека и общества: учебное пособие / В. П. Петров, С. В. Петров. – М.: ЭНАС, 2007. –336 с.

3. ISO TR 13569 Banking and related financial services – Information security guidelines.

Материал поступил в редколлегию 25.03.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 621.394/396.019.3

Добрышин Михаил Михайлович, *к.т.н,*
Реформат Андрей Николаевич
Жук Станислав Иванович
Академия ФСО России
Россия, г. Орёл
zusha@bk.ru

ПРЕДЛОЖЕНИЯ ПО ОЦЕНКЕ ВЕРОЯТНОСТИ ИДЕНТИФИКАЦИИ МОБИЛЬНЫХ УЗЛОВ СВЯЗИ СРЕДСТВАМИ ПОТОКОВОЙ И СЕТЕВОЙ КОМПЬЮТЕРНЫХ РАЗВЕДОК

Представлена модель потоковой и сетевой компьютерных разведок, позволяющая оценить способность злоумышленника идентифицировать искомый узел компьютерной сети.

Перевод практически всех сфер деятельности в информационное пространство позволило на базе арендуемых у провайдеров транспортных сетей связи развертывать и использовать различные частные компьютерные сети. Существующие законы рынка требуют динамичного перемещения части персонала предприятия как внутри страны, так и за ее пределами, что требует и динамического изменения сетей связи.

Данные, публикуемые организациями в сфере информационной безопасности, показывают, что одними из основных угроз информационной безопасности являются различные виды компьютерных разведок (КР) [1]. Средства защиты информационной безопасности, установленные на средствах связи абонентов, находящихся вне контролируемой зоны (мобильные узлы связи), менее эффективны, чем аналогичные средства стационарных узлов. Проводя компьютерные атаки на мобильные узлы связи (МУС), злоумышленник способен получать искомую информацию при меньших затратах.

Анализируя тактику действий злоумышленников, можно сделать вывод о том, что проведению компьютерных атак предшествует проведение разведки, направленной на идентификацию атакуемого МУС, определению его основных характеристик и выявлению уязвимостей. Исходя из данной стратегии, злоумышленник должен на основании множества информационных потоков идентифицировать искомый, далее определить электронный адрес, после чего осуществить сканирование сетевого оборудования с целью определения параметров атакуемого МУС [2]. В связи с этим определение способности злоумышленника эффективно провести КР позволяет определить степень защищенности МУС и определить требуемую стратегию защиты[3].

Для решения данной задачи разработана модель, позволяющая определить вероятность идентификации узла связи средствами потоковой и сетевой КР, имеющихся у злоумышленника.

Сущность моделирования заключается в передаче информации между узлами связи, с учетом переключения информационных потоков между несколькими арендуемыми информационными потоками; имитации переключения между информационными потоками и наблюдении демаскирующих признаков средствами потоковой КР с целью идентификации информационного потока; имитации сканирования сетевого оборудования и выявлении заданных уязвимостей средствами сетевой КР.

Целью моделирования является получение зависимости вероятности идентификации (вскрытия) МУС средствами потоковой и сетевой КР от количества информационных потоков, по которым передается информация, длительности использования каждого из каналов связи, времени выявления демаскирующих признаков, а так же времени сканирования сетевого оборудования узла связи.

Выходным результатом являются зависимость вероятности идентификации МУС ($P_{\text{идент}}(t_{\text{ф}}) = f(R_{\text{есэ}}; t_{\text{ф}i}; R_{\text{ПиС КР}})$ от параметров сегмента RuNet ($R_{\text{есэ}}$), времени использования $i-$го канала связи ($t_{\text{ф}i}$), а так же характеристик средств потоковой и сетевой КР ($R_{\text{ПиС КР}}$).

Основными исходными данными модели являются: время функционирования МУС ($t_{\text{ф}}$); время использования $i-$го канала связи ($t_{\text{ф}i}$) МУС; количество независимых каналов связи в сегменте RuNet ($N_{\text{кан}}$); количество используемых независимых каналов связи в сегменте RuNet ($N^{*}_{\text{кан}}$); количество средств потоковой КР, используемых злоумышленником для ведения потоковой КР ($N_{\text{ПКР}}$); среднее время анализа информационного потока средствами потоковой КР $i-$го канала связи ($t_{\text{идент}}$); объем информации, передаваемый по $i-$го канала связи ($V_{\text{ИП}i}$) за время наблюдения злоумышленником $i-$го канала связи; быстродействие $j-$го средства потоковой КР ($B_j^{\text{пкр}}$); количество параметров анализируемых средством сетевой КР ($N_{\text{парам}}$); быстродействие $j-$го средства сетевой КР ($B_j^{\text{скр}}$).

Основными допущениями считается, что в районе функционирования защищаемого узла функционируют сторонние узлы; ресурс сил и средств потоковой КР конечен и требует конечного времени; злоумышленнику не известен электронный адрес атакуемого узла.

К основным ограничениям относится время идентификации МУС другими видами разведки многим больше, чем аналогичное время средствами сетевой и потоковой КР.

Представляемая модель реализована в имитационной среде моделирования GPSS World и заключается в поэтапном моделировании идентификации МУС средствами потоковой и сетевой КР.

Первый этап моделирования (рис. 1) заключается в имитации отправки МУС (блок 1.1) пакетов по одному из каналов связи. Одновременно осуществляется имитация ведения потоковой КР (отправка пакетов по одному из каналов связи) (блок 1.2). Время имитации отправки узлом пакетов и имитации ра-

боты потоковой КР задается. Переключение между каналами связи осуществляют коммутаторы (блоки 2.1, 2.2) на основании случайного выбора с равномерным распределением.

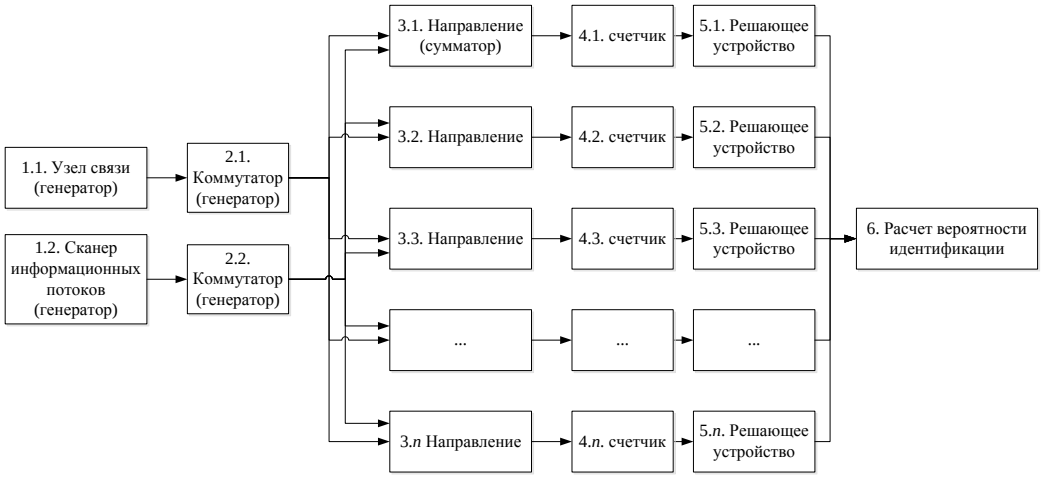


Рис. 1. Схема имитационной модели мобильного узла связи как объекта потоковой компьютерной разведки

В блоках 3.1-3.*n* при одновременном поступлении пакетов от МУС и средства потоковой КР на выходе формируется логическая «1», если на один из входов не поступает сообщение, то присваивается логический «0». На рисунке 2 показано визуальное представление имитируемого процесса. В качестве исходных данных $t_{\text{ф}i} = 10$ (тактов), $t_{\text{пкр}i} = 5$.

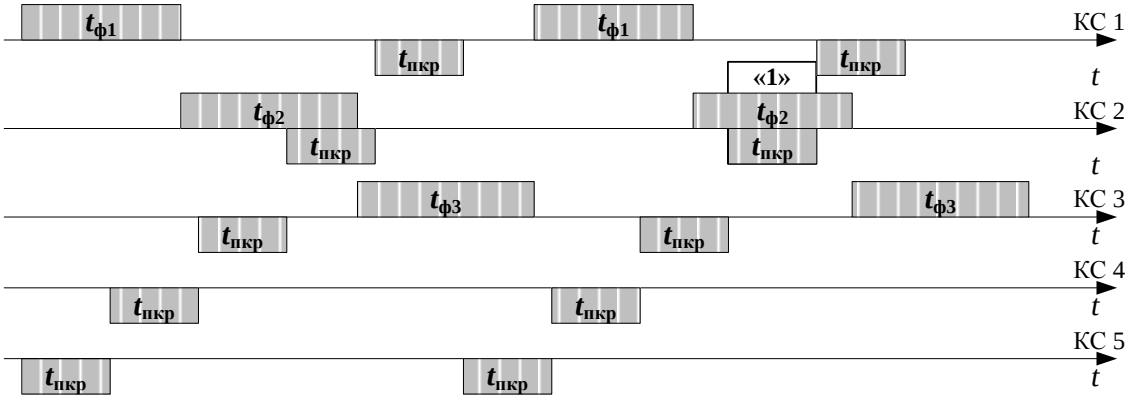


Рис. 2. Визуальное представление имитации процесса идентификации информационного потока защищаемого узла средствами потоковой компьютерной разведки

В блоках 4.1-4.*n* подсчитываются поступившие «1», если на вход поступил логический «0», то счетчик обнуляется.

В блоках 5.1-5.n осуществляется принятие решения об идентификации информационного потока защищаемого узла. Если количество логических единиц

соответствует заданному значению, то считается, что информационный поток идентифицирован и в блоке 6 рассчитывается вероятность идентификации информационного потока защищаемого узла.

Далее осуществляется имитация процессов сканирования сетевого оборудования и определяется своевременность и вероятность выявления уязвимости узла в течение заданного времени. Результаты моделирования представлены на рисунках 3, 4.

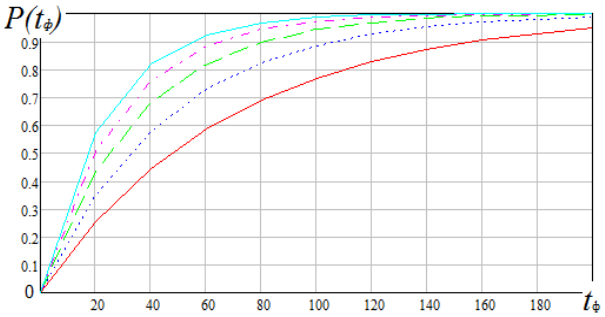


Рис. 3. Зависимость вероятности идентификации МУС средствами потоковой и сетевой КР при различных длительностях использования канала связи

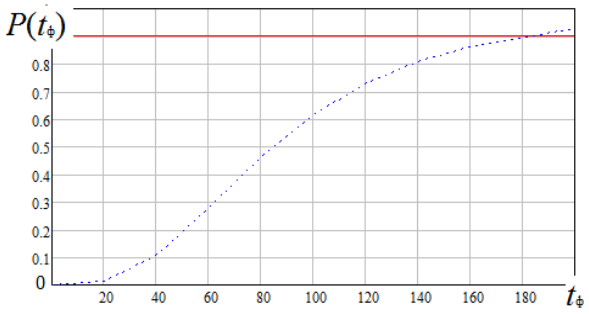


Рис. 4. Зависимость вероятности идентификации МУС средствами потоковой и сетевой КР при переключении информационных потоков между несколькими (5) каналами связи

Из анализа полученных результатов очевидно, что переключение информационных потоков между несколькими каналами связи существенно увеличивает время идентификации защищаемого узла.

Аппроксимация результатов имитационного моделирования выявила зависимость вероятности идентификации ($P_{\text{иденті}}(t_{\text{ф}})$) МУС средствами потоковой и сетевой КР от параметров, указанных в цели разработки модели:

$$P_{\text{иденті}}(t_{\text{ф}}) = 1 - e^{-\frac{K_1 \cdot K_2 \cdot t_{\text{ф}i}}{\overline{T}_{\text{идент}}}}, \quad (1)$$

$$K_1 = \frac{N_i^* \cdot N_{\text{пкр}}}{N_{\text{кан}}}, \quad (2)$$

$$K_2 = \frac{t_{\text{ф}}^2 - (t_{\text{ф}} - t_{\text{ф}i})(t_{\text{ф}} - t_{\text{идент}})}{t_{\text{ф}}^2}, \quad (3)$$

$$\overline{T}_{\text{идент}} = \frac{V_{ИП}}{B_{\text{пкр}\,j}} + \frac{N_{\text{парам}}}{B_{\text{скр}\,j}} + t_{\text{идент}}, \quad (4)$$

$$P_{\text{идент}} = \prod_{i}^{g} P_{\text{идент}i} \,. \qquad (5)$$

Полученная аналитическая модель реализована в виде программы для ЭВМ зарегистрированной в Роспатенте. Внешний вид программы представлен на рисунке 5.

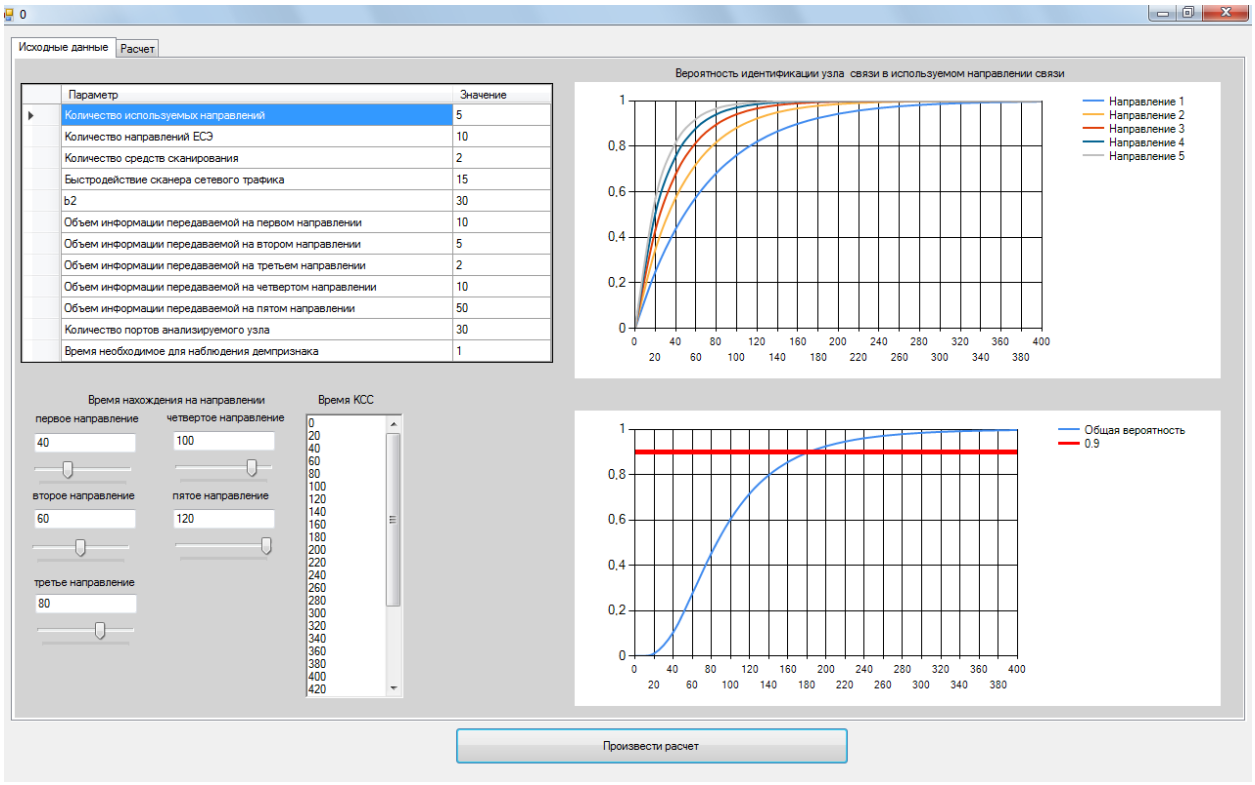


Рис. 5. Внешний вид программы для ЭВМ по расчету вероятности идентификации мобильных узлов связи средствами потоковой и сетевой компьютерных разведок

Научная новизна разработанной модели заключается в учете динамики переключения информационных потоков между несколькими каналами связи, а так же ряд параметров средств сетевой и потоковой компьютерных разведок. Разработанная модель предназначена для научно-исследовательских организаций с целью обоснования и разработки руководящих документов, регламентирующих порядок планирования, развертывания и функционирования МУС интегрированных с ЕСЭ в условиях ведения злоумышленником потоковой и сетевой компьютерной разведки.

Оценка результатов разработанной модели и аналогов [2, 4] показывают выигрыш в 12-15 % достоверности результатов оценки способности злоумышленника идентифицировать узел связи.

Список литературы

1. Кибербезопасность – 2018-2019: итоги и прогнозы / Positive technologies. – 2018. – 14 с.

2. Добрышин, М.М. Модель узла доступа VPN как объекта сетевой и потоковой компьютерных разведок и DDoS-атак / М.М. Добрышин, Е.В. Гречишников, П.В. Закалкин // Вопросы кибербезопасности. – 2016. – № 3 (16). – С. 4-12.

3. Добрышин, М.М. Комплексный алгоритм мониторинга защищенности узлов VPN от компьютерной разведки и DDoS-атак / М.М. Добрышин, А.Н. Реформат, П.В. Закалкин // Научный журнал: Электросвязь-№ 7. – 2018. – № 7. – С. 44-50.

4. Добрышин, М.М., Кузьмич А.А., Макаров В.Н. Расчет возможностей средств сетевой и потоковой компьютерных разведок по вскрытию виртуальной части сети связи. Свидетельство о государственной регистрации программы для ЭВМ № 2016618853 от 09.08.2016 г.

Материал поступил в редколлегию 25.03.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.05

д-р. техн. наук В.Т. Еременко, Ю.С. Скуридина, А.Ю. Ветрова
ОГУ «Орловский государственный университет имени И.С. Тургенева»
Россия, г. Орел
wladimir@orel.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕХНОЛОГИЙ ВИРТУАЛИЗАЦИИ И ВИРТУАЛЬНЫХ КОММУНИКАЦИОННЫХ СРЕД

В статье рассмотрена информационная безопасность технологий виртуализации и виртуальных коммуникационных сред.

Технологии виртуализации имеют намного больше достоинств, по сравнению с классическими сетевыми технологиями. Это значит – удобное управление виртуальной инфо-коммуникационной средой, создание новых серверов с высокой скоростью, своевременное резервное копирование, отсутствие связи с какой-либо реальной машиной, вероятность проверки нового функционала и обновлений на современных дубликатах продуктивных коммуникационных систем, защита реальной машины от нападений, которым подвергается виртуальная коммуникационная среда.

По статистике «Лаборатории Касперского» у 59 % опрошенных компаний в России, которые имеют у себя в локальной сети более 100 компьютеров, уже внедрены или планируются ввести виртуальные сети [1]. Анализ основных аспектов создания и применения виртуальной среды показал, что основным препятствием для широкого внедрения виртуальной среды являются вопросы обеспечения информационной безопасности.

Ведь сейчас всё чаще злоумышленники проявляют интерес к виртуальной среде и отыскания в ней ошибок, недочётов и уязвимостей, что даёт возможность разрушения кода. Таким образом, как за рубежом, так и в России виртуальная сеть нуждается в обеспечении информационной безопасности.

В настоящее время виртуализация нашла применение в следующих системах (сетях) [2]: системах хранения данных; системах памяти; системах обработки данных; вычислительных сетях; вычислительных системах; программного обеспечения.

Технологии виртуализации создают объекты доступа, которые должны быть защищены, как и другие системы, а так же и аппаратные средства инфокоммуникационных систем, которые используют для осуществления виртуальных технологий.

С помощью технологий виртуализации создаются следующие объекты, подлежащие защите [3]:

– *средства создания и управления виртуальной инфраструктурой* (Гипервизор I типа, гипервизор II типа, консоль управления виртуальной инфраструктурой и гипервизор системы хранения данных)

– *виртуальные каналы передачи данных*;

– *виртуальные системы хранения данных*;

– *виртуальные вычислительные системы* (виртуальные машины (ВМ), виртуальные сервера и др.);

– *центральные процессоры и их ядра, адресное пространство памяти, сетевые интерфейсы, порты подключения внешних устройств*, задействованные при реализации технологий виртуализации (периметр виртуальной инфраструктуры).

– *отдельные виртуальные устройства обработки, хранения и передачи данных* (виртуальные процессоры, виртуальные диски, виртуальную память, виртуальное активное и пассивное сетевое оборудование и др.);

– *средства защиты информации*, которые предназначены *для использования в среде виртуализации*, а также виртуальные средства информационной безопасности (ИБ).

Технологии виртуализации на сегодняшний день внедрены большим количеством компаний, однако им требуется контроль текущего состояния виртуальных инфраструктур и процессов обеспечения их ИБ.

Особенности обработки информации в виртуальной среде. Вопрос в том, чем же отличается обычный компьютер от сервера виртуализации и почему он активнее в плане обеспечения безопасности информации в коммуникационной среде. Рассмотрим рисунок (рис.1)

Рис.1. Сервер виртуализации и обычный компьютер

Обычный компьютер состоит из аппаратной платформы, ядра операционной системы и приложений, которые и препятствуют вредоносным программам совершать захват, скачивание и модификацию информации. В состав сервера виртуализации также входит аппаратная платформа. С другой стороны сервер включает ещё гипервизор и подсистему управления виртуальной инфраструк-

турой. Благодаря гипервизору осуществляется управление ресурсами и их разделение между различными операционными системами, выполняется изоляция запущенных операционных систем друг от друга, а также может обеспечиваться их взаимодействие (обмен файлами, сетевое взаимодействие и т.д.)

Во время внедрения виртуальных систем компания меняет очень многое. *Во-первых, изменяется технология хранения данных в виртуальных машинах*. Если раньше каждая прикладная система имела доступ к своему разделу в СХД (система хранения данных) или использовала локальное хранилище, то после внедрения виртуализации сразу несколько виртуальных машин находятся в одном разделе для обеспечения "горячей" миграции и отказоустойчивости.

Во-вторых, изменения происходят в сетевом взаимодействии систем. Создаются дополнительные угрозы за счет нахождения на одном сервере нескольких виртуальных машин. Это приводит к тому, что между ними внутри хоста существуют внутренние соединения на базе виртуальных коммутаторов, у которых есть различные режимы работы (например, режим, в котором все пакеты рассылаются на все порты этого коммутатора).

В-третьих, в виртуальных средах чаще всего применяется подход к резервированию систем на уровне виртуальных машин. Это позволяет создавать не отдельную файловую гостевую операционную систему, а резервные копии ВМ целиком.

Рассмотрим терминологию, предложенную в [4].

Виртуализация – это группа технологий, основанных на преобразовании формата или параметров программных или сетевых запросов к компьютерным ресурсам с целью обеспечения независимости процессов обработки информации от программной или аппаратной платформы информационной системы.

Виртуальная машина (ВМ) – это виртуальная вычислительная система, которая состоит из виртуальных устройств обработки, хранения и передачи данных и которая дополнительно может содержать программное обеспечение и пользовательские данные.

Гипервизор [вычислительных систем] (монитор виртуальных машин) – программа, создающая среду функционирования других программ (в том числе других гипервизоров) за счет имитации аппаратных средств вычислительной техники, управления данными средствами и гостевыми операционными системами, функционирующими в данной среде.

Виртуальная инфраструктура – композиция иерархически взаимосвязанных групп виртуальных устройств обработки, хранения и/или передачи данных, а также группы необходимых для их работы аппаратных и/или программных средств.

Средства управления виртуальной инфраструктурой – это композиция группы необходимых для их работы аппаратных и/или программных средств, также иерархически взаимосвязанных групп виртуальных устройств обработки, хранения и/или передачи данных.

Формулировка представленных выше определений позволяет систематизировать знания в предметной области, выявить уязвимости, позволяющие

изменить функционирование виртуальной инфраструктуры и процессов обработки информации в системе информационной безопасности (СИБ).

Самым опасным компонентом виртуальной инфраструктуры является сервер управления. Злоумышленник, получивший контроль над средствами управления, получает полный доступ ко всем серверам виртуализации, виртуальным машинам, хранилищам данных и сетям хостов. Поэтому необходимо как тщательно защищать сам сервер управления, и использовать средства управления доступом, идентификации и аутентификации. Это позволяет утверждать, что для решения обозначенных задач необходимо использовать специализированное ПО, разработанное специально для виртуальных инфраструктур. Целесообразно проверка его конформности (на соответствие) требованиям ФСТЭК. В виртуальной инфраструктуре доступ администраторов систем (сетей) может быть ограничен по IP-адресам. Однако, доступ к серверу виртуализации должен осуществляться по разработанному безопасному протоколу со специфицированными функциями информационной безопасности.

Необходимо отметить, что использование средств для автоматизации развертывания виртуальных машин имеет целый ряд нюансов. С одной стороны, применение шаблонов вычислительных машин помогает обеспечивать поддержку заданного уровня безопасности внутри лишь одного шаблона и развертывать новые виртуальные системы на его основе с гарантированным уровнем обновлений и требуемой конфигурацией. С другой стороны, вредоносное ПО, внедренное злоумышленником в шаблон, может начать своё распространение самостоятельно. Особенно это касается технологии виртуальных ПК (Virtual Desktop Infrastructure – (VDI)), где новые системы очень часто создаются из одного базового образа. Поэтому в виртуальных средах нужно уделять особое внимание антивирусной защите гостевых операционных систем.

На сегодняшний день разработаны специализированные системы защиты инфраструктуры для конкретной виртуальной сети, которые можно разделить на следующие классы: ***программные продукты для предотвращения вторжений и анализа трафика (***vShield Zones от VMware, VMC от компании Reflex, несколько решений от Trend Micro); ***ПО для разграничения прав доступа в виртуальной инфраструктуре*** (HyTrust от одноименной компании, vGate от российского предприятия "Код Безопасности"); ***продукты для проведения проверки виртуальной среды на наличие тех или иных ошибок в конфигурации безопасности*** (vWire, VMinformer от одноименной компании, ESX Compliance Checker от EMC) [5].

Все эти продукты позволяют повысить безопасность виртуальных инфраструктур, однако ни один из них не обеспечивает полной защиты виртуальной среды. Поэтому государственными регуляторами необходимо разработать и стандартизовать подход к обеспечению информационной безопасности в виде регламентов и стандартов, обязательно учитывая рекомендации производителя платформы виртуализации. Например, такие есть у VMware

под названием Security Hardening Guide, ведь именно технологические особенности платформы определяют необходимые меры по обеспечению безопасности.

Защита средств создания и управления виртуальной инфраструктурой. Несмотря на то, что производители платформ виртуализации заявляют о высоком уровне безопасности, а их продукты имеют ИБ-сертификаты международных компаний, виртуальная инфраструктура требует особого подхода к защите ее компонентов. Для защиты операционной системы и приложений используется классический подход (антивирусы, сетевые экраны и прочее), Однако для гипервизора, виртуальной машины и средств управления виртуализацией требуется стандартизация способов и приемов по обеспечению информационной безопасности.

Организационно-управленческие решения по обеспечению информационной безопасности должны обеспечить регламентирование функций, а с технической – разработать конфигурацию виртуальной инфраструктуры с использованием, в том числе, специализированных средств ИБ и поддержки ее в актуальном состоянии. Необходимо отметить, что с помощью интеллектуальных агентов требуется проведение регулярных проверок инфраструктуры в виртуальной сети на соответствие требованиям регуляторов и корпоративным стандартам ИБ.

Особенности обеспечения безопасности в виртуальной коммуникационной среде. Комплексные задачи, которые решает информационная безопасность в коммуникационной среде – это целостность и доступность информации, обеспечение конфиденциальности, обеспечение требованиям государственных регуляторов.

При обработке информации в виртуальной коммуникационной среде имеются свои особенности, которые отсутствуют в физической среде. Именно их и используют злоумышленники в качестве совершения атак [6]:

– ***средства управления виртуальной инфраструктурой*** представляют собой самостоятельный объект атаки, проникновение в который дает возможность злоумышленнику получить доступ к гипервизорам серверов виртуализации, а затем к конфиденциальным данным, обрабатываемым на гостевых машинах;

– ***каналы передачи служебных данных серверов виртуализации*** обычно не защищены, хотя по этим каналам среди прочих данных передаются фрагменты оперативной памяти гостевых машин, которые могут содержать конфиденциальные данные.

– ***средства информационной безопасности***, разработанные для защиты физической инфраструктуры, могут не учитывать существование гипервизора;

– ***диски гостевых машин обычно размещаются в сетевых хранилищах***, которые должны физически защищаться, как самостоятельные устройства;

– ***традиционные сетевые экраны могут не контролировать трафик внутри сервера виртуализации,*** где находятся гостевые машины, взаимодействующие между собой по сети;

Повышение уровня защищенности виртуальной среды необходимо осуществлять комплексно, комбинируя сетевые и локальные средства защиты *с одновременным использованием большого набора функций информационной безопасности:* сетевой идентификации и аутентификации пользователей; межсетевого экранирования, как внутри сервера виртуализации, так и по периметру виртуальной инфраструктуры; регистрации, сбора и анализа событий безопасности; разграничения доступа к виртуальным машинам и к самому серверу виртуализации (и его гипервизору); контроля целостности конфигураций распределенных компонентов виртуальной среды; антивирусной защиты и управления доступом к элементам виртуальной инфраструктуры.

Угрозы системному программному обеспечению виртуальной коммуникационной среде представлены на рис.2.

Специфические угрозы программному обеспечению в технологии виртуализации:

1. ***Ошибки в работе программного обеспечения гипервизора.*** В данном случае можно наблюдать несанкционированный доступ к ресурсам виртуальных машин вследствие программных закладок (или ошибок) в программном обеспечении гипервизора.

2. ***Некорректная настройка параметров гипервизора и виртуальных машин.*** При создании данной угрозы происходит несанкционированный доступ к ресурсам виртуальных сред вследствие некорректных настроек гипервизора.

3. ***Истощение вычислительных ресурсов сервера с гипервизором***. Данная угроза очень ярко выражена в выполнении атак типа «отказ в обслуживании»

Рис. 2. Новые и старые угрозы программному обеспечению в виртуальной коммуникационной среде

4. ***Подмена исполняемых модулей программного обеспечения гипервизора***. В данном случае может произойти несанкционированный доступ к ресурсам виртуальных машин вследствие искажения работы программного обеспечения гипервизора.

5. ***Некорректное функционирование средств получения контроля над компьютером*** **(**Руткиты (Blue Pill и SubVirt). Представляет собой возможность получения контроля за счет специфики технологии виртуализации и связано с уязвимостями систему Windows Vista (рис.3).

6. ***Случайное (умышленное) искажение (уничтожение) образов виртуальных машин.*** Вследствие данной угрозы происходит стирание или искажение образов виртуальной машины.

Способы и приемы обеспечения информационной безопасности в виртуальных средах:

– обеспечение возможности ***наследования*** установленных на уровне управления прав ***доступа субъектов*** к объектам доступа на уровне виртуализации и оборудования;

– ***автоматическое восстановление всех функций ИБ,*** входящих в состав виртуальной среды;

– ***защита от НСД к вводимой*** субъектами доступа, входящими в состав виртуальной инфраструктуры, ***идентификационной и аутентификационной информации***;

– ***защита от НСД к хранящейся*** в компонентах виртуальной инфраструктуры идентификационной и аутентификационной информации о субъектах доступа;

– ***обеспечение доверенных канала, маршрута внутри виртуальной инфраструктуры*** между администратором, пользователем и средствами ЗИ (функциями безопасности средств ИБ).

– *идентификация и аутентификация субъектов доступа при их локальном или удаленном обращении* к объектам виртуальной инфраструктуры.

Заключение. Существующие системы защиты инфраструктуры можно разделить на несколько групп. Программные продукты для анализа трафика и предотвращения вторжений, разработанные специально для виртуальной среды (vShield Zones от VMware, VMC от компании Reflex, несколько решений от Trend Micro). ПО для разграничения прав доступа в виртуальной инфраструктуре (HyTrust от одноименной компании, vGate от российского предприятия "Код Безопасности"). Программные продукты для проведения аудита виртуальной среды на предмет наличия ошибок в конфигурации безопасности (решения vWire, VMinformer от одноименной компании, ESX Compliance Checker от EMC и т.п.).

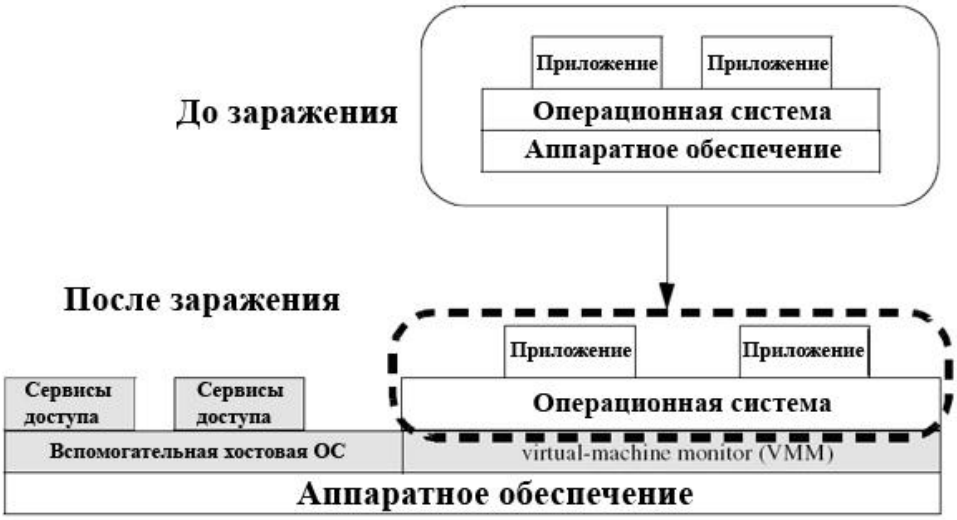


Рис. 3. Механизм работы средства получения контроля над компьютером

Все эти продукты позволяют повысить безопасность виртуальных инфраструктур, однако ни один из них не обеспечивает полной защиты виртуальной среды. Поэтому в компании необходимо выработать и стандартизовать подход к обеспечению ИБ в виде регламентов и стандартов, обязательно учитывая рекомендации производителя платформы виртуализации (такие есть, например, у VMware под названием Security Hardening Guide). Ведь именно технологические особенности платформы определяют необходимые меры по обеспечению безопасности.

Использование средств для автоматизации развертывания виртуальных машин имеет целый ряд нюансов. С одной стороны, применение шаблонов вычислительных машин помогает обеспечивать поддержку заданного уровня безопасности внутри лишь одного шаблона и развертывать новые виртуальные системы на его основе с гарантированным уровнем обновлений и требуемой конфигурацией. С другой стороны, вредоносное ПО, внедренное злоумышленником в шаблон, может начать своё распространение самостоятельно. Особенно это касается технологии виртуальных ПК (Virtual Desktop Infrastructure – (VDI)), где новые системы очень часто создаются из одного базового образа. Поэтому в виртуальных средах нужно уделять особое внимание антивирусной защите гостевых операционных систем.

Список литературы

1. Ледовской, В. П. Виртуальным инфраструктурам – прогрессивная защита [Электронный ресурс]. – Режим доступа: http://www.anti-malware.ru/analytics/Progressive_Defense_for_Virtual_Infrastructures

2. Securing Virtual Applications and Servers [Электронный ресурс]. – Режим доступа: http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/unified-network-services-uns/ white_paper_c11–652663.html

3. Зверев, Г. И. Угрозы и методы обеспечения информационной безопасности виртуальных сред // Молодой ученый. – 2015. – №9. – С. 235-237. – https://moluch.ru/archive/89/17833/

4. Петрухин, В. Безопасность виртуальных сред [Электронный ресурс] — Режим доступа: http://www.osp.ru/os/2011/04/13008785

5. ГОСТ Р 56938-2016 Защита информации. Защита информации при использовании технологий виртуализации. Общие положения [Электронный ресурс] — Режим доступа: http://docs.cntd.ru/document/1200135524

6. Михайлова Анна, Как работает концепция виртуализации сетевых функций (NFV, Network Functions Virtualization) [Электронный ресурс] — Режим доступа: https://www.anti-malware.ru/analytics/Technology_Analysis/network-functions-virtualization

7. VMware vSphere 4.1 Security Hardening Guide [Электронный ресурс] — Режим доступа: https://communities.vmware.com/docs/DOC-15413

Материал поступил в редколлегию 25.03.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.7

Р.Ю. Калашников
Научный руководитель: к.т.н., доц. М.Ю. Рытов
ФГБОУ ВО «Брянский государственный технический университет»
Россия, г. Брянск

МЕТОДИКА ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВНЕШНИХ ПРОГРАММНЫХ ИНТЕРФЕЙСОВ КОНТРОЛЛЕРОВ SDN

Предложена методика оценки и управления рисками программно-определяемых сетей. Предложенная методика способна оценивать риск, связанный с запросами от сервисов, полученными через северный интерфейс контроллера SDN.

В основе концепции программно-определяемых сетей (SDN) лежит отделение плоскости управления от плоскости данных. Плоскость управления представлена логически централизованным контроллером, а плоскость данных состоит из коммутаторов SDN, которые, в отличие от классических коммутаторов, занимаются только пересылкой пакетов, не принимая решения о их направлении. Такой подход обеспечивает возможность внедрения глобальных политик маршрутизации, без необходимости настройки каждого устройства в отдельности.

Интерфейс, обеспечивающий возможность взаимодействия контроллера с внешними приложениями, в терминологии SDN называется северным интерфейсом. Он предоставляет широкие возможности для автоматизации и гибкого управления сетью. Так, например, при помощи северного интерфейса, сервисы могут информировать контроллер об ожидаемых изменениях объемов входящего трафика. Однако такие изменения могут и не произойти, даже если SDN выделит ресурсы для клиентов и потоков трафика. Подобные излишние перестроения виртуальной топологии сети негативно влияют на её производительность – резервирование невостребованных ресурсов ухудшает параметры обслуживания (такие как задержка, полоса пропускания) для других узлов сети. Следовательно, важно выработать критичный подход к оценке информации, предоставляемой сервисами контроллеру SDN.

Существующие методики оценки риска неприменимы к программно-определяемым сетям, поскольку они ориентированы только на традиционные сети и не учитывают динамический характер SDN. Исходя из этого, целесообразна разработка эффективного механизма оценки безопасности SDN с учетом их отличительных особенностей. Для принятия решений в отношении запросов, поступающих контроллеру от внешних сервисов, в данной статье предложен подход к оценке и управлению рисками.

В контексте информации, поступающей от приложений через внешний интерфейс, можно определить два фактора, которые определяют риск входящего запроса: негативное воздействие на сеть и вероятность реализации угрозы.

Негативное воздействие – фактор, связанный с перестроениями сети SDN и её финальной топологией. Когда сервис запрашивает новые параметры полосы пропускания, происходит изменение виртуальной топологии сети. Результатом обработки такого запроса может быть выделение значительных ресурсов и необходимость перестроения сети. Как следствие, качество обслуживания для других клиентов может быть ухудшено. Следовательно, фактор воздействия связан с глобальным статусом всей сети SDN, а его количественная оценка - с критериями оптимизации сети, т.е. с использованием ресурсов контроллера, полосы пропускания и задержками.

Инструменты оптимизации сети способны определять оптимальную виртуальную топологию для потока данных при заданных условиях. Если сервис сообщает, что объем трафика между определенной парой узлов изменится определенным образом, инструмент оптимизации предложит оптимальную виртуальную топологию для новых условий. Полученное значение целевой функции характеризует конечное состояние сети (при заданных условиях). Эта величина позволяет определить количественный подход к оценке фактора негативного воздействия. Однако в действительности трафик между данной парой узлов может не измениться, несмотря на предварительный запрос от сервиса и пересчет топологии сети.

Если предположить, что сервис может верно спрогнозировать изменение объемов трафика, либо наоборот, сделать это совершенно неверно, возможно рассмотреть четыре различных сценария, схематично представленные на рис. 1.

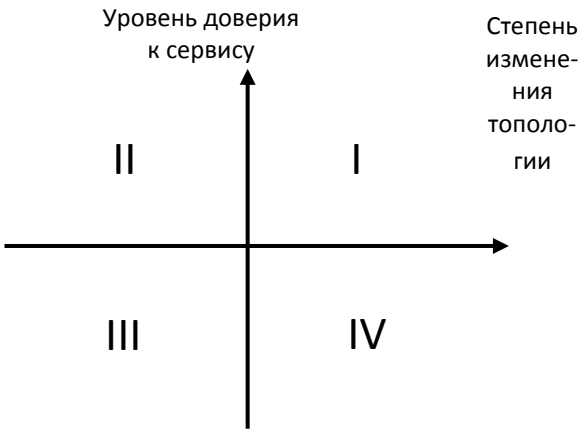


Рис. 1. Сценарии корректных и некорректных прогнозов объема трафика

I. Топология виртуальной сети изменилась, и требуемая полоса пропускания изменилась в соответствии с запросом. Объем входящего трафика изменился в соответствии с прогнозом, поэтому доверие к сервису должно возрасти.

II. Топология виртуальной сети не изменилась, а поток трафика изменился в соответствии с прогнозом сервиса. В этом случае топология сети не является

оптимальной (условия были изменены), но доверие к сервису должно возрасти, потому что объем трафика изменился, как предполагалось.

III. Топология виртуальной сети не изменилась несмотря на то, что внешнее приложение запросило это изменение. Это происходит в том случае, когда существующая топология по-прежнему оптимальна для запрошенных изменений. В данном сценарии доверие к сервису будет снижено, если последующие изменения объемов трафика не будут соответствовать прогнозу.

IV. Топология виртуальной сети изменилась, но объем входящего трафика не изменился, несмотря на соответствующий запрос. Действия сервиса привели к необоснованному перестроению, поэтому доверие к нему должно снизиться.

Рассмотренные сценарии предполагают, что сервис правильно или совершенно неверно прогнозировал изменение трафика. Однако возможны и промежуточные состояния: поток трафика может измениться, но в меньшей степени, чем спрогнозировал сервис. Следовательно, необходимо также рассмотреть оптимальные виртуальные топологии для незначительных изменений потока данных, для того чтобы предоставить оптимальные условия в соответствии с запросом внешнего приложения. Точная оценка требует определения промежуточных состояний для полученного запроса. Для этого необходимо определить матрицу *I*, содержащую состояния сети для различных сценариев:

$$I = \begin{bmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_m \\ \beta_1 & \beta_2 & \cdots & \beta_m \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1 & \omega_2 & \cdots & \omega_m \end{bmatrix} \qquad 1)$$

где *α, β, ... ω* означают разные виртуальные топологии, а m — это число промежуточных состояний. Таким образом, каждая строка представляет собой строго определенную виртуальную топологию (оптимизированную для конкретного объема входящего трафика), а каждый столбец – объем прогнозируемого входящего трафика. В результате каждый элемент в матрице содержит числовое значение, характеризующее требования для полосы пропускания и сетевую топологию.

Вероятность реализации угрозы связана с сервисом, который отправляет запрос, а следовательно зависит от уровня доверия к нему. Как меру количественной оценки доверия к сервису предложено использовать систему репутации, которая устанавливает степень доверенности каждого зарегистрированного сервиса.

Репутация сервиса формируется по мере получения запросов от него, и должна позволять классифицировать приложения не только как доверенные и недоверенные, но и как частично доверенные. Следовательно, репутацию каждого объекта можно обозначить числом в диапазоне [0,1]. Значение 1 обозначает полностью надежный сервис, а значение 0 - совершенно ненадежный сервис. Новому объекту будет присвоено начальное значение (например, 0,5), но оно будет динамически меняться в зависимости от поведения объекта. Система репутации должна принимать в качестве входных данных запросы, значимые для

сетей SDN: предоставление достоверных и полезных сообщений повысит уровень репутации, если информация об изменении трафика неверна – репутация снизится.

Матрица I (1) содержит состояния сети для сценариев с различными требованиями полосы пропускания между рассматриваемой парой узлов. Поэтому также необходимо определить матрицу L, содержащую уровень доверия для каждого запроса, содержащего прогноз об изменении объемов трафика:

$$L = \begin{bmatrix} l_1 & l_2 & \dots & l_m \\ l_1 & l_2 & \cdots & l_m \\ \vdots & \vdots & \ddots & \vdots \\ l_1 & l_2 & \cdots & l_m \end{bmatrix} \qquad 2)$$

где m – показатель степени изменения объемов трафика между заданной парой узлов. Эта матрица специфична для сервиса, который отправляет запросы через северный интерфейс контроллера, и значения в ней напрямую связаны с уровнем доверия к ним, а также с распределением вероятностей, которое характеризует способность сервиса прогнозировать объем входящего трафика.

Уровень риска может быть определен как произведение двух факторов: негативного воздействия и вероятности реализации. Предложенная методика предполагает, что негативное воздействие связано с изменением состояния сети, которое происходит в результате запрошенной полосы пропускания и вероятности, которая связана с уровнем доверия к отправителю запроса.

Номера строк в матрицах I и L идентичны и обозначают количество рассматриваемых виртуальных топологий. Таким образом, принимая во внимание одинаковые размеры матриц I и L, можно определить матрицу оценки риска R как произведение матрицы I, представляющей фактор негативного воздействия, и матрицы L, представляющей фактор вероятности реализации угрозы:

$$R = I \times L = \begin{bmatrix} \alpha_1 \times l_1 & \alpha_2 \times l_2 & \dots & \alpha_m \times l_m \\ \beta_1 \times l_1 & \beta_2 \times l_2 & \cdots & \beta_m \times l_m \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1 \times l_1 & \omega_2 \times l_2 & \cdots & \omega_m \times l_m \end{bmatrix} = \begin{bmatrix} r_{1,\alpha} & r_{2,\alpha} & \dots & r_{m,\alpha} \\ r_{1,\beta} & r_{2,\beta} & \cdots & r_{m,\beta} \\ \vdots & \vdots & \ddots & \vdots \\ r_{1,\omega} & r_{2,\omega} & \cdots & r_{m,\omega} \end{bmatrix} \qquad 3)$$

Матрица R определяет значение риска для каждого рассматриваемого изменения трафика во всех прогнозируемых виртуальных топологиях. Поэтому необходимо суммировать риски для каждой топологии:

$$R_j = \sum_{i=1}^{m} R_{i,j} \;\; j = \alpha, \beta, \dots, \omega \qquad 4)$$

Предложенный подход позволяет найти сценарий с наименьшим уровнем риска. Такие расчеты могут быть выполнены для исходной топологии (неизменной сети) и для прогнозируемых структур, в том числе промежуточных. Результаты покажут, какая структура сети является наиболее безопасной, то есть,

где уровень риска минимален. Используя предложенную методику, сеть SDN способна принять наилучшее решение относительно запросов, полученных от северного интерфейса контроллера.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

Козачок Александр Иванович, *к.п.н., доцент, сотрудник*
Копылов Сергей Александрович, *сотрудник*
Приставка Анастасия Сергеевна, *сотрудник*
Академия ФСО России**,** Орёл, Россия
e-mail: kaiakadem@mail.ru

ПРИНЦИП РАБОТЫ МОДУЛЯ ЗАЩИТЫ ТЕКСТОВЫХ ДАННЫХ ОТ УТЕЧКИ ИНФОРМАЦИИ ЗА СЧЕТ ВНЕДРЕНИЯ РОБАСТНОГО ВОДЯНОГО ЗНАКА

Описан принцип действия модуля защиты текстовых данных различной степени конфиденциальности от утечки. Описаны функциональная модель механизма защиты, порядок маркировки документа и извлечения из него метки.

С ростом количества задач, выполняемых при работе с информационно-вычислительными сетями, значительно увеличиваются и объемы обрабатываемой информации, представленной в текстовом виде. В связи с этим возникла задача перевода всего документооборота в электронный вид, что значительно сокращает временные затраты на обработку данных различных объемов и степени конфиденциальности. Однако любые нововведения, ведущие к упрощению сложных процедур, непременно ведут к новым проблемам. Среди них – увеличение числа инцидентов, связанных с утечками информации. Модернизация систем электронного документооборота (СЭДО) взаимосвязана с вопросами безопасности обрабатываемых текстовых данных. Данная проблема актуальна и для подразделений специальной связи, для которых защита конфиденциальной информации является одним из приоритетных направлений. Для решения этой задачи разработано множество средств, использующих различные методы и способы защиты данных. На данный момент существует большое количество DLP-систем, использующих методы шифрования циркулирующего в организации трафика данных, методы сигнатурного и лингвистического анализов, детектирования, фильтрации, «цифровых отпечатков» и другого. Однако наибольший интерес представляет разработка таких механизмов защиты, факт использования которых оставался бы для злоумышленника неизвестным. В качестве основы для их создания удобно применять различные виды маркировок, выбираемых в зависимости от направления защиты.

Для защиты документов с разной степенью конфиденциальности содержащихся в нем сведений удобно применять цифровые водяные знаки, представляющие собой видимые или невидимые знаки (информационные последовательности), встраиваемые в исходные данные [1]. Наиболее подходящими для данной работы являются невидимые робастные водяные знаки (РВЗ), преимуществом которых являются инвариантность к возможным искажениям и преобразованиям контейнера и то, что факт их внедрения в документы остается для

злоумышленника неизвестным. Данные знаки обладают следующими свойствами [2-4]: емкость встраивания (полезная нагрузка), невидимость (перцепционная прозрачность), необнаруживаемость (сложность обнаружения), робастность и извлекаемость.

Для создания модуля защиты текстовых данных от утечки была составлена *функциональная схема*, представленная на рисунке 1. При описании данной модели предполагается, что на каждой ЭВМ организации установлена и правильно функционирует программа внедрения и извлечения встраиваемой метки (робастного водяного знака). Сотрудник организации выбирает электронный текстовый документ. В момент отправки этого документа на печать программа автоматически встраивает идентификатор в текстовый документ. Длина и составляющие идентификатора выбираются в зависимости от количества строк на той странице, в которую он внедряется. В общем случае идентификатор состоит из двух частей: метки конфиденциальности и данных отправителя. Метка конфиденциальности определяет степень секретности сведений, содержащихся в документе, и состоит из четырех бит. Вторая часть определяет номер, присвоенный каждому сотруднику организации. Процесс встраивания информации осуществляется следующим образом: увеличение величины межстрочного интервала на установленное значение Δ между соседними строками текста интерпретируется как значение «1»; отсутствие изменений в величине межстрочного интервала между соседними строками текста интерпретируется как значение «0».

Рис. 1. Функциональная модель подсистемы защиты текстовых данных от утечки

Для осуществления встраивания необходимо, чтобы число строк на странице было не меньше пяти. Если число строк на данной странице меньше этого значения, то встраивание не производится. Если данная страница содержит от пяти до девяти строк включительно, то встраивание метки конфиденциальности осуществляется циклически, повтором 4-битной комбинации до тех пор, пока это позволяет имеющаяся емкость встраивания. При этом количество встраиваемых символов будет на единицу меньше количества строк документа. Если количество строк на странице больше девяти, то, помимо метки конфиденциальности, в текстовый документ можно встроить данные отправителя документа.

После внедрения идентификатора помеченный документ отправляется на печать, а затем сканируется нарушителем для отправки за пределы организации с серверной машиной. При попытке передачи изображения включается блокировка этого процесса системой контроля. Поступившее изображение подвергается обработке, включающей преобразование цветового пространства изображения к изображению в градациях серого и среднеарифметической фильтрации. Затем из обработанного черно-белого изображения извлекается встроенный идентификатор. Для этого к нему применяется нормальное преобразование Радона и осуществляется поиск межстрочных интервалов текста изображения. Массив вычисленных межстрочных интервалов проходит процедуру коррекции ошибок. Скорректированный массив переводится в двоичный вид и сравнивается с существующими в базе. Таким образом определяем степень конфиденциальности текстовых данных (отправителя документа). Исходя из полученных сведений, принимается решение о возможности передачи отправляемого документа за периметр организации.

Алгоритм работы модуля защиты состоит из двух частей: процесса внедрения метки в контейнер и ее извлечения. Рассмотрим каждую часть.

Процесс внедрения РВЗ в контейнер состоит из следующих шагов:

1. Выбор текстового документа для печати;
2. Подсчет количества строк текстового документа;
3. Выбор размера метки;
4. Если количество строк документа больше размера метки, то встраивание осуществляется, в противном случае переходим к шагу 6;
5. Встраивание метки в исходный текстовый документ;
6. Замена исходного документа документом со встроенными данными.

Процесс извлечения РВЗ из изображения состоит из следующих шагов:

1. Выбор изображения, содержащего текст;
2. Преобразование цветного изображения в изображение в градациях серого;
3. Среднеарифметическая фильтрация изображения;
4. Создание синограммы из изображения посредством нормального преобразования Радона;

5. Вычисление среднеквадратического значения для каждого угла поворота из сформированной синограммы;

6. Выбор из синограммы ряда, обладающего более выровненным по линии чередованием черных и белых полос;

7. Вычисление величин межстрочных интервалов текста изображения;

8. Коррекция ошибок;

9. Перевод скорректированного массива в двоичный вид;

10. Определение идентификатора отправителя.

Таким образом, в результате работы создан алгоритм работы модуля защиты текстовых данных от утечки. Главным преимуществом механизма защиты является скрытие от злоумышленника факта внедрения метки в контейнер, содержащий сведения различной степени конфиденциальности.

Список литературы

1. Gribunin V.G., Okov I.N., Turincev I.V. Cifrovaya steganografiya. [Digital steganography]. M.: SOLON-Press., 2017. 262 p. (In. Russ.).

2. Phadikar A. Robust Watermarking Techniques for Color Images. 2009.

3. Salomon D. Data privacy and security: encryption and information hiding. Springer Science & Business Media. 2003. 469 p.

4. Woo C.-S. Digital image watermarking methods for copyright protection and authentication. Ph.D. Thesis. Queensland University of Technology. 2007. 223 p.

Материал поступил в редколлегию 25.03.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

***Козачок Александр Иванович**, к.п.н., доцент, сотрудник*
***Козлова Валерия Максимовна**, сотрудник*
Академия ФСО России
Россия, г. Орёл
e-mail: kaiakadem@mail.ru

АНАЛИЗ ПОДХОДОВ К ВЕРОЯТНОСТНОЙ ОЦЕНКЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Рассмотрены основные подходы к вероятностной оценке защищенности на основе теории вероятностей и нечеткой логики. Особое внимание уделено вероятностным подходам, основанным на представлении возможных действий нарушителей в виде построения деревьев или графов атак и последующей проверки свойств этого дерева (графа) на основе использования различных методов.

Возросшая сложность информационно-телекоммуникационных систем (ИТКС) и механизмов их защиты, увеличение количества уязвимостей и потенциальных ошибок в их использовании, а также возможностей нарушителей по реализации атак обуславливает необходимость разработки систем анализа защищенности [5]. Эти системы призваны выполнять задачи по обеспечению информационной безопасности (ИБ) ИТКС: обнаружение и исправление ошибок в конфигурации сети и используемой политике безопасности, выявление возможных трасс атакующих действий различных категорий нарушителей, определение критичных сетевых ресурсов и выбор адекватного угрозам защитного механизма [7].

В основе проектирования таких систем лежат различные методы анализа защищенности и определения общего уровня защищенности, в том числе использующие математический аппарат теории вероятностей. В связи с этим, анализ существующих подходов к оценке защищенности ИТКС представляется актуальным, а последующий выбор оптимального из них – залог успешной реализации политики ИБ.

Оценка защищенности на основе модели комплекса механизмов защиты (МЗ), предлагаемая Осовецким Л.Г. [6], осуществляется в два этапа: 1 – оценка наборной модели средств защиты информации (СЗИ); 2 – оценка структурной модели СЗИ. Предполагая, что на всех уровнях число МЗ – максимально возможное и вероятность нейтрализации угрозы на каждом последующем уровне СЗИ будет больше, чем на предыдущем, формируют вектор распределения вероятности нейтрализации угроз по уровням СЗИ, (1).

$$P = \begin{pmatrix} P_1 \\ P_2 \\ \dots \\ P_j \end{pmatrix} \qquad (1)$$

К недостаткам модели следует отнести статичный характер оценки защищенности, не учитывающей такие параметры, как ущерб от реализации угроз ИБ и частоту осуществления атак.

При проведении инвестиционного анализа СЗИ или для оценки ущерба в случае реализации угроз Карпычевым В.Ю. [3] учитывается ущерб, как в стоимостном исчислении, так и нематериальный ущерб, нанесенный репутации, конкурентным возможностям хозяйствующего субъекта. Вводятся семантические показатели «величина нематериального ущерба» и «вероятность нанесения ущерба», которые связаны с частотой реализации угрозы за конкретный период времени. При оценке эффективности защиты информации в ИТКС посредством нечетких множеств защищенность определяется исходя из ущерба системы, связанного с реализацией угроз, носящих вероятностный характер, который оценивается через коэффициенты опасности угроз [1].

Коэффициент опасности каждой угрозы описывается функцией принадлежности треугольной формы, то есть представляется тройкой чисел, при этом значения функции для средней точки наибольшее, остальные два остаются нулевыми (рисунок, 1).

Зная нечеткие значения и функции принадлежности коэффициентов опасности угроз, можно, с учетом вероятностей реализации угроз, по правилам теории нечетких множеств рассчитать нечеткие значения степени защищенности объекта информатизации от комплекса угроз.

Недостатками подобного оценивания являются статичность оценки защищенности и отсутствие взаимосвязи показателей защищенности с местоположением МЗ в структуре системы информационной безопасности (СИБ).

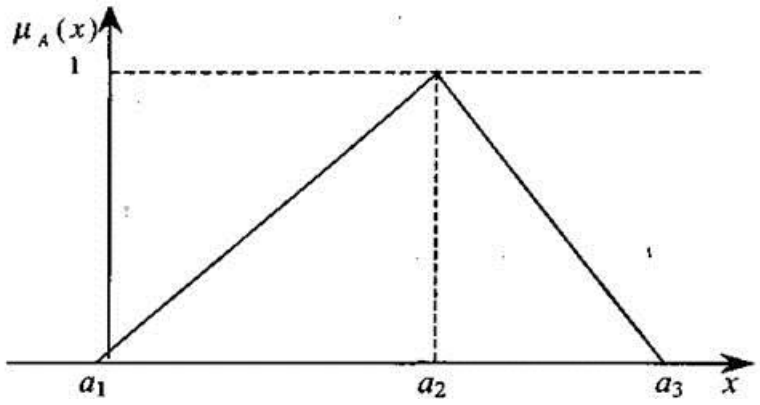


Рис. 1. Треугольное представление нечеткого числа

Согласно вероятностной модели, описанной В.В. Карповым [2], защищенность может быть оценена следующими показателями:

– вероятностью защиты – n;

– средним временем между пропущенными НСД – Tn;

– вероятностью пропуска определенного числа попыток несанкционированного доступа (НСД) на интервале работы;

– средним числом пропущенных НСД на интервале времени работы;

– интенсивностью потока пропущенных НСД – k.

Вероятность обеспечения защиты означает вероятность отсутствия несанкционированных запросов к информации на выходе средств защиты и определяется следующим образом:

$$n=P\{\tau_{НСД} > t\}=1-k, \qquad (2)$$

где $k=P\{t_{i+1}-t_i=\tau_{НСД} \le t\}$ является функцией распределения случайной величины $\tau_{НСД}$, которая представляет собой время между двумя соседними пропусками НСД.

Присутствующая в формуле вероятность пропуска НСД имеет реальное воплощение и является характеристикой качества того или иного метода защиты. Основное влияние на значение указанной вероятности оказывают два фактора: методическая вероятность используемого способа защиты и вероятность работоспособности механизма защиты в момент совершения попытки НСД.

Перспективным направлением в оценке уровня защищенности являются вероятностные подходы, основанные на представлении возможных действий нарушителей в виде построения деревьев или графов атак и последующей проверки свойств этого дерева (графа) на основе использования различных методов, например, методов верификации на модели (*model checking*), а также вычисления на базе данного представления разнообразных метрик защищенности. Так, методика оценки защищенности на основе сценарного логико-вероятностного моделирования Котенко Д.А. [4] предусматривает последовательное выполнение трех этапов (рис. 2).

Рис. 2. Этапы вероятностной оценки риска ИБ

Этап определения факторов риска включает анализ «дерева событий (ДС)» и «дерева нарушений (ДН)», позволяющий идентифицировать ситуации риска на основе правил-продуктов, построение сценария развития угроз в ИТКС путем синтеза функционального и системного ДС, что позволяет формировать итерации на этапах анализа событий ИБ.

Этап построения Л-функции риска включает математическое описание сценариев ситуаций риска. Математическая модель риска в виде Л-функции позволяет не только оценить степень участия каждого из элементов ДН ИБ в сценарии, но и уточнить сценарий путем определения ранга и «веса» аргументов Л-функции для выявления важности нарушений ИБ в исследуемой ситуации. Экспертом предлагаются методы определения величин ранга и «веса». Для определения Л-функции используется метод прямой аналитической подстановки, который предполагает замену всех интегративных k функций их уравнениями. Такая подстановка выполняется до тех пор, пока в полученном выражении не остается ни одной нераскрытой функции k, и все они оказываются заменены простыми случайными логическими переменными. Этап определения В-полинома риска включает построение многочлена расчетной вероятностной функции. Методы построения В-полинома и расчета вероятностных характеристик риска известны. Констатируется, что для практического применения наиболее удобными являются алгоритмы ортогонализации Л-функции.

Предложенный оригинальный подход к анализу защищенности ИТКС предназначен для использования как на этапах их проектирования, так и эксплуатации. Направлениями дальнейших исследований является совершенствование моделей компьютерных атак и оценки уровня защищенности, в частности системы метрик защищенности и правил их вычисления, развитие программного прототипа средств автоматизированной защиты и проведение дальнейшей экспериментальной оценки предложенных решений.

Проведенный анализ показал необходимость разработки обобщенного количественного показателя для оценки свойства «защищенность» ИТКС, который должен объединить положительные стороны известных подходов с целью его дальнейшего использования в качестве целевой функции для оптимизации структуры ИТКС по критерию «стоимость/защищенность».

Список литературы

1. Жижелев, А. В. К оценке эффективности защиты информации в телекоммуникационных системах посредством нечетких множеств / А. В. Жижелев, А. П. Панфилов, Ю. К. Язов, Р. В. Батищев // Изв. вузов. Приборостроение, 2003. – т. 46, № 7.

2. Карпов, В. В. Методика синтеза оптимального варианта аппаратно-программного комплекса защиты информации от несанкционированного доступа по критерию защищенности / В. В. Карпов. – https://cyberleninka.ru/article/n/

3. Карпычев, В. Ю. Цена информационной безопасности / В. Ю. Карпычев, В. А. Минаев // Системы безопасности, 2003. – № 5.

4. Котенко, Д. А. Метод оценки риска информационной безопасности на основе сценарного логико-вероятностного моделирования / Д. А. Котенко. – http://aspirantura.ifmo.ru/file/other/oLTQGtaprg.pdf

5. Котенко, И. В. Оценка безопасности компьютерных сетей на основе графов атак и качественных метрик защищенности / И. В. Котенко, М. В. Степашкин, В. С. Богданов // Труды СПИИРАН. – Вып. 3, т. 2. – СПб.: Наука, 2006.

6. Осовецкий, Л. Г. Оценка защищенности сетей и систем / Л. Г. Осовецкий, В. В. Шевченко // Экспресс электроника, 2002. – № 2 - 3.

7. Суханов, А. В. Комплексная оценка свойства «защищенность» информационных систем /А. В. Суханов. – http://www.inside-zi.ru/pages/5_2008/75.html

Материал поступил в редколлегию 25.03.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

***Козачок Александр Иванович**, к.п.н., доцент, сотрудник*
***Кравчук Татьяна Анатольевна**, сотрудник*
Академия ФСО России
Россия, г. Орёл
e-mail: kaiakadem@mail.ru

АНАЛИЗ СТАНДАРТОВ В ОБЛАСТИ ОБРАБОТКИ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассматриваются основные стандарты в области инцидентов информационной безопасности. Проведен анализ основных категорий инцидентов и особенности их реализации.

Система защиты от утечек информации основывается в том числе на выявлении, предотвращении, регистрации и устранении последствий инцидентов информационной безопасности или событий, нарушающих регламентированные процедуры защиты информационной безопасности. Инцидент информационной безопасности – событие, являющееся следствием одного или нескольких нежелательных или неожиданных событий информационной безопасности, имеющих значительную вероятность компрометации процессов деятельности и создания угрозы информационной безопасности [1]. В качестве причин инцидентов информационной безопасности могут выступать как технические, так и физические средства. Последствия могут представлять собой любые несанкционированные изменения информации, ее уничтожение или другие события, которые делают ее недоступной. С целью классификации инцидентов информационной безопасности был произведен анализ стандарта ГОСТ ISO/IEC TR 18044:2007 [1] и концепции защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации [2] , результат которого представлен на рисунке 1. Важно заметить, что данная классификация не является исчерпывающей, а служит лишь для иллюстрации выбранных примеров инцидентов информационной безопасности.

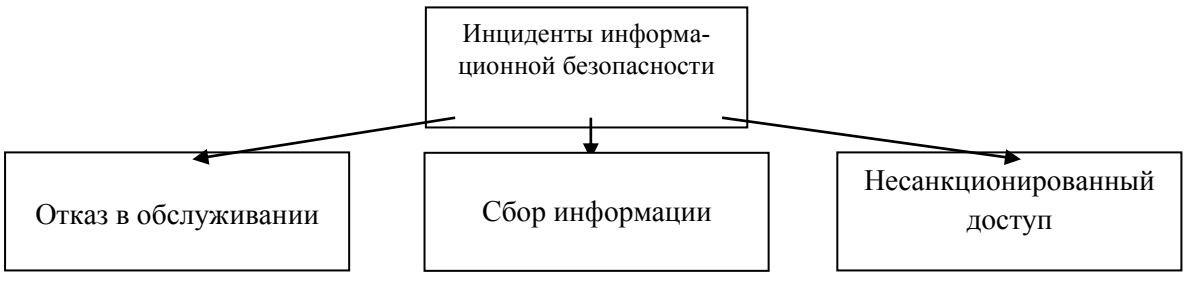


Рис.1. Классификация инцидентов информационной безопасности

Инциденты, относящиеся к категории "отказ в обслуживании", приводят к сбоям в системах, сервисах или сетях, которые не могут продолжать работу с прежней производительностью, чаще всего при полном отказе в доступе авторизованным пользователям. Различают два типа подобных инцидентов, создаваемых техническими средствами: уничтожение ресурсов и истощение ресурсов. Примерами подобных инцидентов могут послужить следующие события:

– зондирование сетевых широковещательных адресов с целью полного заполнения полосы пропускания сети трафиком ответных сообщений;

– передача данных в непредвиденном формате в систему, сервис или сеть с целью разрушения или нарушения нормальной работы;

– одновременное открытие нескольких сеансов с конкретной системой, сервисом или сетью с целью исчерпать ее ресурсы (т. е., замедлить ее работу, блокировать ее или разрушить).

Кроме того, существуют инциденты "отказ в обслуживании", создаваемые нетехническими средствами, приводящие к потере информации, сервиса и(или) устройств обработки. К таковым относятся:

– нарушение физических систем безопасности, приводящие к хищению, или преднамеренному нанесению ущерба, или разрушению оборудования;

– случайное нанесение ущерба аппаратуре и(или) ее местоположению от огня или воды/наводнения;

– неправильное функционирование программного или аппаратного обеспечения.

Категория инцидентов "сбор информации" включает действия, связанные с определением потенциальных целей атаки и получением представления о сервисах, запущенных на идентифицированных целях атаки.

К атакам, направленных на сбор информации техническими средствами, принято относить:

– сбрасывание записей DNS (системы доменных имен) для целевого домена Интернета (передача зоны DNS);

– отправка тестовых запросов по случайным сетевым адресам с целью найти работающие системы.

Инциденты, направленные на сбор информации, создаваемые нетехническими средствами, чаще всего бывают связаны, например, с нарушениями физической защиты безопасности, приводящими к несанкционированному доступу к информации и хищению устройств хранения данных, содержащих значимые данные (ключи шифрования).

Под несанкционированным доступом понимается доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированных систем [2]. К основным способам осуществления несанкционированного доступа обычно относят:

– создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;

– модификация средств защиты, позволяющая осуществить НСД;

– внедрение в технические средства вычислительной техники или автоматизированных систем программных или технических механизмов, нарушающих предполагаемую структуру и функции объекта и позволяющих осуществить НСД;

– непосредственное обращение к объектам доступа.

Инциденты несанкционированного доступа, создаваемые нетехническими средствами, которые приводят к прямому или косвенному раскрытию или модификации информации, к нарушениям учета или неправильному использованию информационных систем, могут вызываться следующими факторами:

– разрушением физической защиты безопасности с последующим несанкционированным доступом к информации;

– неудачно и(или) неправильно сконфигурированной операционной системы по причине неконтролируемых изменений в системе, или неправильного функционирования программного или аппаратного обеспечения, приводящих к тому, что персонал организации или посторонний персонал получает доступ к информации, не имея на это разрешения.

В общих чертах, эта категория инцидентов состоит из фактических несанкционированных попыток доступа в систему или неправильного использования системы, сервиса или сети [2].

Таким образом, проведенный анализ позволяет структурировать инциденты информационной безопасности, что несомненно будет крайне важным для будущих исследований в области разработки надежной защиты телекоммуникационной системы, неуязвимой перед вышеизложенными угрозами.

Список литературы

1. ГОСТ ISO/IEC TR 18044:2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. – 2007. – 46 с.

2. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации от 30.03.1992.

Материал поступил в редколлегию 25.03.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

***Козачок Александр Иванович**, к.п.н., доцент, сотрудник*
***Мельников Антон Дмитриевич**, сотрудник*
Академия ФСО России
Россия, г. Орёл
e-mail: kaiakadem@mail.ru

ИНЦИДЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ПРОЯВЛЕНИЕ НАРУШЕНИЯ ПРОЦЕССА ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ

Представлено исследование подходов к анализу инцидентов информационной безопасности с их длительным проявлением во времени на основе исследования статистических характеристик, наблюдаемых параметров компьютерной системы и методики выявления их скачкообразного изменения в форме нарушения процесса функционирования системы. Для этого исследуются различные подходы к выявлению изменений в наблюдаемых параметрах компьютерной системы, на основе которых можно сделать вывод о наличии инцидента информационной безопасности.

В современных информационных инфраструктурах существует множество разнообразных возможностей возникновения инцидентов информационной безопасности (ИИБ). В соответствии с ГОСТ Р ИСО/МЭК 27001-2006, инцидентом ИБ является «любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность». В настоящей работе рассматривается частный тип инцидентов ИБ, которые соответствуют выявленным изменениям в работе системы, отраженным на некоторых ее параметрах и произошедшим в результате неправомерных действий, совершаемых в ней, и/или неисправностях в программном или аппаратном обеспечении. Стандартный сценарий работы компьютерной системы (КС) в случае возникновения инцидента изменяется. Возникает необходимость выделения наблюдаемых характеристик, общих для различных сценариев работы, но поразному используемых в штатных и нештатных режимах функционирования.

Модель наблюдаемых параметров КС строится в виде случайного процесса. Преимущество статистического метода моделирования заключается в универсальности метода выявления ИИБ независимо от источника угрозы. Существуют два подхода к обеспечению защиты, которые зависят от степени важности информации, которая подлежит обработке: априорный и апостериорный. Априорный подход применяется в основном в системах, обрабатывающих чрезвычайно важную информацию, например, содержащую сведения, относящиеся к государственной тайне. Апостериорный подход в большей степени подходит для систем с конфиденциальной информацией, не содержащих чрезвычайно важных данных, но ориентированных на применение новейших ин-

формационных технологий. Одним из ключевых моментов в апостериорной системе защиты является блок обработки больших объемов данных о работе защищаемой системы, в котором производится автоматизированное исследование и выявление признаков ИИБ по разработанным алгоритмам. Этот блок обработки данных можно назвать центром системы апостериорной защиты. Алгоритмы обработки основаны на определенных моделях данных о КС, которые должны отражать существенную часть функционирования КС.

Методика применения статистического подхода изложена на рис 1.

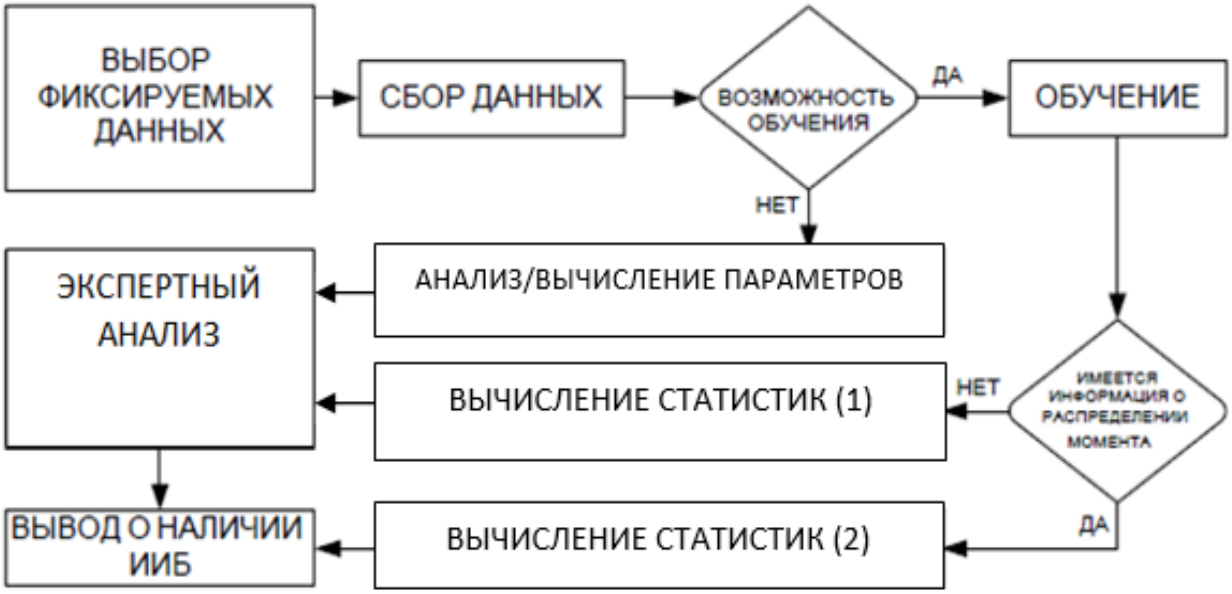


Рис. 1. Методика применения предложенного подхода

Особо следует остановиться на рекомендациях по выбору фиксируемых данных. Объем возможных вариантов значений должен быть не очень большим. С другой стороны, необходимо чтобы в эти данные вошли параметры, характеризующие парадигму действий пользователя или функционирования защищаемой системы при решении конкретной задачи.

Для решения данной задачи нельзя рассматривать критерий Неймана-Пирсона, в силу сложности его статистик. Поэтому вместо оптимальной статистики необходимо использовать ее упрощенный вариант, который основан на результатах обучения, на основе поступающих данных.

На рисунке данная статистика отображена как «статистика (2)».

В условиях, когда определить момент нарушения процесса на этапе обучения не удается, для оценки момента возникновения ИИБ предлагается применять статистику (1), так как предварительное обучение возможно не всегда, и его данные могут не переноситься на будущую работу КС.

Поскольку прикладные задачи, решаемые при помощи КС, чрезвычайно разнообразны, дать универсальные рекомендации по выбору фиксируемых системой мониторинга параметров не представляется возможным. Подборка данных и их представление в значительной степени зависит от предметной области и способа реализации прикладного ПО.

В качестве примеров контролируемых параметров предлагается использовать сетевые подключения и работающие процессы в КС. Для мониторинга данных параметров необходимо специальное прикладное ПО, которое в должной степени обеспечит надлежащей информацией о состоянии КС в рассматриваемом ракурсе. Предлагаемое ПО должно обеспечивать устойчивую работу КС, и своевременное обнаружение и оповещение о происходящих изменениях в контролируемых параметрах, которые можно рассматривать как нарушение процесса функционирования КС и расценивать как ИИБ.

Процесс функционирования прикладного ПО, описанного выше, должен заключаться в следующем:

1. Должен вестись постоянный мониторинг контролируемых параметров.
2. При обнаружении изменении контролируемых параметров система должна выполнять процессы, которые отображены на рисунке.
3. При необходимости данное ПО должно иметь возможность обучения, для более устойчивого функционирования и наиболее точного оценивания контролируемых параметров с целью выявления ИИБ.
4. Модуль экспертного анализа должен с необходимой точностью определять наличие ИИБ в текущем состоянии КС.
5. Должно иметь место сетевое взаимодействие между администратором данного ПО и пользователей, на основе логики «агент-менеджер» для автоматизации работы системы выявления ИИБ.

В заключение необходимо отметить то, что обнаружение ИИБ возможно при наличии определенных статистических критериев оценивания КС, на основе которых система, при проведения экспертного анализа, может сделать вывод о наличии ИИБ. В случае реализации возможности обучения и наличии поступающих данных, которые подходят для процесса обучения, система может сделать вывод о наличии ИИБ при имеющейся информации о распределении момента нарушения процесса функционирования КС.

Список литературы

1. Баранов, В.А. Применение статистик критерия однородности для выявления разладки. / В.А.Баранов // М.: Системы высокой доступности. Из-во «Радиотехника», 2012. – №1. – Т. 8. – С. 59-70.
2. Баранов, В.А. Оценка момента вторжения статистическими методами. / В.А. Баранов // Проблемы информационной безопасности. Компьютерные системы, /СПбГПУ, 2011. – № 2. – С. 24-31.
3. Котенко, И.В. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах / И.В. Котенко, И.Б. Саенко, О.В. Полубелова, А.А. Чечулин // Труды СПИИРАН. Вып.1 (20). – СПб.: Наука, 2012. – С.27-56.
4. Котенко, И.В. Интеллектуальные механизмы управления кибербезопасностью / И.В. Котенко // Управление рисками и безопасностью: труды Института системного анализа Российской академии наук (ИСА РАН). – М: URSS, 2009. – Т. 41. – С.74-103.

5. Баранов, В.А. Выявление разладки процесса наблюдений как метод определения вторжения / В.А. Баранов // Проблемы информационной безопасности. Компьютерные системы/ СПбГПУ. – 2011. – № 1. – С. 7-16.

6. Баранов, В.А. О доверительном интервале для момента вторжения. / В.А. Баранов // Проблемы информационной безопасности. Компьютерные системы / СПбГПУ. – 2012. – № 1. – С. 46-56.

Материал поступил в редколлегию 09.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

***Козачок Александр Иванович**, к.п.н., доцент*
***Пастухов Игорь Васильевич**, сотрудник*
Академия ФСО России
Россия, г. Орёл
e-mail: pdtr77@mail.ru

МОДЕЛЬ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ ОТ ТЕХНИЧЕСКОЙ РАЗВЕДКИ

Описана модель защиты информации объекта информатизации от технической разведки. Модель разработана на основе частных моделей типовых объектов защиты от технической разведки.

Защита информации в современных условиях становится все более сложной проблемой, что обусловлено рядом обстоятельств, основными из которых являются: массовое использование средств электронной вычислительной техники; необходимость защиты не только государственной и военной тайны, но и промышленной, коммерческой и финансовой тайн; расширяющиеся возможности несанкционированных действий над информацией.

Кроме того, в настоящее время получили широкое распространение средства и методы несанкционированного и негласного получения информации. Они находят все большее применение в деятельности разного рода преступных группировок.

Необходимо отметить, что естественные каналы утечки информации образуются спонтанно, в силу специфических обстоятельств, сложившихся на объекте защите (информатизации). В свою очередь искусственные каналы утечки информации создаются преднамеренно с применением активных методов и способов получения информации [1].

Техническая разведка классифицируется по физическим принципам построения и месту размещения аппаратуры.

По физическим принципам построения аппаратуры техническая разведка разделяется на оптическую, оптико-электронную, радиоэлектронную, акустическую, компьютерную, гидроакустическую, химическую, радиационную, сейсмическую и магнитометрическую.

По месту размещения аппаратуры техническая разведка подразделяется на космическую, наземную, воздушную и морскую.

В соответствии с ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» **Защита информации; ЗИ**: Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [2].

В соответствии с документами Гостехкомиссии под *моделью защиты* понимается абстрактное (формализованное или неформализованное) описание

комплекса программно-технических средств и организационных мер защиты от несанкционированного действия [3].

Для определения термина *объект защиты (разведки) (от технической разведки)* представим его признаки с точки зрения технической разведки:

а) объект разведки (защиты) является элементом системы функционирования (управления, эксплуатации, обеспечения) организации. В нём находится (циркулирует) защищаемая информация. Этот элемент является источником этой защищаемой информации, потому что в нём протекают информационные процессы обмена, обработки, воспроизведения и связанного с ними хранения информации;

б) указанный элемент имеет функциональные единство и целостность, а также типовую структуру;

в) указанный элемент системы является объектом технической разведки, если он доступен для добывания с него защищаемой информации (разведывательной информации);

г) структура и информационные процессы позволяют обнаруживать этот элемент, распознавать его назначение, а также смысл и содержание информации и информационных процессов в нем;

С учетом приведенных признаков можно дать следующее краткое определение объекта защиты (разведки) от технической разведки.

Объект защиты (разведки) от технической разведки – это элемент организационной или технической системы функционирования организации, имеющий функциональные единство и целостность, типовую структуру и являющийся местом протекания информационных процессов, что позволяет технической разведке распознавать его назначение, смысл и содержание указанных процессов и применяемой при этом информации.

В настоящее время в зависимости от целевого предназначения существует значительное количество моделей защиты информации [4].

Для анализа частных моделей типовых объектов защиты от технической разведки разработаем общую модель объекта информатизации от технической разведки, модель которого представлена на рис. 1.

В её состав входят три части:

– первая часть – внешние технические средства, сооружения и коммуникации;

– вторая часть – элементы системы управления и обеспечения функционирования.

Первая часть системы охватывает вторую часть. Её элементы размещены в непосредственной близости от общедоступных мест за пределами контролируемой зоны. Объекты защиты от технической разведки второй части размещаются на охраняемой территории.

Рис. 1. Модель защиты информации объекта информатизации от технической разведки

Вторая часть модели в свою очередь имеет частные, входящие в их состав объекты защиты от технической разведки.

Вторая часть размещается, как правило, стационарно в зданиях. В её состав входят объекты защиты от технической разведки организационно-технической подсистемы в виде выделенных помещений и объектов средств вычислительной техники (СВТ) и технической подсистемы в виде электрических технических средств и систем. Выделенные помещения могут совпадать с объектами СВТ.

Электрические технические средства и системы включают в себя следующие объекты защиты (разведки) от технической разведки:

– основные технические средства и системы (ОТСС) в виде систем звукоусиления (данные средства могут размещаться в выделенных помещениях);

– ОТСС в виде СВТ (размещаются в объектах СВТ);

– ОТСС в виде локальных сетей связи и передачи данных (размещаются в помещениях и коммуникациях здания);

– вспомогательные технические средства и системы (ВТСС) (размещаются в помещениях и коммуникациях здания).

Одно и то же помещение может быть выделенным помещением и (или) объектом СВТ.

Указанные объекты могут быть размещены стационарно в зданиях или на подвижных объектах.

Представленная модель объекта информатизации как объекта защиты (разведки) от технической разведки включает в себя частные модели типовых объектов защиты от технической разведки.

Каждая из этих моделей в соответствии с данным выше определением объекта защиты (разведки) от технической разведки включает следующие признаки этого объекта, как источника информации:

– структура, условия размещения элементов, их конструкция и особенности, которые определяют доступность объекта для технической разведки;

– характеристика информационных процессов и защищаемой информации, которые определяют вид добываемой с объекта информации;

– виды, средства и способы технической разведки, которые могут применяться для добывания защищаемой информации.

Таким образом, проблема защиты информации и обеспечения информационной безопасности на объектах информатизации приобретает все большую актуальность. Разработанная модель защиты информации может быть использована для повышения эффективности разработки систем защиты информации объектов информатизации.

Список литературы

1. Техническая защита информации: учебное пособие/ А.А. Хорев. – Москва: НПЦ «Аналитика», 2008. – 435с.

2. ГОСТ Р 50922–2006 «Защита информации. Термины и определения».

3. Защита от несанкционированного доступа к информации. Термины и определения. Руководящий документ/ Сборник руководящих документов по защите информации от несанкционированного доступа. – М.: Гостехкомиссия России, 1998.

4. Основы технической защиты информации: учебное пособие/ В.А. Шалагинов [и др.]; под общ. ред. В.А. Шалагинова. – Орел: Академия ФСО России, 2019. – 259 с.

Материал поступил в редколлегию 09.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 621.391.18

Козленко Андрей Владимирович, *к.т.н., сотрудник*
Жусов Дмитрий Владимирович, *к.т.н., сотрудник*
Толкунов Александр Александрович, *к.т.н., сотрудник*
Академия ФСО России
Россия, г. Орёл
e-mail: et-ak@yandex.ru

КОНТРОЛЬ ЦЕЛОСТНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ВЕДОМСТВЕННЫХ ВЕБ-ПОРТАЛОВ

Показана актуальность задачи контроля целостности информационных ресурсов ведомственных веб-порталов. Предложен способ и приведен пример расчета периода контроля целостности информационных ресурсов ведомственных веб-порталов.

Нарушение нормального функционирования компьютерных сетей большинства промышленных, правительственных, банковских, оборонных и правоохранительных организаций вследствие НСД к обрабатываемой в них информации влечет за собой значительный ущерб. Достижение научно-обоснованного уровня защищенности информации от НСД обуславливает необходимость проведения оценки и контроля защищенности на всех этапах жизненного цикла компьютерных сетей при различной степени полноты и достоверности имеющейся информации [1]. При этом в ведомственных компьютерных сетях в настоящее время активно развивается технология веб-порталов, представляющая следующие преимущества:

– предоставление пользователям единой точки персонифицированного доступа к различным информационным ресурсам;

– интеграция разнородных информационно-аналитических и информационно-справочных систем;

– унификация подходов к использованию большого количества существующих и разрабатываемых информационных систем;

– масштабируемость системы (увеличение количества пользователей, подключение новых информационных ресурсов, создание дополнительных портальных сервисов).

С целью повышения защищенности информационных ресурсов ведомственных веб-порталов и постоянного мониторинга его функционирования предлагается использовать процедуру контроля целостности информационных веб-ресурсов.

Расчет необходимого периода контроля произведем на основе модификации модели [2] путем решения следующего уравнения при фиксации требуемого значения вероятности сохранения целостности информационных ресурсов $P_{\text{КЦ}}(T_{\text{КЦ}})$:

$$P_{\text{КЦ}}(T_{\text{КЦ}}) = \begin{cases} \left(\sigma - \beta_{\text{КА}}^{-1}\right)^{-1} \left\{\sigma\, e^{-T_{\text{КЦ}}/\beta_{\text{КА}}} - \beta_{\text{КА}}^{-1}\, e^{-\sigma T_{\text{КЦ}}}\right\}, \text{если } \sigma \neq \beta_{\text{КА}}^{-1} \\ e^{-\sigma T_{\text{КЦ}}}\left[1 + \sigma T_{\text{КЦ}}\right], \text{если } \sigma = \beta_{\text{КЦ}}^{-1}; \end{cases} \quad (1)$$

где σ – частота проявления компьютерных атак;

$\beta_{\text{КЦ}}$ – среднее время изменения информационных ресурсов при успешной реализации компьютерной атаки.

Его точное решение в общем случае можно получить, осуществив вычисление значения функции e^x при помощи степенного ряда для заданной точности вычислений:

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots + \frac{x^n}{n!} + \ldots \quad (2)$$

Более простым и наглядным является решение данного уравнения в графическом виде относительно $T_{\text{КЦ}}$ при фиксированных значениях σ, $\beta_{\text{КЦ}}$ и P. В этом случае получим рассчитанное значение периода контроля. Например, для значений $\beta_{\text{КЦ}} = 1$ с, $\sigma = 1$ мин и $P = 0{,}9$ решение уравнения можно представить следующим образом (рис. 1), что соответствует значению $T_{\text{КЦ}} = 7{,}329$ с.

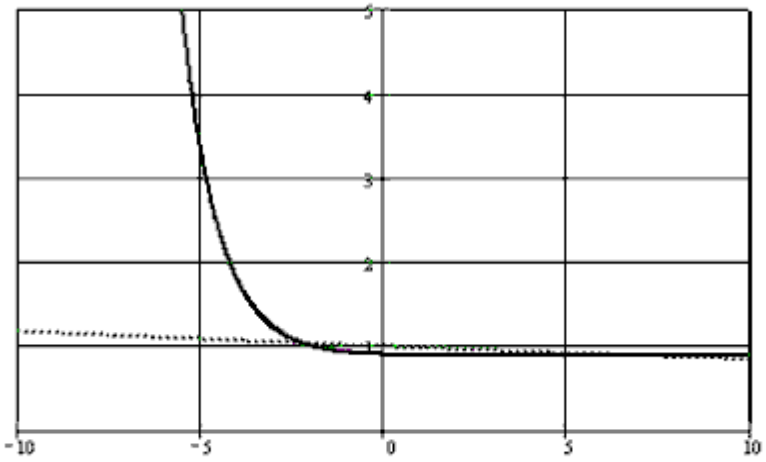


Рис. 1. Графическое решение уравнения по расчету периода контроля целостности информационных ресурсов ведомственных веб-порталов

Физический смысл данной величины свидетельствует о том, что его значения могут лежать только в области неотрицательных значений. В связи с этим в качестве решения уравнения выбирается значение, лежащее справа от нуля по оси абсцисс. Аналогично решая данное уравнение для других значений σ, $\beta_{\text{КЦ}}$

и P получаем набор временных характеристик процесса контроля целостности информационных ресурсов ведомственных веб-порталов (табл. 1):

Таблица 1

Пример расчета необходимого периода контроля целостности информационных ресурсов ведомственных веб-порталов $T_{КЦ}$ (сек)

σ, мин	β, с	P									
		0,5	0,7	0,75	0,8	0,85	0,9	0,93	0,95	0,97	0,99
1	1	42,597	22,409	18,269	14.397	10,76	7,329	5,358	4,068	2,77	1,344
2		84,182	43,805	35,526	27,781	20,506	13,645	9,712	7,158	4,649	2,083
3		125,762	65,169	52,756	41,149	30,247	19,867	14,057	10,218	6,447	2,729
4		167,347	86,557	70,006	54,53	39,993	26,284	18,532	13,338	8,281	3,35
5		208,933	107,945	87,256	67,911	49,74	32,604	22,933	16,44	10,116	3,96
1	2	43,671	23,439	19,154	15,365	11,769	8,325	6,293	4,922	3,363	1,835
2		85,302	44,83	36,544	28,622	21,462	14,745	10,511	8,138	5,535	2,63
3		126,944	66,233	53,802	41,888	31,157	21,368	15,004	10,965	7,092	3,324
4		168,589	87,639	71,064	55,156	40,854	27,261	19,505	14,111	8,934	3,961
5		210,236	109,046	88,326	68,426	50,552	33,566	24,008	17,261	10,781	4,575
1	3	44,687	24,505	20,342	16,305	12,804	9,253	7,104	5,626	4,053	2,3
2		86,266	45,922	37,589	29,822	22,39	15,529	11,699	9,03	6,272	3,005
3		127,87	67,366	54,859	43,205	31,969	22,378	15,656	12,219	8,289	3,708
4		169,48	88,816	72,136	56,594	41,552	30,858	20,263	14,654	10,219	4,345
5		211,1	110,27	89,416	69,986	51,135	34,499	24,876	17,856	11,206	4,956
1	4	45,948	25,619	21,395	17,201	13,584	10,101	7,809	6,219	4,524	2,758
2		87,787	47,149	38,681	30,863	23,288	16,214	12,619	9,822	6,89	3,277
3		129,68	68,721	55,993	44,253	32,685	23,298	17,1	13,136	9,022	3,978
4		171,58	90,306	73,317	57,653	42,078	30,396	20,919	16,315	11,042	4,609
5		213,49	111,9	90,647	71,058	51,473	35,407	25,644	18,34	12,993	5,214
1	5	46,751	26,788	22,443	18,034	14,322	10,877	8,43	6,731	4,926	3,214
2		88,113	48,6	39,842	31,917	24,144	17,661	13,473	10,525	7,418	3,486
3		129,55	70,457	57,252	45,333	33,293	24,176	18,075	13,982	9,658	4,178
4		171	92,335	74,679	58,759	44,079	31,521	21,523	17,254	11,773	4,802
5		212,46	114,22	92,115	72,193	53,832	36,291	26,363	18,768	13,802	5,401

Графическая интерпретация полученных значений представлена на рис. 2.

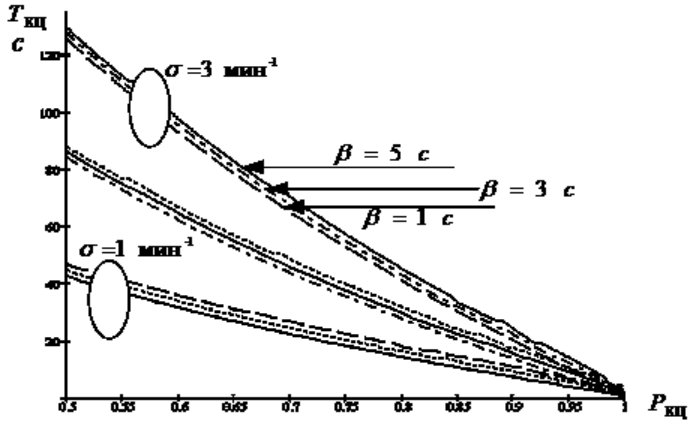


Рис. 2. График зависимости необходимого значения периода контроля от требуемой вероятности сохранения целостности информационных ресурсов ведомственных веб-порталов

Из представленных расчетов видно, что на значения вероятности сохранения целостности информационных ресурсов ведомственных веб-порталов в большей степени оказывает влияние частота проявления компьютерных атак, а не среднее время изменения информационных ресурсов при успешной реализации компьютерной атаки. Это свидетельствует о том, что в реальных условиях предупреждения компьютерных атак необходимо тщательно контролировать частоту проявления компьютерных атак.

Список литературы

1. Козленко, А.В. Метод оценки уровня защиты информации от НСД в компьютерных сетях на основе графа защищенности / А.В. Козленко, В.С. Авраменко, И.Б. Саенко, А.В. Кий // Труды СПИИРАН, 21 – 2012. – С. 41–55.

2. Безкоровайный, М.М. Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем "КОК": Руководство системного аналитика. – 2-е изд. / М.М. Безкоровайный, А.И. Костогрызов, В.М Львов. – М.: Вооружение. Политика. Конверсия, 2002. – 305 с.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

Е.В. Лексиков
ФГБОУ ВО «Брянский государственный технический университет»
Россия, г. Брянск
Jl32@yandex.ru

МОДЕЛЬ ПРОГНОЗИРОВАНИЯ ARIMAX ПРИМЕНИТЕЛЬНО К ПРОЦЕССУ ОЦЕНКИ ВОЗМОЖНОСТИ РАСШИРЕНИЯ ИНФОРМАЦИОННОГО ПОРТАЛА РЕГИОНАЛЬНЫХ ОРГАНОВ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ

Рассмотрена модель прогнозирования Arimax применительно к процессу оценки возможности расширения информационного портала региональных органов исполнительной власти.

Возможность учета необходимости расширения функционала системы в будущем, а соответственно необходимость в расширении производственных мощностей системы, напрямую влияют на возможность управления тем или иным процессом. Например, Заказчик не может знать потребуется ли ему в будущем механизм согласования ОРД в рамках информационного портала, что является достаточно трудоемкой задачей. А данный механизм напрямую влияет на скорость, качество и полноту принятия управленческих решений.

Предположим, что имеется временной ряд $Z(t)$. Есть необходимость вычислить будущее значение временного ряда в определенной точке №10, т.е. значение $Z(10)$ на основании предыдущих точек, т.е. от $Z(1)$ до $Z(9)$ с использованием модели авторегрессии (AR – autoregression).

Формула для определения $Z(10)$ выглядит следующим образом и называется авторегрессией порядка p:

$$Z(10) = a_0 + a_1 \times Z(9) + a_2 \times Z(8) + a_3 \times Z(7) + \cdots + a_p \times Z(10 - p)$$

В это формуле мы знаем значения Z(9), Z(8), Z(7) и т.д., но не знаем коэффициенты a. Как их определить?

Если для Z(10) работает такая зависимость, значит, она работает и для предыдущих точек, т.е. мы можем получить систему уравнений:

$$Z(9) = a_0 + a_1 \times Z(8) + a_2 \times Z(7) + a_3 \times Z(6) + \cdots + a_p \times Z(9 - p)$$
$$Z(8) = a_0 + a_1 \times Z(7) + a_2 \times Z(6) + a_3 \times Z(5) + \cdots + a_p \times Z(8 - p)$$
$$Z(7) = a_0 + a_1 \times Z(6) + a_2 \times Z(5) + a_3 \times Z(4) + \cdots + a_p \times Z(7 - p)$$

В этой системе уравнений мы знаем все значения Z(t), следовательно, можем легко определить коэффициенты a.

Когда нам нужно прогнозировать временной ряд $Z(t)$, то иногда удобнее и точнее прогнозировать не само значение процесса $Z(t)$, а только его изменение, т.е. провести интеграцию (I – integrated). То есть на первом этапе мы из ис-

ходного временного ряда $Z(t)$ получаем временной ряд $\bar{Z}(t)$, который является разностью соседних значений:$\bar{Z}(t) = Z(t) - Z(t-1)$

Далее, мы работаем уже с полученным рядом $Z(t)$ и определяем будущее значение не $Z(t+1)$, а $\bar{Z}(t+1)$ с использованием уже рассмотренной модели авторегрессии.

Отчего такая операция называется integrated, то есть интегрированием. В действительности, приведенная разность является обратной операцией, однако при использовании такого подхода для получения в конечном итоге будущего значения искомого временного ряда $\hat{Z}(t+1)$ необходимо будет суммировать $\hat{Z}(t+1) = Z(t) + \bar{Z}(t+1)$, то есть к текущему значению процесса прибавлять спрогнозированную разность. Так как суммировать в итоге нужно единожды, то говорят об интеграции первого порядка.

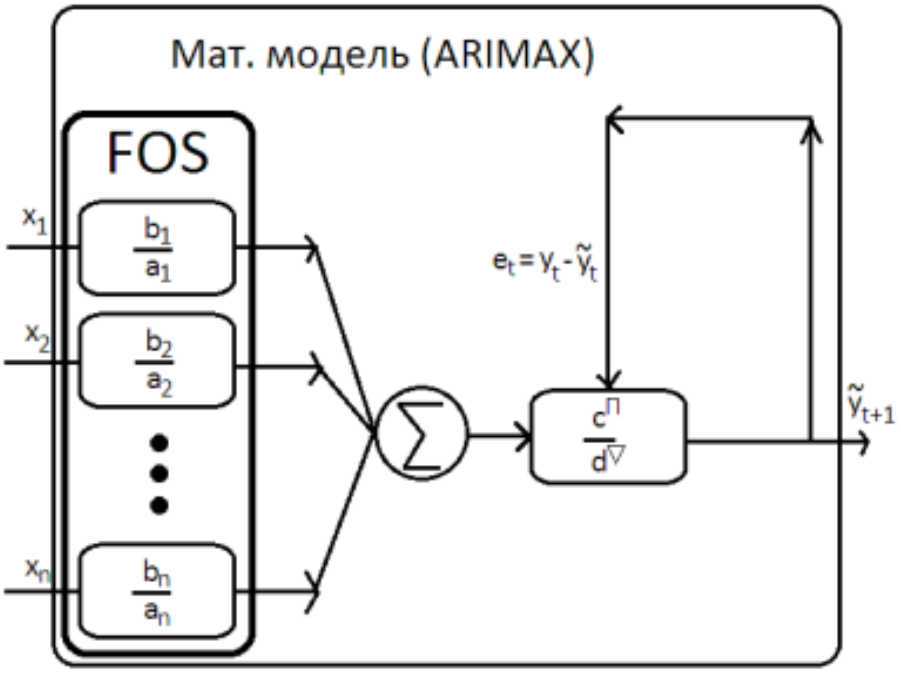


Рис. 1.Структурная схема модели ARIMAX

Расширение модели ARIMAX (X – eXtended) имеет дело с моделью авторегрессии AR(p). Формула для определения Z(10) описана выше. Если же нам нужно добавить в модель учет, например, двух показателей, представленных в виде временных рядов X(t) и Y(t), то выражение авторегрессии будет иметь вид:

$$Z(10) = \alpha_0 + \alpha_1 \times Z(9) + a_2 \times Z(8) + \cdots + \alpha_p \times Z(10-p) + \alpha_I \times X(10) + \alpha_{II} \times Y(10)$$

В линейную комбинацию добавлены два члена (их называют регрессорами), которые позволяют учет значений рассматриваемых внешних факторов. Коэффициенты данной линейной регрессии находятся аналогичным образом при помощи метода наименьших квадратов для набора уравнений:

$$Z(9) = \alpha_0 + \alpha_1 \times Z(8) + a_2 \times Z(7) + \cdots + \alpha_p \times Z(9-p) + \alpha_I \times X(9) + \alpha_{II} \times Y(9)$$

$$Z(8) = \alpha_0 + \alpha_1 \times Z(7) + a_2 \times Z(6) + \cdots + \alpha_p \times Z(8-p) + \alpha_I \times X(8) + \alpha_{II} \times Y(8)$$

$$Z(7) = \alpha_0 + \alpha_1 \times Z(6) + a_2 \times Z(5) + \cdots + \alpha_p \times Z(7-p) + \alpha_I \times X(7) + \alpha_{II} \times Y(7)$$

Имея все фактические значения Z(t), X(t) и Y(t), мы легко составляем систему для определения коэффициентов.

Важно отметить, что в моделях прогнозирования внешние факторы, то есть показатели X(t) и Y(t) должны учитываться в соответствующие моменты времени. Если мы прогнозируем временной ряд Z(t) на завтра, то нам нужно иметь под рукой значения внешних факторов X(t) и Y(t) на то же самое завтра, иначе модель будет работать некорректно.

Таким образом, модель авторегрессии с одной стороны довольно проста, так как принцип ее работы понятен и нагляден; с другой - сложна тем, что в ней имеет место множество нюансов, которые требуют кропотливого труда разработчика. Однако, не смотря на все нюансы, рассмотренная модель является частью большой модели ARIMAX, которая на сегодняшний день чрезвычайно популярна для решения задач прогнозирования.

Прибегая к прогнозированию, мы можем постараться определить будущие уязвимые места, опираясь на аналитические данные, полученные в ходе обследования и проектирования информационного портала.

Таким образом, одна из основных проблем решается посредством осуществления процесса прогнозирования использовать авторегрессионую модель ARIMAX, которая позволяет рассматривать процесс изменения нагрузочных показателей в определенные промежутки времени, на основании собранных данных.

Материал поступил в редколлегию 24.04.19.г

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

***Лексиков Евгений Вячеславович**, ст. преподаватель каф. «Системы информационной безопасности» БГТУ*
***Горлов Алексей Петрович**, к.т.н., доцент каф. «Системы информационной безопасности» БГТУ*
***Гулак Максим Леонидович**, к.т.н., доцент каф. «Системы информационной безопасности» БГТУ*
ФГБОУ ВО «Брянский государственный технический университет»
Россия, г. Брянск
Jl32@yandex.ru

ФОРМАЛИЗАЦИЯ ПРОЦЕССА ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННЫХ ПОРТАЛОВ И ПРОВЕДЕНИЕ АНАЛИТИЧЕСКОГО ОБСЛЕДОВАНИЯ ПРИ ПОМОЩИ НЕЧЕТКОГО КОГНИТИВНОГО МОДЕЛИРОВАНИЯ

Рассмотрены проблемы проектирования информационных порталов региональных органов исполнительной власти. Приведен алгоритм разработки информационного портала. Предложен метод проведения анализа организации на основе метода нечеткого моделирования и построения нечетких когнитивных карт.

Информационные технологии являются одной из основных возможностей реализации процесса принятия управленческих решений в региональных органах исполнительной власти. Выявлено, что важную роль в управлении социальными и экономическими системами играют информационные порталы, которые выполняют функции информационно-управляющих систем (ИУС). Данные системы позволяют оперативно осуществлять сбор, хранение, передачу, анализ и обработку информации об изменяющейся обстановке для выработки решений. В результате выполнения задачи по сопоставлению общего процесса проектирования ПО с процессом анализа и синтеза информационных порталов органов исполнительной власти – была сформирована расширенная модель алгоритма анализа и синтеза ИП ОИВ (рис.1). Данная модель дала возможность выделить 4 уровня этапа проектирования:

- 1-й уровень – проведение аналитического обследования, где проводится сбор, анализ и формализация функциональных и нефункциональных требований.
- 2-й уровень – подготовка ТЗ. На уровне 2 формируется техническое задание к разработке АС (ТЗ по конкурсу), в котором оформляются первичные требования различных направлений к АС.
- 3-й уровень – выбор вида ИП. На третьем уровне выбирается основное техническое решения для поставленной задачи в ТЗ, определяется функциональная структура.

- 4-й уровень – выдача проекта и прогнозирование рисков. На выходе после первых трех уровней должен получиться технический проект по реализации заданной АС.

Где самыми сложными являются уровни 1, 3, 4, поскольку только организационных мер недостаточно.

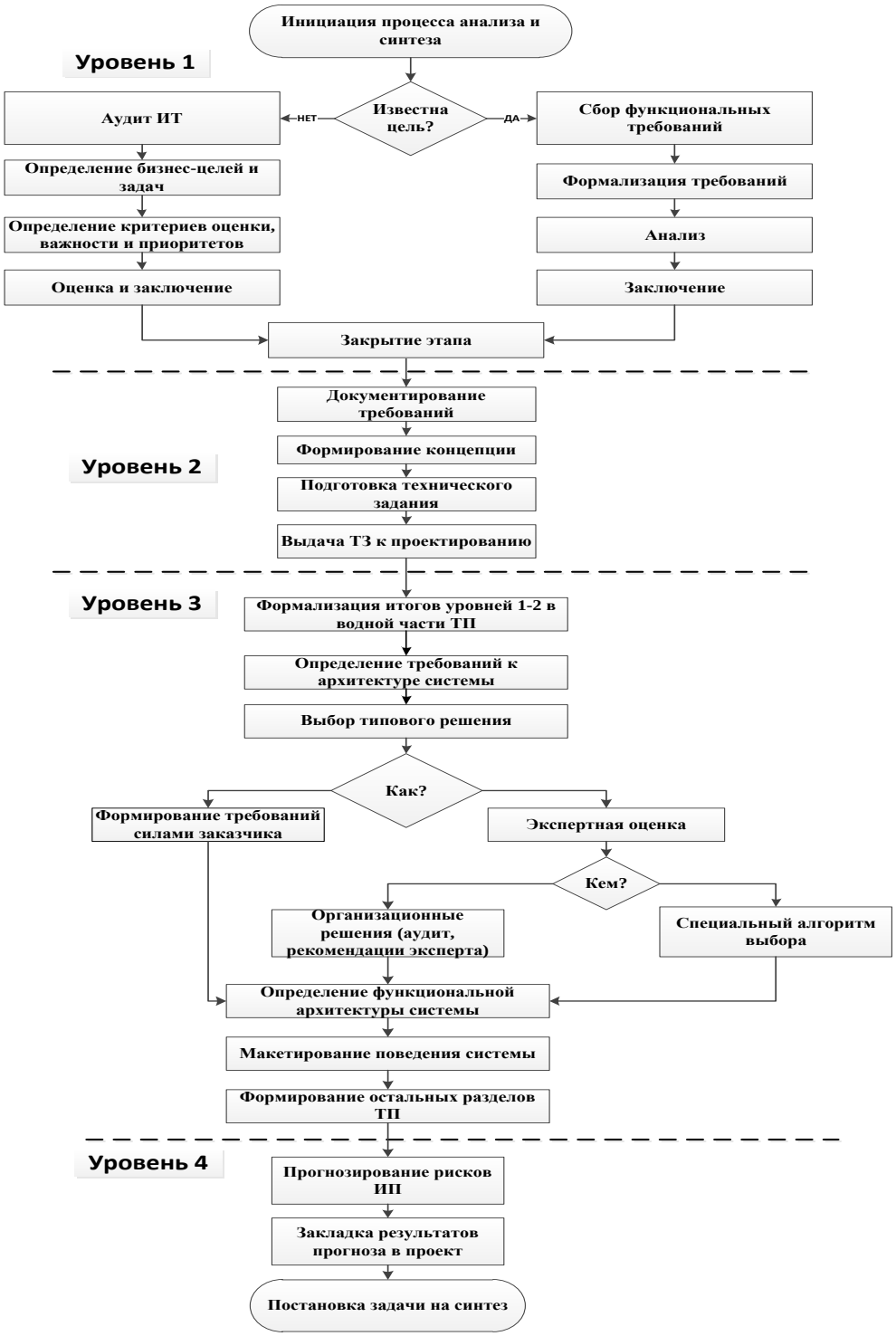


Рис.1 – Расширенная модель процесса анализа и синтеза ИП

Для данных сложных уровней был использованы следующие специальные методы:

1. Модель проведения процесса аналитического обследования предприятия посредством нечеткого когнитивного моделирования.
2. Методика определения функциональной архитектуры и инфраструктуры (типа) информационного портала посредством метода анализа иерархий.
3. Алгоритм прогнозирования возможности расширения информационного портала посредством модели прогнозирования ARIMAX.

В соответствии с данным утверждением была разработана навигационная карта движения по уровням процесса анализа и синтеза с обозначением предлагаемых инструментов (рис.2).

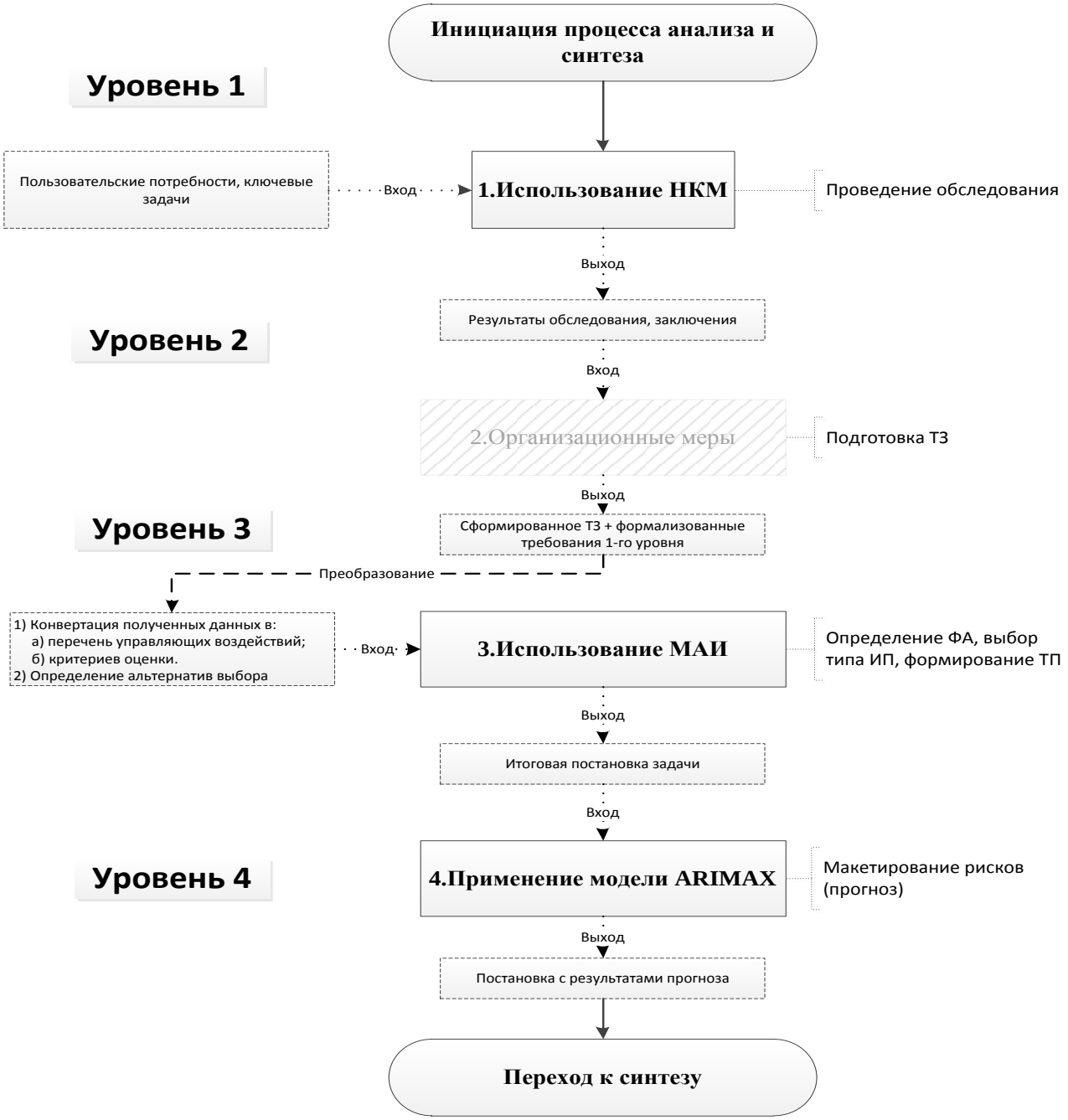


Рис. 2. Навигационная карта процесса анализа и синтеза ИП ОИВ

Исходя из основной задачи, поставленной в работе, было предложено математическое представление процесса анализа и синтеза ИП ОИВ:

$$M = <T, K, N, A, O>, \quad (1)$$

где

$T = \{t_1, t_2, \dots, t_{tc}\}$ множество бизнес-требований, которые предъявляются информационному порталу при конечном количестве tc.

$K = \{k_1, k_2, \dots, k_{kc}\}$ множество критериев, перечень которых формируется при выборе функциональной архитектуры при конечном количестве kc.

$N = \{n_1, n_2, \dots, n_{nc}\}$множество задач, которые были определены, исходя из пожеланий заказчика.

$A = \{a_1, a_2, \dots, a_{ac}\}$ множество вариантов функциональности информационного портала, исходя из сформированной классификации.

$O = \{o_1, o_2, \dots, o_{oc}\}$ множество ограничений и допущений, которые накладываются заказчиком и исполнителем на информационный портал при проектировании.

Данная модель отражает процесс анализа и синтеза информационных порталов с уже предложенными инструментами работы на каждом этапе. В оде дальнейших изысканий модель была упрощена до:

$$M = \langle X, Y, Z \rangle, \quad (2)$$

где

$X = \{x_1, x_2, \dots, x_{xc}\}$ множество результатов, которые были получены на первом уровне методики – на этапе аналитического обследования при помощи нечеткого когнитивного моделирования. Каждому результату соответствует множество бизнес-задач $N = \{n_1, n_2, \dots, n_{nc}\}$, которые ставятся перед системой, а также множество бизнес-требований $T = \{t_1, t_2, \dots, t_{tc}\}$.

$Y = \{y_1, y_2, \dots, y_{yc}\}$ множество результатов, которые были получены на втором уровне методики – на этапе формирования функциональной архитектуры решения при использовании метода анализа иерархий. Каждому результату соответствуют набор различных критериев $K = \{k_1, k_2, \dots, k_{kc}\}$ и множество вариаций $A = \{a_1, a_2, \dots, a_{ac}\}$, на основании которых были получены результаты множества X.

$Z = \{z_1, z_2, \dots, z_{zc}\}$ множество результатов, которые были получены на заключительном этапе методики – на этапе прогнозирования и учета рисков. Каждому результату соответствует множество ограничений и допущений $O = \{o_1, o_2, \dots, o_{oc}\}$, на которое опираются при проведении процесса прогнозирования и макетирования рисков.

Элемент модели X – это первый уровень создания информационного портала, т.е. проведение аналитического обследования предприятия при помощи нечеткого когнитивного моделирования. Элемент модели Y – это второй уровень процесса, т.е. определение функциональной архитектуры посредством метода анализа иерархий. Оба элемента являются обязательными, т.к. совокупность результатов их выполнения дает стартовый набор входных данных на третьем уровне. Т.е. эти данные необходимы для прогнозирования.

Выявлено, что в целях более корректного процесса проектирования модель допускает внесение дополнительных ограничений на компонентный состав, например: время процесса анализа и синтеза и т.д. Исходя из результатов и исследования данной модели видно достаточность введенных в модель системы компонентов для решения поставленных задач.

Материал поступил в редколлегию 24.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.048

Макеев Сергей Михайлович, *к.т.н., сотрудник*
Беликов Илья Владимирович, *сотрудник*
Академия ФСО России
Россия, г. Орёл
e-mail: Maksm57@yandex.ru

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ APACHE MAHOUT И WEKA

Рассмотрены структурные особенности технологий машинного обучения, их преимущества и недостатки. Сделан вывод о применимости каждой технологии в информационно-аналитической деятельности.

Обеспечение безопасности в алгоритмах машинного обучения имеет огромное значение для корректности и релевантности результатов работы технологий машинного обучения. В настоящее время специалистами в области Internet Technologies решается колоссальный объем задач, одной из которых является создание масштабируемых технологий машинного обучения, ориентированных, прежде всего на область совместной фильтрации, кластеризации и классификации. Существует несколько технологий, реализующих решение данной задачи. Рассмотрим две из них, Apache Mahout и Weka.

Основные алгоритмы Mahout направлены на решение задач путем кластеризации, классификации и коллаборативной фильтрации. Технология реализована на платформе Hadoop с использованием парадигмы MapReduce, добавляя совершенно новый функционал, позволяющий решать вышеперечисленные задачи, с обеспечением определенного уровня безопасности, которого не достаточно для сохранения безопасности корпоративных данных. Hadoop использует для аутентификации Kerberos. Но, вопреки данному факту, реализация данного протокола очень трудна и ресурсоемка в реализации. Также Hadoop не поддерживает протокола LDAP и каталога Active Directory для задействования политик безопасности.

Ниже перечислены основные особенности и возможности Apache Mahout:

- алгоритмы Mahout написаны поверх Hadoop, благодаря этому технология отлично функционирует в распределенной среде. Также технология Mahout масштабируема в облаке.
- представляет собой инфраструктуру для реализации задач интеллектуального анализа больших наборов данных.
- предоставляет несколько вариантов выполнения задач кластеризации и классификации разнородной информации с поддержкой MapReduce.
- обеспечивает эффективность и скорость процесса анализа разновидной информации.
- содержит матричные и векторные библиотеки [1].

На рис. 1 представлена архитектура Apache Mahout:

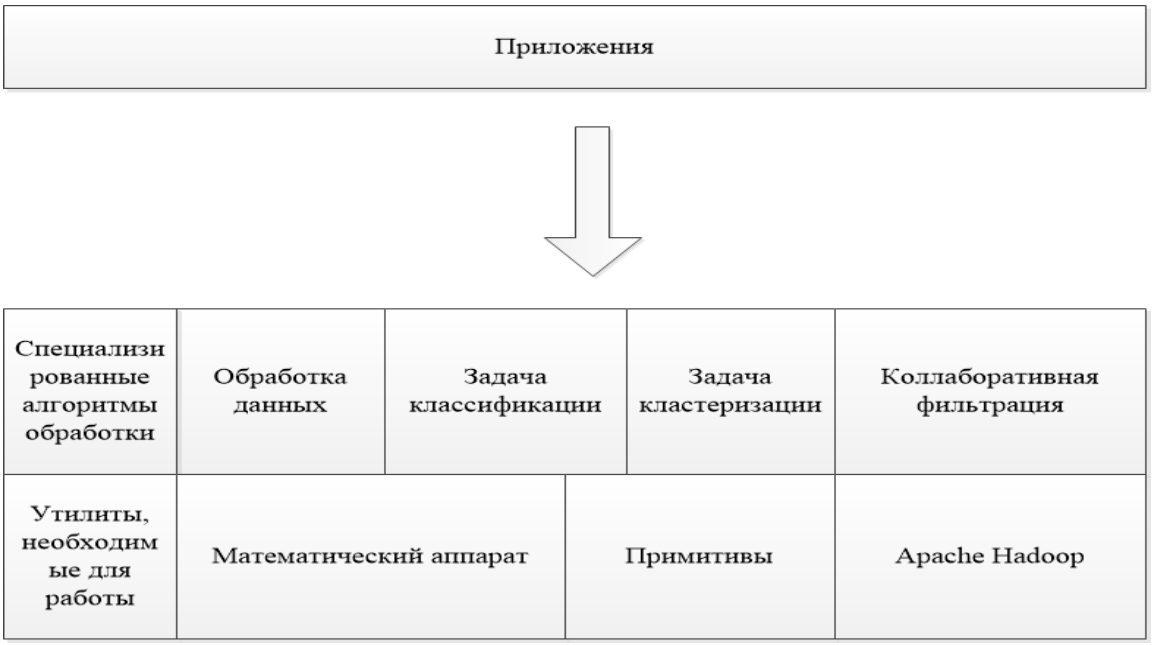


Рис. 1. Типовая архитектура Mahout

Технология Apache Mahout реализует задачу классификации и кластеризации, используя различные подходы и методы [1]:

1. Dirichlet-кластеры. Процесс Дирихле – это распределение вероятностей, диапазон которого сам по себе является набором распределений вероятностей. Он часто используется в байесовском алгоритме для описания предшествующих знаний о распределении случайных величин, то есть насколько вероятно, что случайные переменные распределены в соответствии с тем или иным конкретным распределением.

2. Mean-Shift. Среднее смещение является независимым от приложения инструментом, подходящим для анализа реальных данных. Не принимает какой-либо предопределенной формы в кластерах данных. Он способен обрабатывать произвольные объемы признаков.

3. K-Means. Входящий вектор разбивается на заранее определенное количество k- кластеров, в зависимости от геометрического расстояния между признаками.

4. Canopy. Он предназначен для ускорения операций кластеризации на больших наборах данных, где использование другого алгоритма напрямую может быть нецелесообразным из-за размера набора данных.

Преимущества Apache Mahout [2]:

1. Библиотека является бесплатной и открытой. Алгоритмы решают задачи кластеризации, классификации и коллаборативной (совместной) фильтрации. Решаемые задачи относятся к задачам искусственного интеллекта.

2. Функционал Mahout позволяет реализовывать алгоритмы машинного обучения сразу на нескольких машинах.

3. Является java библиотекой. Фреймворк, предназначенный для использования и адаптации под свои системы разработчиками. Что заметно облегчает эксплуатацию и установку данной системы.

WEKA – представляет собой набор алгоритмов машинного обучения, которые можно применять непосредственно к набору данных или вызывать из собственного кода Java. Weka содержит инструменты для предварительной обработки данных, классификации, регрессии, кластеризации, правил ассоциации и визуализации.

Чтобы классифицировать набор данных на основе характеристик атрибутов, Weka использует классификаторы. **Кластеризация:** вкладка кластера позволяет пользователю идентифицировать сходства или группы вхождений в наборе данных. Кластеризация может предоставить данные для анализа пользователем. Учебный набор, процентное разделение, поставляемый набор тестов и классы используются для кластеризации, для которой пользователь может игнорировать некоторые атрибуты из набора данных в зависимости от требований. Доступные схемы кластеризации в Weka: k-Means, EM, Cobweb, X-means и FarthestFirst. **Ассоциация:** Единственная доступная схема для ассоциации в Weka - это алгоритм Apriori. Он определяет статистические зависимости между кластерами атрибутов и работает только с дискретными данными. Алгоритм Apriori вычисляет все правила, имеющие минимальную поддержку и превышающие заданный уровень достоверности. **Выбор атрибутов. При выборе** атрибутов просматриваются все возможные комбинации атрибутов в данных, чтобы решить, какой из них лучше всего подходит для требуемого расчета - какой набор атрибутов лучше всего подходит для прогнозирования. Метод выбора атрибута состоит из двух частей:

1. Метод поиска: Best-first, прямой выбор, случайный, исчерпывающий, генетический алгоритм, алгоритм ранжирования
2. Метод оценки: на основе корреляции, обертка, получение информации.[3]

Визуализация: пользователь может увидеть последний фрагмент головоломки, полученный на протяжении всего процесса. Он позволяет пользователям визуализировать двумерное представление данных и используется для определения сложности проблемы обучения. Мы можем визуализировать отдельные атрибуты (1D) и пары атрибутов (2D), а также вращать 3D-визуализации в Weka. У него есть опция Jitter для работы с номинальными атрибутами и для обнаружения «скрытых» точек данных.

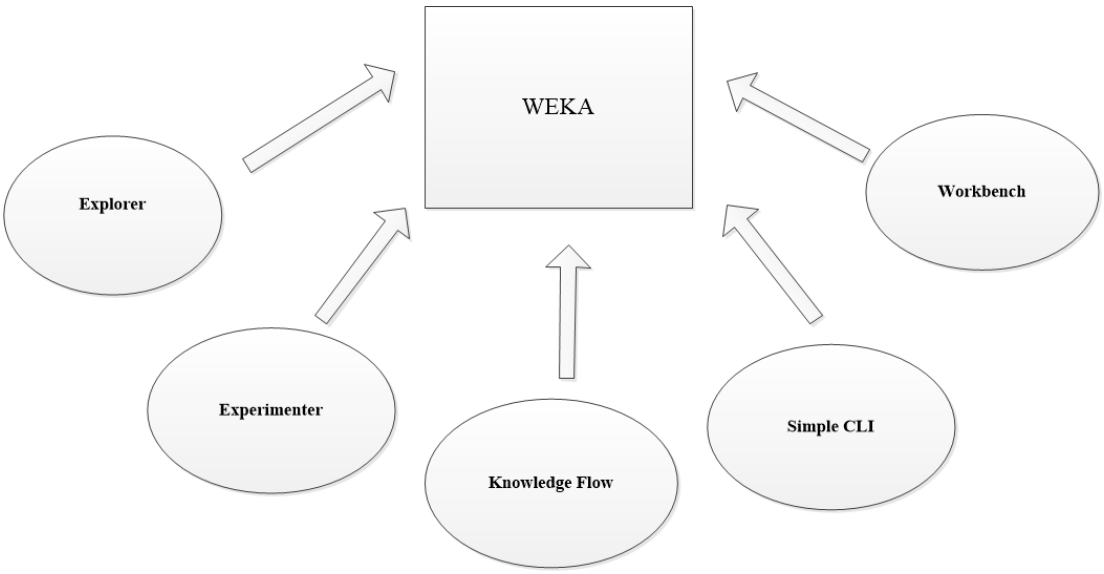


Рис. 2. Состав WEKA

На рис. 2 представлено структурное описание технологии WEKA:

1. **Explorer.** Интерфейс для выполнения задач интеллектуального анализа данных на необработанных данных.
2. **Experimenter.** Позволяет пользователям выполнять различные экспериментальные варианты наборов данных.
3. **Knowledge.** Поддерживает пошаговое обучение, основанное на предыдущих результатах исследований.
4. **Simple CLI.** Интерфейс командной строки, необходимый для отображения терминальных команд.
5. **Workbench.** Соединяет все интерфейсы в единое приложение.

Основные преимущества WEKA:

1. Независимая платформа.
2. Бесплатное ПО. Предоставляемые ей алгоритмы и технологии являются open stack.
3. Графический интерфейс пользователя позволяет повысить оперативность обучения начинающих специалистов и упростить пользовательский интерфейс.
4. Различные алгоритмы машинного обучения и обработки данных.

Подводя итог, можно сделать вывод, что оптимальных алгоритмов не существует, каждая технология и реализуемый в ней алгоритм имеет свои преимущества и недостатки, оценивая соотношение которых лицо, принимающее решение, выбирает наилучшую технологию для решения задач, поставленных перед ним. Современная информационная безопасность сталкивается с рядом сложностей, среди которых следует назвать огромные потоки событий, снижение экспертизы и нехватку персонала. При этом число атак растет, несмотря на принимаемые меры защиты. В настоящее время средний период необнаружения угроз составляет около 200 дней [4], что становится результатом реактивности используемых защитных средств. Поэтому сегодня, как никогда, важно

применять новые методы борьбы с вредоносной активностью, самым перспективным из которых представляется машинное обучение.

Список литературы

1. Макеев, С. М. Исследование возможностей применения модуля Apache Spark для интеллектуальной обработки разнородных данных / С. М. Макеев, А. А. Воробьев, Е. В. Грушевая // Известия Тульского государственного университета. Технические науки. Тула. – 2019. Вып. 3 – С. 254–262
2. Vorobiev, A. A. Method of configuring modules for collection, storage and processing of big data on the basis of free software / A. A. Vorobiev, S. M. Makeev, E. V. Grushevaya, O. D. Mysin, V. V. Shnibaev // Modern informatization problems in the technological and telecommunication systems analysis and synthesis (MIP-2019'AS): Proceedings of the XXIV-th International Open Science Conference (Yelm, WA, USA, January 2019) / Editor in Chief Dr. Sci., Prof. O.Ja. Kravets. – Yelm, WA, USA: Science Book Publishing House, 2019. – P. 382–387
3. S. Owen, R. Anil Mahout in Action: P. 54–213
4. S. A. Svetlana, Machine Learning with WEKA
5. Chandramani T., Learning Apache Mohout: P. 123–178

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

Макеев Сергей Михайлович, *к.т.н., сотрудник*
Лебедев Илья Владимирович, *сотрудник*
Академия ФСО России
Россия, г. Орёл,
e-mail: Maksm57@yandex.ru

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В СИТУАЦИОННЫХ ЦЕНТРАХ

Рассмотрены существующие на сегодняшний день способы защиты информации в ситуационных центрах, включая организационные, технические и программные методы, а также представлены конкретные предложения для решения актуальных задач информационной безопасности.

В настоящее время ситуационные центры (СЦ) все активнее внедряются в работу во многих регионах страны [1]. Одной из насущных проблем при рассмотрении данной технологии является создание комплекса средств защиты информации от угроз различного типа. Особенно остро встает вопрос, когда речь идет о конфиденциальных данных. В большинстве случаев для полного информационного охвата проблемной области и принятия грамотного и обоснованного решения необходима информация, содержащая конфиденциальные данные [2].

Одновременно с ростом ситуационных центров по всей территории страны, растет и количество угроз безопасности, в частности информационной безопасности. К злоумышленникам относятся объекты от продвинутых хакеров до спецслужб других государств. СЦ не являются хранилищем секретных документов, и зачастую нет необходимости использовать такие документы в повседневной деятельности центра. Но иногда в случаях чрезвычайных ситуаций происходит обмен и использование оперативной информации, которая в дальнейшем может стать неподлежащей разглашению.

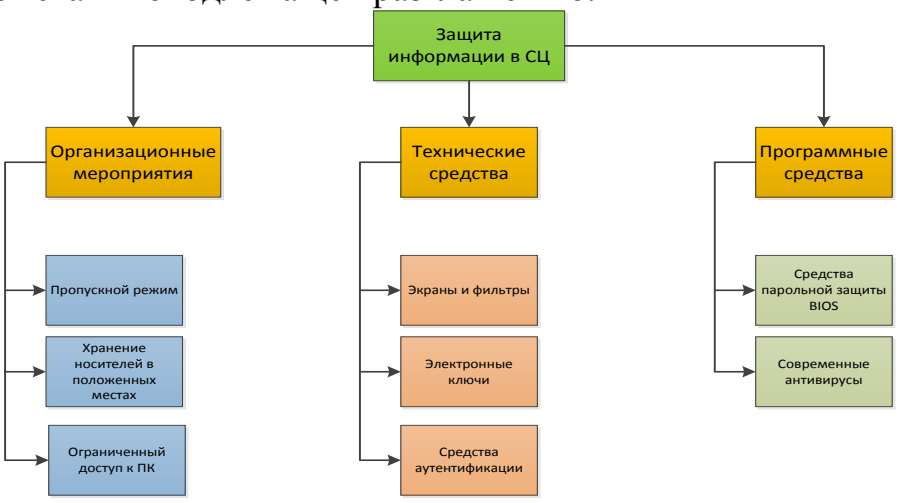


Рис. 1. Методы защиты информации

Для сохранности информации необходимо предпринять организационные меры, не позволяющие посторонним лицам проникнуть на объект обработки информации; технические, не позволяющие перехватить информацию с помощью технических средств, а также программные, которые надёжно защитят объекты информатизации. Только при использовании всех этих мер, представленных на рис. 1, можно говорить об информационной защищенности СЦ.

Очевидно, что для надежности функционирования системы необходимо проанализировать все возможные атаки на ситуационный центр, начиная от аппаратных закладок в устройствах, применяемых для построения системы распределенных ситуационных центров (СРСЦ) и заканчивая облачными сервисами. Для обеспечения полной защиты СЦ желательно использовать собственную элементную базу, поскольку у иностранных производителей всегда остается возможность получить доступ к данным и системам. На этапе развития производства аппаратных средств практически невозможно перейти к полной замене импортных товаров на отечественные, но существует необходимость увеличивать степень импортозамещения. В этих условиях большое распространение получили программные комплексы "Соболь", имеющий ряд преимуществ: простота в установке, наличие сертификатов ФСБ, поддержка различных операционных систем. Также большое количество программно-аппаратных средств для комплексной защиты СЦ имеется в арсенале компании "Код безопасности" [3].

Что касается, программной поддержки, то для обработки информации, требующей защиты и содержащей разные уровни конфиденциальности, целесообразно использовать различные виртуальные машины для разных уровней защищенности, гарантируя тем самым разделение систем на уровне гипервизора. Сегодня уже имеются российские разработки гипервизоров, которые обеспечивают приемлемый уровень разделения контуров безопасности, обрабатывающих данные различной категории секретности, в частности одна из разработок компании "Криптософт" QP ОС [3].

В качестве организационных мер имеется необходимость создания выделенного СЦ, который будет осуществлять функцию контроля корректности обработки информации в СРСЦ и всех ее компонентов. Такая необходимость обусловлена в первую очередь для того, чтобы отражать все совершенные атаки на систему, прогнозировать их в дальнейшем и на основе анализа совершенных атак и угроз создавать системы для эффективной защиты СРСЦ. Этим целесообразно заняться российской системе реагирования на кибератаки “ГосСОПКА”. Эта организация должна выполнять ряд обязанностей, таких как:

- разрабатывать правила работы с компьютерной техникой и конфиденциальной информацией;
- проводить периодические проверки персонала;
- разграничивать зоны ответственности, чтобы исключить ситуации, когда массивы наиболее важных данных находятся в распоряжении одного из сотрудников;
- внедрять программные продукты, которые защищают данные от копирования или уничтожения любым пользователем;

- составлять планы восстановления системы на случай выхода из строя.

Специфика задач СЦ диктует свои особенности функционирования всей системы и порождает ряд задач, которые необходимо решать в целях обеспечения информационной безопасности системы. На сегодня эти задачи стали наиболее актуальными в связи с необходимостью обработки конфиденциальных данных. К таким задачам относятся:

1. Создание единой защищенной линии обмена информацией, в том числе между различными ведомствами.
2. Безопасное хранение информации внутри СЦ, учитывая все требования ФСБ и ФСТЭК. Здесь необходимо учитывать технические и организационные меры защиты информации.
3. Сегментирование защищаемых ресурсов СЦ. Это решение считается одним из доверенных механизмов защиты накопительных информационных систем с большими объемами разнородной поступающей информации.

Список литературы

1. Ильин, Н. И. Ситуационные центры. Опыт, состояние, тенденции развития / Н. И. Ильин, Н.Н. Демидов, Е. В. Новикова.– М.: МедиаПресс, 2011. – 336 с.
2. Алексеев, Д. С. Ситуационные центры / Д.С. Алексеев. – М.: Компьютерная неделя, 2008. – 97 с.
3. Шаньгин, В. Ф. Комплексная защита информации в корпоративных сетях. – М. : ИД"ФОРУМ" : ИНФА-М, 2010 – 592 с.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

Маркин Дмитрий Олегович, *сотрудник*
Вихарев Антон Николаевич, *сотрудник*
Академия ФСО России
Россия, г. Орёл
e-mail: admin@nikitka.net

СПОСОБ ЗАЩИТЫ СИСТЕМЫ ТУМАННЫХ ВЫЧИСЛЕНИЙ НА ОСНОВЕ ЛУКОВИЧНОЙ ВИРТУАЛИЗАЦИИ АКТИВНЫХ ДАННЫХ

Описана модель системы защиты программного обеспечения от анализа на основе применения виртуальных машин с неизвестной архитектурой и алфавитом байт-кода, а также, применения луковичной архитектуры на передаваемые данные.

Повсеместное внедрение информационных технологий, средств автоматизации и автоматизированных систем в повседневную жизнь, развитие цифровой экономики значительно повышает роль программного обеспечения в современной экономике. В связи с этим недостаточная защищенность программного обеспечения от анализа, нарушения его работоспособности, модификации и других угроз может привести к серьезным неблагоприятным последствиям различного характера. Таким образом, проблема обеспечения защищенности программного обеспечения (ПО) является актуальной и требует применения новых методов и средств, способных обеспечить требуемый уровень защиты в современных условиях.

Проблема защиты программных реализаций на основе применения технологий виртуализации и других методов защиты затрагивалась в научных трудах Аранова В. Ю., Петрова А. С., а также Казарина О. В., Варнавского Н. П., Захарова В. А., Кузюрина Н. Н. и Шокурова А. В., Зегжды П. Д., Бойко В. П., Заборовского В. С., Подловченко Р. И., Иванникова В. П., Сомборсона К., Викстромома Д. и других. В указанных работах отмечалась необходимость защиты программных реализаций от технологий обратной разработки, основанных, в том числе на методах статического и динамического анализа ПО.

Обобщенная схема «атаки» на программную реализацию показана на рис. 1.

Модель нарушителя, используемая в указанной системе защиты, предполагает использование всего инструментального комплекса средства анализа ПО, к которым в настоящее время относятся автоматизированные методы и средства анализа ПО: в области статического анализа основанные на методах компьютерной лингвистики (SVACE, АК-ВС, AppChecker. OWASP, АИСТ-С и др.), динамического – методах динамической бинарной инструментации (DBI – dynamic binary instrumentation) (PIN, Frida, DinamoRIO, Valgrind и др.), а также средства фаззинга и профилирования ПО.

Кроме того, нарушитель (исследователь) имеет полный доступ к ресурсам (ЦП, ПЗУ, ОЗУ, устройства ввода/вывода и т. п.), ПО и ОС данной ПЭВМ, на которой реализуется указанная схема исследования; способен создавать копии исследуемого экземпляра ПО агента и активных данных.

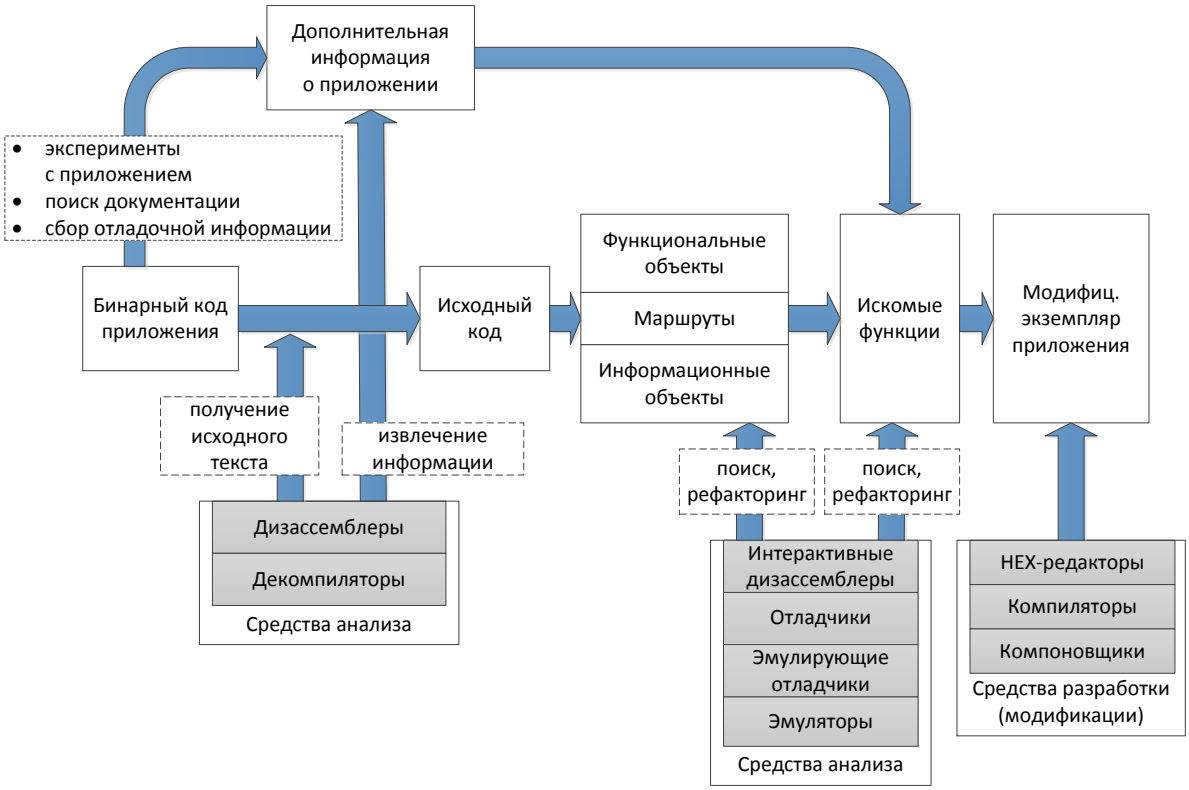


Рис. 1. Схема исследования и модификации экземпляра приложения

Схема формирования байт-кода X_B с учетом его алфавита K_B и архитектуры виртуальной машины K_{VM} представлена на рис. 2.

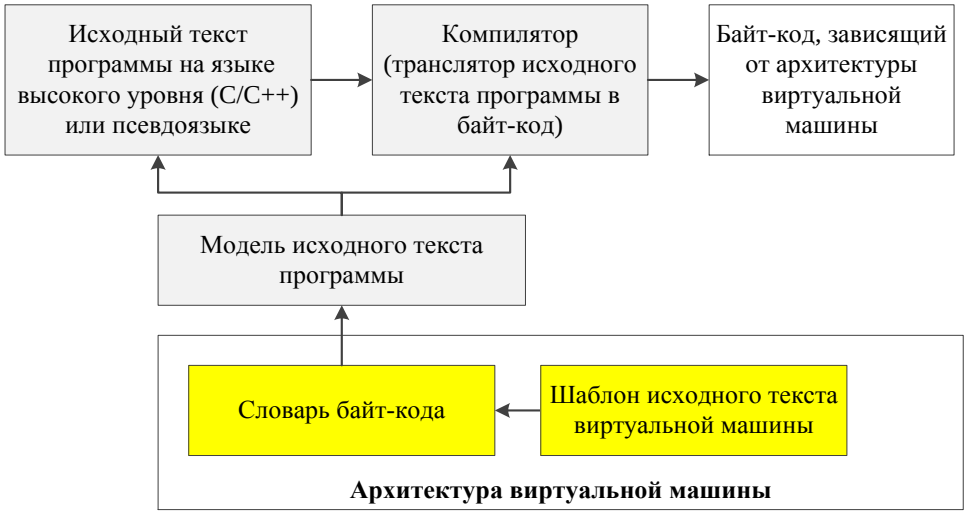


Рис. 2. Схема формирования байт-кода виртуальной машиной

В свою очередь, исполняемый машинный код виртуальной машины также должен быть сформирован с учетом используемого словаря байт-кода $(K_X, K_B) \subset K$, а также избранной архитектуры виртуальной машины K_{VM}. С учетом изложенного схема формирования виртуальной машины будет выглядеть как представлено на рис. 3.

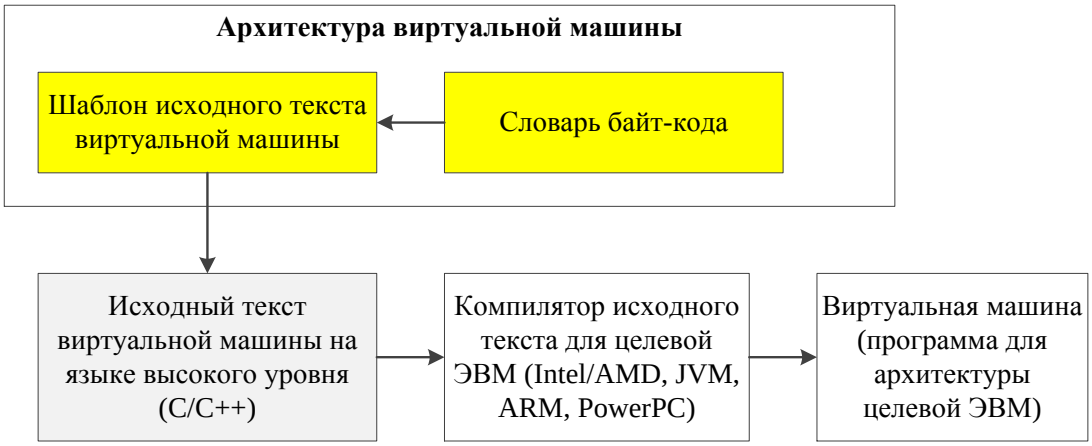


Рис. 3. Схема формирования виртуальной машиной

Суть предлагаемого решения заключается в том, что каждый экземпляр реализации виртуальной машины и исполняемый на нем байт-код являются уникальными, строго соответствующими друг другу. Иными словами, байт-код и виртуальная машина, сформированные с использованием разных ключей $K = (K_X, K_B, K_{VM})$ будут несовместимы.

Обобщенная схема программной реализации такой криптосистемы представлена на рис. 4.

На рисунках 2-4 секретным ключом являются:

- словарь байт-кода bytecode.json;
- архитектура виртуальной машины vm-template.cpp и получаемая на ее основе виртуальная машина vm.cpp.

Процедуру формирования vm.cpp можно описать отображением

$$F \xrightarrow{E_F(K_{VM}, K_B)} F_{VM},$$

или $F_{VM} = E_F(F, K_{VM}, K_B)$.

Процедуру формирования байт-кода, способного выполняться только в заданной виртуальной машине, можно описать отображением

$$X \xrightarrow{E_B(K_X, K_B)} X_B,$$

или $X_B = E_B(X, K_{VM}, K_B)$.

Таким образом, представленная криптосистема обеспечит получение выходных данных $Y' = Y$, где $Y' = F_{VM}(X_B)$, а $Y = F(X, K)$, а $(E_B, E_F) \in E$, но при

это процесс анализа экземпляра программной реализации $F_{VM}\left(X_B\right)$ по сравнению с реализации $F\left(X,K\right)$ будет значительно затруднен.

Таким образом, сущность защиты программного кода на основе обфускации с использованием виртуальных машин заключается в том, чтобы заставить исследователя перейти от анализа машинных инструкций известной архитектуры (например, x86) к незнакомому набору виртуальных команд, которые увеличат сложность и, соответственно, затрачиваемое время на анализ защиты.

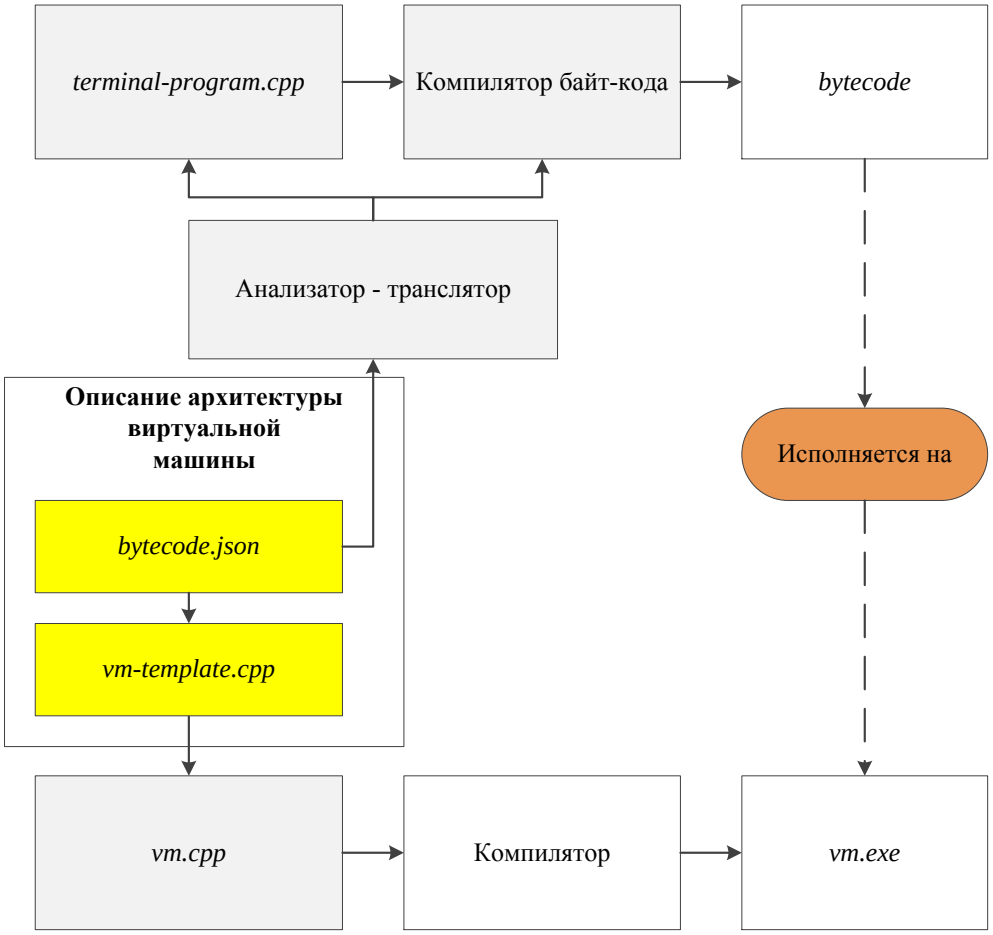


Рис. 4. Структурная схема программной реализации криптосистемы на основе виртуальных машин

Для обеспечения защиты от компрометации активных данных предлагается использовать луковичную архитектуру активных данных.

<table>
<tr><td rowspan="6">IP заголовок для узла № 1</td><td colspan="5">Зашифровано на открытом ключе (ОК) узла № 2</td></tr>
<tr><td rowspan="5">IP заголовок для узла № 2</td><td colspan="4">Зашифровано на ОК узла № 3</td></tr>
<tr><td rowspan="4">IP заголовок для узла № 3</td><td colspan="3">Зашифровано на ОК узла № 4</td></tr>
<tr><td rowspan="3">IP заголовок для узла № 4</td><td colspan="2">Зашифровано на ОК получателя</td></tr>
<tr><td>IP заголовок для получателя</td><td>Данные приложения с HTTP и TCP заголовоком</td></tr>
</table>

Рис. 5. Структура данных, предаваемых через луковичную архитектуру инфотелекоммуникационной сети

В рассматриваемой в работе несимметричной криптосистемы процесс зашифрования на открытом ключе эквивалентен процессу трансляции (отображению) E_B защищаемого исходного текста X в байт-код X_B:

$$X \xrightarrow{E_B(K_X, K_B)} X_B,$$

или $X_B = E_B\left(X, K_{VM}, K_B\right)$, где K_X – множество подстановок, определяющих соответствие между элементами множества X и элементами множества X_B – элементы алфавита байт-кода (словаря байт-кода); K_B – множество подстановок, определяющих соответствие между инструкциями или операциями (правилами преобразования) из множества F (множество инструкции исходного текста защищаемого приложения) и элементами подмножества F_{VM} – элементы алфавита байт-кода (словаря байт-кода), используемые в виртуальной машине.

При этом открытым ключом является словарь байт-кода K_X, а закрытым – архитектура виртуальной машины, скомпилированная на основе того же словаря байт-кода $\left(K_X, K_B\right) \subset K$.

Исходя из изложенных предложений, предлагается модифицировать структуру данных, так, как показано на рисунке 6.

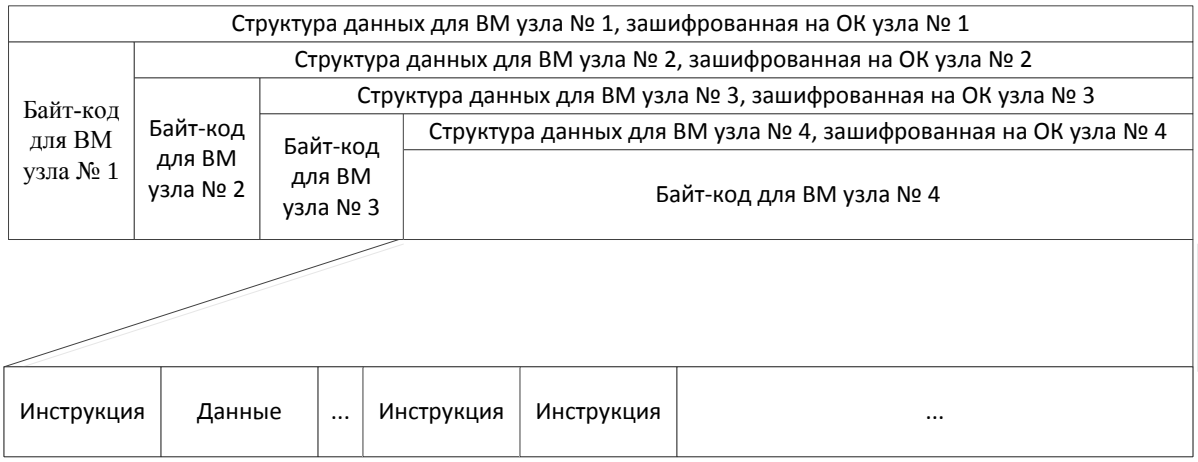


Рис. 6. Модифицированная структура активных данных, предаваемых через луковичную архитектуру системы туманных вычислений

Предложенный способ защиты системы туманных вычислений позволяет защитить программные реализации ПО агентов системы от обратной разработки, а также обеспечить защиту всей системы от компрометации отдельных указанных реализаций.

Список литературы

1. Петров, А. С. Методы защиты программного кода / А. С. Петров, А. А. Петров // Системы обработки информации. – 2010. – Вып. 3 (84). – С. 68–71.

2. Петров, А. С. Технология защиты программного кода посредством применения виртуальной машины / А. С. Петров, А. А. Петров // Вестник ВНУ. – 2009. – № 9 (103), часть 1. – С. 117-122.

3. Аранов, В. Ю. Метод и средства защиты исполняемого программного кода от динамического и статического анализа : автореф. дис, … канд. техн. наук : 05.13.19 / Аранов Владислав Юрьевич. – Санкт-Петербург, 2014. – 18 с.

4. Kaiyuan Kuang Enhanced virtual-machine-based code obfuscation security through dynamic bytecode scheduling / Kaiyuan Kuang, Zhanyong Tang, Xiaoqing Gong, Dingyi Fang, Xiaojiang Chen, Zheng Wang // Computers & Security. – 2018. – № 74. – P. 202–220.

5. Garlic Routing and "Garlic" Terminology // Garlic Routing : web-site. 2015. URL: https://geti2p.net/en/docs/how/garlic-routing. Access date: 08.10.2015.

6. Barak B., Goldreich O., Impagliazzo R., Rudich S., Sahai A., Vadhan S., Ke Yang. On the (im)possibility of obfuscating programs // Advances in Cryptology – CRYPTO'01, Lecture Notes in Computer Science, v. 2139, 2001, p. 1-18 (см. также Journal of the ACM 2012).

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.492.3

Маркин Дмитрий Олегович, *сотрудник*
Зверев Артем Александрович, *сотрудник*
Академия ФСО России
Россия, г. Орёл,
e-mail: admin@nikitka.net

АЛГОРИТМ И ПРИЛОЖЕНИЕ АДАПТИВНОГО ФАЗЗИНГА ВЕБ-ПРИЛОЖЕНИЙ

Рассматривается фаззер, осуществляющий тестирования на основе создания информационной модели тестируемого веб-ресурса.

Повсеместное внедрение информационных технологий, развитие цифровой экономики, а также повышение доступности и цифровизация государственных услуг обуславливает потребность в повышенном внимании к информационной безопасности предоставляемых услуг в целом и обеспечении защищенности веб-ресурсов, в частности. Как показывает статистика, современные веб-приложения имеют большое число проблем, связанных с обеспечением информационной безопасности, а поиск уязвимостей требует серьезных вычислительных ресурсов и высокой квалификации персонала, отвечающего за вопросы информационной безопасности. В связи с этим актуальной задачей является создание автоматизированных и автоматических средств поиска уязвимостей веб-приложений, позволяющих осуществлять эффективный анализ защищенности веб-ресурсов.

Одним из эффективных способ решения данной задачи является фаззинг веб-приложений [1, 2]. Данный метод тестирования представляет собой тестирование на основе модели «черного» ящика (в условиях отсутствия сведений о приложении) или в отдельных случаях модели «серого» ящика (о веб-приложении имеется некоторая информация). Фаззинг может использоваться и в условиях модели «белого» ящика (при наличии полной информации о приложении) как эффективное средство тестирования корректности обработки входных данных.

Полученный от приложения-объекта ответ может содержать различные данные о том, какое влияние оказал изначальный фаззинговый запрос [3]. Хотя не вполне реально вручную подробно разобрать все ответы веб-сервера, остается надежда на то, что некие части ответа будут содержать информацию об аномальном явлении. При запуске фаззера существование ошибки может быть отражено в следующих полях информации:

- коды статуса HTML
- имеющиеся в ответе сообщения об ошибке
- имеющиеся в ответе данные, введенные пользователем
- снижение эффективности

- перерывы в запросах
- сообщения фаззера об ошибке
- обработанные и необработанные исключения

На сегодняшний день существует множество фаззеров для веб-приложений: Web Scarab, BurpSuite, Skyfish, SPIKE Proxy, OWASP WSFuzzer (SOAP), Rfuzz, Fuzzops, PowerFuzzer, w3af, WebFuzz. Однако данные средства имеют ряд недостатков. Существенной проблемой при построении эффективного фаззера веб-приложений является отсутствие средства автоматизированного создания модели веб-ресурса, на основе которой могли бы формироваться исходные данные для фаззинга.

Для эффективного фаззинга необходимо выполнение следующих требований: возможность неоднократного использования; состояние и глубина процесса; отслеживание, покрытие кода и система показателей; определение ошибок; ресурсные ограничения. Схема фаззинга с обратной связью и интеллектуальным формированием входных данных представлена на рис. 1.

Рис. 1. Схема фаззинга с обратной связью при формировании входных данных

Представленный вариант автоматического фаззинга позволяет повысить эффективность анализа объекта тестирования за счет адаптивного формирования входных данных. Для моделирования данного процесса необходимы специальные средства моделирования, способные формализовать все аспекты случайности и предоставить инструменты реализации всех этапов управления тестированием. Байесовские модели имеют широкий потенциал средств для решения перечисленных выше задач тестирования веб-приложений [5].

На рис. 2 приведена концептуальная модель статических и динамических байесовских сетей для моделирования процесса управления тестированием веб-приложений методом фаззинга.

Чем более качественно будут формироваться входные данные для очередной итерации тестирования, тем выше вероятность обнаружения ошибок либо недекларируемых возможностей. В то же время, большинство современных фаззеров построено на основе базы данных известных сигнатур разрушающих программных воздействий и практически не учитывают

актуальную модель исследуемого объекта. Наличие такой модели позволяет учитывать важную информацию при формировании очередной выборки входных данных и, соответственно, повышает результативность фаззинга. С учетом предложенного подхода схема фаззинга [2] будет выглядеть так, как показано на рис. 3.

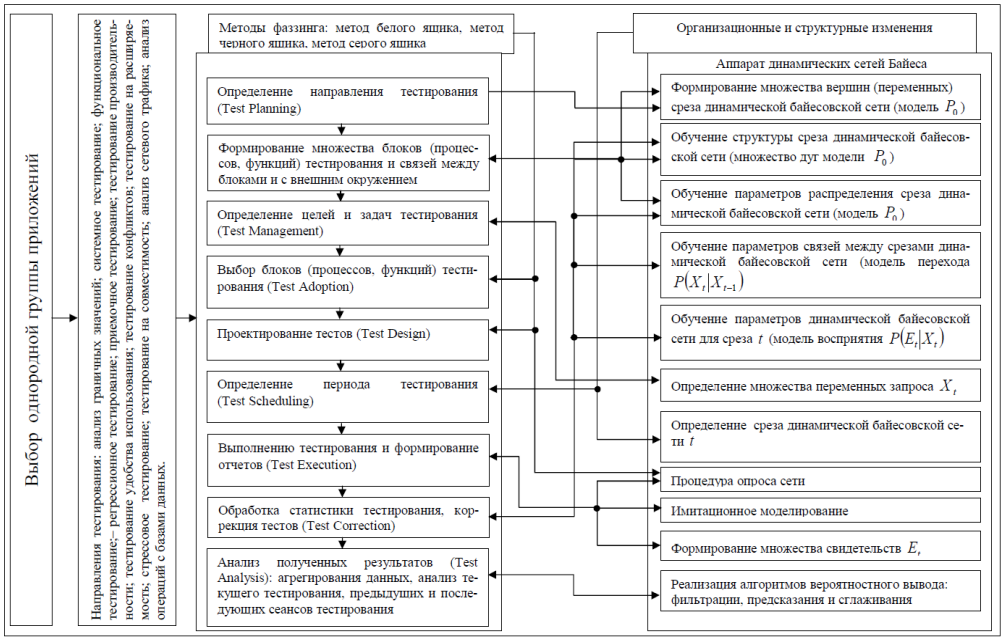


Рис. 2. Концептуальная модель применения аппарата ДБС в процессе управления тестированием веб-приложений

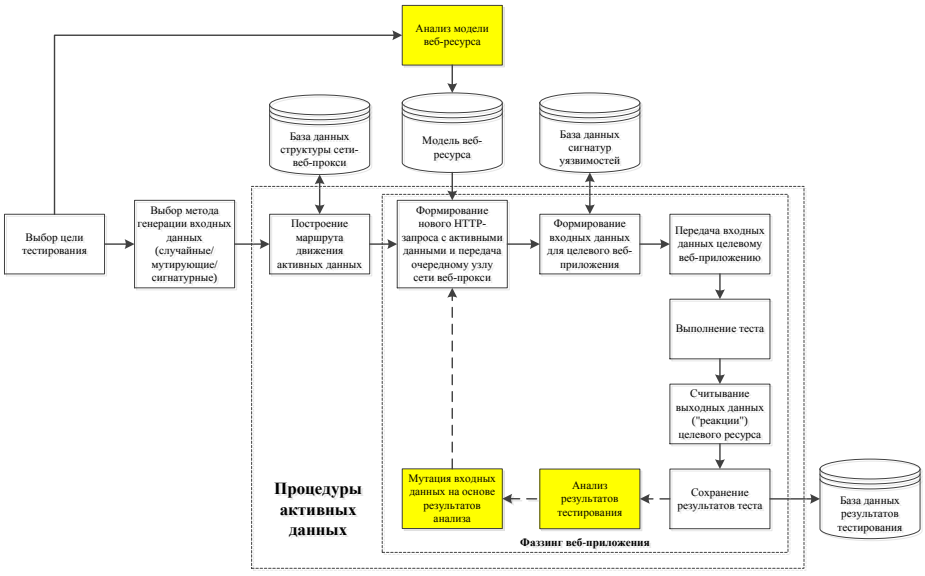


Рис. 3 Схема фаззинга с обратной связью и модель веб-ресурса

В данной схеме для формирования входных данных дополнительно используются данные описания модели веб-ресурса, подготовленные на предварительном этапе средством анализа, которое фактически формирует «индекс» веб-ресурса.

С задачей создания модели веб-ресурса можно справиться с помощью фреймворка для сбора данных, имеющего название "scrapy". Scrapy – одна из наиболее популярных и производительных библиотек Python, которая включает в себя большинство общих функциональных возможностей. Она позволяет создать на своей основе поисковый робот с функциями выполнения GET-запросов, извлекания данных из HTML-документа, обработки и экспортирования полученных данных, предназначенный для перебора страниц Интернета с целью занесения информации о них в базу данных. Примерная структурно-логическая модель данных описания модели веб-ресурса представлена на рис. 4.

Рис. 4. Структурно-логическая модель данных описания модели веб-ресурса

С учетом представленных схем общая структурная схема адаптивного фаззера на основе сети веб-прокси-серверов [4, 5] может выглядеть так, как показано на рис. 5.

Темным цветом на рисунке выделены элементы адаптивного фаззера веб-приложений. Совокупность данных элементов и связи между ними представляет собой автоматизированную системы адаптивного фаззинга веб-приложений, позволяющего анализировать уязвимости целевого тестируемого веб-ресурса с учетом его структуры. Управление данным средством тестирования может осуществляться через веб-интерфейс за счет изменения конфигурационной информации в базе данных.

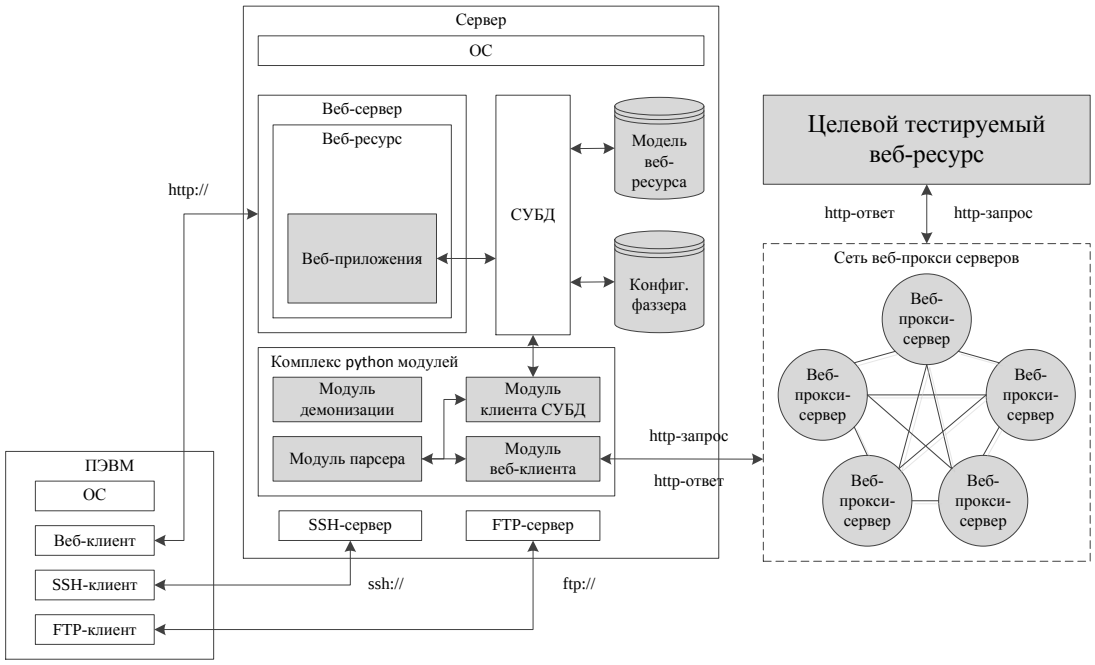


Рис. 5. Структурная схема адаптивного фаззера на основе сети веб-прокси-серверов

Разработка и эксплуатация представленной системы автоматизированного адаптивного фаззинга позволит повысить эффективность поиска и анализа уязвимостей веб-ресурсов с целью выбора и оптимизации средств их защиты от разрушающих программных воздействий.

Список литературы

1. 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.

2. Маркин, Д. О. Распределенное тестирование веб-приложений методом фаззинга на основе технологий веб-прокси и активных данных // Д. О. Маркин, А. С. Галкин // Труды Северо-Кавказского филиала Московского технического университета. – Ростов-на-Дону : ПЦ «Университет» СКФ МТУСИ , 2017. – Ч. 2. 442 с. – С. 61-72.

3. Саттон М., Грин А., Амини П. Fuzzing: исследование уязвимостей методом грубой силы: [пер. с англ.]. – СПб.: Символ-Плюс, 2009. – 560 с.

4. 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.

5. Полухин П.В. Байесовские модели и алгоритмы управления процессом тестирования веб-приложений методом фаззинга: дис. 05.13.18 / Полухин Павел Валерьевич. Воронеж, 2016. 180 с.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.272

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

АЛГОРИТМ РЕШЕНИЯ ЗАДАЧИ ФАКТОРИЗАЦИИ СРЕДСТВАМИ ТУМАННЫХ ВЫЧИСЛЕНИЙ

Обоснована необходимость использования туманных вычислений для решения вычислительно сложных задач, предложена схема инфраструктуры сети мобильных устройств, разработана схема клиент-серверного взаимодействия, определен алгоритм функционирования серверного приложения на примере решения задачи факторизации и база данных.

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) [1]. 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 алгоритм решения задачи факторизации средствами туманных вычислений. 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 рас-

пространенными 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).

В данной работе рассматривается задача, актуальная для систем, использующих криптографические протоколы.

Была разработана структура сети, обеспечивающая оптимальное функционирование вышеобозначенного алгоритма. Данная структура представлена на рис. 1.

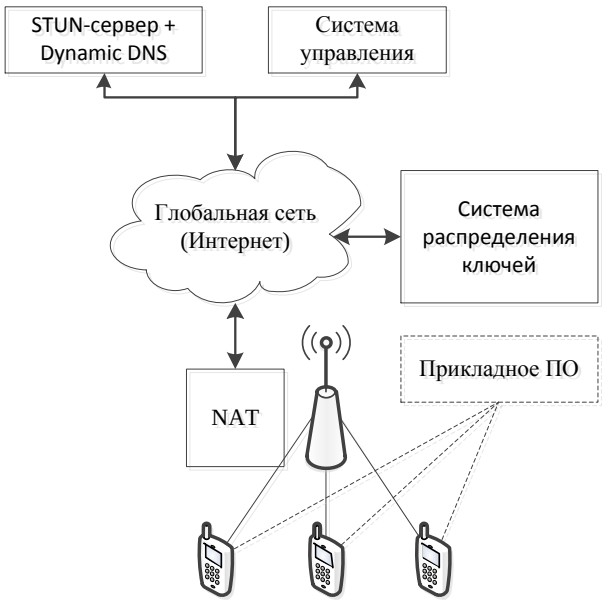


Рис. 1. Типовая структурная схема инфраструктуры сети мобильных устройств

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 применения 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.

Разработка алгоритма системы управления сетью МАУ

Для решения данной задачи был разработан алгоритм параллельных вычислений, который представлен на рис. 2.

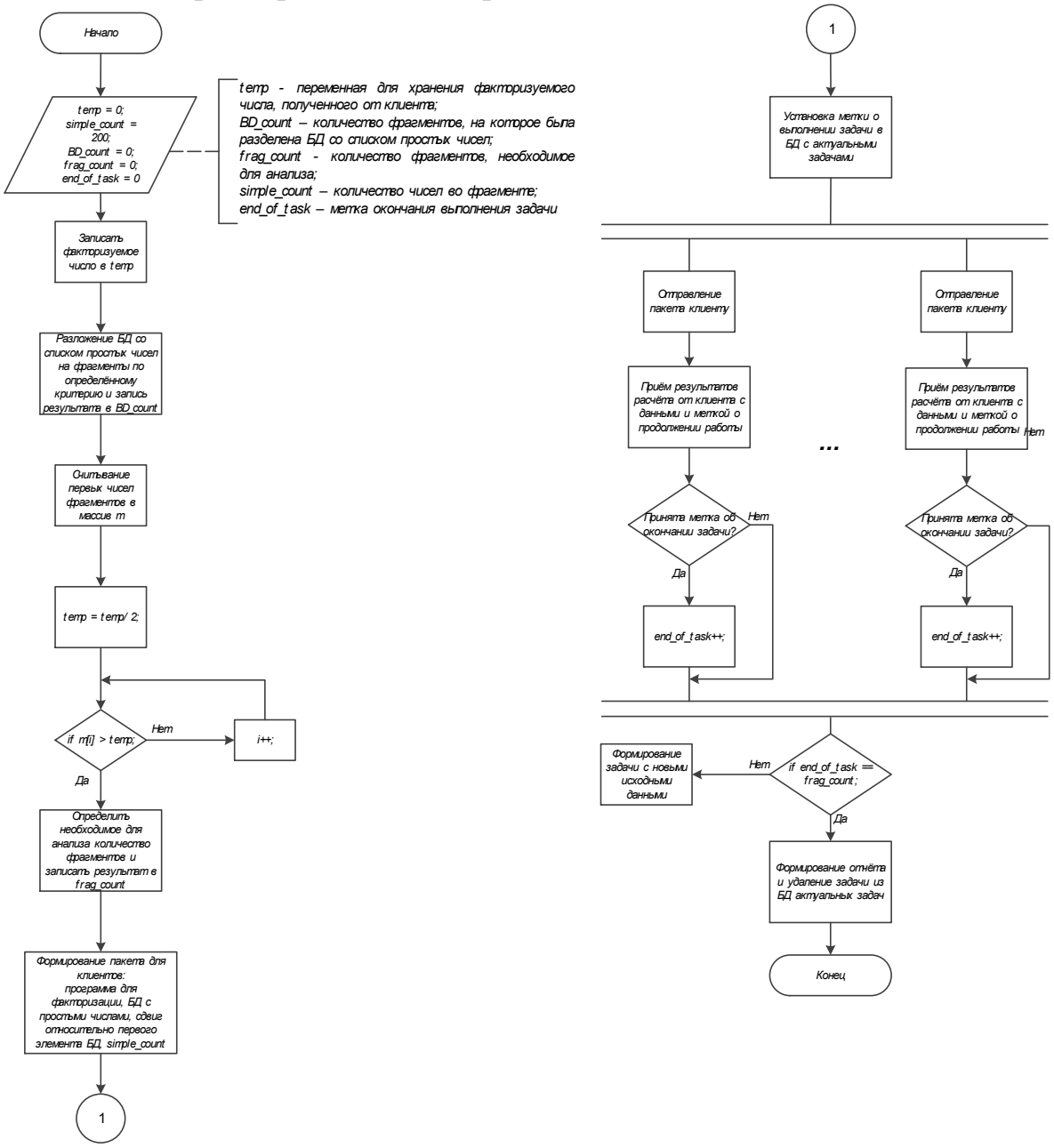


Рис. 2. Блок-схема распределенного алгоритма факторизации

Для обеспечения функционирования системы необходимо структурированное хранение данных, учет вычислительных операций и отчетов об их исполнении. Типовая структурно-логическая схема базы данных, необходимая для решения данной задачи, представлена на рис. 3.

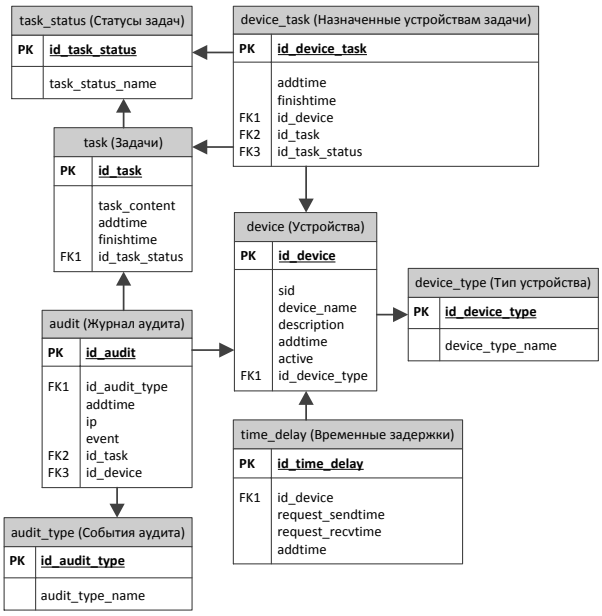


Рис. 3. Структурно-логическая схема базы данных системы туманных вычислений

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, то 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

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

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

3. 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.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

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

МЕТОДИКА РАЗВЕРТЫВАНИЯ ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ДИНАМИЧЕСКОГО АНАЛИЗА 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 в случае возникновения острых конфликтов возможны внешние воздействия на данное оборудования в целях 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: дизассемблеры, отладчики, средства виртуализации 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.

Для анализа системного программного обеспечения телекоммуникационного оборудования компании *Cisco System* был разработан лабораторный стенд, схема которого представлена на рис. 1.

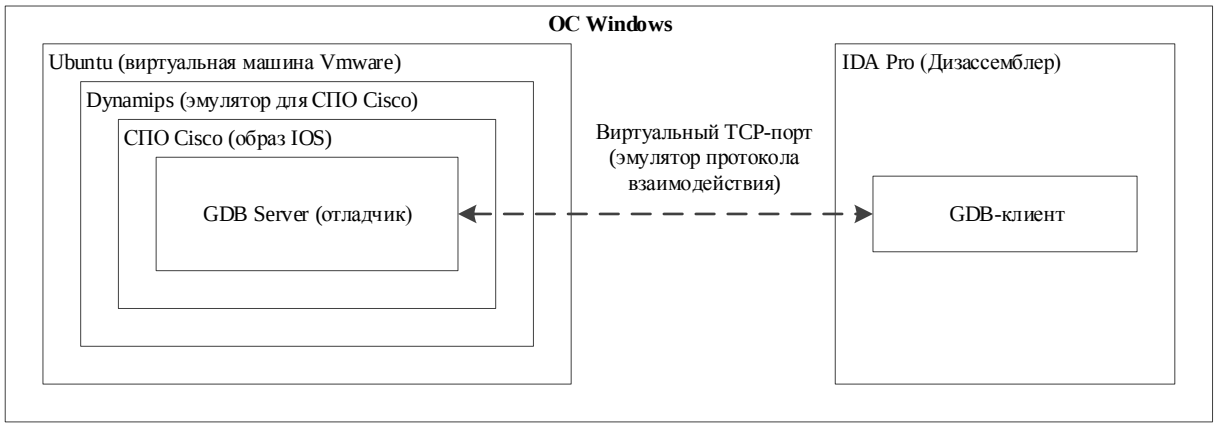


Рис. 1. Схема лабораторного стенда

В состав лабораторного стенда входят:

- виртуальная машина с ОС *Ubuntu*;
- *dynamips* (Эмулятор сетевого оборудования семейства *CISCO*);
- *IDA Pro* (Дизассемблер);
- образ СПО *CISCO*.

Подготовка лабораторного стенда на основе виртуальной машины с образом ОС *Ubuntu* необходимо осуществлять в следующей последовательности:

1. Создать виртуальную машину на основе ОС *Ubuntu*. В данной ОС будет осуществляться основная работа.

2. Загрузить дистрибутивы для дальнейшей разборки, отладки и сборки образа: *dymanips*, *putty*, *radare2*, *net-tools*, *uml-utilities* и *hexedit*.

3. Войти в систему:

1) для активации входа от имени пользователя курсор мыши необходимо навести на имя пользователя, нажать правую кнопку мыши;

2) осуществить ввод пароля.

4. После входа в систему для обеспечения быстрого доступа к стенду необходимо перенести приложение *Terminal* на панель задач:

1) войти в меню приложений;

2) выбрать приложение *Terminal* указателем мыши;

3) зажав левую кнопку, перетащить ярлык приложения *Terminal* на панель задач.

5. Запустить приложение *Terminal*. *Terminal* оповестит об использовании команды *sudo*, необходимой для исполнения команд от имени супер пользователя.

Для дальнейшей работы необходимо использовать суперпользователя, но в *Ubuntu* 18.04 изначально он заблокирован.

6. Чтобы разблокировать суперпользователя, необходимо:

1) задать пароль, использовав следующую последовательность команд:

user@ubuntu:~$ sudo passwd root

2) ввести пароль:

[sudo] password for user:

3) ввести новый пароль *root*-пользователя:

Enter new UNIX password:

4) Подтвердить введенный пароль:

Retype new UNIX password:

Пароль при вводе не отображается.

7. После разблокировки суперпользователя необходимо войти в него с помощью команды:

user@ubuntu:~$ su

8. *Terminal* запрашивает ввод пароля:

Password:

Примечание. При введении пароль не отображается.

Далее работа в *Terminal* осуществляется с правами суперпользователя:

root@ubuntu:/home/user#

9. Осуществить загрузку установочных пакетов (дистрибутивов).

Примечание. Для выполнения данного этапа необходим доступ к хранилищам установочных пакетов (репозиторию) либо используя доступ в сеть Интернет, либо доступ к локальному хранилищу.

Рекомендуемый порядок установки пакетов следующий:

1) установить эмулятор для СПО *Cisco Systems* – приложение *dynamips*;

root@ubuntu:/home/user# apt install dynamips

2) установить средство доступа к удаленным приложениям с использованием протоколов *Telnet, SSH* и д. - приложение *putty*:

root@ubuntu:/home/user# apt install putty

В процессе загрузки появится запрос на подтверждение продолжения загрузки. Подтвердить его введением команды:

Do you want to continue?[Y/n] y

После загрузки и установки приложения *putty* для обеспечения быстрого доступа к нему, перенести приложение на панель задач. Для этого необходимо

- зайти в меню приложений;
- навести указатель мыши на приложение *putty*;
- зажав левую копку, перетащить его на панель задач.

3) установить программное средство настройки сетевой конфигурации – пакет *net-tools*:

root@ubuntu:/home/user# apt install net-tools

4) установить комплекс программных средств настройки виртуального интерфейса для доступа к эмулируемому СПО *Cisco Systems* – пакеты *uml-utilities*:

root@ubuntu:/home/user# apt install uml-utilities

5) установить дизассемблер *radare2*:

root@ubuntu:/home/user# apt install radare2

В процессе загрузки появится запрос на подтверждение продолжения загрузки. Подтвердить его введением команды:

Do you want to continue?[Y/n] y

6) установить шестнадцатеричный редактор данных *hexedit*:

root@ubuntu:/home/user# apt install ht hexedit

Загрузка установочных пакетов (дистрибутивов) завершена.

10. Подготовка образа СПО *Cisco Systems* к дизассемблированию:

1) Открыть в панели задач файл менеджер *Nautilus*.

2) В открытом файле менеджере необходимо выбрать рабочую папку (Пример: *Documents*) и открыть её. В рабочую папку нужно поместить файл образа СПО *Cisco*. Для этого необходимо:

- перейти в хостовую ОС;
- найти файл образа СПО Cisco (*c2600-bino3s3-mz.123-22.bin*);
- выбрать файл СПО *Cisco* указателем мыши;
- зажав левую кнопку, перетащить файл СПО *Cisco* в рабочую папку виртуальной машины.

3) Вернуться в Terminal и перейти в рабочую папку командой:

root@ubuntu:/home/user# cd Documents/

4) Извлечь образ СПО *Cisco* для осуществления отладки с помощью команды:

root@ubuntu:/home/user/Documents# unzip c2600-bino3s3-mz.123-22.bin

В результате разархивирования создается файл *C2600-BI.BIN*.

5) Для создания файла для дизассемблирования нужно воспользоваться копированием файла с помощью команды:

root@ubuntu:/home/user/Documents# cp C2600-BI.BIN C2600-BI.BIN.ida

В результате разархивирования создается файл *C2600-BI.BIN.ida*.

6) Открыть файл для дизассемблирования через *HEX*-редактор командой:

root@ubuntu:/home/user/Documents# hte C2600-BI.BIN.ida

Примечание. Появляется окно с предупреждение нажать Enter.

7) Нажать *F6* для изменения режима отображения.

8) Выбрать режим – *elf/header* с помощью клавиши *Tab*, затем *Enter*.

9) Переместиться стрелками на клавиатуре на строку с именем machine.

10) Нажать *F4* изменить значение 002b на 0014. Для сохранения изменений нажать *F2*. Таким образом изменяется значение архитектуры процессора, которое считывает дизассемблер. Выйти из *HEX*-редактора кнопкой *F10*.

11) Нужно извлечь файл для дизассемблирования. Для этого необходимо:

- перейти в файл менеджер;
- выбрать файл *C2600-BI.BIN.ida* указателем мыши;
- зажав левую кнопку, перетащить файл *C2600-BI.BIN.ida* на хостовую машину.

11. Открыть файл для дизассемблирования с помощью *IDA Pro*.

1) Запустить программу *IDA Pro*.

2) Выбрать на панели программы кнопу *New*.

3) Выбрать файл *C2600-BI.BIN.ida* и нажать открыть.

4) В окне для задания параметров открытия файла нажать на кнопку *Kernel options 1*. В появившемся окне выбрать все пункты и нажать *OK*.

5) Аналогично повторить для *Kernel options 2*.

6) Завершить настройку параметров, нажать *OK*.

7) Дождаться выполнения дизассемблирования.

12. В виртуальной машине запустить эмуляцию образа СПО *Cisco*.

1) В *Terminal* создать виртуальный интерфейс и настроить его, для подключения по протоколу *Telnet*, командой:

root@ubuntu:/home/user/Documents# tunctl -t tap1

root@ubuntu:/home/user/Documents# ifconfig tap1 up

root@ubuntu:/home/user/Documents# ifconfig tap1 192.168.23.1/24

2) Узнать *ip-адрес* самой виртуальной машины командой:

root@ubuntu:/home/user/Documents# ifconfig

3) Запускаем эмулятор образа с помощью команды:

root@ubuntu:/home/user/Documents# dynamips -T 2003 -j -P 2600 -t 2621 -s 0:0:tap:tap1 C2600-BI.BIN

4) Запустить *Putty* на панели задач.

5) В поле *Host Name* ввести 127.0.0.1, в поле *Port* 2003, в *Connection type:* выбрать *Telnet* и нажать кнопу *Open*.

6) В открывшемся терминале настройки маршрутизатора осуществить настройку маршрутизатора с помощью команд:

Router>enable

Router#configure terminal

Router(config)#interface f0/0

Router(config-if)#ip address 192.168.23.2 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#line vty 0 15

Router(config-line)#password 12345

Router(config-line)#login

Router(config-line)#end

Router#wr

7) Запустить *GDB* сервер командой:

Router#gdb kernel

Настройка стенда завершена.

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*.

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.

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 исследование 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: 22.03.19..

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: 06.04.2018.

1. 3. IDA: About [Электронный ресурс] : [сайт] / Hex-Rays SA. – Rue Rennequin Sualem, 2016– . – Режим доступа: https://www.hex-rays.com/products/ida/. – Дата обращения: 06.04.2018.

3. Санников, И. А. Исследование защищенности системного программного обеспечения сетевого оборудования семейства Cisco // Д. О. Маркин, И. А. Санников, А. А. Хомякова // Информационная безопасность и защита персональных данных. Проблемы и пути их решения : материалы X Межрегиональной научно-практической конференции [Электронный ресурс] / под ред. О. М. Голембиовской. – Брянск: БГТУ, 2018. – 187 с. – С. 99–103. ISBN 978-5-906967-92-3.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

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

РАЗРАБОТКА АГЕНТА ТУМАННЫХ ВЫЧИСЛЕНИЙ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ ПОД УПРАВЛЕНИЕМ ОПЕРАЦИОННОЙ СИСТЕМЫ ANDROID

Описана необходимость использования мобильных устройств для выполнения распределенных вычислений, разработаны структурная и функциональная схемы инфраструктуры сети мобильных устройств, разработана схема клиент-серверного взаимодействия, разработан алгоритм функционирования клиентского приложения для мобильных абонентских устройств, также разработан граф состояния сети мобильных устройств.

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) [1]. 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 [2]. Описана типовая инфраструктура, необходимая для управления распределенными вычислениями. (рис.1). 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.

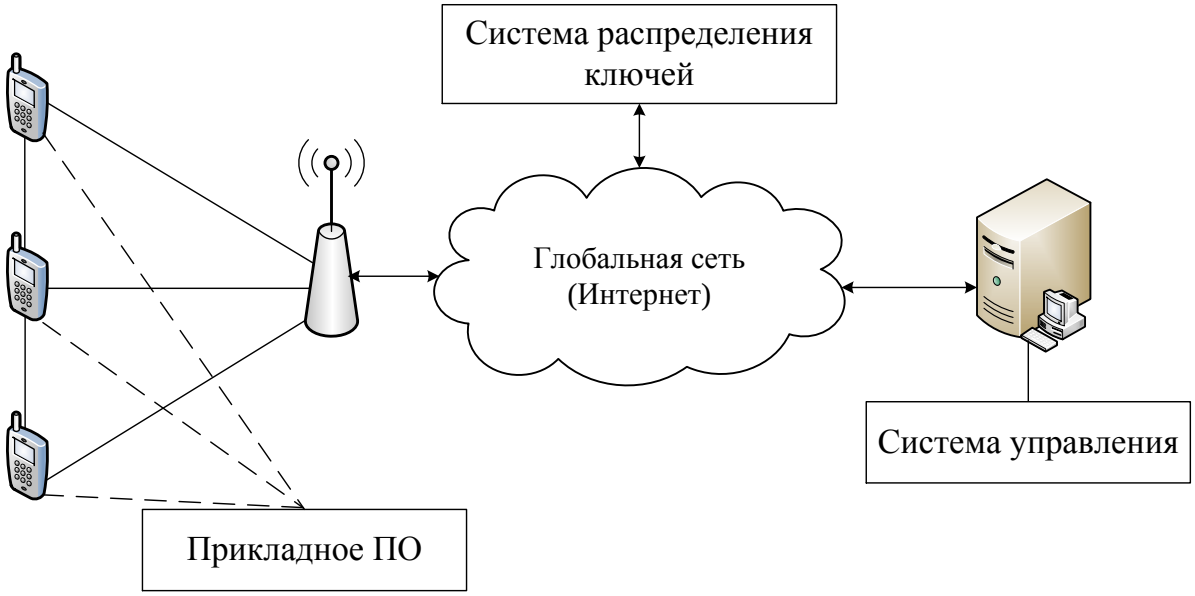


Рис.1 Структурная схема инфраструктуры сети мобильных устройств

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).

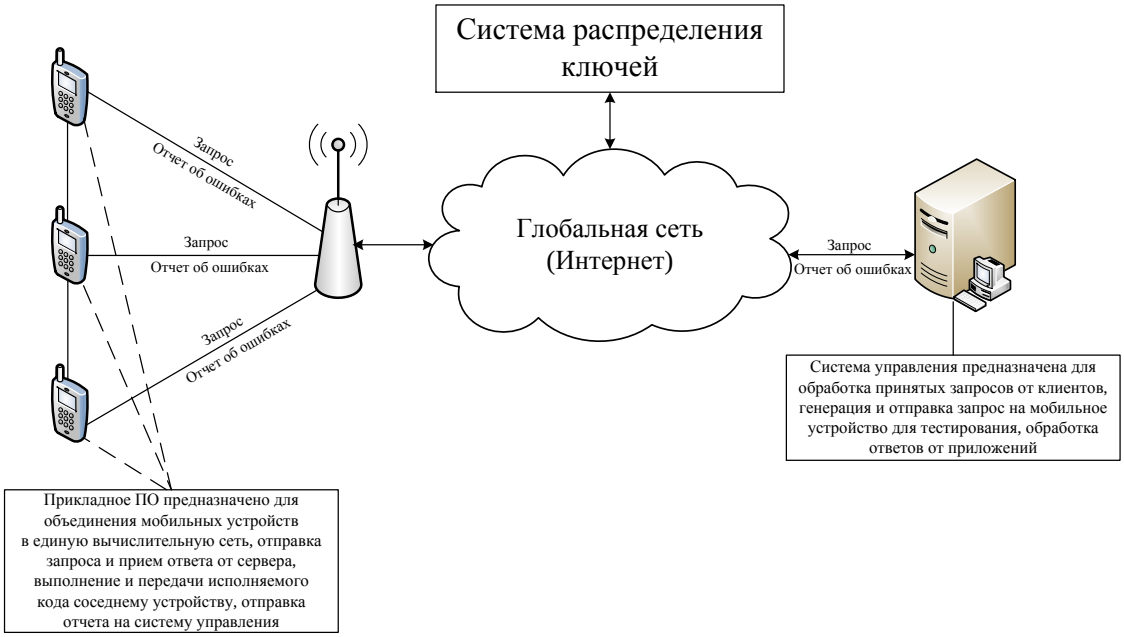


Рис. 2 Функциональная схема инфраструктуры сети мобильных устройств

В представленной схеме описаны функциональные возможности элементов вычислительной сети на базе мобильных абонентских устройств.

На рис. 3 описана схема клиент-серверного взаимодействия между агентом туманных вычислений, представленным в виде приложения для мобильного устройства, и приложением на сервере, обеспечивающим управление вычислительным процессом.

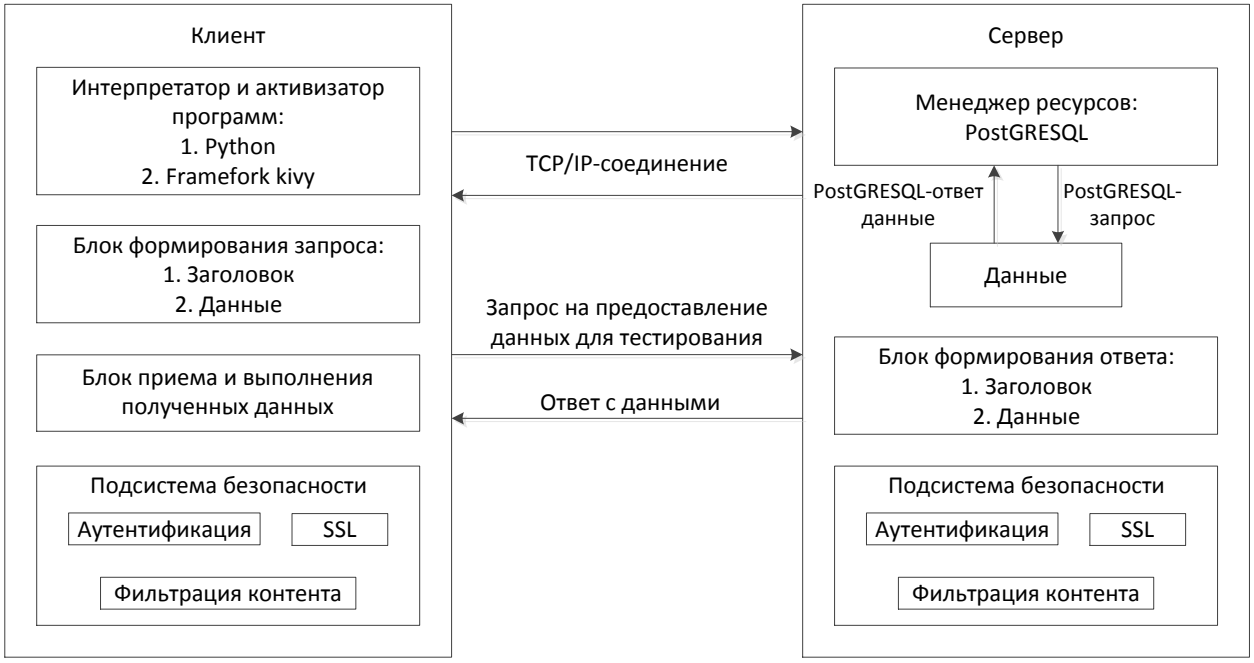


Рис. 3 Схема клиент-серверного взаимодействия

В представленной схеме описаны функциональные возможности и необходимые для них компоненты, а также вид соединения между клиентом и сервером для возможности обмениваться данными друг с другом.

Провести вычислительный эксперимент для оценивания эффективности алгоритмов и приложений ЗВС МУ по реализации распределенных вычислений. Был проведен анализ сред разработки для ОС Android, позволяющих создать приложение для МАУ с возможность 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.

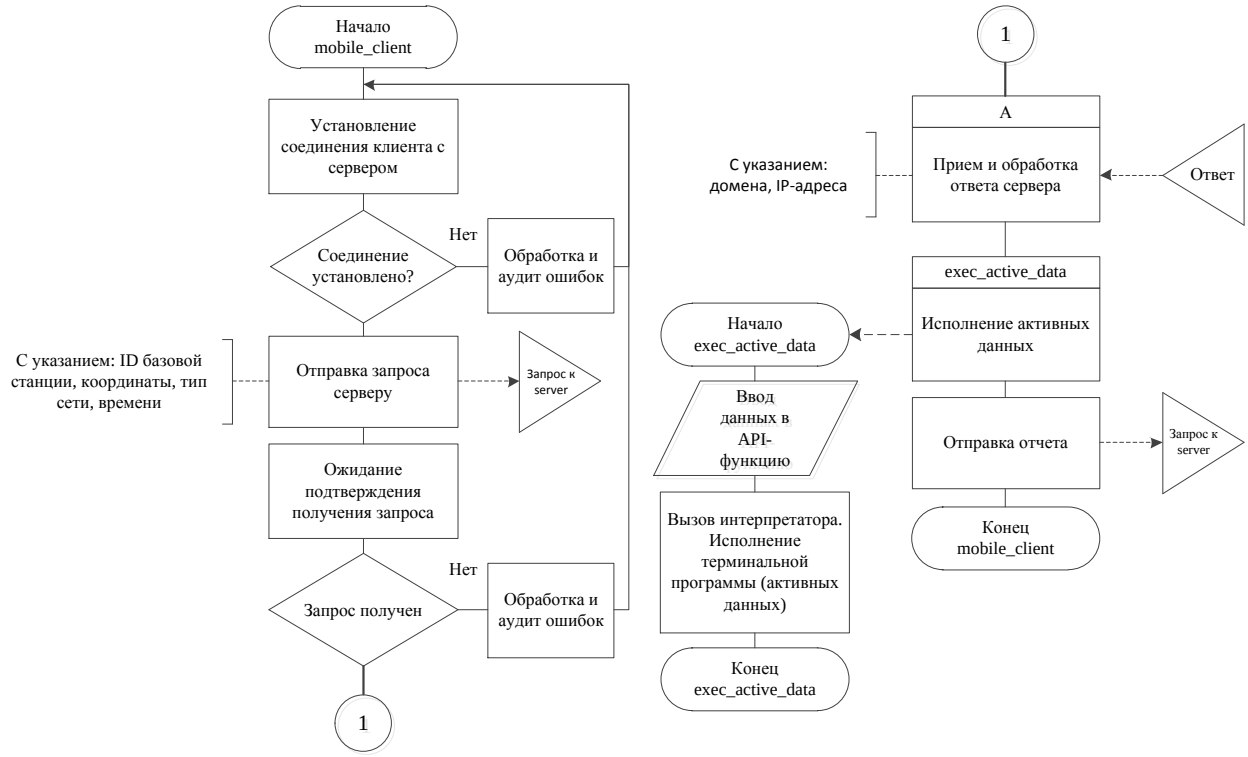


Рис. 4 Алгоритм функционирования клиентского приложения для МАУ

Для выполнения распределенных вычислений необходимо объединить несколько мобильных устройств в единую вычислительную сеть, а также необходимо устойчивое соединение с сервером и получение данных, а именно, IP-адрес, домен соседнего устройства и код на выполнения. Для этого разработан типовой алгоритм функционирования клиентского приложения для МАУ. Мобильное приложение выполняет следующие функции: отправляет запрос на соединения, отправляет запрос на предоставление исполняемой программы для тестирования, принимает и выполняет полученную программу, отправляет отчет на сервер для внесения его в базу данных.

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 (использование протокола TCP);
- распределенная память;
- централизованность управления задачами.

На рис. 5 описан граф состояния сети мобильных устройств, с помощью которого происходит объединение агентов туманных вычислений в единую сеть

для выполнения распределенных вычислений. Происходит соединение с сервером, получение активных данных для выполнения поставленной задачи.

Рис. 5. Граф состояния сети мобильных устройств

В ходе исследования проведен эксперимент по оценке времени жизни UDP-соединения. Проведен анализ сред разработки для ОС Android, позволяющих создать приложение для МАУ. Разработано приложение для мобильного устройства под управлением ОС Android, которое выполняет активные данные, принятые с сервера.

Список литературы

1. 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.

2. Маркин, Д. О. Система распределенных защищенных вычислений на основе сети мобильных устройств и технологии активных данных // Д. О. Маркин, М. А. Трохачёв, А. Э. Земцов // Информационная безопасность и защита персональных данных. Проблемы и пути их решения : материалы X Межрегиональной научно-практической конференции [Электронный ресурс] / под ред. О. М. Голембиовской. – Брянск: БГТУ, 2018. – 187 с. – С. 104–109.

3. Маркин, Д. О. Концепция построения распределенной интеллектуальной защищенной сети мобильных устройств на основе активных данных // Д. О. Маркин, М. А. Трохачев, А. Э. Земцов // Безопасные информационные технологии : сборник трудов Восьмой всероссийской научно-технической конференции / под ред. М. А. Басараба. – Москва : МГТУ им. Н. Э. Баумана, 2017. – С. 277-281.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.4

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

ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОГРАММНО-ОПРЕДЕЛЯЕМЫХ СЕТЯХ

Рассмотрены подходы к повышению информационной безопасности в программно-определяемых сетях.

С развитием облачных вычислений и интернета вещей традиционная сетевая архитектура не всегда может удовлетворить требованиям пользователей. На смену приходит архитектура следующего поколения – программно-определяемые сети (SDN). Суть нового подхода в разделении уровня управления сетью и уровня передачи данных. При этом управление сетью выносится на отдельное устройство – контроллер. Контроллер владеет информацией о существующих в сети потоках (flow) трафика и выдает управляющее воздействие на устройства, выполняющие непосредственно пересылку данных. Новая сетевая архитектура может повысить эффективность использования оборудования в Центрах Обработки Данных (ЦОД) и обеспечить новый уровень информационной безопасности передаваемых данных.

Поскольку вся информация о существующих в сети потоках данных концентрируется на контроллере, у администратора появляется возможность внедрить простые и естественные политики контроля доступа на канальном уровне. С одной стороны, независимо от топологии сети, с другой – скрывая информацию о топологии и сервисах от тех, кому не нужно знать подробностей. Так при организации взаимодействия между клиентом и сервером надо пройти три шага:

1. Каждая сторона должна пройти проверку подлинности с помощью контроллера;
2. Сервер сообщает контроллеру, какой сервис он готов предоставить, а клиент запрашивает у контроллера необходимый ему сервис;
3. Контроллер, сверив все политики доступа, дает команду на разрешение соответствующего потока данных телекоммуникационному оборудованию.

Преимущества SDN становятся более очевидными, когда речь идет о виртуальных и облачных средах. Администратор получает возможность применять различные типы политик к различным типам виртуальных машин, предоставляя услуги защиты, аналогичные межсетевому экранированию. Поскольку контроллер имеет точный список как потоков, так и возможных путей в своей сети, применение политик защиты от подмены MAC и IP адресов становится более эффективным. Например, зная что единственный путь от A к D содержит

устройства B и C, можно легко определить поддельный поток от A к D, если он не проходил через B.

Еще одним направлением повышения уровня информационной безопасности в SDN сетях является предотвращение DOS-атак. Ключевым моментом защиты сетей от DOS-атак является быстрое определение параметров вредоносного трафика. Традиционно для этого применяется машинное обучение, основанное на анализе журналов аудита или непосредственно проходящих пакетов. Технология SDN в этом случае решает проблему требовательности к вычислительным ресурсам в плоскости данных. Счетчики пакетов встроены в каждое устройство в плоскости данных. Статистика относительно проходящих потоков всегда готова и может быть запрошена контроллером. Оперативная память и вычислительный ресурс процессора для распознавания DOS-атаки необходим только на контроллере.

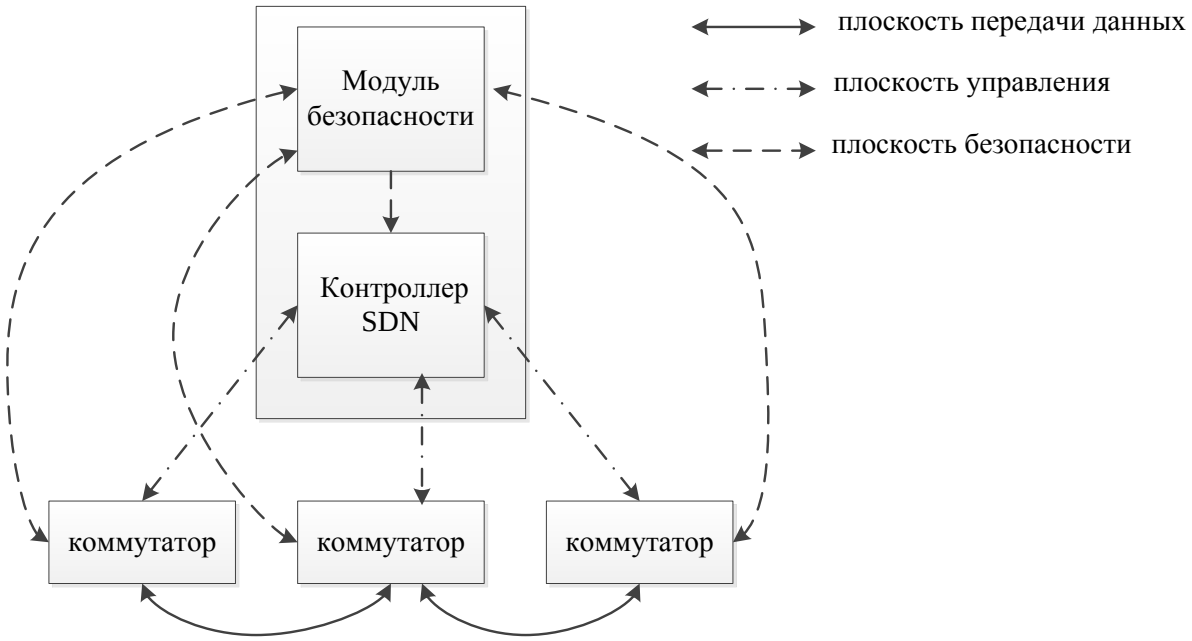


Рис. 1. Архитектура безопасности SDN сети

Реализовывать функции безопасности в облачной сети достаточно сложно. С одной стороны, маршрут движения трафика между сервисами может быть очень сложным. С другой стороны, сложно выполнить анализ сетевого пакета с уровня облачного приложения, все поля пакета скрыты. Технология SDN позволяет облачным сетевым службам безопасности решать эти проблемы: манипулировать трафиком с минимальным копированием данных, работать как на уровне пакетов, так и на уровне запросов, генерировать обратные вызовы через существующие API. Многие высокоуровневые алгоритмы маршрутизации могут быть спроектированы и реализованы таким образом, чтобы гарантировать, что все пакеты будут проверены хотя бы одним устройством безопасности.

В рамках работы исследуются варианты применения рассмотренных выше подходов к построению телекоммуникационной составляющей узла сети RSNet. На функциональном уровне узел представляет собой гиперконвергент-

ную защищенную доверенную инфраструктуру, построенную по принципам организации частного облака и обладающую высокой степенью отказоустойчивости, масштабируемости и управляемости. Узел взаимодействует с инфраструктурой сети RSNet путем соединения телекоммуникационной инфраструктуры с инфраструктурой сети, а также путем передачи информации в системы мониторинга и управления сетью с использованием стандартных коммуникационных протоколов.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

Рытов М.Ю., Горлов А.П., Лысов Д.А., Лысова К.М.
ФГБОУ ВО «Брянский государственный технический университет»
Россия, г. Брянск
lysovdmitriia@gmail.com

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ РАСПОЗНАВАНИЯ ЛИЦ ЧЕРЕЗ КАМЕРУ ПРИ АУТЕНТИФИКАЦИИ В СИСТЕМАХ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Рассматривается процесс аутентификации личности в системах контроля и управления доступом посредством распознавания лица через камеру.

Система контроля и управления доступом – совокупность программно-аппаратных технических средств безопасности, имеющих целью ограничение и регистрацию входа-выхода объектов (людей, транспорта) на заданной территории через «точки прохода»: двери, ворота, КПП.

СКУД широко применяются для обеспечения безопасности охраняемой территории за счет ограничения доступа посторонних лиц, а также учета рабочего времени сотрудников. На сегодняшний день они представлены, в основном, автоматизированными проходными с применением турникетов, шлагбаумов, цифровых считывателей. При всем разнообразии и надежности СКУД, необходимо признать, что они не позволяют гарантировать абсолютную безопасность охраняемой территории.

Несмотря на уникальность каждой конкретной системы контроля доступа, общую схему СКУД можно представить в виде схемы (рис. 1).

Например, посторонний может проникнуть на охраняемую территорию по чужому пропуску, несколько человек могут пройти турникет друг за другом за один его поворот. А в случае аварийного отключения СКУД территория фактически остается без охраны. Наиболее оптимальным решением в данной ситуации является обеспечение комплексных мер безопасности, в частности, интеграция системы контроля доступа и системы видеонаблюдения.

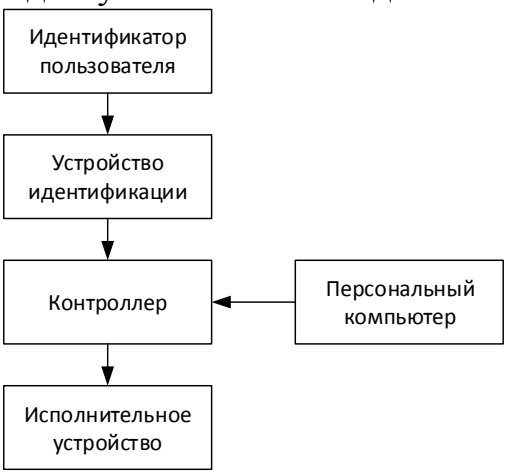


Рис. 1. Общая схема СКУД

Интерес к применению процесса распознавания лиц велик в связи с разнообразием их практического применения в таких областях, как системы, верификация, телеконференции, компьютерные игры и т. д [1].

К недостаткам распознавания человека по изображению лица следует отнести то, что сама по себе такая система не обеспечивает высокой надежности идентификации. Основной трудностью данной технологии является зависимость качества результата распознавания человека по изображению лица от ракурса, положения, условий освещенности т. д.

В процессе функционирования таких систем могут возникать ошибки первого и второго рода. Ошибкой первого рода, называется ситуация, когда объект заданного класса не распознается (пропускается) системой. Ошибка второго рода, в данном контексте, происходит, когда объект заданного класса принимается за объект другого класса [2].

В силу вышесказанного, разработка программного комплекса аутентификации личности в системе контроля и управления доступом посредством распознавания лица через камеру является актуальной задачей.

В общем случае процесс распознавания лиц можно представить в виде схемы (рис. 2).

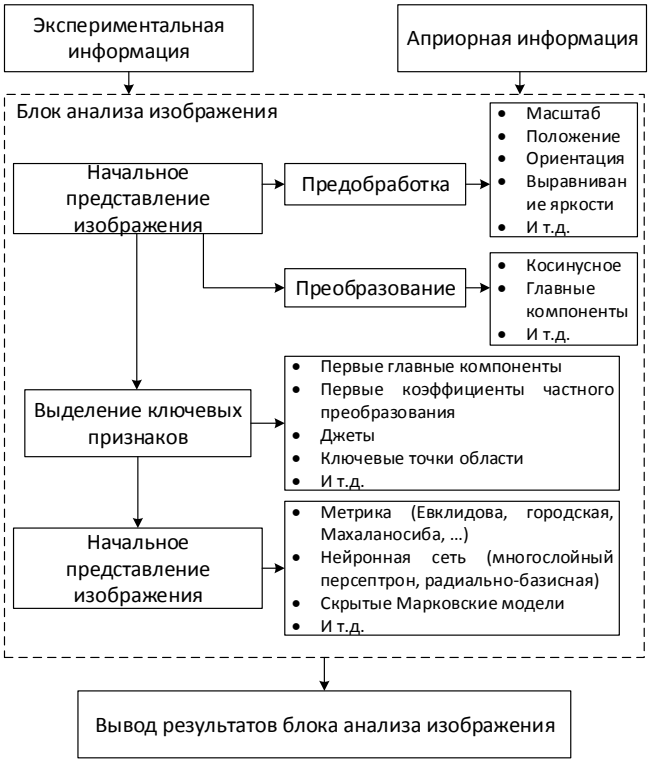


Рис. 2. Общий алгоритм работы методов распознавания изображений

Основной задачей программного комплекса является сокращение времени на аутентификацию, упрощение ввода идентификационных признаков и повышение защищенности объектов от несанкционированного доступа, что достигается путем использования комплексного применения методов распознавания лиц, формализацию работы которого можно представить в виде кортежа:

$$R =< N, M, A >,$$

где N – процесс математического анализа изображений с использованием нейронных сетей, M - формализация процесса функционирования Марковских моделей, A – процесс работы математического анализа изображения с использованием Марковских моделей.

Рассмотрим структурно-функциональную схему работы программного комплекса распознавания лиц через камеру (рис. 3).

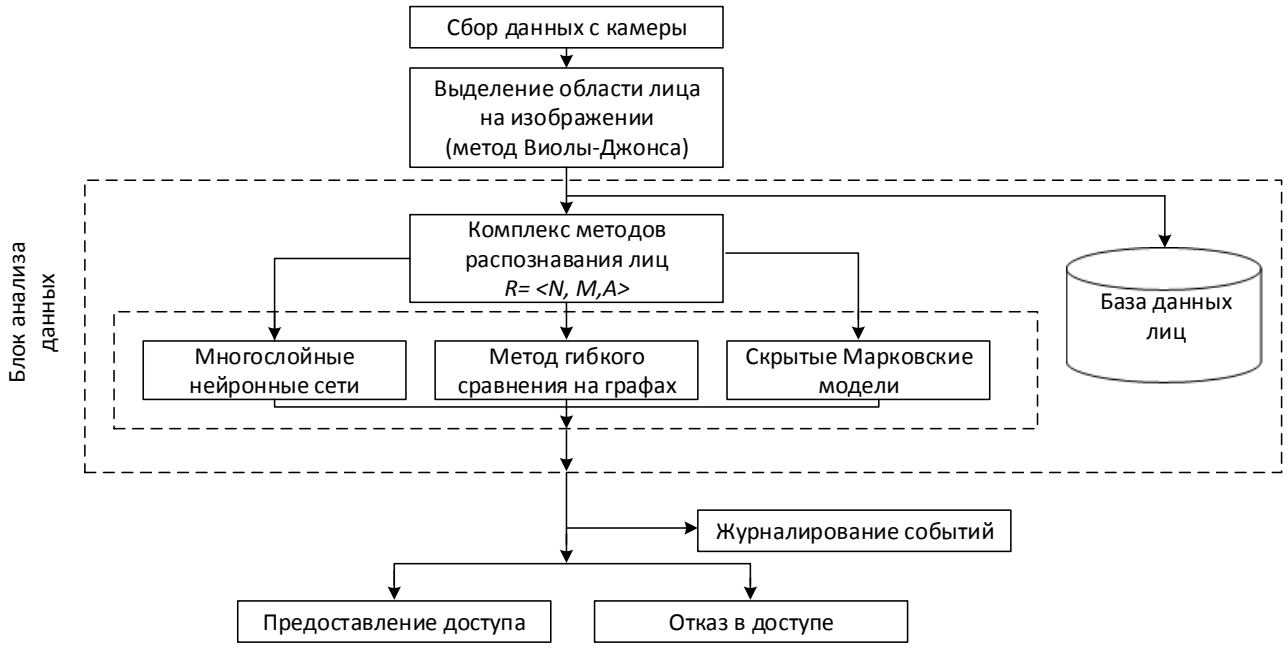


Рис. 3. Структура работы программного комплекса распознавания лиц

Работа системы начинается со сбора данных с камеры и выделения области лица на изображении, которое выполняется методом Виолы-Джонса.

Далее происходит анализ данных. Для анализа данных были выбраны 3 алгоритма распознавания лиц (многослойные нейронные сети, метод гибкого сравнения на графах, скрытые Марковские модели). После блока анализа данных система принимает решение о предоставлении доступа и пополняет базу данных лиц для дальнейшей безошибочной работы программного комплекса при принятии решений.

Программный комплекс оснащен системой журналирования событий, а это означает, что при попытке несанкционированного доступа к устройству будет сделан снимок с камеры, что поставит в известность пользователя о личности нарушителя.

Рассмотрим методы распознавания лица программного комплекса.

Многослойные нейронные сети

Архитектура многослойной нейронной сети состоит из последовательно соединённых слоёв, где нейрон каждого слоя своими входами связан со всеми нейронами предыдущего слоя, а выходами – следующего. Активационными функциями для таких нейронов служат разновидности линейных, пороговых и сигмовидных функций [3-5].

НС с одним решающим слоем способна формировать линейные разделяющие поверхности, что сильно сужает круг решаемых задач, в частности, такая сеть не сможет решить задачу типа "исключающее или". НС с нелинейной функцией активации и двумя решающими слоями позволяет формировать любые выпуклые области в пространстве решений, а с тремя решающими слоями – области любой сложности, в том числе и невыпуклой формы. При этом МНС не теряет своей обобщающей способности [7].

Процесс математического анализа изображений с использованием нейронных сетей в формализованном виде можно представить, как кортеж:

$$N =< S, \sum_{i-1}^{n} w_i x_i, T, F >,$$

где $x_1 .. x_n$ – значения, поступающие на входы (синапсы) нейрона, $w_1 .. w_n$ – веса синапсов (могут быть как тормозящими, так и усиливающими), S – взвешенная сумма входных сигналов, T – порог нейрона (во многих моделях обходятся без него), F – функция активации нейрона, преобразующая взвешенную сумму в выходной сигнал $y = F(S)$.

Метод гибкого сравнения на графах

В этом методе лицо представляется в виде графа, вершины которого расположены на ключевых точках лица, таких как контуры головы, губ, носы и их крайних точках. Каждая грань помечена расстояниями между ее вершинами.

Формализацию процесса функционирования Марковских моделей можно представить в виде кортежа:

$$M =< J, a_j, \phi_j, G^I, B, E, N, \lambda >,$$

где J – набор коэффициентов, a_j - амплитуда точек, ϕ_j – фаза точек, G^I – граф изображения лица, B – набор графов, E - количество граней, N - количество вершин λ - коэффициент относительной важности топографической информации.

Существуют также более ранние разновидности этого метода. Они используют решетки джетов, наложенные на изображение.

Скрытые Марковские модели

Марковские модели являются мощным средством моделирования различных процессов и распознавания образов [8].

По своей природе Марковские модели позволяют учитывать непосредственно пространственно-временные характеристики сигналов, и поэтому получили широкое применение в распознавании речи, а в последнее время – изображений (в частности, изображений лиц). Процесс работы математического анализа изображения с использованием Марковских моделей можно представить в виде кортежа:

$$A =< \lambda, N, S, V, M, q_t, T, b_{jk}, P >,$$

где λ – модель процесса распознавания лица, N – набор состояний, S – состояние системы, V – набор символов для каждого состояния, M – количество символов, q_t – символ состояния, T – число наблюдений в последовательности, b_{jk} – вероятность генерации символа состояния, P – вероятность генерации последовательности состояний.

Таким образом, комплексное использование выбранных методов распознавания лиц позволяет сократить вероятность возникновения ошибок первого и второго рода, а применение программного комплекса аутентификации личности в системах контроля и управления доступом посредством распознавания лица через камеру сокращает время, затрачиваемое на эти процессы.

Список литературы

1. Лысов, Д.А. Обеспечение информационной безопасности информационной советующей системы / Аверченкова Е.А., Гончаров Д.И., Лысов Д.А.// Вестник Иркутского государственного технического университета, 2016. – С.46-56.

2. Лысов, Д.А. Авторизация пользователей на основе комплексного применения методов распознавания лиц / М.Ю. Рытов, В.А. Шкаберин, Д.А. Лысов, А.П. Горлов // Информация и безопасность. – 2016. – №1. – С. 106-109.

3. Лебеденко, Ю.И. Биометрические системы. – Тула: Издательство ТулГУ, 2012. – 159 с.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004

Рытов М.Ю., Горлов А.П., Лысов Д.А., Лысова К.М.
ФГБОУ ВО «Брянский государственный технический университет»
Россия, г. Брянск
lysovdmitriia@gmail.com

УГРОЗЫ УТЕЧКИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ ПОСРЕДСТВОМ ИСПОЛЬЗОВАНИЯ УЛЬТРАЗВУКОВЫХ БОКОВЫХ КАНАЛОВ НА МОБИЛЬНЫХ УСТРОЙСТВАХ

Рассматриваются возможности ультразвукового межсетевого отслеживания для использования полученных данных в рекламных целях, а также для деанонимизации пользователей.

В конце 2016 года в Германии прошел 33-й по счету, ежегодный Всемирный конгресс хакеров, организованный хакерской группой Chaos Computer Club. Многочисленные семинары и лекции конгресса посвящены техническим и общественно-политическим аспектам. Из множества докладов внимание публики привлекло выступление представителей компании Silverpush. Тема презентации «The Tor de-anonymization Attack».

Silverpush – это рекламная компания, расположенная недалеко от города Дели (Индия), которая разрабатывает продукты для отслеживания на разных устройствах и целевые рекламные продукты, включая неслышимые ультразвуковые звуковые маяки.

Во время одного из выступлений докладчик на макбуке через Tor браузер перешел по onion ссылке, и через некоторое время на экране уже красовались его реальный ip адрес, геоданные, номер его личного телефона, имей телефона, мак адрес, личный email. Увиденное повергло публику в шок.

Для получения таких результатов используется так называемая технология Cross-device tracking. Изначально она была изобретена для получения дополнительной информации маркетологами для формирования целевой аудитории. Суть этой технологии в распространении и считывании близкого к ультразвуковому диапазону частот. Эти сигналы находятся в диапазоне 18-19,5 кГц. Такие диапазоны используют в телевизионных рекламных роликах или в случаях, когда пользователь сталкивается с рекламой в интернете. Несмотря на то, что человеческое ухо не может услышать этот звук, его могут уловить находящиеся поблизости мобильные устройства. Когда это происходит, файлы cookie определяют несколько устройств пользователя и отслеживают, какие телевизионные ролики он смотрит, как долго это делает и реагирует ли на рекламу (поиск в интернете, покупка товаров). В течение дня люди используют как минимум пять устройств: телефон, компьютер, планшет, устройство, следящее за здоровьем и т.д. «Когда человек занят своими обычными делами, его активность на каждом устройстве и сервисе генерирует различные потоки данных, несущие информа-

цию о предпочтениях и поведении. Cross-device tracking позволяет маркетологам объединить эти потоки, связав их с одной личностью, и увеличить уровень детализации информации об этом человеке».

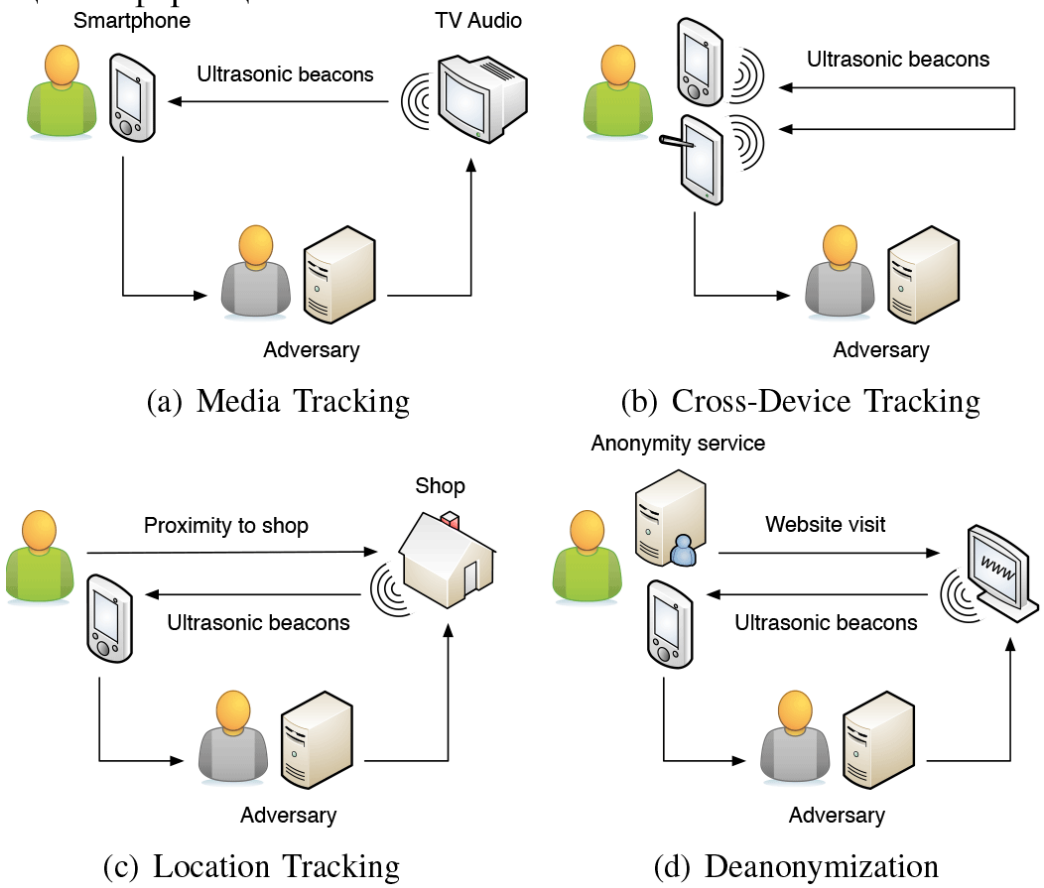


Рис. 1. Схема работы технологии ультразвуковых следящих маячков

Согласно отчету исследователей Технического университета Брауншвейга (Германия), за 2016 год было обнаружено 234 Android-приложения, способных «слушать» ультразвуковые сигналы без ведома пользователя. Некоторые программы даже используют специальные биконы (маячки ближнего действия с поддержкой Bluetooth Low Energy) для отображения на устройстве пользователя рекламы в соответствии с его текущим местоположением. В нескольких магазинах двух неназванных европейских городов уже установлены такие ультразвуковые биконы. Технология позволяет рекламодателям отслеживать местоположение пользователя, взаимодействие с телефоном, покупки и на основании этой информации делать рекламу более таргетированной. Тем не менее, по мнению экспертов, технология угрожает конфиденциальности данных. С ее помощью можно деанонимизировать пользователей биткойнов и браузера Tor.

Обычно деанонимизация предполагает получение подлинного IP-адреса, но получить его непросто, особенно если пользователь находится в другой стране или использует технологию Parallrl VPN. В случае cross-device tracking телефон может отправить и координаты, и номер телефона, и контакты в адресной книге, и аккаунт Google/Apple, и историю звонков/СМС, и список используемых Wi-Fi, а этого более чем достаточно для установления личности.

Рис. 2. Тестовая установка в лаборатории Брауншвейгского технического университета. Распознавание маячков с расстояния 2 метра на частоте 18 кГц составляет от 70% до 100%, а на частоте 20 кГц — от 75% до 100%, в зависимости от качества телефона

Использование близкого к ультразвуковому диапазона частот для сбора информации о пользователях имеет некоторое сходство с badBIOS. Она использует неслышимые звуки, чтобы «связать» физически разделенные компьютеры. Существование badBIOS не доказано, но возможность использования высокочастотных звуков для отслеживания пользователей подчеркивает жизнеспособность этой концепции.

Сейчас технологию Cross-device tracking применяют SilverPush и другие компании, которые, вероятнее всего, будут использовать её и дальше (в той или иной форме). Обычные люди не могут узнать, следят за ними или нет, и никак не могут на это повлиять. О использовании данной технологии спецслужбами можно только догадываться.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

Рытов М.Ю., Горлов А.П., Лысов Д.А.
ФГБОУ ВО «Брянский государственный технический университет»
Россия, г. Брянск
lysovdmitriia@gmail.com

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ОЦЕНКИ ЭФФЕКТИВНОСТИ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Рассматривается процесс автоматизации оценки эффективности программно-аппаратных средств защиты информации, путем создания автоматизированной системы.

На сегодняшний день проблема защиты конфиденциальной информации стоит особенно остро. Ущерб от реализации угроз компьютерным системам (КС) и обрабатываемой в них конфиденциальной информации превышает миллионы рублей.

По статистике за 2018 год на территории РФ зафиксировано около 300 тысяч преступлений в сфере информационной безопасности. К этим преступлениям относятся несанкционированный доступ к конфиденциальной информации, утечка и разглашение атрибутов доступа к подсистемам КС, создание, использование или распространение вредоносных программ для ЭВМ или машинных носителей с такими программами.

Компьютерная система – любое устройство или группа взаимосвязанных, или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных.

Объектом информатизации называется совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов, в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведений конфиденциальных переговоров.

В общем случае на компьютерную систему влияет ряд факторов, который можно условно разделить на две категории: требования законодательства и стандартов в области защиты информации, а также различные угрозы информационной безопасности. Автоматизированная система оценки эффективности программно-аппаратных средств защиты информации позволит привести КС в соответствие установленным требованиям, противостоять актуальным угрозам, снизить трудоемкость работ, сэкономить время и значительно сократить материальные затраты на проведение аудита и разработку ПАСЗИ.

Ввиду этого разработка системы автоматизированной оценки эффективности программно-аппаратных средств защиты представляется актуальной. На данный момент автоматизированная оценка уровня информационной безопас-

ности производится исключительно по стандартам ISO, однако в РФ более распространена организационно-распорядительная документация.

В предлагаемом подходе в основу положена оценка защищенности объекта информатизации согласно положениям законодательной базы РФ, требованиям государственных стандартов, а также проверка наличия организационно-технической документации (далее – ОТД), регламентирующей защиту компьютерных систем.

Основной задачей разрабатываемой АС является выявление уязвимостей существующих систем обработки и защиты информации. В качестве входных данных используются данные о КС. Данные вводятся на основе специально разработанных опросных анкет.

Алгоритм работы АС:

7. Ввод исходных данных.
8. Формирование информационной модели компьютерной системы, определение целей и задач по ЗИ.
9. Оценка состояния защищенности ОИ.
10. Формирование модели угроз ИБ.
11. Формирование рекомендаций по совершенствованию системы защиты информации.
12. Формирование организационно-технической документации.

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

Структурно-функциональная схема разработанной АС представлена на рис. 1.

Ввод исходных данных представляет собой заполнение опросных анкет, которые позволят выявить вид обрабатываемой информации, существующие программно-аппаратные средства защиты информации, угрозы ИБ, уязвимости системы защиты информации, а также прочие данные, позволяющие составить информационную модель объекта информатизации.

Следующим этапом является оценка состояния защищенности КС. Выделяется 3 основных направления оценки защищенности:

1. Оценка на соответствие требованиям стандартов (ГОСТ, СТР-К, ISO).
2. Определение наличия программно-аппаратных средств защиты информации на объекте информатизации.
3. Выявление ОТД, регламентирующей защищенную обработку конфиденциальной информации.

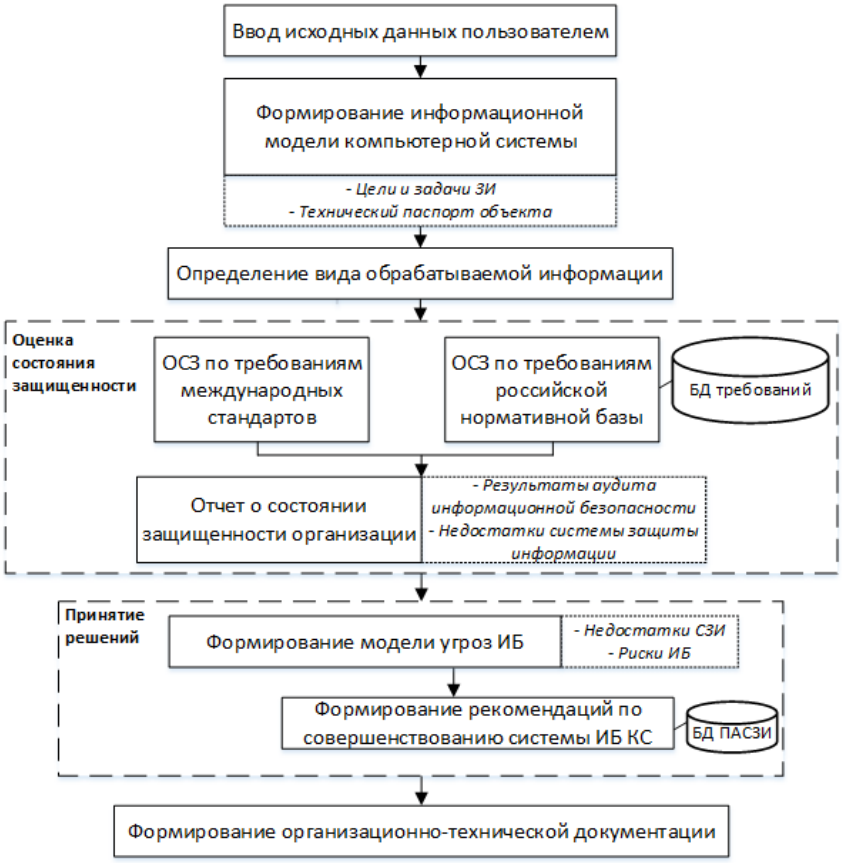


Рис. 1. Структурно-функциональная схема автоматизированной системы

По результатам данного этапа формируется отчет о состоянии защищенности компьютерной системы.

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, режиму обработки данных и т.д.

Однако 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.

Основываясь на выделенных критериях актуальности, возможно формализовать расчет вероятности реализации угроз:

$$\boldsymbol{P(i)} = \frac{\sum \boldsymbol{f(j)}}{\boldsymbol{N}} * \mathbf{100\%}$$

$\boldsymbol{P(i)}$ – вероятность реализации i-ой угрозы, $\boldsymbol{f(j)}$ – функция расчета влияния j-го критерия на защищенность системы от i-ой угрозы, $\boldsymbol{N}$ – кол-во факторов.

На данном этапе результатом работы является модель угроз, на основании которой можно выделить оптимальные средства защиты от наиболее актуальных и вероятных угроз.

Для обеспечения защиты от таких угроз предусмотрен процесс выборки программных и аппаратных средств защиты информации из базы данных. Выборка производится исходя из стоимости средств защиты и оптимальных технических характеристик, необходимых для обеспечения требуемого уровня защищенности.

Формализацию процесса формирования модели угроз можно представить в виде кортежа:

$$\boldsymbol{M =< Di, T, Th, Ka, P >},$$

где $\boldsymbol{D_i}$ – уровень исходной защищенности, $\boldsymbol{T}$ – тип системы обработки информации, $\boldsymbol{Th}$ – угрозы информационной безопасности, $\boldsymbol{K_a}$ – критерии актуальности угроз, $\boldsymbol{P}$ – вероятность реализации угроз

Следующим этапом является формирование рекомендаций по совершенствованию системы защиты информации. Рекомендации разделяются на 4 основных раздела:

1. Рекомендации по антивирусной защите информации.
2. Рекомендации по защите информации от несанкционированного доступа (НСД).
3. Рекомендации по применению средств межсетевого экранирования.
4. Рекомендации по применению средств обнаружения вторжений.

По каждому разделу приводится ряд мер, выполнение которых необходимо для защиты от выявленных угроз. Так же на данном этапе происходит подбор оптимальных средств программно-аппаратной защиты информации, исходя из допустимой стоимости и набора необходимых характеристик.

Заключительным этапом является формирование ОТД, регламентирующей защиту конфиденциальной информации. На данном этапе производится оценка наличия ОТД на объекте, выявляются недостающие документы, если необходимо, производится сбор дополнительных данных, необходимых для формирования дополнительных документов.

В качестве выходных данных по результатам работы данного блока является комплект ОТД, регламентирующей эксплуатацию программно-аппаратных средств защиты.

Результаты работы автоматизированной системы представлены на рис.2.

Рис. 2. Результаты работы АС

Таким образом, разработанная автоматизированная система оценки эффективности программно-аппаратных средств защиты информации позволяет в автоматизированном режиме построить модель угроз информационной безопасности, сформировать организационно-техническую документацию регламентирующую защиту конфиденциальной информации, а также сформировать рекомендации по усовершенствованию программно-аппаратной системы защиты информации. Применение данной системы позволит значительно сократить временные и материальные затраты на проведение аудита информационной безопасности и разработку дополнительных мер защиты информации.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

Рытов Михаил Юрьевич, *к.т.н., доцент, зав. каф. «Системы информационной безопасности»*
Еременко Владимир Тарасович*, д.т.н.. профессор каф. «Системы информационной безопасности»*
ФГБОУ ВО «Брянский государственный технический университет»
Россия, г. Брянск
e-mail: rmy@tu-bryansk.ru

ПОДХОД К ОБЕСПЕЧЕНИЮ НАДЕЖНОСТИ КОММУНИКАЦИОННОЙ СРЕДЫ ИНФОРМАЦИОННЫХ ПОРТАЛОВ РЕГИОНАЛЬНЫХ ОРГАНОВ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ

Рассмотрены вопросы обеспечения надежности коммуникационной среды информационных порталов региональных органов исполнительной власти, а также определены основные пути их решения.

В настоящее время для поддержки принятия управленческих решений на основе комплексного мониторинга состояния наблюдаемых объектов, событий, процессов, анализа их причин и последствий, а также прогнозирования развития ситуации применяются ситуационные центры (СЦ). Согласно Федеральному закону № 172-ФЗ от 28 июня 2014 г. «О стратегическом планировании в Российской Федерации» и Указу Президента РФ от 25 июля 2013 г. № 648 «О формировании системы распределенных ситуационных центров, работающих по единому регламенту взаимодействия», создана *федеральная информационная система стратегического планирования на основе распределенной информации*, обеспечивающая формирование и обработку информации, содержащейся в федеральных, региональных и муниципальных информационных ресурсах и системах региональных органов исполнительной власти, необходимых для обеспечения поддержки принятия управленческих решений. Развитие системы СЦ и организация их взаимодействия на основе единого регламента позволяет повысить эффективность информационной поддержки реализации государственной политики в сфере социально-экономического развития России и обеспечения национальной безопасности [1 - 2].

Особенности информационного обмена на региональном уровне (включая органы исполнительной власти и местного самоуправления) связаны с тем, что разнородная информация обрабатывается как на вертикальном уровне иерархической структуры государственного управления, так и на горизонтальном уровне, что приводит к дублированию, избыточности и снижению надежности её обработки.

Функционально-структурная избыточность среды ИП, как сложной системы СЦ, характеризует ее резервные возможности по обеспечению надежности инфокомуникационных процессов [2].

Трудности обеспечения надежности инфокоммуникационных процессов связаны со сложностью описания интегрированных информационных потоков (объем, формат, распределенность) и вычислительной сложностью, что обуславливает переход от модельных решателей задач к генерации знаний. Это, в свою очередь, приводит к необходимости новой трактовки понятия «надежность среды информационного портала», под которой следует понимать способность системы функционировать в условиях несанкционированных воздействий в ОП. Кроме того, существует риск получения неполной и не своевременной информации в условиях несанкционированного воздействия при ее обработке в среде ИП ОИВ.

Развитие методов совершенствования инфокоммуникационных процессов в коммуникационной среде ИП органов исполнительной власти осуществляется в направлении все более полного удовлетворения требований, выдвигаемых ее представителями для улучшения характеристик передачи.

Первое направление проявляется в ведении расширенных функциональных возможностей (РФВ), обеспечиваемых алгоритмами обработки информации в определенном режиме («Запрос – Ответ», «Доставка», «Диалог»).

Второе направление заключается во введении специальных алгоритмов информационного обмена, предназначенных для установления оптимальных параметров обработки информации в среде информационного портала за счет: длины поля данных пользователя органов исполнительной власти в информационном массиве; параметров тракта передачи, используемых для нумерации массивов.

При этом необходимо указать на факторы, общие для обоих направлений. Например, предварительное согласование пропускной способности косвенно связано с регулированием входящего и исходящего трафика. Предоставление точки доступа к вычислительным ресурсам, ресурсам информационного портала, приложениям может быть связано с другими источниками данных внутри и вне информационного портала. При этом, информация должна быть персонифицирована, интегрирована и агрегирована – то есть ее представление максимально направлено на поддержку процессов принятия решений и решений функциональных задач и проблем.

Выявленные противоречия, в первую очередь, выступают как результат основного противоречия между традиционными принципами и методами высоконадежной обработки информации в среде ИП как сложной системы, и изменившимся содержанием процессов ее обработки в современных информационных порталах в условиях конвергенции и несанкционированных воздействий.

Это вызывает необходимость разработки методологических основ функциональной стандартизации средств в среде информационного портала и исследования путей решения слабоструктурированной проблемы обеспечения надежности инфокоммуникационных процессов в условиях конвергенции на основе введения в них структурно - функциональной избыточности, разработки специализированных алгоритмов функционирования в условиях несанкционированных воздействий.

Таким образом, решение рассмотренных проблем, возникающих при создании СЦ региональных органов исполнительной власти, является актуальной научной задачей, требующей оперативного решения.

Список литературы

1. Рытов, М.Ю. Актуальные проблемы управления информационными потоками в коммуникационной среде информационного портала регионального органа исполнительной власти / М. Ю. Рытов, В.Т. Еременко, Д.С. Мишин, // Информационные системы и технологии. – 2017. – № 2 (100). – С. 40-50.

2. Рытов, М.Ю. Моделирование процессов защиты данных в информационных порталах региональных органов исполнительной власти/ М.Ю. Рытов, В.Т. Еременко, А.П. Горлов. // Вестник информационных технологий – 2016. - № 9 (97). – С. 48 –53.

3. Рытов, М.Ю. Метод оптимизации дополнительных технических возможностей алгоритмов обработки информации в среде портала органов исполнительной власти // Информационные системы и технологии. – Орел: ОГУ им. И.С. Тургенева, 2016. – № 4. – С. 94-103.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

Рытов Михаил Юрьевич, *к.т.н., доцент, зав. каф. «Системы информационной безопасности»*
Луценко Игорь Владимирович, аспирант *каф. «Системы информационной безопасности»*
ФГБОУ ВО «Брянский государственный технический университет»
Россия, г. Брянск
eropa@live.ru

АВТОМАТИЗИРОВАННАЯ СИСТЕМА НАХОЖДЕНИЯ ОПТИМАЛЬНОГО НАБОРА ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ МАЛОГО ПРЕДПРИЯТИЯ

Предложена структура модулей для разработки автоматизированной системы по нахождению оптимального набора средств технической защиты информационной системы малого предприятия.

Малое предприятия является основным локомотивом в экономике во многих странах. Деятельность такого предприятия влияет на экономический рост страны, подталкивает на новые инновационные разработки продукции, применения нанотехнологий и решение социальных проблем страны.

Для достижения высокого уровня конкурентоспособности российским предприятиям, нужно использовать современные инновационные методы управления, которые подходят современной экономической среде.

Малые масштабы деятельности предприятия, узость рынка сбыта позволяют руководителю (владельцу) быть в курсе всех дел, дают возможность владеть всей полнотой информации и осуществлять индивидуальное руководство и контроль за работой сотрудников и бизнесом в целом. Наемные работники выполняют либо производственные функции (рабочие), либо те из них, которые руководитель не в состоянии выполнять в силу их определенной специфики, например, бухгалтерский учет, информационные технологии.

Информационные технологии позволили упростить и усовершенствовать бизнес-процесс, что привело к появлению ряда проблем. Одной из важных проблем выделяют процесс формирование комплексной системы защиты информации на малом предприятия. С каждым днем проблема становиться важнее,так как перечень угроз и их модификация всегда развиваются. Источники угроз можно выделить как внешние или внутренние. Успешная совершенная атака на информационную систему малого предприятия может быть чревата временными и финансовыми потерями.

Для того чтобы за короткий момент времени качественно и эффективно собрать оптимальный набор барьеров из технической защиты информационной системы, используют различные автоматизированные системы. В основу автоматизированных систем положены различные модели. Можно выделить наибо-

лее популярную для проектировании автоматизированной системы модель “Клементса-Хофмана”. Данная модель позволяет найти оптимальный набор средств защиты информации с оценкой защищённости.

В основу разработки структурно-функциональной схемы программного комплекса для проектирования комплексной системы защиты малого предприятия заложены принципы системного единства, совместимости, типизации, развития и модульности (рис. 1).

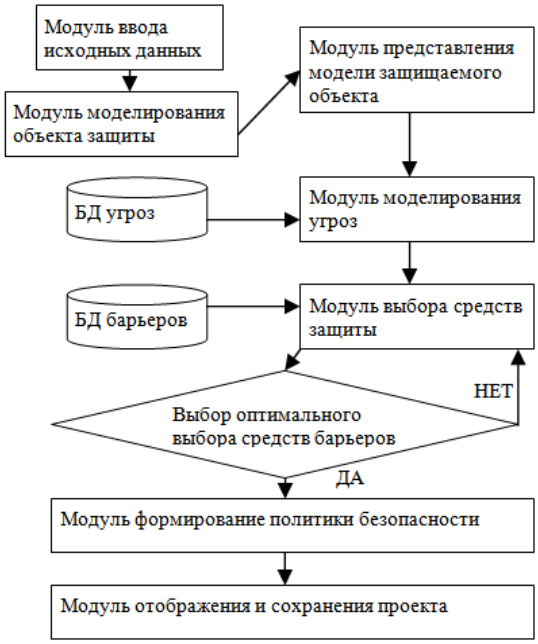


Рис. 1. Схема автоматизированной системы проектирования комплексной системы защиты информации малого предприятия

В состав разработанной системы входят следующие модули:

Модуль ввода исходных данных об объекте предназначен для ввода исходных данных об объекте защиты и описания характеристик элементов объекта, получаемых в результате проведения аудита технической защиты объекта защиты. В качестве исходных данных для проектирования систем технической защиты рассматриваются характеристики защищаемого объекта (с помощью каких видов угроз можно достичь).

На основе этих характеристик все защищаемые объекты были поделены на группы, каждой из которых соответствует определённый набор требований по защите.

Сохранение набора таких требований и характеристик в базе данных необходима для последующей загрузки в автоматизированной системе. С помощью этого обеспечивается гибкость и переносимость требований по комплексной защите информации объектов в другие модули программы.

- ***Модуль моделирования объекта защиты*** предназначендля моделирования объекта защиты и определения защищаемого объекта. Все данные по защищаемому объекту хранятся в базе данных.

- ***Модуль представления модели защищаемого объекта*** предназначен для преобразования исходных данных и модели объекта защиты в доступный всем проектным модулям ПКП КСЗ.
- ***Модуль моделирования угроз и определения рисков проникновения*** предназначен для определения всех вероятных угроз безопасности и ранжирования данных угроз.

Каждому носителю информации соответствует многочисленный набор угроз, реализуемых при ненулевом значении пространственного, временного и энергетического факторов. Оценку защищённости каждого барьера оценивают эксперты, и все эти данные хранятся в базе данных. Для определения риска производится пересчет факторов угроз в числовом значении. Заключительным этапом является определение затрат при наборе барьеров при каждом наборе угроз.

- ***Модуль выбора средств защиты,*** производящий по «*критерию источника угроз*» выбор методов и средств защиты информационной системы из базы данных технических средств.

Главным принципом создания систем защиты является комплексность. Так как при недостаточном удаление внимания какой-либо составляющей системы защиты, появляется возможность беспрепятственного воздействия злоумышленника на защищаемый объект. Поэтому при создании системы технической защиты необходимо её рассматривать как единую систему, состоящую из программно-аппаратных средств защиты информации. Каждый элемент комплексной системы защиты предназначен для противодействия определенным видам источника угроз и проектируется каждый самостоятельно.

Модуль формирования политики безопасности предназначен для формирования политики безопасности при оптимальном наборе барьеров информационной системы малого предприятия. Из базы данных берем рекомендации для формирование барьеров. Полученный результат в дальнейшем передает в модуль отображения отчета.

- ***БД барьеров*** содержат перечень методов и средств технической защиты и их характеристик.
- ***Модуль отображения и сохранения проекта*** служит для документирования, сохранения и дальнейшего использования результатов проектирования.

Для обеспечения периодического контроля эффективности выбора оптимального набора барьеров можно периодически отслеживать коэффициент стойкости против угроз, которые периодически заполняются с базы угроз ФТСЭК.

Разработанная комплексная защиты информации информационной системы малого предприятия позволяет получать для объекта законченный проект системы технической защиты информационной системы малого предприятия и материальных ценностей в автоматизированном режиме при изменении исходных данных на проектирование.

Результатом работы автоматизированной системы является комплект документов на проектирование, в состав которой входят:

1) список, против каких угроз данные меры будут эффективными;
2) список средств и методов защиты;
3) рекомендации при создании технической защиты информационной системы малого предприятия.

Разработанная автоматизированная система позволила ускорить и увеличить качество защиты информации на малом предприятии в несколько раз, а (рис.2) также позволила сократить расходы на закупку только нужного перечня оборудования и его настройки для защиты информации. Благодаря нахождению оптимального варианта, автоматически время на проектирование комплексной системы защиты сократилось в 5 раз, уменьшилось появление ошибок при проектировании, а также закупка оборудования сократилась на 30 процентов.

Рис. 2. Сравнительный анализ времени проектирования с помощью системы или ручным методом

Таким образом, предложенный подход создания автоматической системы для проектирования комплексной системы защиты может быть использована для широкого круга объектов, нуждающихся в защите.

Список литературы

1. Аверченков, В.И. Организационная защита информации / В.И. Аверченков, М.Ю. Рытов. – Брянск: Изд-во БГТУ, 2015. – 184 с. – (Серия «Организация и технология защиты информации»).
2. Алаухов, С.Ф. Вопросы создания систем информационной безопасности для крупных промышленных объектов / С.Ф. Алаухов, В.Я. Коцеруба // Системы безопасности. – 2011. – № 41. – С. 93.
3. Баранова, Е.К. Моделирование системы защиты информации. Практикум: учеб.пособие / Е.К. Баранова, А.В. Бабаш. – М.: РИОР: ИНФРА-М, 2016. – 224 с

4. Луценко, И.В. Способы и приемы оценки защищенности данных малого предприятия / И.В. Луценко, М.Ю. Рытов // Информационные системы и технологии. – 2018. - №3(107). –125 с.

5. Рытов, М.Ю. Использование специализированной САПР для проектирования комплексных систем защиты информации / М.Ю. Рытов, И.В. Луценко, М.А. Луценко // Инновационные, информационные и коммуникационные технологии. – Москва. Ассоциация выпускников и сотрудников ВВИА им проф. Жуковского, 2018. – 652 с.

Материал поступил в редколлегию 24.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056.53

Рытов М. Ю. *к.т.н., доц., зав. кафедры ”СИБ”*
Мусиенко Н.О. *асс. кафедры «СИБ»*
ФГБОУ ВО «Брянский государственный технический университет»
Россия, г. Брянск
musienkono@yandex.ru.

ОБЗОР СОВРЕМЕННЫХ ПРОБЛЕМ МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ ИНФРАСТРУКТУРАХ

Представлен обзор современных проблем моделирования угроз безопасности информации в критических информационных инфраструктурах.

Определение основных проблем в процессе моделирования угроз безопасности информации в критических информационных инфраструктурах согласно 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации»[2].

Введение

Одним из основных этапов выполнения требований 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [2] является категорирование объектов КИИ. Согласно формулировке установленной в тексте закона, категорирование понимается как установление соответствия объекта КИИ критериям значимости и показателям их значений, а также присвоение ему одной из категорий значимости или не присвоение такой категории. Процесс категорирования условно можно разделить на несколько этапов, которые представленны на рисунке 1.

Каждый из представленных этапов заключает в себе ряд смежных задач, которые выполняются комиссией по категорированию или субъектом КИИ и регламентированны постановлением Правительства РФ №127 «Об утверждении Правил категорирования объектов КИИ РФ» [3, 4] (далее Постановление). Данное постановление в полной мере дает возможность осуществить процесс категорирования согласно принятым в нём правилам. Однако один из этапов категорирования в постановлении упоминается в недостаточном объеме для формулировки четкого порядка действий и правил. А именно процесс анализа угроз безопасности информации и рисков, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ.

Анализ угроз безопасности информации объекта КИИ

Согласно пунктам г, д, статьи 14 Постановления: *«Комиссия по категорированию в ходе своей работы:*

г) рассматривает возможные действия нарушителей в отношении объектов критической информационной инфраструктуры, а также иные источники угроз безопасности информации;

д) анализирует угрозы безопасности информации и уязвимости, которые могут привести к возникновению компьютерных инцидентов на объектах критической информационной инфраструктуры;»

Указанные пункты затрагивают анализ возможностей нарушителя, угроз и уязвимостей. Т.о. становится понятно, что речь идет о разработке комиссией по категорированию модели угроз и модели нарушителя для объекта КИИ. Федеральный орган исполнительной власти, курирующий вопросы категорирования объектов КИИ – ФСТЭК России, дает следующие разъяснительные комментарии по данной проблеме.

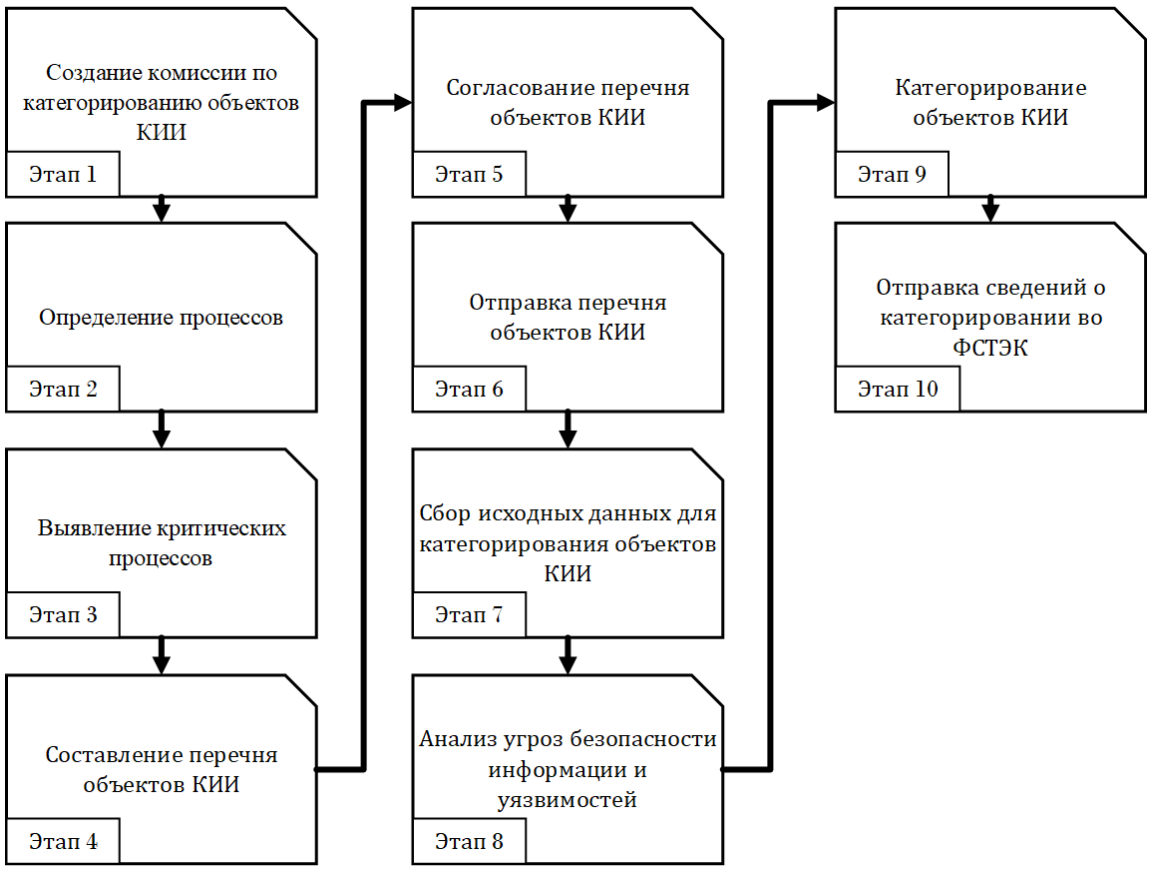


Рис. 1. Этапы категорирования объекта КИИ

В соответствии с информационным сообщением ФСТЭК России от 4 мая 2018 г. N 240/22/2339, Базовая модель угроз безопасности информации КСИИ и методика моделирования угроз КСИИ, официально могут применяться для моделирования угроз значимых объектов КИИ.

«При этом Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18 мая 2007 г., а также Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18 мая 2007 г., могут применяться для моделирования угроз безопасности информации на значимых объектах критической информационной инфраструктуры Российской Федерации.»

13 февраля 2019 года в рамках IX конференции «Актуальные вопросы защиты информации», представитель ФСТЭК России дал дополнительный комментарий по данной проблеме: *«Комиссия по категорированию должна руководствоваться уже имеющейся моделью угроз хотя бы на концептуальном уровне, а также перечнем актуальных угроз из Банка данных угроз безопасности информации ФСТЭК России.»* Комментарий касается базовой модели угроз безопасности персональных данных при их обработке в ИСПДн.

Таким образом присвоение объекту КИИ одной из категорий значимости должно основываться в том числе и на данных из модели угроз объекта КИИ.

Сравнение методик моделирования угроз безопасности информации объекта КИИ

Рассмотрим подробнее документы, на основе которых ФСТЭК России предлагает разрабатывать модель угроз для объекта КИИ, а именно «Базовая модели угроз безопасности персональных данных при их обработке в ИСПДн» и «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры».

Согласно 152-ФЗ от 27.07.2006 «О персональных данных» – основная цель моделирования угроз безопасности персональных данных, определить наиболее опасные и актуальные для ИСПДн способы атак и сценарии воздействий, для того чтобы далее подобрать для них контрмеры. Однако при данном подходе моделирования совершается ряд избыточных действий, которые в рамках 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» не несут существенной пользы. Основная цель анализа угроз в рамках категорирования объектов КИИ – это оценить максимально возможный ущерб. В рамках моделирования угроз в ИСПДн, расчет потенциального ущерба переносится на второй план, а основное внимание концентрируется на актуальных угрозах и способах атак на систему. Такая модель угроз не способна формализовать всю необходимую информацию для обеспечения безопасности объекта КИИ, и может использоваться только на концептуальном уровне. Т. о. применение документа «Базовая модели угроз безопасности персональных данных при их обработке в ИСПДн» не способно в полной мере удовлетворить все требования при моделировании угроз объекта КИИ.

Учитывая специфику нормативно-правовой базы КСИИ и базовый Федеральный закон 256-ФЗ от 29.12.2006 «О безопасности объектов топливно-энергетического комплекса (ТЭК)»*в котором были введены понятия КВО и КСИИ*, стоит упомянуть что в его тексте присутствуют следующие положения: «*В целях обеспечения безопасности объектов ТЭК субъекты ТЭК создают на этих объектах системы защиты информации и ИТКС от неправомерного доступа к информации и иных неправомерных действий и обеспечивают функционирование таких систем.*»

Наряду с этим, в документе «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры», КСИИ рассматривается как: «*информационно-управляющая или ИТКС, которая осуществля-*

ет управление критически важным объектом (процессом), или информационное обеспечение управления таким объектом (процессом) в результате деструктивных информационных воздействий на которую может сложиться чрезвычайная ситуация или будут нарушены выполняемые системой функции управления со значительными негативными последствиями.»

При анализе документа, утвержденного Советом Безопасности Российской Федерации в 2005 году «Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий», и пакета документов ФСТЭК России по обеспечению ИБ в КСИИ, утвержденных в 2007 году, можно сделать вывод, что среди систем, относящихся к КСИИ упоминаются системы, относящиеся к отрасли электроэнергетики и это в первую очередь АСУ ТП.

Таким образом, к КСИИ в первую очередь относятся автоматизированные системы управления технологическими процессами объектов атомной промышленности, топливно-энергетического комплекса, транспортной отрасли. Учитывая данные обстоятельства возникает конфликт в терминологии и общем описании объекта информационной инфраструктуры, т.к. согласно 187-ФЗ, объектам дается более широкое определение, а именно: «объекты КИИ– информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ.»

Оценка возможного ущерба от реализации угроз безопасности информации объекта КИИ

Из представленной выше информации можно сделать вывод, что на данный момент в нормативно-правовой базе РФ не существует документа, который регламентирует моделирование угроз безопасности информации в критических информационных инфраструктурах на должном уровне [1]. Из этого следует необходимость в создании такой методики, которая будет соответствовать актуальной нормативно-правовой базе в сфере КИИ и будет удовлетворять все требования при моделировании угроз объекта КИИ.

Учитывая установленные Постановлением правила категорирования [3, 4], основновная задача моделирования угроз объектов КИИ – оценка максимального возможного ущерба, будет происходить по заданным показателям значимости, а именно: социальная, политическая, экономическая, экологическая и значимость для обеспечения обороны страны. Величину ущерба, в соответствии с Постановлением, следует оценивать качественно по вербальной шкале. При этом предлагается каждый определенный показатель значимости (I, II, III категория) приравнять к качественным показателям ущерба. I категория – Максимальный ущерб, II категория – Средний ущерб, III – Низкий ущерб. Согласно правилам категорирования [4], любому полученному комиссией по категорированию значению показателя значимости должна быть присвоена категория, а результирующие данные должны быть перенаправлены в ФСТЭК России. По этому всем показателям значимости, значение которых не привышает минимальное значение III категории будет соответствовать Минимальный показа-

тель ущерба. Присвоение ИС, АСУ ТП или ИТКС такого показателя говорит о том что объект КИИ не является значимым. Данный шаг направлен на упрощение работы комиссии по категорированию и самого процесса категорирования в целом.

Рассмотрим возможный варианты определения степени на примере экологического ущерба. Экологический ущерб оценивается в том случае, когда вследствие нарушений доступности или целостности системного, прикладного программного обеспечения или используемых данных может произойти нарушение функционирования объекта КИИ и с развитием чрезвычайной ситуации, связанной с гибелью людей или нарушением условий их жизнедеятельности. Определение величины (степени) экологического ущерба производится по двуп показателям, на основе данных о масштабе прогнозируемой чрезвычайной ситуации и количистве людей, которые могут быть подвержены вредным воздействиям. Комиссия по категорированию при моделировании угроз, методом экспертных оценок определяет каждый из показателей ущерба (правила оценки возможного экологического ущерба приведены в таблице 1, 2) и формирует итоговый показатель на основе максимальной оценки полученной экспертами.

Т.о. комиссия получает актуальную оценку возможного ущерба при моделировании угроз объекта КИИ. Данная экспертная оценка служит одним из обоснований присвоения категории значимости объекту КИИ в процессе категорирования и непосредственно влияет на качество применяемых решений комиссией. Предложенная методика соответствует актуальной нормативно-правовой базе в сфере КИИ и удовлетворяет все требования при моделировании угроз объекта КИИ.

Таблица 1

Правила оценки возможного экологического ущерба

	Территориальный масштаб экологических последствий		
	Вредные экологические воздействия на оркужающую среду в пределах территории нескольких субъектов РФ или за пределами территории города федерального значения	Вредные экологические воздействия на оркужающую среду в пределах территории одного субъекта РФ или города федерального значения	Вредные экологические воздействия на оркужающую среду на территории одного муниципального образования или одной внутригородской территории города федерального значения
Возможный экологический ущерб	Низкий	Средний	Высокий

Таблица 2

Правила оценки возможного экологического ущерба

	Масштаб экологических последствий по кол. людей			
	Вредные экологические воздействия на людей, до 50 тыс. человек	Вредные экологические воздействия на людей, от 50 до 1000 тыс. человек	Вредные экологические воздействия на людей, от 1000 до 5000 тыс. человек	Вредные экологические воздействия на людей, от 5000 или более тыс. человек
Возможный экологический ущерб	Минимальный	Низкий	Средний	Высокий

Вывод

Обзор современных проблем моделирования угроз безопасности информации объектов КИИ выявил недостатки в текущей нормативно-правовой базе в сферее КИИ. Недочеты в сопутствующих методиках к данному закону связаны с новизной всей сферы КИИ и отсутствием накопленной базы прецендентов информационной безопасности. Но наряду с этим, стоит учитывать и то, что выполнение требований 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации» необходимо осуществлять с момента вступления документа в силу. Для устранения недочетов в сфере КИИ и упрощения выполнения требований закона могут применятся следующие решения:

- создание методики оценки возможного ущерба от реализации угроз безопасности информации объекта КИИ;
- создание методики моделирования угроз безопасности информации объекта КИИ;
- создание автоматизированной системы категорирования объектов КИИ.

Все указанные решения должны разрабатываться в соответствии с актуальной нормативно-правовой базой в сфере КИИ и удовлетворять всем требованиям категорирования объектов КИИ.

Список литературы

1. Рытов, М.Ю. Автоматизация процесса оценки уровня информационной безопасности объекта информатизации / М.Ю. Рытов, А.П. Горлов// Информация и безопасность. – 2014. – Т.17, вып.2. – С. 280-283.
2. Федеральный закон №187-ФЗ от 26.07.2017 «О безопасности КИИ РФ»
3. Постановление Правительства РФ №127 от 08.02.2018 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»
4. Постановление Правительства Российской Федерации от 13.04.2019 № 452 "О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127"

Материал поступил в редколлегию 26.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

Рытов Михаил Юрьевич, *к.т.н., доцент, зав. каф. «Системы информационной безопасности»*
ФГБОУ ВО «Брянский государственный технический университет»
Россия, г. Брянск
e-mail: rmy@tu-bryansk.ru

РАЗРАБОТКА ЧИСЛЕННОГО МЕТОДА АНАЛИЗА И ОЦЕНКИ ХАРАКТЕРИСТИК ИНФОКОММУНИКАЦИОННЫХ ПРОЦЕССОВ В СРЕДЕ ИНФОРМАЦИОННЫХ ПОРТАЛОВ

Рассмотрен численный метод анализа и оценки характеристик инфокоммуникационных процессов в процессе разработки алгоритмов информационного обмена в среде информационного портала органов исполнительной власти.

При решении задач, возникающих в процессе разработки алгоритмов информационного обмена в среде информационного портала органов исполнительной власти (ИП ОИВ), появляется потребность в сведениях о характеристиках алгоритма, не содержащихся в дисперсии и математическом ожидании анализируемой случайной величины. К классу таких задач следует отнести [1]:

1) выявление распределения времени доставки массива данных заданного приоритета и длины (фиксированной или переменной) в сквозном тракте среды ИП «пользователь-отправитель – пользователь-получатель»;

2) определение характеристик процесса занятия памяти в межсетевых шлюзах и компонентах среды информационного портала (КИП) в динамике обмена массивами данных;

3) определение характеристик производительности КИП.

Для решения поставленной задачи обоснованно применяется численный метод графической оценки и анализа (МГОА или GERD - сети), а компоненты среды ИП ОИВ в качестве узлов стохастических сетей. В процессе решения задачи введены ограничения, обусловленные отсутствием последствия при обработке массивов данных в КИП [2].

Формализация процессов обмена массивами данных в среде ИП ОИВ. Последовательность действий в процессе реализации обмена массивами данных инфокоммуникационного процесса B' представим в соответствии общими принципами МГОА множеством узлов и ориентированных дуг, объединенной стохастической сетью. Отметим, что, в этом случае, дискретные состояния технических и программных средств соответствуют узлам, участвующим в реализации инфокоммуникационного процесса. Что касается возможных направлений движения в пространстве дискретных состояний, то они могут, в этом случае, описываться соответствующими дугами. В рассматриваемом классе задач обработки массивов данных примем следующие условия [2]:

1) Если на любой вход каждого узла поступает сигнал только по одной из возможных дуг, то входная функция характеризуется выполнением операции.

2) Выходные функции узлов инфокоммуникационного процесса классифицируются как детерминированные и вероятностные. В случае вероятностного характера функций и узлов должно выполняться равенство $\sum_{k'=1}^{z^{\bullet}} \overline{w}_{k'} = 1$, где Z^0 – число дуг, исходящих из узла инфокоммуникационного процесса, $\overline{w}_{k'}$ – вероятность включения k'-й дуги (рис. 2).

3) Процессы, связанные с реализацией операций в отдельных узлах инфокоммуникационного процесса, будем полагать независимыми. Это позволяет утверждать, что данная модель не может быть применена для инфокоммуникационных процессов, описываемых сложными цепями Маркова или, если такие цепи используются в качестве компонентов общего описания.

4) Исследуемые характеристики инфокоммуникационного процесса обладают свойством аддитивности.

Условия 1) – 4) позволяют трактовать анализируемые инфокоммуникационные процессы, как стохастические сети, содержащие МГОА-узлы и МГОА-дуги. Общее описание стохастических сетей, отображающих конкретные инфокоммуникационные процессы, может быть сделано с учетом условий 1) – 3), стандартными методами вероятностных графов.

Представим инфокоммуникационный процесс B' в виде стохастической сети K^0 (D^0, C^0), которая включает множество D^0 МГОА-узлов и C^0 МГОА-дуг. Для каждой пары узлов $x,y \in D^0$ стохастической сети инфокоммуникационного процесса K^0 введем условные вероятности (при дискретном распределении) или плотность распределения (при непрерывном распределении) $f(g_{xy})$ случайной величины характеристики алгоритма g_{xy}. Тогда, если узлы x, y не соединены, то принимает значение $f(g_{xy}) = 0$.

Каждой паре МГОА-узлов $x,y \in D^0$ может соответствовать ряд анализируемых характеристик g_{xy}. Предположим, что часть анализируемых характеристик задается дискретными, а часть непрерывными распределениями. Отметим, что задание, таким образом, характеристик типично для расчета достоверности массивов данных. Что касается времени доставки массива данных, то здесь целесообразно применение непрерывных распределений. Такая градация при выборе распределения анализируемых характеристик является несколько условной. Это обусловлено тем, что всегда может иметь место предельный переход от дискретной величины к непрерывной. Такие условия могут возникнуть при достаточно большом значении длины массива данных.

Список литературы

1. Еременко, В.Т. Теоретические основы управления процессами обработки информации в среде информационных порталов региональных органов исполнительной власти [Текст]+[Электронный ресурс]: монография/ В.Т. Еременко, М.Ю. Рытов, – Тирасполь: Изд-во Приднестр. ун-та, 2017. – 256 с.

2. Еременко, С.В. Теоретические основы управления обменом данными

в среде корпоративного портала промышленного предприятия [Текст]+[Электронный ресурс]: монография/ С.В. Еременко, М.Ю. Рытов, К.А. Мегаев – Брянск: БГТУ, 2014. – 196 с.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

***Свечников Дмитрий Александрович**, к.т.н., сотрудник*
***Кривко Дмитрий Витальевич**, сотрудник*
***Степина Олеся Александровна**, сотрудник*
Академия ФСО России
Россия, г. Орёл
e-mail: yuaa33@academ.msk.rsnet.ru

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ РЕАЛИЗАЦИИ L2 И L3 VPN ТУННЕЛЕЙ В ПРОГРАММНО-АППАРАТНОМ КОМПЛЕКСЕ VIPNET COORDINATOR HW

Представлены результаты исследований особенностей реализации L2 и L3 VPN туннелей в программно-аппаратном комплексе ViPNet Coordinator HW 1000. Испытания проводились на основе специального программно-аппаратного стенда, состоящего из оборудования и программного обеспечения ViPNet.

В соответствии с требованиями руководящих документов подключение информационных систем и информационно-телекоммуникационных сетей, в которых обрабатывается конфиденциальная информация, к транспортным сетям общего пользования, в том числе сети "Интернет" должно осуществляется с использованием шифровальных (криптографических) средств соответствующего класса защиты [1].

Для обеспечения защиты информации, передаваемой между территориально удаленными сегментами сетей, применяются различные технологии и протоколы VPN. В настоящее время наибольшее распространение получили технологии VPN, реализованные на сетевом L3 и канальном L2 уровне ЭМВОС.

Для реализации криптографически защищенных соединений VPN на сетевом уровне L3 наиболее часто применяются протоколы Generic Routing Encapsulation (GRE) и IP Security (IPSec). Общей характеристикой данных протоколов является то, что исходный IP пакет отправителя целиком подвергается шифрованию и инкапсулируется в новый IP-пакет, а на приемной стороне он расшифровывается, извлекается и передается получателю. Для выполнения маршрутизации зашифрованных пакетов IP-адрес отправителя и IP-адрес получателя должны принадлежать разным IP-сетям.

Криптографическая защита соединений на канальном уровне L2 VPN обеспечивается посредством протоколов обеспечения безопасности при удаленном доступе L2TP, PPTP и др., а также протоколов VPN реализующих технологию L2overIP.

Особенность технологии VPN L2overIP в том, что она обеспечивает передачу кадров Ethernet между территориально удаленными объектами через транспортную сеть путем их шифрования и инкапсуляции в IP-пакеты посред-

ством протокола IPSec или его аналогов. Соединения могут быть установлены по схеме точка-точка Pseudo-Wire Emulation Edge to Edge (PWE3) или точка-многоточка Virtual Private LAN Service (VPLS). Кадр Ethernet, сформированный отправителем, зашифровывается и передается по транспортной сети без изменений, на приемной стороне он расшифровывается и доставляется получателю. В данном случае IP-адрес отправителя и IP-адрес получателя должны принадлежать одной подсети и могут даже совпадать.

В настоящее время на отечественном рынке СКЗИ выделяются следующие сертифицированные СКЗИ, позволяющие на базе одного устройства одновременно реализовывать L3 и L2 VPN туннели, это программно-аппаратный комплекс (ПАК) ViPNet Coordinator HW (класс защиты КС3) и криптомаршрутизаторы КМ-МПМ исполнений Р1 – Р4 (класс защиты КС3, КВ, КА). Данные СКЗИ имеют сертификаты ФСБ и ФСТЭК, которые подтверждают возможность их использования для криптографической защиты информации (шифрования и имитозащиты IP-трафика), не содержащей сведений, составляющих государственную тайну.

В ПАК ViPNet для создания проекта сети применяется программное обеспечение (ПО) ViPNet Administrator [2, 3]. В его состав входит ViPNet "Центр управления сетью" и "Удостоверяющий и ключевой центр".

С помощью ПО ViPNet "Центр управления сетью" создаются сетевые узлы и связи между объектами, настраиваются параметры узлов, выполняется централизованное обновление справочников, ключей и программного обеспечения. ПО ViPNet "Удостоверяющий и ключевой центр" обеспечивает формирование ключей узлов сети, издание и управление сертификатами пользователей.

ПАК ViPNet Coordinator HW выполняет функции: сервера ip-адресов, маршрутизатора VPN-пакетов, VPN-шлюза, сервера-маршрутизатора, межсетевого экрана и обеспечивает одновременное создание L2 и L3 VPN туннелей на базе одного изделия.

Для взаимодействия изделий ПАК ViPNet используется два протокола: IP/241 и IP/UDP, порт 55777. Первый применяется без использования ViPNet Coordinator, когда защищаемый узел имеет IP-адрес, доступный по правилам маршрутизации другим узлам, с которыми нужно установить соединение. Протокол IP/UDP применяется, когда соединения устанавливаются через ViPNet Coordinator со статической или динамической трансляцией IP-адресов.

В ПАК ViPNet L3 VPN туннели формируются между следующими изделиями:

- ViPNet Client – ViPNet Client;
- ViPNet Client – ViPNet Coordinator;
- ViPNet Coordinator – ViPNet Coordinator.

На рис. 1 представлен вариант схемы установления L3 VPN туннеля между двумя устройствами ViPNet Coordinator. Технология ViPNet L3 VPN обеспечивает взаимодействие узлов сети, как с установленным ПО ViPNet, так и без него.

Для создания L3 VPN туннелей необходимо на этапе формирования проекта сети посредством ПО ViPNet "Центр управления сетью" выполнить настройку ролей и связей для устройств ViPNet Client и ViPNet Coordinator.

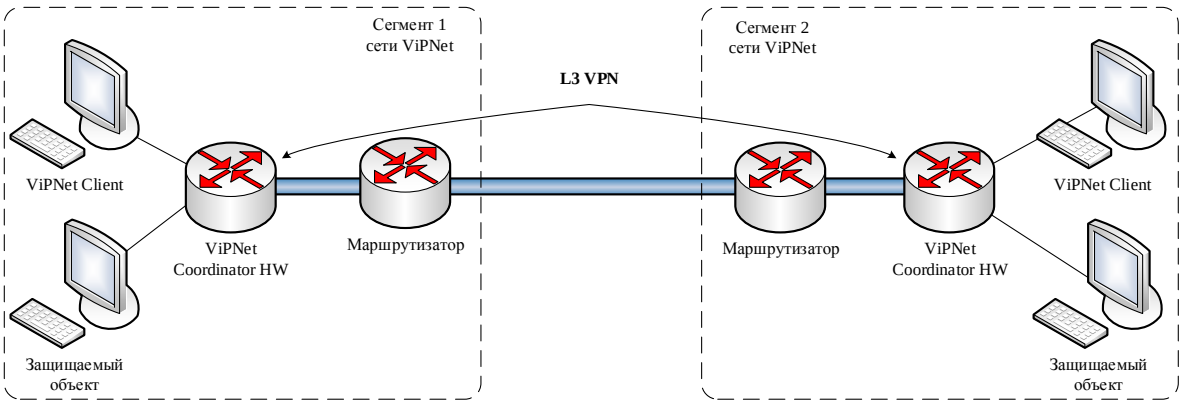


Рис. 1. Схема L3 VPN туннеля между устройствами ViPNet Coordinator

Для обеспечения криптографической защиты информации объектов, на которые не установлено ПО ViPNet, необходимо посредством ПО ViPNet "Центр управления сетью" выполнить настройку параметров туннелируемых соединений L3 VPN. К ним относятся: количество туннелируемых соединений, диапазон IP-адресов или IP-адрес объектов, чей трафик должен быть зашифрован.

Посредством ПО ViPNet "Удостоверяющий и ключевой центр" создаются ключи для всех устройств ViPNet.

При настройке ViPNet Coordinator указывается номер внешнего интерфейса, его IP-адрес, маска и IP-адрес шлюза, вводится полученный ключ и сетевые справочники, проверяется правильность функционирования L3 VPN туннеля.

Технологической особенностью настройки параметров L3 VPN туннеля является то, что все параметры задаются посредством ПО ViPNet "Центр управления сетью" на этапе создания проекта сети. Внесение изменений в существующие связи возможно только при повторной конфигурации сети и создании новых ключей и сетевых справочников.

Настройка параметров L3 VPN туннеля выполняется после введения в эксплуатацию ViPNet Coordinator HW, путем конфигурирования файла драйвера IpLir.

Технология L2 VPN в ПАК ViPNet Coordinator HW предназначена для обеспечения защищенного взаимодействия удаленных сегментов сети ViPNet, использующих единое пространство IP-адресов, и реализована посредством драйвера L2OverIP. ПАК ViPNet Coordinator HW позволяет объединить 31 сегмент сети, при этом одно устройство ViPNet Coordinator HW реализует подключение только одного сегмента (рис. 2). Для пользователей группа устройств ViPNet Coordinator HW выглядит как один большой L2 коммутатор. Кроме это-

го, технология ViPNet L2OverIP позволяет коммутировать объекты по специальному VLAN-идентификатору.

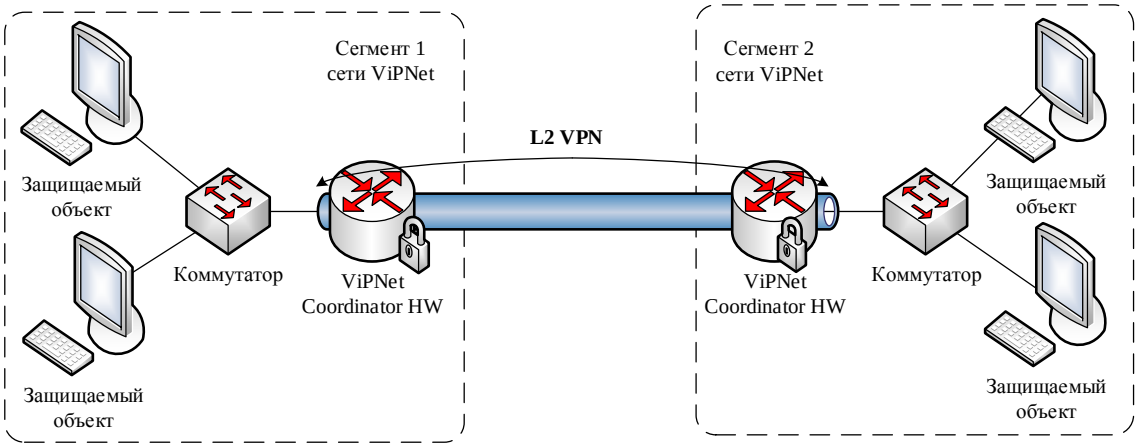


Рис. 2. Схема L2 VPN туннеля между устройствами ViPNet Coordinator

Для создания L2 VPN туннелей необходимо на этапе формирования проекта сети посредством ПО ViPNet "Центр управления сетью" выполнить настройку ролей и связей для устройств ViPNet Coordinator HW. Далее посредством ПО ViPNet "Удостоверяющий и ключевой центр" создать ключи для всех устройств ViPNet.

Настройка технологии L2OverIp осуществляется после введения в эксплуатацию устройства ViPNet Coordinator HW по следующему алгоритму:

- назначить сетевой интерфейс координатора, который будет использоваться при установлении соединений L2OverIp;
- указать номер локального порта и его IP-адрес;
- указать номер удаленного порта и его IP-адрес;
- выполнить команду для коммутации портов;
- создать правило фильтрации межсетевого экрана, разрешающее прохождение трафика.

Пример настройки драйвера L2OverIp представлен на рисунке 3.

Для демонстрации возможностей устройств ViPNet Coordinator HW было проведено испытание, в рамках которого на защищаемых объектах было установлено программное обеспечение Polycom PVX и организован сеанс видеосвязи.

```
Coordinator-3# inet ifconfig eth1 up
Coordinator-3# iplir set l2overip interface eth1
Coordinator-3# iplir set l2overip local-port 1 192.168.206.1
Coordinator-3# iplir set l2overip remote-port 2 192.168.206.2
Coordinator-3# iplir set l2overip mode switch
Module l2overip configured
Coordinator-3# firewall vpn add src @any dst @any proto 97 pass
Coordinator-3#
```

Рис. 3. Пример настройки драйвера L2OverIp

На рис. 4 представлено содержимое заголовка пакета, зашифрованного ViPNet Coordinator HW и записанного анализатором трафика Wireshark в транспортной сети передачи данных.

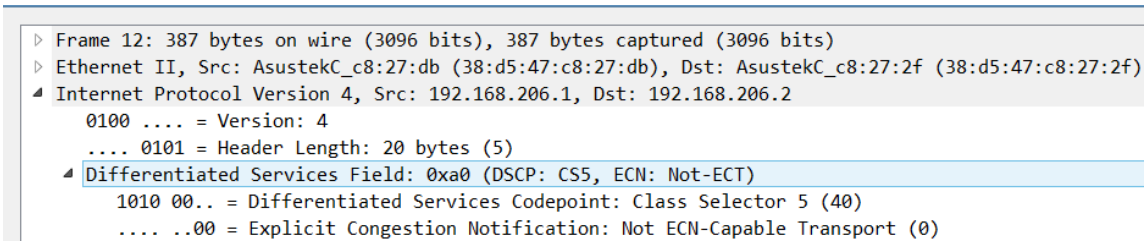


Рис. 4. Содержимое заголовка пакета, зашифрованного ViPNet Coordinator HW

Программное обеспечение позволяет определить приоритет трафика путем добавления в пакет метки DSCP 0xA0, которая обозначает 5-й класс. Как показывают исследования, устройства ViPNet Coordinator HW выполняют обработку трафика с учетом меток DSCP и обеспечивают их перенос в соответствующее поле зашифрованного ViPNet пакета. Это необходимо для того, чтобы оборудование транспортной сети также обеспечивало обработку пакетов в соответствии с определенной дисциплиной обслуживания.

Для повышения надежности связи в ViPNet также реализованы механизмы агрегации физических интерфейсов, переключения на резервный канал связи и балансировки нагрузки.

Основное отличие реализации в ViPNet технологий L2 и L3 VPN состоит в том, что в первом случае ViPNet Coordinator HW фрагментирует Ethernet-кадры, зашифровывает и упаковывает их в IP-пакеты специального формата (Ethernet в IP), а во втором – зашифровывается защищаемый IP-пакет и упаковывается в IP-пакет специального формата (IP в IP). Установление защищенных VPN соединений и передача данных между устройствами ViPNet Coordinator HW при этом не отличаются. Другой особенностью технологии L2OverIP является отсутствие в необходимости ПО ViPNet на защищаемых объектах.

Список литературы

1. Указ Президента РФ от 22.05.2015 №260 «О некоторых вопросах информационной безопасности Российской Федерации».

2. Технология построения VPN ViPNet: курс лекций / под ред. А. О. Чефрановой. – М.: Горячая линия-Телеком, 2017. – 338 с.

3. Администрирование системы защиты информации ViPNet версии 4: учебно-методическое пособие / под ред. А. О. Чефрановой. – М.: Горячая линия-Телеком, 2017. – 188 с.

Материал поступил в редколлегию 22.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056:004.272

Свечников Дмитрий Александрович, к.т.н., *сотрудник*
Кривко Дмитрий Витальевич, сотрудник
Степина Олеся Александровна, *сотрудник*
Академия ФСО России
Россия, г. Орёл
e-mail: yuaa33@academ.msk.rsnet.ru

КОНТРОЛЬ ЗАЩИЩЕННОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ВЕБ-ПОРТАЛОВ

Рассмотрен метод контроля защищенности программного обеспечения веб-порталов. Описаны основные направления проведения исследований и способы их реализации.

Наличие уязвимостей в веб-приложениях является одним из наиболее распространенных путей проникновения нарушителей в защищаемые информационные системы. Это подтверждается исследованиями, которые ежегодно проводятся экспертами компании Positive Technologies и др.

При этом, необходимо отметить, что в области анализа уязвимостей веб-приложений в настоящее время существует большое количество проектов и решений, например, Open Web Application Security Project (OWASP) и др. Основные средства характеризуются тем, что являются англоязычными, содержат большое количество разрозненных данных и касаются приложений, функционирующих, как правило, в открытых системах и сетях и не учитывают требования по обеспечению информационной безопасности руководящих документов России [1 – 4].

Контроль защищенности предполагает проведение тестов веб-портала и его компонентов для выявления уязвимостей, которые могут быть использованы нарушителем для реализации угроз ИБ [5]:

- контроль защищенности ПО;
- контроль защищенности веб-портала от НСД (Penetration Testing).

Контроль защищенности ПО веб-порталов и их компонент выполняется по следующим направлениям:

- выявление (поиск) дефектов безопасности программного обеспечения (Common Weakness Enumeration, CWE) на этапах его разработки и 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 нарушителей;
- 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 нарушителем;

- выявление (поиск) неразрешенного ПО (компонентов ПО);
- выявление уязвимостей "нулевого дня", о которых стало известно, но информация о которых еще не включена в сканеры уязвимостей;
- выявление новых уязвимостей, информация о которых еще не опубликована в общедоступных источниках;
- проверку правильности установки и настройки средств защиты информации, технических средств и ПО;
- проверку корректности работы средств защиты информации при их взаимодействии с техническими средствами и ПО;
- проверку своевременности обновлений ПО средств защиты информации, общесистемного и прикладного ПО;
- выявление (поиск) уязвимостей в информационной системе с использованием учетных записей на сканируемых ресурсах.

Контроль защищенности ПО осуществляется в сетевых службах и веб-приложениях.

Уязвимости ПО могут быть диагностированы следующими способами:

- идентификацией версии ПО веб-портала и поиском в базах данных уязвимостей (CWE, CVE и др.);
- запуском программ-тестов (эксплойтов), воспроизводящих в полном объеме или частично выполнение компьютерных атак с использованием уязвимостей.

В зависимости от начальных условий для выявления уязвимостей могут использоваться методы черного ящика и белого ящика.

При применении метода черного ящика исследователю предоставляется доступ к составным частям веб-портала на уровне протокола IP. Предметом исследования являются уязвимости сетевых служб компонентов веб-портала.

При использовании метода белого ящика исследователю предоставляется доступ к операционным системам, телекоммуникационному оборудованию, СУБД и серверам приложений с необходимыми правами доступа. Предметом исследования являются уязвимости программных компонент веб-портала, сведения о которых содержатся в используемой базе данных уязвимостей.

Степень важности выявленных уязвимостей целесообразно определять в соответствии с международной методикой Common Vulnerability Scoring System (CVSS).

Поиск уязвимостей в сетевых службах производится посредством метода черного ящика. Исследование включает:

- идентификацию серверов и рабочих мест по их IP-адресам или именам;
- идентификацию сетевых протоколов, доступных для взаимодействия;

- идентификацию программ, обеспечивающих реализацию указанных сетевых протоколов, с определением их наименований и версий по информации, передаваемой при сетевом взаимодействии;
- поиск идентифицированных уязвимостей в базах данных;
- поиск уязвимостей сетевых служб путем запуска соответствующих им эксплойтов.

Поиск уязвимостей в веб-приложениях осуществляется с помощью метода черного ящика. Определяется уязвимость веб-портала к атакам следующих типов:

- различные виды инъекций: SQL, LDAP, XPath и др.;
- подбор данных аутентификации;
- незащищенная передача данных;
- ошибки при разграничении доступа;
- межсайтовый скриптинг (XSS);
- подделка межсайтовых запросов (CSRF);
- расщепление и перенаправление запроса HTTP;
- идентификация приложений;
- чтение данных;
- переполнение буфера.

Выявление уязвимостей ПО выполняется с использованием метода белого ящика и включает:

- инвентаризацию установленного ПО, идентификацию наименований и версий программ, а также установленных обновлений безопасности;
- поиск уязвимостей в специальных базах данных.

Выявление учетных записей с известными паролями, проводится с использованием методов черного и белого ящика. В методе черного ящика реализуются попытки аутентификации с использованием имен и паролей из специального словаря. В методе белого ящика производится выборка хеш-значений паролей из конфигурационных файлов, таблиц баз данных и сравнение их с хеш-значениями паролей из используемого словаря.

По результатам исследований уязвимостей ПО оформляется отчет, включающий:

- обследованные компоненты веб-портала;
- выявленные уязвимости, оценку степени их критичности для обеспечения ИБ;
- рекомендации по устранению уязвимостей.

Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и эксплуатации информационной системы. Периодичность проведения диагностики на предмет выявления уязвимостей, информация о которых еще не опубликована в общедоступных источниках, устанавливается заказчиком.

В случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и

программном обеспечении, применяемом в информационной системе, поиск и анализ уязвимостей осуществляется немедленно.

Контроль проведения диагностики проводится с периодичностью, установленной заказчиком в организационно-распорядительных документах по защите информации и фиксируется в соответствующих журналах.

Разработанные предложения по проведению контроля защищенности программного обеспечения веб-порталов позволят оценить безопасность информационных систем, построенных на основе веб-технологий.

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 : ввод в действие с 01.09.14. – М. : Банк России, 2014. – 34 с.

5. Свечников Д.А. и др. Предложения по построению комплексной методики анализа защищенности информационных ресурсов веб-порталов [Электронный ресурс] // Информационная безопасность и защита персональных данных. Проблемы и пути их решения : материалы X межрегион. науч. практ. конф., Брянск, 30 апр. 2018 г. Брянск: БГТУ, 2018. С. 157–160. URL: http://mn.tu-bryansk.ru/files/IB2018.pdf (дата обращения 22.01.19.)

Материал поступил в редколлегию 12.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

Свечников Дмитрий Александрович, *к.т.н., сотрудник*
Кривко Дмитрий Витальевич*, сотрудник*
Степина Олеся Александровна, *сотрудник*
Академия ФСО России
Россия, г. Орёл
e-mail: yuaa33@academ.msk.rsnet.ru

ПРОГРАММНО-АППАРАТНЫЙ УЧЕБНО-ТРЕНИРОВОЧНЫЙ КОМПЛЕКС ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО НАСТРОЙКЕ И ЭКСПЛУАТАЦИИ ОБОРУДОВАНИЯ "VIPNET"

Рассмотрено применение программно-аппаратного учебно-тренировочного комплекса для подготовки специалистов по настройке и эксплуатации оборудования "ViPNet". Описаны основные задачи, решаемые посредством комплекса, его структура, используемые инновации и технологии.

Разработанный учебно-тренировочный комплекс предназначен для развития творческих способностей и самостоятельности обучающихся при изучении вопросов обеспечения информационной безопасности посредством применения средств криптографической защиты информации "ViPNet".

Основными целями создания комплекса являются: формирование у обучающихся способностей осуществлять эксплуатацию современных средств криптографической защиты информации (СКЗИ), находить и обосновывать рациональные организационно-технические решения по применению СКЗИ, обеспечивающие требуемое качество обслуживания абонентов.

Основные задачи, решаемые посредством комплекса:

– активизация познавательной деятельности обучающихся по вопросам применения СКЗИ;

– реализация возможности углубленного изучения способов криптографической защиты информации и закрепления обучающимися своих знаний и умений;

– структурирование и визуализация содержания учебного материала с целью эффективного его восприятия обучающимися;

– получение специальных профессионально-ориентированных компетенций в области профессиональной деятельности;

– совершенствование практических навыков и умений по настройке СКЗИ при решении вопросов защиты информации.

При реализации данного комплекса использованы следующие инновации [1]:

– реализация в процессе обучения профессионально-ориентированной технологии обучения;

– применение личностно-ориентированного подхода к процессу обучения;

– использование программ автоматизированного контроля знаний обучающихся;

– использование проблемных заданий, связанных с применением криптографических методов защиты информации.

В состав комплекса входят электронное учебно-методическое пособие (ЭУМП) и программно-аппаратный комплекс (ПАК).

ЭУМП включает в себя электронные учебные пособия, комплект технической документации, технологические карты и комплекс вспомогательных материалов для отработки теоретических и практических вопросов по изучению возможностей ПАК "ViPNet", свойств протоколов, применяемых для криптографической защиты информации, а также систему проверки и оценки знаний [2, 3].

Основными компонентами ЭУМП являются:

1. Методические рекомендации по изучению теоретического материала.
2. Методические рекомендации по выполнению практических заданий.
3. Справочная информация.
4. Система проверки и оценки знаний.

В состав ПАК входят следующие компоненты:

– ПО ViPNet Administrator, включающее программы "Центр управления сетью" (ЦУС) и "Удостоверяющий и ключевой центр" (УКЦ);

– ПО ViPNet Coordinator для ОС Windows и ОС Linux;

– ViPNet Coordinator HW-VA для работы в виртуальных средах VMware или Virtualbox;

– ViPNet Client.

Необходимые условия для функционирования ЭУМП:

– технологическая инфраструктура должна содержать компьютерные классы, оборудованные ПЭВМ с процессором не ниже Intel Core i5 CPU 3,20 ГГц, ОЗУ 8 Гб, с установленными ОС MS Windows и программным обеспечением, из расчета одна ПЭВМ на одного человека;

– подготовка преподавателей и обучающихся к использованию ЭУМП;

– управление познавательной деятельностью обучающихся на всех этапах образовательного процесса.

Основой комплекса является авторское программное приложение, отображающее по запросу пользователя текстовые и графические документы, позволяющее обучающимся осуществлять поиск как по содержанию, так и по ключевым словам. Программные компоненты разработаны на языке программирования C#. Применение данной технологии позволяет, с одной стороны, организовать интерфейс доступа к учебным материалам с встроенной функцией поиска, а с другой стороны – предоставить обучающимся возможность работы с различными форматами мультимедиа ресурсов.

Для реализации обучающего комплекса преподаватель должен сформировать структуру учебного материала, включающую тему, название и

вопросы учебных занятий. Элементы учебного материала представлены в виде отдельных модулей, связанных с разделом или темой гиперссылками. В материалы можно включать любые объекты (изображения, сценарии, элементы ActiveX, мультимедийные элементы). Допускается возможность вставки в текстовые документы таблиц, рисунков, гиперссылок, аудио- и видеофайлов, GIF-анимации, стандартных элементов Windows (кнопок, обычных и выпадающих списков).

После подготовки исходных файлов создается файл проекта и формируется его содержание. Затем с помощью языка программирования C# реализуется процесс компиляции, при котором отдельные файлы собираются в единый файл. Формат файлов данного типа поддерживается во всех версиях ОС Windows.

Разработанный комплекс применяется в процессе проведения групповых, практических и лабораторных занятий, курсового проектирования и самостоятельной работы. Ведущий преподаватель выдает обучающимся дистрибутив ЭУМП и разъясняет порядок его использования. Накануне занятий, на которых предполагается применение ЭУМП, проводятся консультации с указанием конкретных разделов. Преподаватель определяет порядок использования ЭУМП и последовательность проведения занятий.

При проведении практических и лабораторных занятий проводится проверка подготовленности обучающихся к занятию с применением системы проверки и оценки знаний. В ходе занятия преподаватель направляет познавательную деятельность обучающихся согласно методике проведения занятия. При этом каждый обучающийся имеет доступ ко всем методическим и программным продуктам ЭУМП.

Выполнение лабораторных занятий и курсового проектирования включает разработку системы защиты информации, позволяющей в соответствии с исходными данными реализовывать различные способы защиты информации: фильтрацию, межсетевое экранирование, преобразование IP-адресов и портов, шифрование информации, формирование VPN туннелей и др.

Применение ЭУМП способствует своевременному и качественному выполнению учебных задач на практических и лабораторных занятиях, самостоятельной работе под руководством преподавателя при выполнении заданий курсового проекта и самостоятельной работе.

Повышение качества подготовки обучающихся выразилось:

– в повышении активности обучающихся в ходе выполнения исследовательских задач по изучению свойств криптографических алгоритмов защиты информации;

– в углублении теоретических знаний и умений в области применения криптографических методов защиты информации;

– в получении дополнительного практического опыта по применению современных средств криптографической защиты информации;

– в развитии профессиональных компетенций.

Применяемые технологии обучения позволяют получить положительный развивающий и воспитательный эффект. Способствуют лучшему усвоению знаний и развитию творческих способностей обучающихся, формирую у будущих специалистов информационной безопасности четкое представление об условиях и необходимых требованиях по применению методов и средств криптографической защиты информации.

Внедрение данного обучающего комплекса позволяет преподавателю повысить динамику проведения занятий, более эффективно реализовывать дифференцированный подход в обучении, что способствует повышению качества подготовки специалистов.

Основными достоинствами являются: практическая направленность, проведение научных исследований, стимуляция познавательной активности обучающихся, привлечение к исследовательской деятельности посредством выдачи каждому обучающемуся индивидуального задания, возможность адаптации содержания комплекса к изменению ФГОС.

Список литературы

1. Корольков, А. Ф. Методика разработки электронного учебно-методического комплекса по дисциплине для дистанционного обучения: учеб. Пособие / А. Ф. Корольков, Ю. Р. Стратонович, В. В. Фролова. – М.: Изд-во МСХА, 2004. – 83 с.

2. Технология построения VPN ViPNet: курс лекций / под ред. А. О. Чефрановой. – Москва: Горячая линия - Телеком, 2017. – 338 с.

3. Администрирование системы защиты информации ViPNet версии 4: учебно-методическое пособие / под ред. А. О. Чефрановой. – М.: Горячая линия-Телеком, 2017. – 188 с.

Материал поступил в редколлегию 12.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056.53

С.В. Усов
ФГБОУ ВО «Омский государственный университет им. Ф.М. Достоевского»
Россия, г. Омск
e-mail: raintower@mail.ru

О ВОЗМОЖНОСТИ ПРЕДСТАВЛЕНИЯ РОЛЕВЫХ ПОЛИТИК БЕЗОПАСНОСТИ В РАМКАХ МОДЕЛИ OOHRU

Рассматривается возможность представления ролевых политик безопасности с помощью объектно-ориентированных дискреционных моделей разделения доступа.

Объектно-ориентированные дискреционные политики безопасности, актуальность которых вызвана возрастающей частотой применения объектно-ориентированного подхода при построении компьютерных систем, описаны в работе [1]. По сравнению с традиционной дискреционной моделью Харриссона-Руззо-Ульмана [2], известной с 70-х годов прошлого века, расшился охват систем, поддающихся представлению с помощью модели OOHRU. С точки зрения устройства самой модели, модификации подверглись структура объектов, элементарные операторы, структура команд. Объекты системы распределены по классам по структурным и семантическим признакам.

Фактически, более широкий спектр инструментов позволяет описывать с помощью OOHRU другие модели разграничения доступа (возможно, с некоторыми ограничениями). Данная работа посвящена возможности описания инструментарием OOHRU ролевых моделей.

Ролевые политики разграничения доступа стали широко известны только в 90-х годах после выхода работ Феррайоло и Куна [3]. Компьютерная система представляется совокупностью следующих множеств: множества пользователей $\boldsymbol{U}$, множества ролей $\boldsymbol{R}$, множества полномочий $\boldsymbol{P}$ и множества сеансов $\boldsymbol{C}$ работы пользователей с системой. Множество объектов системы не задается в явном виде, а представляется через множество полномочий $\boldsymbol{P}$: каждое полномочие фактически заключает в себе отношение на декартовом произведении множества прав доступа и множества объектов системы.

На множестве ролей в реальных системах обычно возникает иерархия, индуцированная организационно-управленческими схемами организаций, в которых эксплуатируется система. Как правило, подчиненность ролей в иерархии включает наследование прав и полномочий, которое может быть направлено как «снизу», так и «сверху».

При наследовании «сверху» подчиненный субъект наследует права родительских субъектов. Такой подход, тесно связанный с объектно-ориентированной парадигмой, редко упоминается при рассмотрении ролевых

моделей разграничения доступа, но на деле бывает очень полезен, когда иерархия ролей строится путем «от абстрактного к конкретному». Так, например, можно рассмотреть фрагмент иерархии «Сотрудник – Сотрудник финансового отдела – Бухгалтер – Главный бухгалтер». Здесь каждая последующая роль цепочки является уточнением предыдущей. Сохраняя полномочия роли-родителя, она получает новые полномочия.

Однако базовые ролевые модели эксплуатируют наследование «снизу». Здесь можно выделить три ключевых подхода к построению иерархии:

1. Строгий таксономический листовой подход. Все множество полномочий разбивается на непересекающиеся подмножества, каждое из подмножеств приписывается листу дерева иерархии ролей. Роль в нелистовой вершине наделяется множеством полномочий, являющимся объединением множеств полномочий непосредственно подчиненных ролей (соответствие между ролями и полномочиями, таким образом, индуцируется полномочиями листовых вершин и устанавливается при движении по дереву ролей снизу вверх).

2. Нестрогий таксономический листовой подход. Единственное отличие от предыдущего подхода – отсутствие требования на запрет пересечения подмножеств полномочий, сопоставленных листовым вершинам.

3. Иерархически охватный подход. Граф такой иерархии ролей не обязан быть деревом (но, конечно, не может содержать сильных циклов). При таком подходе считается, что если пользователю сопоставлена некоторая роль $r \in \boldsymbol{R}$, то ему также должны быть сопоставлены и все роли, подчиненные r. Что позволяет исключить из роли r полномочия, уже содержащиеся подчиненных ей ролях.

В работе [1] была предложена иерархическая модель OOHRU, устройство которой подразумевает, что объект o, находящийся на более низком уровне иерархии, чем объект o', обладает меньшим набором прав (как в отношении доступа к другим объектам, так и в отношении ограничения доступа других объектов по отношению к себе) по сравнению с объектом o'. Такая структура может быть успешно использована для представления иерархии ролей в базовых ролевых моделях.

Результатом данной работы является ряд следующих утверждений (каждое из которых доказывалось отдельно, поскольку различные виды иерархий ролей, эксплуатируемые в ролевых моделях, требовали индивидуального подхода к построению реализующих их иерархических моделей OOHRU, за исключением двух случаев таксономического листового подхода, которые были реализованы одной и той же конструкцией модели OOHRU):

Теорема 1. Для любой субъектно-объектной базовой ролевой модели, свободной от иерархии, существует реализующая ее иерархическая модель OOHRU.

Теорема 2. Для любой субъектно-объектной иерархической ролевой модели с наследованием «сверху» существует реализующая ее иерархическая модель OOHRU.

Теорема 3. Для любой субъектно-объектной иерархической ролевой модели с таксономическим листовым подходом к наследованию существует реализующая ее иерархическая модель OOHRU.

Теорема 4. Для любой субъектно-объектной иерархической ролевой модели с иерархически охватным подходом к наследованию существует реализующая ее иерархическая модель OOHRU.

Общий алгоритм построения модели OOHRU, реализующей ролевую политику безопасности, следующий:

1. Из полномочий ролевой модели «вычленяем» множество объектов системы и множество прав доступа к ним.
2. Формируем иерархию на множестве классов модели OOHRU. Иерархия строится в любом случае, даже при представлении ролевой модели, свободной от иерархии: в этом случае, например, каждому подмножеству α множества ролей системы сопоставляется свой класс k_α, частичный порядок на классах индуцируется соответствующими им подмножествами ролей (по включению).
3. Отдельно создается класс, содержащий все объекты системы (полученные в пункте 1), и класс пользователей системы.
4. При назначении пользователя u на роль (набор ролей) α в классе k_α, соответствующем этой роли (набору ролей) создается объект, соответствующий пользователю u, и методам этого объекта даются разрешения на доступ, индуцированные полномочиями набора ролей α. Разрешения отражаются в матрицах доступов путем их модификации средствами команд OOHRU.

Список литературы.

1. Усов, С.В. Неоднородные объектно-ориентированные модели с иерархией. Проблемы обработки и защиты информации. Книга 3. Модели разграничения доступа. – Коллективная монография / под общей редакцией С.В. Белима. – Омск: ООО «Полиграфический центр КАН», – 2013. – С. 93-114.
2. Harrison M.A., Ruzzo W.L., Ulman J.D. Protection in Operating Systems // Communications of the ACM. – 1975. – p. 14-25.
3. Ferraiolo D. F., Kuhn D. R.. Role-Based Access Control. 15th National Computer Security Conference, October 1992. – p. 554–563,

Материал поступил в редколлегию 26.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 5.007

Халимов Дж.М.
Научный руководитель: к.т.н., доц. М.Ю. Рытов
ФГБОУ ВО «Брянский государственный технический университет»
Россия, г. Брянск
h_jamshed@bk.ru

МЕТОДЫ АУТЕНТИФИКАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ TFMIS SGB.NET

Описана существующая процедура аутентификации и рассматрено ее применения ко всем потенциальным пользователям информационной системы TFMIS SGB.net. Раскрыт механизм процесса аутентификации и предлагается алгоритм новой формы модели.

Достижения поставленных целей, применяемых сегодня в информационной безопасности для активных информационных систем прежде всего основано на правильном обеспечении аутентификации пользователей из числа сотрудников, партнеров, клиентов и гостей системы в целом. Управление процессом аутентификации и авторизацией пользователей становится более сложной при использовании ресурсов, активно проходящих транзакцию в информационных потоках.

Централизуя управление безопасности при выполнении функции защиты системы, аутентификация позволяет повысить уровень надежности использования информационной системы. В процессе применения механизма многофакторной аутентификации, повышается процедура контроля распределения ступенчатой роли доступа к информационным сервисам. Контролируемая процедура доступа в систему включает в себя аудит на уровне разделения и распределения соответствующих прав пользователей.

Необходимо отметить, что за время аутентификации пользователя системы происходит проверка его целостности и функция разрешительного порядка доступа с соблюдением политики безопасности. удовлетворяющий результатам авторизации, для предотвращения несанкционированного доступа к информационным ресурсам.

Алгоритм работы данной функции прежде всего направлен на ограничения и распределения прав доступа к системе от несанкционированного доступа неавторизированных и не идентифицированных пользователей.

Следует отметить, что процесс аутентификации различается по степени защиты и группы классов, основанных на статистических и динамических методах авторизации пользователя, независимо от объекта и субъекта взаимной проверки подлинности системы.

Характерной схемой при использовании важных систем, связанных с финансовой политикой, транзакцией и приемом выдачей денежных средств ис-

пользуют двухфакторные методы на базе различных классов защиты информации.

Сегодня, все сервисы, обеспечивающие подлинность пользователей в сочетании с логическим контролем доступа, находятся на сервере данных, данные и ресурсы которых распределенные по резервным репликантам. Прежде всего все функции безопасности, обеспечивающие взаимосвязь между получением доступа пользователя (имитации) и ее модификацией направлены на сохранения информационных ресурсов для предотвращения несанкционированного доступа к системе. На этапе авторизации, пользователь аутентифицирует свою подлинность серверу на основе двухстороннего идентификатора, сеанса связи. Отсутствие механизмов аутентификации и контроля менеджмента на уровни конфиденциальности, целостности и доступности с использованием набора эффективных функций безопасности, требует определенную степень уверенности в надежности любой информационной системы, независимо от параметров ее внедрения.

В свою очередь используемая в государственных учреждениях, внедренная система управления государственными финансами Республики Таджикистан (TFMIS SGB.net) не исключения. Она является неотъемлемой частью электронного правительства и предназначена для регулирования и управления финансовыми транзакциями с элементами встроенной интеграции бухгалтерских операций. Аутентификация этой системы построена на базе ступенчатой роли и распределена по категориям пользователей. Алгоритм системы предполагает пошаговую авторизацию пользователей с учетом функциональных требований к применяемым режимам функционирования.

Авторизация в системе TFMIS SGB.net проходит с целью проверки подлинности пользователя и данных источника. За продолжительностью сеанса отвечает специальная процедура проверяющая данные пользователя с источником для получения доказательства о субъекте на уровне программно-технических средств. Проверка подлинности необходима для содержания информационных ресурсов в состоянии активности и защищенности, строго говоря обеспечить надежность и сохранность аутентификационных данных.

В системе TFMIS SGB.net основным методом аутентификации считается парольная авторизация идентификационного ключа, присвоенная каждому субъекту в отдельности по уровню и распределению прав доступа к модулям информационной системы.

Само по себе аутентификация в системе TFMIS SGB.net является шифровальным средством, охватывающим ключевую информацию к получению доступа защищаемых ресурсов, циркулирующих при финансовых операциях. Наличие такой процедуры в информационной системе считается обязательным условием при распределении прав доступа субъектов к объектам, измеряющих биометрические параметры пользователя к существующим модулям системы TFMIS SGB.net.

При аутентификации в системе TFMIS SGB.net, она сравнивает идентификаторы авторизованного пользователя в базе идентификаторов, а затем на осно-

ве предоставленного статуса и полномочий предоставляет доступ к информационным ресурсам. Система защищена от случайных наборов символов и при вводе таких значений выдает ошибку с отрицательным результатом. На этапе разработки интерфейса авторизации, в информационной системе не была предусмотрена процедура временной блокировки, возникающей после превышения ограничений ввода аутентификационных данных, поэтому пользователю системы TFMIS SGB.net данное условие неприменима. При завершении процедуры аутентификации и определению полномочий по уровню доступа к данным и модулям системы, включается процесс циклического контроля и механизма защиты за информационными ресурсами.

В процессе работы с модулями системы происходит протоколирование данных и аудит состояния обращающихся циклов, обеспечивающая идентификацию каждого блока при транзакции финансовых данных, тем самым предохраняя информационные ресурсы от модификации и изменения в информационной системе TFMIS SGB.net.

Сегодня на этапе подключения всех государственных учреждений республики Таджикистан к информационной системе TFMIS SGB.net возникла необходимость подключения дополнительного блока аутентификации пользователя на базе электронно-цифровой подписи, обеспечивающая конфиденциальность и аутентификацию данных, являющимся обязательным элементом безопасности на основе сформированного и идентичного крипто ключа пользователя.

Такая аутентификация служит для последующего контроля санкционированного доступа владельца ключа к отдельным блокам и элементам системы, одновременно проверяя уровень доступа по матрице разграничения прав пользователей.

Такую форму безопасности можно присудить к категории постоянной аутентификации делающие обращения к авторизованному ключу от сеанса к сеансу финансовой транзакции в системе TFMIS SGB.net.

Рассмотрев существующую структуру метода аутентификации информационной системы TFMIS SGB.net, автором предлагается для укрепления ее сущности прежде всего применить диапазон блокировки и ограничения ввода данных, при не соответствии идентификаторов пользователя, либо после ограничительного ввода применить другие модели подтверждения подлинности, с целью запуска нового сеанса для авторизации идентификационных данных.

Применения новых критерий регулирующих процесс безопасности не должен быть обременительным, его эффект должен быть новым уровнем защиты процесса финансовых транзакций и сократить риск несанкционированного доступа, не только по корпоративной сети, но и в сети интернет.

Примерный алгоритм процедуры аутентификации в системе TFMIS SGB.net с условием всех категорий безопасности предлагается в следующем рисунке 1:

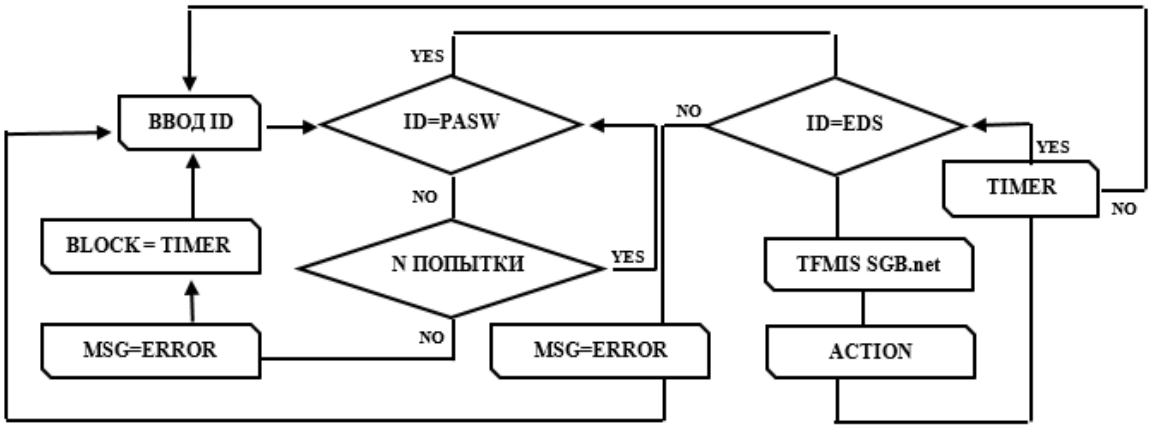


Рис. 1. Механизм аутентификации информационной системы TFMIS SGB.net

Список литературы

1. Варфоломеев, А.А. Основы информационной безопасности: учеб. пособие. – М.: РУДН, 2008. – 412 с.

2. Марков, А.С. Методы оценки несоответствия средств защиты информации / А.С.Марков, В.Л. Цирлов, А.В.Барабанов; под ред. А.С.Маркова. – М.: Радио и связь, 2012. – 192 с.

3. Блинов, А.М. Информационная безопасность: учебное пособие. Часть 1. – СПб.: Изд-во СПбГУЭФ, 2010. – 96 с.

4. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. — М.: ИД «ФОРУМ»: ИНФРА - М , 2011. – 416 с.

Материал поступил в редколлегию 25.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056.55

П.Г. Черепанов
Научный руководитель: д.физ.-мат.н., проф. С.В. Белим
ФГБОУ ВО «ОмГУ им. Достоевского»
Россия, г. Омск
sbelim@mail.ru, pcherepanov@gehtsoft.com

ВЫБОР ОБЛАСТЕЙ ДЛЯ ВСТРАИВАНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В ВИДЕОПОТОК

Предложен алгоритм встраивания цифровых водяных знаков в видеоконтейнер с использованием трехмерного дискретного косинусного преобразования и голограммы. Проведено исследование по выборке областей для встраивания.

Описание предложенного алгоритма для встраивания

Как основа для алгоритма встраивания используется модифицированный до трехмерного случая метод Жао и Коха. Видеопоток представляется как трехмерный набор точек, в котором в качестве координаты Z определяется номер кадра, а в качестве X и Y – положение точки непосредственно на кадре. Для встраивания видеопоток разбивается на блоки по N кадров в каждом. Далее каждый блок разбивается на подблоки из N×N пикселей, слева-направо, сверху-вниз. В результате получается набор блоков размером N×N×N. Если не получается сформировать какие-то блоки полностью, то такие блоки не участвуют при встраивании и извлечении. Далее для каждого полученного блока следующим образом высчитываются спектральные коэффициенты дискретно-косинусного преобразования:

$$f^{i}_{\upsilon,\nu,\kappa} = \left(\zeta(\upsilon)\cdot\zeta(\nu)\cdot\zeta(\kappa) \Big/ \sqrt{\frac{8}{N^3}} \right) \times \sum_{x=0}^{N-1}\sum_{y=0}^{N-1}\sum_{z=0}^{N-1} f^{i}_{x,y,z} \cdot \cos\left(\frac{\pi\cdot\upsilon\cdot(2\cdot x+1)}{2\cdot N} \right) \times$$

$$\cos\left(\frac{\pi\cdot\nu\cdot(2\cdot y+1)}{2\cdot N} \right) \cdot \cos\left(\frac{\pi\cdot\kappa\cdot(2\cdot z+1)}{2\cdot N} \right)$$

, где $f_{\upsilon,\nu,\kappa}$ - значение спектрального коэффициента дискретно косинусного преобразования для точки (υ,ν,κ), $f^{i}_{x,y,z}$ - значение яркостной компоненты в изначальном кадре для точки (x,y,z), а $\zeta(\upsilon)$ для произвольной точки υ вычисляется следующим образом

$$\zeta(\upsilon) = \begin{cases} \frac{1}{\sqrt{2}}, & \text{если } \upsilon > 0 \\ 1, & \text{если } \upsilon = 0 \end{cases},$$

Для того чтобы обеспечить максимальное соотношение устойчивости встраивания к заметности, встраивание осуществляется в область среднечастотных компонент. Выбираются две точки: $(\upsilon_1, \nu_1, \kappa_1)$, $(\upsilon_2, \nu_2, \kappa_2)$. Экспериментальным образом определяется величина порога разности модулей коэффициентов Р. В качестве ЦВЗ используется монохромное изображение. Для повышения устойчивости встраивания используется не само изображение, а его цифровая голограмма. Для построения голограммы когерентный луч света разделяется на два луча – опорный и объектный. Объектный луч направляется на исходное изображение, а опорный луч отправляется непосредственно на результирующую пластинку. Полученная интерференция лучей фиксируется. Для повышения устойчивости голограммы выполняется масштабирование голограммы в два раза по каждой из осей относительно исходного изображения. Далее вычисляется интенсивность лучей света от каждой точки изображения по следующей формуле:

$$\varepsilon_{об}(\tilde{x}, \tilde{y}) = \sum_{x=0}^{N} \sum_{y=0}^{N} I(x, y) \times 3 \times \cos\frac{d}{\lambda}$$

где под точкой изображения и голограммы подразумеваются геометрические координаты пикселей, $(\tilde{x}, \tilde{y})$ – координаты пикселя в голограмме, (x, y) - координаты пикселя в изображение, $I(x, y)$ – интенсивность света исходного изображения, а λ – длина волны. Расстояние между точками исходного изображения и голограммы - $d = \sqrt{(x*2-\tilde{x})^2 + (y*2-\tilde{y})^2 + (z*2-\tilde{z})^2}$, где $(z*2-\tilde{z})^2$ – единица, так как голограмма является двумерной.

Для того чтобы получить голограмму, выполняется сложение интенсивности объектного света с интенсивностью опорного света для каждой из точек голограммы. Далее полученная голограмма представляется в виде битового массива m.

Непосредственно для встраивания производится подсчет вспомогательных функций

$$\omega_1^i(\upsilon_1, \nu_1, \kappa_1) = \left| f^i_{\upsilon_1, \nu_1, \kappa_1} \right|$$

$$\omega_2^i(\upsilon_2, \nu_2, \kappa_2) = \left| f^i_{\upsilon_2, \nu_2, \kappa_2} \right|$$

$$Z_1^i(\upsilon_1, \nu_1, \kappa_1) = \begin{cases} -1, & \text{если } f^i_{\upsilon_1, \nu_1, \kappa_1} < 0 \\ 1, & \text{если } f^i_{\upsilon_1, \nu_1, \kappa_1} \geq 0 \end{cases}$$

$$Z_2^i(\upsilon_2, \nu_2, \kappa_2) = \begin{cases} -1, & \text{если } f^i_{\upsilon_2, \nu_2, \kappa_2} < 0 \\ 1, & \text{если } f^i_{\upsilon_2, \nu_2, \kappa_2} \geq 0 \end{cases}$$

Для встраивания голограммы следующим образом выполняется модификация коэффициентов ДКП:

$$\varpi_1^i(\upsilon_1,\nu_1,\kappa_1)=\begin{cases}P+\omega_2^i(\upsilon_2,\nu_2,\kappa_2)+1, & \text{если } (\omega_1-\omega_2)\le P \text{ и } m_i=0\\ \omega_1^i(\upsilon_1,\nu_1,\kappa_1), & \text{если } (\omega_1-\omega_2)>P \text{ и } m_i=1\end{cases}$$

$$\varpi_2^i(\upsilon_2,\nu_2,\kappa_2)=\begin{cases}P+\omega_1^i(\upsilon_1,\nu_1,\kappa_1)+1, & \text{если } (\omega_1-\omega_2)\ge P \text{ и } m_i=1\\ \omega_2^i(\upsilon_2,\nu_2,\kappa_2), & \text{если } (\omega_1-\omega_2)<P \text{ и } m_i=0\end{cases}$$

$$\tilde{f}^i_{\upsilon_1,\nu_1,\kappa_1}=Z_1^i(\upsilon_1,\nu_1,\kappa_1)\cdot\tilde{\omega}_1^i(\upsilon_1,\nu_1,\kappa_1)$$

$$\tilde{f}^i_{\upsilon_2,\nu_2,\kappa_2}=Z_2^i(\upsilon_2,\nu_2,\kappa_2)\cdot\tilde{\omega}_2^i(\upsilon_2,\nu_2,\kappa_2)$$

Чтобы получить модифицированный видеопоток, выполняется обратное ДКП и полученные подблоки собираются в том же порядке, как происходило разбиение: слева-направо, сверху-вниз.

Как показали компьютерные эксперименты, при наличии на кадрах видеопотока больших областей равномерной заливки или заливки близкой к равномерной, появляются визуальные эффекты, позволяющие легко определять наличие цифрового водяного знака. Избавиться от этих визуальных эффектов можно выбирая блоки, которые по своей структуре делают встраивание наименее заметным. Было выявлено, что данная операция легко выполняется в ручном режиме, но требует поиска характеристик блоков для автоматизации процесса.

Для оценки влияния встроенного ЦВЗ на видеопоток предложено использовать величину отношения сигнала к шуму (PSNR). Кроме того было введено две характеристики – нулевой коэффициент ДКП, который показывает яркость фона участка кадров, входящих в блок, и среднеквадратичное отклонение яркости пикселей, входящих в блок от среднего значения яркости. Проведен компьютерный эксперимент для определения зависимости PSNR блоков с встроенным ЦВЗ от введённых характеристик. Для исследования было взято 100 видеофайлов длительностью около 20 секунд с размером кадра 512×512. Видеопоток разбивался на блоки размером 8×8×8 пикселей.

В результате экспериментов все видеофайлы разделились на три группы:

1. Видеофайлы, в которых PSNR растет с увеличением характеристик. В этих видеофайлах кадры представляют собой преимущественно светлые области с зернистой структурой.
2. Видеопотоки, в которых PSNR убывает с увеличением характеристик. В этих видеофайлах большое количество деталей представлено именно в частях кадра с низкой интенсивностью цвета.
3. Видеопотоки, в которых присутствуют зависимости PSNR от характеристик двух типов - возрастающие и убывающие. В таких видеофайлах присутствуют как светлые области, разбитые на мелкие детали, так и темные области, имеющие зернистую структуру, т.е. комбинация варианта 1 и 2.

Материал поступил в редколлегию 10.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.056

Чупахин Павел Анатольевич, *сотрудник*
Кривенцов Илья Олегович, *сотрудник*
Академия ФСО России
Россия, г. Орёл
e-mail: Vhwlv2@yandex.ru

ПРОСТОЙ ПРОТОКОЛ УПРАВЛЕНИЯ СЕТЬЮ

Описаны основные составляющие протокола SNMP, его структура и возможные реализации. Описаны основные версии протокола, их основные преимущества и недостатки. Представлена логика функционирования протокола.

Самым известным и наиболее часто использующимся протоколом, который применяется для управления устройствами в сети, является протокол SNMP (Simple Network Management Protocol – «простой протокол сетевого управления»). Он может использоваться, если необходимо контролировать выполнение на подключенных к сети устройствах задач, поставленных администратором.

Основной особенностью данного протокола является удаленная настройка устройств в сети с помощью главного компьютера без использования стороннего ПО. В ходе управления сетевыми процессами можно проводить работу не только с определенными процедурами, но и наблюдать за производительностью в целом, проводить мониторинг ресурсов, а также определять возникающие неполадки в инфраструктуре. Поэтому протокол SNMP пользуется большой популярностью среди системных администраторов.

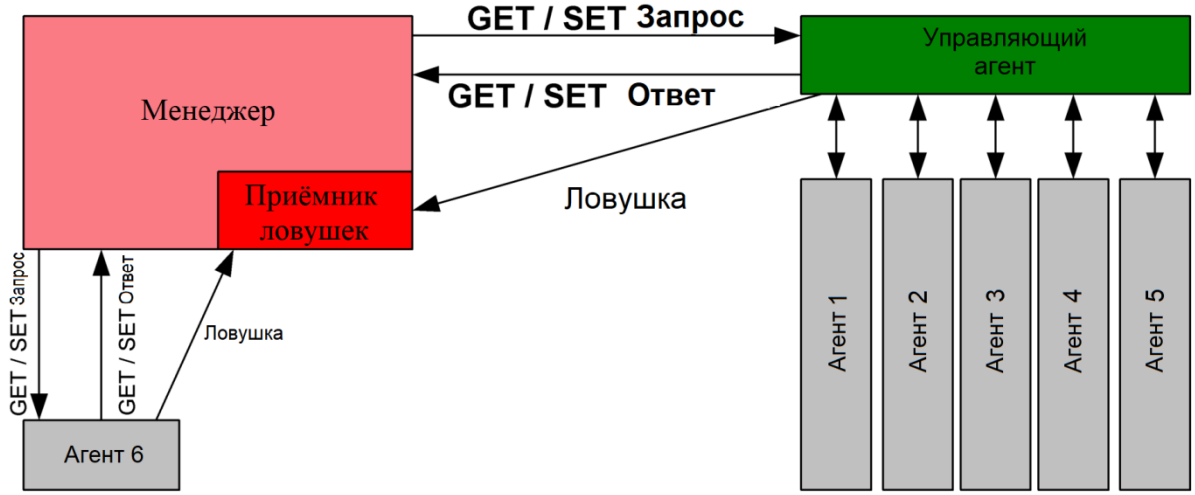


Рис. 1. Схема функционирования SNMP протокола

Выделяют пять самых распространенных составляющих SNMP протокола: подчиненный объект, MIB (Management Information Base) базы данных, управляющая программа, подчиненная программа, так называемый агент, система, обеспечивающая сетевое взаимодействие.

Подчиненное устройство – элемент сети, который реализует интерфейс управления, разрешающий односторонний или двухсторонний доступ к информации об элементе. Устройства обмениваются информацией с менеджером, который в свою очередь собирает, анализирует и хранит полученную информацию.

Подчиненная программа(агент) – это программный модуль сетевого управления, который располагается на управляемом устройстве, либо на устройстве, которое подключено к интерфейсу управления. Агент владеет управляемой информацией и переводит полученную информацию в понятную, для протокола SNMP, форму.

Важной частью протокола SNMP является MIB база. Это виртуальная база данных, используемая для управления объектами в сети связи. Она описывает структуру управляемых данных на подсистеме устройства, использует иерархическое именное пространство, которое содержит идентификаторы объектов (OID-идентификатор).

OID (Object Identifier) – идентификатор объекта, необязательный атрибут сертификата, который предоставляет дополнительную информацию о владельце, ключах, или несет дополнительные данные для сервисов, которые используют этот сертификат.

SNMP-ловушка – это сигнальное сообщение, которое подает устройство, поддерживающее протокол SNMP, основным назначением которого является оповещение администратора о каких-либо события, произошедших в процессе мониторинга сети. Администратор сети либо имеет возможность самостоятельно создавать и добавлять SNMP-ловушки в систему мониторинга и управления, либо определенный их набор уже заложен в используемое программное обеспечение.

Существует три вида протокола SNMP – SNMP версии 1, SNMP версии 2, SNMP версии 3.

Протокол SNMP версии 1 (SNMPv1) является изначальной реализацией протокола SNMP. Он позволяет работать с протоколами UDP, IP, CLNS, DDP и IPX. В настоящее время широко используется, впервые появился в 1998 году. Эта версия протокола была недостаточно защищена, так как аутентификация клиентов происходила с помощью «community string», которая представляла собой пароль, который передавался в открытом виде.

Протокол SNMP версии 2 (SNMPv2) является усовершенствованной версией протокола SNMPv1 и включает в себя улучшения в области производительности, безопасности, конфиденциальности. Также протокол получил возможность получения большого количества управляющих данных через один запрос. Существует две подверсии этого протокола- SNMP на основе сообществ(SNMPv2c), который включает в себя SNMPv2 без его модели безопасно-

сти, а использует схему из SNMPv1, а также SNMPv2 на основе пользователей(SNMPv2u), считающийся компромиссом, предлагающий более высокую безопасность и в то же время – без излишней, для SNMPv2, сложности. Протокол SNMP версии 3 (SNMPv3) не принес никаких изменений, кроме появления криптографической защиты, он является лучшей реализацией за счет новых текстовых соглашений и концепций. В отличии от предыдущих версий, SNMPv3 содержит параметры безопасности, закодированных как строка октета, значения которых зависит от используемой модели безопасности. Третья версия предоставляет такие особенности, как аутентификация, конфиденциальность и целостность информации.

Таким образом, мы рассмотрели состав протокола SNMP, его структуру и реализацию, основные версии протокола. Протокол SNMP предполагает осуществление между различными элементами инфраструктуры, управляемыми устройствами и управляющими серверами, обмена сообщениями. При этом происходит обращение к базе данных MIB устройства. В рамках протокола SNMP посредством стандартизованных сообщений могут осуществляться запросы одного или нескольких параметров MIB, установка значений для одной или нескольких переменных MIB, последовательное прочтение различных значений по тем или иным параметрам, возврат устройством на запрос другого устройства ответа, отправка уведомлений о тех или иных сетевых процессах. Алгоритмы MIB могут являться общими для всех устройств, как те, что прописываются производителем для некоторых типов сетевого оборудования. Данный протокол можно отнести к числу важнейших и не имеющих альтернативы.

Материал поступил в редколлегию 10.04.19.

ISBN 978-5-907111-88-2 Информационная безопасность и защита персональных данных. Проблемы и пути их решения, Брянск, 2019

УДК 004.3

Яковлев Алексей Викторович, *к.т.н., сотрудник*
Марковин Александр Юрьевич*, сотрудник*
Академия ФСО России
Россия, г. Орёл
e-mail: rf.rvr@yandex.ru

РАЗРАБОТКА ПРЕДЛОЖЕНИЙ ПО РЕАЛИЗАЦИИ АВТОНОМНОЙ ПОДСИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ В ВЫНОСНОМ МУЛЬТИМЕДИЙНОМ КОМПЛЕКСЕ СИТУАЦИОННОГО ЦЕНТРА

Рассмотрена система видеонаблюдения выносного мультимедийного комплекса ситуационного центра, реализующая ее технология SDI. Анализируются возможные варианты замены данной технологии в связи с её устареванием.

Система видеонаблюдения является важной частью современных объектов. Её построение является актуальной проблемой для многих организаций как в гражданской, так и в военной сфере. Данную задачу необходимо решать и при построении выносного мультимедийного комплекса ситуационного центра (ВМК СЦ), являющегося важным инструментом, повышающим эффективность управления и оперативность принятия решений.

Под ВМК СЦ понимается удаленный элемент ситуационного центра, позволяющий обеспечить оперативное представление информационно-аналитических и справочных материалов лицам, принимающим решения (ЛПР). Благодаря этому комплексу, ЛПР могут следить за текущей обстановкой со своего рабочего места в режиме реального времени, используя информационные, аналитические и справочные ресурсы ситуационного центра.

Можно сделать вывод, что наиболее важными параметрами выбора видеосистемы являются: оперативное доведение информации до ЛПР (обеспечение передачи видео заданного качества при отсутствии задержек, в режиме реального времени), возможность передачи видеоинформации на достаточно большие расстояния (ВМК СЦ находится на удалении от СЦ).

В настоящее время в составе технологического оборудования ситуационных центров широкое применение находят матричные коммутаторы видеосигналов, осуществляющие передачу видео при помощи технологии SDI. На данный момент времени SDI считается устаревшим стандартом, это связанно с тем, что для отправки сигнала на большие расстояния необходимо докупать дорогое оборудование. Стоит отметить, что передачу видео таким способом возможно осуществить на 150 – 200 метров. Из этого можно сделать вывод, что использование технологии SDI в будущем будет являться слишком дорогостоящим и невыгодным. В качестве альтернативы рассматривается две технологии. Первая из них основывается на передаче данных в цифровом формате при помощи IP-камер. Видеосистемы на их основе сейчас имеют наибольшую рас-

пространенность в коммерческих и государственных учреждениях. Несмотря на распространенность IP-систем, необходимо внимательно изучить их достоинства и недостатки.

Достоинства IP систем видеонаблюдения:

- позволяют просматривать видео на мобильных устройствах, смартфонах/планшетах;
- IP-системы видеонаблюдения являются легко масштабируемыми, ограничениями для которых могут явиться пропускная способность сети, технические характеристики оборудования;
- существует большее количество разработчиков программного обеспечения в данной сфере.

Недостатки IP систем видеонаблюдения:

- в IP системах расстояние между камерой и сетевым регистратором/видеосервером не может превышать 100 метров без дополнительного оборудования;
- требуется проприетарное программное обеспечение для обеспечения функций резервного копирования;
- большая задержка внутри сети;
- требуется отдельная сеть для реализации системы видеонаблюдения;
- если система видеонаблюдения была аналоговой, то при замене её на IP, придется полностью менять оборудования и инфраструктуру сети.

Второй вариант представляет собой аналоговую технологию AHD (analog high definition), видео передается при помощи коаксиального кабеля. На данный момент системы, построенные на основе данной технологии, являются одним из конкурентов IP- технологий для построения систем видеонаблюдения. Для более глубокого понимания данной технологии необходимо знать её достоинства и недостатки.

Достоинства AHD – технологии:

- при использовании данной технологии возможно осуществлять передачу видео на расстояние до 500 метров;
- отсутствие задержек сигнала;
- возможности модернизации аналоговой системы видеонаблюдения не приобретая дополнительного оборудования;
- возможность построения гибридных систем видеонаблюдения совместно с аналоговыми и IP камерами;
- возможность удаленного управления видеосистемы;
- дешевизна монтажа, обслуживания, настройки системы видеонаблюдения;
- монтаж системы не требует специальных навыков от работника;
- возможность архивации, сохранения видео на выделенном сервере, кроме того это не требует дополнительных затрат на ПО.

Основные недостатки AHD:

- плохая масштабируемость;
- камеры с высоким разрешением (более 2 МП) отсутствуют в продаже;
- существуют IP камеры с разрешением, большим, чем предлагают AHD – камеры.

Кроме перечисленных достоинств и недостатков стоит отдельно рассмотреть вопрос информационной безопасности. В связи с тем, что IP – камеры находятся на рынке уже длительное время, то установка такой системы требует наличия опытного специалиста по безопасности, который сможет защитить систему от основных уязвимостей. Одной из основных проблем IP-систем является то, что получить доступ к камере возможно с помощью широкого круга устройств, что усложняет противодействие взлому, в сети "Интернет" возможно найти материалы по применению методов взлома таких систем, данная информация расположена как в открытых источниках, так и в закрытых. Рядом таких проблем обладают и AHD – камеры, но для них обычно необходимо специфическое ПО и оборудование, что снижает ряд потенциальных угроз. Кроме того передача на большие расстояния видеосигнала позволит значительно упростить ряд организационных мер защиты.

Исходя из приведенных выше данных, можно сделать вывод, что AHD камеры позволяют получать изображение высокого качества с меньшей задержкой на большем расстоянии, но они не настолько хорошо масштабируемы, как IP камеры и имеют не так много проприетарного ПО на рынке. Но стоит принять во внимание 2 фактора, первый, то что для ВМК СЦ одним из основных показателей является оперативное наблюдение за обстановкой, что не всегда могут позволить ip-системы, второй, то что AHD – камеры могут работать на старом оборудовании SDI – систем, это позволит сэкономить достаточно много ресурсов. Из этого следует, что переход на AHD систему с большой вероятностью будет более рациональным.

Список литературы

1. Ильин, Н. И. Ситуационные центры. Опыт, состояние, тенденции развития / Н.И. Ильин, Н.Н. Демидов, Е.В. Новикова. – М.: МедиаПресс, 2011. – 336 с.
2. https://bezopasnik.info/ahd-videonablyudenie-tekhnicheskie-harakt/ https://securesys.pro/difference-between-ahd-h_ahd-nh_ahd-m_ahd-l.html
3. https://vidsyst.com/videonablyudenie/ahd-kamery.html
4. https://habr.com/en/post/367989/
5. http://pin-kod74.ru/catalog/bezopasnost/literatura/klyuchevyie-osobennosti-texnologii-ahd.html

Материал поступил в редколлегию 22.04.19.

СОДЕРЖАНИЕ