ТЕХНОЛОГИЯ ПРОГРАММИРОВАНИЯ И ЗАЩИТА ИНФОРМАЦИИ

УДК 004.056

МОДЕЛИ ЗАЩИТЫ КАНАЛОВ УПРАВЛЕНИЯ РОБОТОТЕХНИЧЕСКИХ СИСТЕМ

А.Л. Дранник
Научный руководитель – к.ф.-м.н., доцент И.И. Комаров

В исследовании предполагается рассмотрение комплекса угроз процессу управления бытовой робототехникой посредством удаленного доступа с мобильных устройств (смартфонов, планшетов) в сетях мобильного интернета технологии 4G (LTE). В качестве роботехнических устройств подразумеваются автономные устройства для уборки помещений, наблюдения, комплексные системы «умный дом» и т.п.

Актуальность изучения данного вопроса связана как с растущими темпами развития и внедрения в повседневный обиход бытовых робототехнических приборов, тенденцией производителей интегрировать их с мобильными телефонами и планшетными компьютерами пользователей для достижения максимальной простоты и комфорта управления, в том числе удаленного [1–3], так и с возрастающей степенью угроз мобильным устройствам, связанной с распространением вредоносных приложений и перспективами перехода на высокоскоростной мобильный интернет стандарта 4G.

В ходе исследования представляется необходимым отдельно рассмотреть возможные угрозы, направленные на канал передачи информации, а также на приложения, обеспечивающие процесс удаленного управления на мобильном девайсе, и непосредственно на устройствах или сервере домашней сети.

В качестве перспектив возможного сужения темы рассматривается уделение особого внимания защите приложений, обеспечивающих инфраструктуру управления на мобильном устройстве. (Планируется рассмотрение в первую очередь устройств на платформе Android, ввиду широкого распространения данной ОС, ее лидирующего положения на рынке и долговременных перспектив сохранения данных позиций [4–6]).

Для технологии мобильного интернета стандарта 4G (под 4G в первую очередь имеется в виду LTE, поскольку эта технология в настоящий момент признается коммерчески перспективной, нежели WiMAX [7, 8]) имеются стандартизированные требования и разработанная архитектура систем безопасности [9]. Защита взаимодействия базовых станций и опорной сети основывается на протоколах IPsec и IKE со стойкими алгоритмами шифрования. Разумеется, это не снимает целого ряда проблем безопасности данного канала передачи, включая уязвимость базовых станций. Также необходимо учитывать угрозы, связанные с потерями связи, тем более, что сантиметровые волны, на которых частично базируются каналы LTE (тенденция к переходу на волны СВЧ будет только усиливаться) хуже проходят через здания, что актуально в условиях плотной городской застройки. С другой стороны, есть огромная проблема выделения частот данного диапазона для сетей мобильной связи, что снижает в ближайшем будущем актуальность подобных угроз.

Наряду с этим, вопросы защиты управляющего приложения на мобильном телефоне/планшете являются значительно менее изученными. Основные угрозы мобильным приложениям Android создаются и развиваются непосредственно в настоящий момент, именно поэтому данный аспект имеет большой потенциал для изучения. Появляющиеся параллельно с возникновением все новых угроз средства защиты, «антивирусные» программы для мобильных устройств (которые правильнее было бы именовать «антивредоносными», учитывая специфику организации Android-приложений, с которыми они борются – это не вирусы в классическом смысле) также еще недостаточно апробированы

на практике и сами по себе могут представлять определенную угрозу для пользователей. В качестве примера можно привести одно из весьма распространенных приложений для защиты мобильных устройств на платформе Android, в котором функция защиты от вредоносных приложений дополнена модулем Anti-Theft, позволяющим в случае кражи устройства осуществить целый ряд функций удаленного управления украденным телефоном, вплоть до дистанционного удаления данных и запуска приложений на устройстве. К сожалению, можно заметить уязвимость данного ПО при определенных настройках (вполне возможных со стороны пользователя). В случае реализации атаки, оно способно сделать телефон/планшет, на котором установлено, удаленно управляемым злоумышленником, который получает возможность путем команд по смс, в том числе, запускать мобильные приложения и вмешиваться в их работу. Следует отметить, что, помимо данного частного случая, существуют специализированные вредоносные приложения, непосредственно ориентированные на получение контроля над мобильными устройствами, а также известны алгоритмы атак на мобильные телефоны/планшеты с помощью сетей Wi-Fi и Bluetooth, которые могут быть реализованы в тот момент, когда данные сервисы активированы на устройстве либо способны активировать эти функции без ведома владельца.

При наличии огромного множества угроз мобильным устройствам размещение на них приложений удаленного управления бытовыми роботехническими приборами и комплексными системами «умный дом» (включающими в том числе функции контроля нагревательных приборов, отопительных систем и т.п.), само по себе превращается в реальную угрозу. Вместе с тем прогнозируемо, что в будущем развитие технологий бытовой робототехники будет двигаться в этом направлении. Это обуславливает актуальность выработки общих алгоритмов защиты против описанных угроз мобильным устройствам, а также написания отдельных узкоспециализированных программных модулей и комплексных программ защиты мобильных устройств. Автор предполагает в дальнейшем двигаться в указанном направлении. В настоящий момент, для написании магистерской работы, ставится цель построения модели защиты процесса удаленного управления робототехническими устройствами. Для реализации данной цели предполагается решить задачи построения модели угроз и выработки возможных алгоритмов защиты, которые могли бы быть в дальнейшем реализованы в соответствующем программном обеспечении.

Литература

1. Сторожевой робот от SK Telecom будет управляться с мобильника [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/news/line/index.shtml?2004/03/15/156369, своб.
2. Расцвет масс-маркета: репортаж с MobileWorldCongress 2013 [Электронный ресурс]. – Режим доступа: http://www.rbcdaily.ru/cnews/562949985915618, своб.
3. Android-телефон может стать мозгом робота HOVIS [Электронный ресурс]. – Режим доступа: http://www.xakep.ru/post/57998/default.asp, своб.
4. Википедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Android, своб.
5. Платформа Android уверенно лидирует на рынке мобильных устройств [Электронный ресурс]. – Режим доступа: http://news.kosht.com/tendency/2012/02/15/Platforma_Android_yverenno_lidiryet_na_ryinke_mobilnyih_ystroiistv.html, своб.
6. Доля GoogleAndroid на рынке смартфонов стремительно растет [Электронный ресурс]. – Режим доступа: http://www.vedomosti.ru/tech/news/2012/08/09/2671721, своб.
7. Операторы ставят на LTE [Электронный ресурс]. – Режим доступа: http://telecomideas.ru/news-it/-/view-content/716341, режим доступа своб.
8. Королев И. Yota отключает WiMAX и бесплатно раздает LTE-модемы [Электронный ресурс]. – Режим доступа:

http://www.cnews.ru/top/2012/02/21/yota_otklyuchaet_wimax_i_besplatno_razdaet_ltemodemy_spisok_zameny_478557, своб.
9. 3GPP System Architecture Evolution (SAE); Security architecture [Электронный ресурс]. – Режим доступа: http://www.3gpp.org/ftp/Specs/html-info/33401.htm, своб.

УДК 004.02

РАЗРАБОТКА МЕТОДИКИ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ МЕТОДА ДИНАМИЧЕСКОГО ПРОГРАММИРОВАНИЯ

А.С. Ендовский
Научный руководитель – д.т.н., профессор И.А. Зикратов

В работе рассматривается возможность использования метода динамического программирования для управления рисками информационной безопасности. Кратко описано обоснование выбора данного метода, приведена информация о пробном практическом применении метода в рабочей системе оценки рисков.

Введение. Задача оценки и управления рисками информационной безопасности является актуальной на всех этапах внедрения системы информационной безопасности на защищаемых объектах. Без четкого понимания рисков, а именно какие угрозы являются действительными и какой ущерб потенциально возможен, не представляется возможным создать и корректно внедрить ту систему информационной безопасности, которая будет достаточной для удовлетворения поставленных целей.

Минимизация рисков информационной безопасности это комплексная и объемная задача, в которой учитывается большое количество параметров и состояний, вычисление которых, как правило, однотипно. Основные входные параметры это массив информационных активов хранящийся, обрабатывающийся и передающийся в разных информационных системах, при этом для каждого информационного актива необходимо учесть актуальные для него угрозы, для информационной системы – уязвимости. Решение данной задачи можно упростить, если разбить ее на этапы (множество мелких задач), для оптимизации времени вычисления актуального риска и ресурсов, необходимых для полной оценки рисков информационной безопасности в каждый отдельно взятый момент времени.

Целью исследования является разработка методики управления рисками информационной безопасности, позволяющей актуализировать данные для вычисления значения риска и калькулировать действительное значение риска, при этом использовать ограниченное количество ресурсов. Методика должна позволить упростить и ускорить процесс управления рисками информационной безопасности на этапе оценки и минимизации.

Анализ методов оптимизации. На данный момент в процессе анализа использования различных методов исследования операций для выявления наиболее подходящего метода, применимого к процессу управления рисками информационной безопасности, проанализированы методы линейного и динамического программирования. В свою очередь линейное программирование обладает одним существенным недостатком – поставленная до начала решения задача, а именно использующиеся переменные, не могут быть изменены в процессе решения, в противном случае, даже при незначительном изменении параметров, конечное решение будет сильно отличаться от прогнозируемого [1]. Так как управление рисками информационной безопасности подразумевает постоянное изменение входных параметров, то использование метода линейного программирования является

нерациональным.

Динамическое программирование, наоборот, позволяет изменять исходные данные в процессе решения для корректировки и актуализации конечного результата. При этом стоит отметить, что решение каждого отдельного этапа, в случае правильной постановки задачи, может использоваться и как отдельный самостоятельный результат.

Основное рекуррентное уравнение динамического программирования, выражающее условный оптимальный выигрыш:

$$W_i(S) = \max_{x_i} \{ f_i(S, x_i) + W_{i+1}(\varphi_i(S, x_i)) \}$$

Таким образом, для управления рисками информационной безопасности на данный момент рассматривается вариант использования метода динамического программирования. Входными данными будет массив информационных систем и содержащие информационные активы. Для активов – множество потенциальных угроз, а для информационных систем – множество уязвимостей. Вышеуказанные данные могут изменяться и актуализироваться в процессе управления рисками информационной безопасности, но на выходе предполагается получать актуальное на данный момент времени значение риска по каждому информационному активу, и по всей информационной инфраструктуре в целом.

Прогнозируемые результаты. Предполагаемым результатом использования динамического программирования в целях управления рисками информационной безопасности является сокращение времени получения результатов, снижение минимально необходимого уровня ресурсов и вычислительных мощностей, а так же возможность актуализировать процедуру без внесения критичных изменений в структуру процесса управления рисками.

На данном этапе проведено тестирование метода динамического программирования на процедуре оценки рисков информационной безопасности, в которой процесс разбит на блоки вычисления рисков для каждого актива в отдельности с учетом всех возможных угроз и уязвимостей. Тестирование показало, что основные идеи метода динамического программирования применимы к процедуре управления рисками информационной безопасности.

Литература

1. Зикратов И.А., Одегов С.В., Смирных А.В. Оценка рисков информационной безопасности в облачных сервисах на основе линейного программирования // Научно-технический вестник информационных технологий, механики и оптики. – 2013. – №1(83) С. 141–144.
2. Беллман Р. Динамическое программирование. – М.: Изд-во иностранной литературы, 1960. – 400 с.
3. Коган Д.И. Динамическое программирование и дискретная многокритериальная оптимизация: учебное пособие. – Н. Новгород: Изд-во Нижегородского университета, 2004. – 150 с.
4. Пастоев А. Методологии управления ИТ-рисками // Открытые системы. – 2006. – №8. – С. 44–48.

УДК 004.056.2, 004.056.5, 004.056.55, 003.26, 355.405.2

ПРОЕКТ РАЗРАБОТКИ ПРОГРАММНОГО МОДУЛЯ ЗАЩИТЫ КРИПТОАЛГОРИТМARIJNDAEL (AES) ОТ АТАК ПО ВРЕМЕНИ ВЫПОЛНЕНИЯ НА ОСНОВЕ ПРОМАХОВ КЭША

Д.А. Калинин
Научный руководитель – к.ф.-м.н., доцент А.Б. Левина

Введение. Криптографические алгоритмы сегодня используются повсеместно, для поддержания целостности и конфиденциальности защищаемой информации, противодействию несанкционированному доступу к ней.

Существует два способа исследование криптоалгоритмов:

1. криптографический анализ – исследование и поиск уязвимостей в математическом аппарате алгоритма, способных привести к получению секретного ключа только методами математического анализа;
2. атаки по сторонним каналам (sidechannelattacks) – методы получения секретного ключа на основе использования уязвимостей математической модели алгоритма и конкретных его реализаций, при помощи побочной информации, получаемой криптоаналитиком во время процесса шифрования и ее дальнейшего исследования.

Постоянные исследования в области криптографических методов защиты информации привели к тому, что практически все современные криптоалгоритмы можно назвать вычислительно защищенными, многие являются стойкими к криптографическому анализу, но всегда имеется вероятность и возможность взлома алгоритма при помощи атак по сторонним каналам, поэтому исследования различных атак по сторонним каналам и методов противодействия им является актуальными сегодня.

Цель. Спроектировать программный модуль защиты криптоалгоритмаRijndael (AES) от атаки по времени выполнения на основе промахов кэша.

Назначение разработки. Обеспечение защиты криптоалгоритмаRijndael (AES) от атаки по времени выполнения на основе промахов кеша, и последующее использование модуля в исследовательских работах по изучению атак по сторонним каналам на алгоритм Rijndael (AES) и разработке эффективных методик противодействия подобным атакам.

Общие сведения об алгоритме и атаке. КриптоалгоритмRijndael (AES) является блочным алгоритмом симметричного шифрования. Алгоритм широко применяется в различных программных и программно-аппаратных комплексах шифрования (к примеруOpenSSL, AESCrypt, PolarSSL, Ccrypt), и является государственным стандартом шифрования США (стандарт FIPS 197). На текущий момент является защищенным от взлома посредством криптографического анализа, но уязвим для ряда атак по сторонним каналам, в силу недостатков конкретных реализаций криптоалгоритма, а также ряда фундаментальных уязвимостей.

Одним из актуальных видов атак на алгоритм Rijndael (AES) являются атаки по времени выполнения, в частности атаки по времени выполнения на основе промахов кеша.

Эти атаки разделяют на три категории:

1. time-driven, т.е. временные – в них измеряется полное время выполнения процесса шифрования. Из этих измерений получается информация об общем количестве кэш-промахов и кэш-попаданий;
2. trace-driven, отслеживающие атаки – в них получают профиль активности кэша во время шифрования и делаются выводы, какие обращения к памяти, инициированные процессом шифрования, привели к кэш-попаданиям;

3. access-driven, атаки по доступу – позволяют определить, к каким блокам кэша обращался процесс. На основе этого узнается, к каким элементам массива состояния обращался алгоритм.

Атаки всех перечисленных категорий производятся путем анализа времени, которое затрачивается на исполнение отдельных операций криптоалгорита, и частоты промахов в кэш процессора.

Промежуточные результаты. На текущий момент на основании исследования предметной области, осуществлено описание возможных аналогов проектируемого модуля, сформированы функциональные требования, на основе используемых в атаке уязвимостей и принято решение об актуальности дальнейшего проектирования и исследований в описанной области; обзор аналогов и функциональные требования представлены ниже.

На сегодня, по информации из открытых источников, не имеется прямых аналогов проектируемого модуля, осуществляющих противодействия атакам по времени выполнения на основе промахов кеша на алгоритм Rijndael (AES). К косвенным аналогам можно отнести антивирусные программы, но при их использовании возникают вопросы в рамках требований доверия, сертификации и политики безопасности конкретных организаций, и потенциальной их возможности противодействовать подобным атакам.

На основе выявленных в алгоритме уязвимостей, делающих возможным проведения атаки, сформирован список функциональных требований к проектируемому модулю:

- обеспечивать защиту программы-процесса шифрования, посредством косвенного управления процессом шифрования;
- ограничить возможность получения таймингов при помощи таких методов защиты как: добавление избыточных вычислений, добавление случайных задержек, использование механизмов обфускации, дублирование модулей шифрование.

В дальнейшем предполагается реализация описанного программного модуля, согласно сформированным функциональным требованиям и исследование его возможностей по противодействию атак по времени выполнения на основе промахов кеша на алгоритм Rijndael (AES).

УДК 004.056.2, 004.056.5, 004.056.55, 003.26, 355.405.2

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ SIDECHANNEL АТАКИ НА АЛГОРИТМ RIJNDAEL (AES)

Д.А. Калинин
Научный руководитель – к.ф.-м.н., доцент А.Б. Левина

Введение. Криптографические алгоритмы сегодня используются повсеместно, для поддержания целостности и конфиденциальности защищаемой информации, противодействию несанкционированному доступу к ней.

Существует два способа исследование криптоалгоритмов:

1. криптографический анализ – исследование и поиск уязвимостей в математическом аппарате алгоритма, способных привести к получению секретного ключа только методами математического анализа;
2. атаки по сторонним каналам – методы получения секретного ключа на основе использования уязвимостей математической модели алгоритма и конкретных его реализаций, при помощи побочной информации, получаемой криптоаналитиком во время процесса шифрования и ее дальнейшего исследования.

Постоянные исследования в области криптографических методов защиты информации привели к тому, что практически все современные криптоалгоритмы можно назвать

вычислительно защищенными, многие являются стойкими к криптографическому анализу, но всегда имеется вероятность и возможность взлома алгоритма при помощи атак по сторонним каналам, поэтому исследования различных атак по сторонним каналам и методов противодействия им является актуальными сегодня.

Цель. Реализовать на практике атаку по сторонним каналам на алгоритм Rijndael (AES) для различных длин секретного ключа.

Сведения об алгоритме и атаке. Криптоалгоритм Rijndael (AES) является блочным алгоритмом симметричного шифрования. Алгоритм широко применяется в различных программных и программно-аппаратных комплексах шифрования (к примеру OpenSSL, AESCrypt, PolarSSL, Ccrypt), и является государственным стандартом шифрования США (стандарт FIPS 197). На текущий момент является защищенным от взлома посредством криптографического анализа, но уязвим для ряда атак по сторонним каналам, в силу недостатков конкретных реализаций криптоалгоритма, а также ряда фундаментальных уязвимостей.

Одним из актуальных и эффективных видов атак на алгоритм Rijndael (AES) являются атаки на основе генерируемых ошибок.

Атака на основе генерируемых ошибок использует фундаментальную уязвимость алгоритма при его программно-аппаратных реализациях – итерационную структуру и отсутствие связи между раундовыми ключами. Атака базируется на потенциальной возможности возникновения ошибки (как преднамеренной, так и специально внесенной) в процессе шифрования и дальнейшее использование ошибочных результатов работы для анализа и сравнения с валидными результатами, что позволяет получить секретный ключ. Получение ошибки возможно широким набором способов: изменение напряжения на входе шифратора, изменение частоты тактового генератора, внесение ошибки оптическим способом, посредством случайной или преднамеренной ошибки в работе аппаратных средств и/или программного обеспечения, использования различного специального ПО или применение НДВ используемого.

Атака на основе генерируемых ошибок является целым семейством атак, отличающихся по необходимому количеству и типу ошибок, необходимых для успешного проведения атаки.

Возможные варианты атак на основе генерируемых ошибок, с точки зрения характера используемых ошибок:

- одиночная битовая (в известном или случайном месте);
- одиночная байтовая (в известном или случайном месте);
- множественная ошибка (в известном или случайном месте).

Также на эффективность атаки и на количество ошибочных шифротекстов, необходимых для получения ключа влияет характер шифруемого текста, например для нулевого текста необходимо меньшее число шифротекстов с ошибкой в процессе проведения атаки.

Промежуточные результаты. В рамках проведенной атаки на текущий момент были получены результаты для различных входных данных криптоалгоритма (размер блока и ключа):

- полностью получен секретный ключ для случайной байтовой ошибки (размер блока и ключа 128 бит) при использовании ненулевого шифротекста;
- полностью получен секретный ключ для байтовой ошибки в известном месте для нулевого и ненулевого текста (размер блока и ключа 192 бит);
- полностью получен секретный ключ для случайной байтовой ошибки для нулевого текста (размер блока и ключа 192 бит);

– частично получен секретный ключ для случайной байтовой ошибки для ненулевого текста (размер блока и ключа 192 бит).

Дальнейшая работа предполагает получение секретного ключа для всех возможных комбинаций входных данных криптоалгоритма при случайной ошибке и ненулевомшифротексте, а также исследование и разработка методов противодействия подобным атакам.

УДК 004.02

ПРОБЛЕМЫ ОПТИМИЗАЦИИ ЗАЩИЩЕННОСТИ КАНАЛОВ УПРАВЛЕНИЯ РОБОТОТЕХНИЧЕСКИМИ СИСТЕМАМИ

В.А. Кустов
Научный руководитель – к.ф.-м.н., доцент И.И. Комаров

В последние годы наблюдаются высокие темпы технологического развития, и одним из передовых направлений развития является робототехника, имеющая очень широкую область применения. При таком обширном использовании робототехнических устройств и систем возникает вопрос обеспечения безопасности их управления. Основными параметрами защищенности для робототехнических систем, как и для любого объекта защиты, являются целостность, доступность и конфиденциальность. К этим параметрам, учитывая специфику рассматриваемых систем можно добавить непрерывность, гибкость (многоканальность) и скрытность. Непрерывность обуславливается необходимостью постоянного управления системой. Гибкость управления характеризуется возможностью восстановления управления при выходе из строя основного канала и переходом на другой канал или метод управления. Непрерывность появляется вследствие необходимости маскировки осуществления управления робототехнической системой.

Построение систем защиты каналов управления должно происходить в соответствии с характером использования той или иной робототехнической системы. Целесообразно оценивать риск информационной безопасности перед началом проектирования систем защиты и в соответствии с рисками, выдвигать различные требования защищенности для различных робототехнических систем.

После получения необходимых требований разрабатывается система защиты на основе существующих средств и технологий защиты информации. Но здесь необходимо принять во внимание ограничение ресурсов. Ограничение ресурсов может быть различным: финансовые, аппаратные, ограничения по мощности, размеру, производительности и т.п.

В результате должна получиться система защиты каналов управления робототехническими системами, учитывающая характер использования системы, т.е. риски информационной безопасности (выбор оптимальных требований по защите), существующее разнообразие средств защиты информации (выбор оптимальных средств защиты) и ограничение ресурсов (выбор оптимальной стратегии защиты, учитывающей риски, ресурсы и разнообразие средств защиты).

Самым актуальным методом контроля над робототехническими системами является использование радиоуправления. В данном случае лучшим решением при защите каналов управления будет применение криптографических преобразований, а также кодов, исправляющих ошибки. Также нельзя забывать о средствах, обеспечивающих непрерывность и гибкость системы управления.

Для упрощения создания систем защиты каналов управления робототехническими каналами необходимо разработать методику оптимизации построения этих систем. При построении данной методики предполагается использовать лучшие практики построения систем защиты и методы оптимизации. Данное сочетание должно обеспечить максимальную

эффективность систем защиты в рамках имеющихся ограничений и экономически выгодное расходование ресурсов на защиту. Ожидаемым результатом работы является методика оптимизации защищенности каналов управления робототехническими системами, работающая в рамках ограниченных ресурсов.

УДК 004.056.53

ОЦЕНКА КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ В ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЯХ СВЯЗИ

Г.А. Малышкин
Научный руководитель – д.в.н., профессор Ю.Ф. Каторин

В работе рассматривается проблема защиты информации в волоконно-оптических линиях связи.

Волоконно-оптические линии связи (ВОЛС) – это каналы связи, в которых информация передается по оптическим диэлектрическим волноводам, известным под названием «оптическое волокно». Оптическое волокно в настоящее время считается самой совершенной физической средой для передачи информации, а также самой перспективной средой для передачи больших потоков информации на значительные расстояния.

Цель работы – оценка каналов утечки информации в ВОЛС.

Высокие требования, предъявляемые к современным системам телекоммуникаций (высокая скорость передачи информации, надежность, защищенность от несанкционированного доступа), приводят к осознанию неоспоримого преимущества ВОЛС. В ближайшем будущем, можно ожидать, что ВОЛС заменят все существующие магистральные линии передачи информации.

До недавнего времени считалось, что системы связи на основе оптических волокон не только устойчивы к электромагнитным помехам, но и передаваемая по световодам информация надежно защищена от несанкционированного доступа. Считается, что ВОЛС нельзя подслушать неразрушающим способом. Всякие воздействия на волокно могут быть зарегистрированы методом непрерывного контроля целостности линии.

Однако это не совсем так. ВОЛС имеют более высокую степень защищенности информации от несанкционированного доступа, чем какие-либо иные линии связи, что связано с физическими принципами распространения электромагнитной волны в световоде. В оптическом волноводе электромагнитное излучение выходит за пределы волокна на расстояние не более длины волны при отсутствии внешнего воздействия на оптоволокно, поэтому формирование каналов утечки на участках волоконно-оптического тракта, как правило, требуют прямого доступа к оптоволокну и специальных мер отвода части излучения из оптоволокна или регистрации прохождения излучения, но при этом разрушать оптоволокно совершенно не обязательно.

Основные физические принципы формирования каналов утечки в ВОЛС без нарушения целостности оптоволокна можно разделить на следующие типы:

1. нарушение полного внутреннего отражения;
2. регистрация рассеянного излучения на длинах волн основного информационного потока и комбинационных частотах;
3. параметрические методы регистрации проходящего излучения.

Наиболее перспективным направлением является нарушение внутреннего отражения. К этим способам относятся:

– изменение угла падения, до значения при котором начинает наблюдаться полное внутреннее отражение;

- изменение отношения показателя преломления оболочки к показателю преломления сердцевины оптоволокна;
- оптическое туннелирование.

В работе рассмотрены условия, при которых удается получить побочное излучение в точке воздействия на световод. Приводятся формулы позволяющие определить интенсивность излучения вышедшего из сердцевины в оболочку оптоволокна. Анализируются преимущества и недостатки указанных методов. Отмечается, что отличительной особенностью оптического туннелирования является отсутствие обратно рассеянного излучения, что затрудняет детектирование несанкционированного доступа к каналу связи. Этот способ съема информации наиболее скрытный. Это опровергает утверждение о невозможности формирования скрытого канала утечки из оптического волновода.

В результате сделан вывод, что каналы оптоволоконной связи нельзя считать совершенно недоступными для технических средств негласного съема информации. Между тем это заблуждение прослеживается и в повседневной жизни и в российских нормативных документах. Предлагаются некоторые способы скрытой передачи информации по оптическим линиям связи.

Литература

1. Бусурин В.И., Носов Ю.Р. Волоконно-оптические датчики: Физические основы, вопросы расчета и применения. – М.: Энергоатомиздат, 1990. – 256 с.
2. Введение в интегральную оптику. Под ред. М. Барноски, пер. с англ. под ред. Т.А. Шмаонова. – М.: Мир, 1977. – 368 с.
3. Попов С., Шубин В., Ивченко С., Волков А., Курило А., Зайцев Н., Кращенко И. О защите информации в волоконно-оптических системах // Вопросы защиты информации: Науч.-практ.журн. – ФГПУ «ВИМИ». – 1993. – № 1(24) . – С. 39–43.
4. Сивцов А.Г. ВОСП и защита информации // Фотон-Экспресс. – 2000. – № 18. – С. 16–20.
5. Попов С., Шубин В., Ивченко С., Волков А., Курило А., Зайцев Н., Кращенко И. Исходные данные для построения модели съема информации, передаваемой по волоконно-оптическому тракту // Вопросы защиты информации: Науч.-практ. журн. – ФГПУ «ВИМИ». – 1993. – № 1(24) . – С. 43–48.
6. Годный В.Г. Вопросы информационной безопасности в волоконно-оптических линиях связи // Системы безопасности. – 2002. – № 2(44) . – С. 44–47.
7. Бородакий Ю.В., Добродеев А.Ю., Дмитриев С.В., Ермоних М.И., Фурсов С.Г. Проблема защиты волоконно-оптических систем и сетей от НДС. Пути и перспективы ее решения // Системы безопасности связи и телекоммуникаций. – ФГУП «Концерн Системпром». – 2001. – № 41(5). – С. 83–86.
8. Румянцев К.Е., Хайров И.Е. Передача конфиденциальной информации по волоконно-оптическим линиям связи, защищенная от несанкционированного доступа // Информационное противодействие угрозам терроризма: Научн.-практ. журн. – 2003. – №1. – С. 72–79.
9. Спирин А.А. Введение в технику оптоволоконных сетей. – М.: Наука. 1998. – 428 с.
10. Гришачев В.В., Кабашкин В.Н., Фролов А.Д. Анализ каналов утески информации в оптиковолоконных системах связи. Факультет защиты информации, ИИНиТБ, РГГУ физический факультет МГУ им. М.В. Ломоносова // Вопросы защиты информации: Науч.-практ.журн. ФГПУ «ВИМИ». – 2003. – № 1(44). – С. 39–43.

УДК 004.4

РАЗРАБОТКА МЕТОДИКИ ВЫБОРА МЕР И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ АНАЛИЗА РИСКОВ

Р.А. Нурдинов
Научный руководитель – д.в.н., профессор Ю.Ф. Каторин

Краткое вступление, постановка проблемы. Развитие информационных технологий привело к тому, что обладание ценной информацией является одним из ключевых факторов успешного ведения бизнеса. Вместе с тем появляется все большая необходимость в защите информации, доступ к которой ограничен. Вопрос выбора мер и средств защиты информации из всего их многообразия является проблемой для многих предприятий. Часто можно наблюдать ситуации, когда выделенные на защиту информации денежные ресурсы не используются должным образом и как следствие – не окупаются.

Цель работы – разработка методики выбора мер и средств защиты информации для конкретного объекта защиты.

Базовые положения исследования. Информационная безопасность обычно рассматривается в двух значениях: как состояние определенного объекта и как деятельность, направленная на обеспечение защищенного состояния объекта. Для защиты информации на предприятии используется определенный набор мер и средств защиты. Мера защиты – это мера, используемая для уменьшения риска [3]. В работе под мерами защиты понимаются организационные меры, включающие в себя включают законодательные, административные и процедурные меры защиты. Средства защиты информации (СЗИ) – это технические, программные, программно-технические средства, предназначенные или используемые для защиты информации [2].

Для выбора конкретных мер и средств защиты информации на предприятии необходимо использовать определенную методику, позволяющую оценить техническую и экономическую целесообразность данного выбора. Большинство таких методик основано на анализе существующих и потенциальных угроз, определении уязвимостей, оценке рисков.

Под риском информационной безопасности понимается потенциальная угроза эксплуатации уязвимости актива, вызывающая, таким образом, вред организации. Это измерение комбинации вероятности случая и его последствия [1]. Для оценки рисков существует ряд известных методик, таких как CRAMM, RiskWatch, OCTAVE, ГРИФ. Основные их недостатки: во-первых, высокая стоимость, а во-вторых, отсутствие единой базы данных, включающей в себя объекты защиты, активы, угрозы, уязвимости и их взаимосвязи, которая могла бы дополняться специалистами, использующими данный продукт. Главная идея создаваемой методики – ее программная реализация в виде web-интерфейса с единой базой данных, в результате чего знания и опыт отдельных специалистов, а также статистические данные будут накапливаться.

Промежуточные результаты. В работе описываются основные теоретические аспекты информационной безопасности. Подробно рассматриваются все этапы методики выбора мер и средств защиты информации на предприятии: характеристика объекта защиты, определение стоимости информационных активов, составление перечня актуальных угроз, обнаружение уязвимостей, которые могут способствовать реализации угроз, оценка рисков, анализ мер и средств защиты и оценка технической и экономической целесообразности их выбора. Предлагается два последовательно усложняющихся подхода к выбору мер и средств защиты информации. Первый подход основан на построении модели угроз и расчете коэффициента нейтрализации угроз с помощью экспертных оценок. Второй подход

учитывает дополнительно величину риска и стоимость информационных активов. Кроме определения коэффициента экономической эффективности использования СЗИ предлагается ввести показатель затратоемкости информационных активов, который учитывает отношение суммы затрат на обеспечение безопасности и цены остаточного риска к стоимости информационных активов.

Предполагаемые практические результаты. Полученные теоретические результаты планируется реализовать на практике. Будет разработан web-интерфейс, с помощью которого пользователь сможет поэтапно провести оценку рисков информационной безопасности для конкретного объекта защиты и определить целесообразность выбора конкретных мер и средств защиты.

Данный программный продукт может вызвать интерес благодаря своей простоте и небольшой стоимости, а также обширной базе данных, в том числе и статистических, которая будет непрерывно дополняться пользователями и экспертами.

Литература

1. ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».
2. ГОСТ Р ИСО/МЭК 50922-2006 «Защита информации. Основные термины и определения».
3. ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты».

УДК 004.056.53

ПРИМЕНЕНИЕ СКРЫТЫХ МАРКОВСКИХ МОДЕЛЕЙ ДЛЯ ПОСТРОЕНИЯ СИСТЕМЫ НЕЙРОАУТЕНТИФИКАЦИИ ЛИЧНОСТИ

А.В. Поляков, Р.Д. Лебедев
(Московский государственный университет им. М.В. Ломоносова)
Научный руководитель – д.ф.-м.н., профессор А.В. Михалёв
(Московский государственный университет им. М.В. Ломоносова)

Проблема. В настоящее время существующие системы аутентификации, как правило, базируются на секретности ключей, выдаваемых легальным пользователям. Подавляющее большинство таких систем не способно противостоять атакам, в которых атакующий насильственно (путем шантажа, угроз, пыток и т.п.) принуждает легального пользователя выдать ему секретный ключ (метод бандитского криптоанализа).

В 2012 году на конференции UseNIXSecurity'12 (г. Белвью, США) сотрудником Стэнфордского университета ХристоБожиновым была впервые представлена система нейроаутентификации личности, призванная решить поставленную проблему. Данная система имеет преимущества перед традиционными методами защиты информации от данной атаки (двусмысленное шифрование, биометрические системы аутентификации), однако, одновременно и имеет недостатки, существенно ограничивающие возможности ее практического применения, а именно:

- данная система не может применяться для удаленной аутентификации пользователя;
- данная система требует большого количества времени на обучение пользователя и на его последующую аутентификацию пользователя;
- данная система не защищена от прослушивания противником;
- не установлены психофизиологические ограничения на пользователя, влияющие на успешность аутентификации.

Цель работы. Построение модификации представленной системы аутентификации, устойчивой не только к атаке бандитского криптоанализа, но и к атаке прослушивания.

Базовые положения исследования. На практике для достижения данной цели необходимо исследовать вопрос о возможности неявного обучения пользователя более сложным структурам, чем повторяющаяся последовательность символов (на которой построена исходная система нейроаутентификации), а именно, скрытым марковским моделям, для чего необходимо построить корректную математическую модель новой системы нейроаутентификации, ее программную реализацию и провести исследование на пользователях, по итогам которого можно сделать выводы окачественных результатах решения данной проблемы и провести сравнительный анализ количественных характеристик (сложность пароля, время обучения и аутентификации пользователя в системе, вероятности ошибок 1-го и 2-го рода) исходной системы нейроаутентификации и ее модифицированной версии.

Промежуточные результаты. Построена математическая модель системы нейроаутентификации, построена ее программная реализация, проведено исследование с участием 20 пользователей по возможностям неявного обучения человека скрытым марковским моделям.

Практические результаты. Выявлена способность человека к неявному обучению скрытым марковским моделям, построена модифицированная система нейроаутентификации личности, устойчивая к атакам бандитского криптоанализа и прослушивания; указаны ее основные характеристики (сложность пароля, время обучения и аутентификации пользователя в системе, вероятности ошибок 1-го и 2-го рода), приведен сравнительный анализ новой системы с системой нейроаутентификации личности, предложенной сотрудниками Стэнфордского университета, наглядно демонстрирующие преимущества новой системы.

УДК 004.08

ОСОБЕННОСТИ РАСПРЕДЕЛЕНИЯ ЗАПРОСОВ ВО ВРЕМЯ НАГРУЗОЧНОЙ АТАКИ В ОБСЛУЖИВАНИИ ВЕБ-СЕРВЕРОВ

В.Е. Пряхин
Научный руководитель – д.т.н., профессор И.А. Зикратов

В настоящее время проблема отказа в обслуживании веб-серверов в связи с запредельной нагрузкой, вызванной резким всплеском посещаемости, либо распределенной атакой (DDoS) является актуальной: многие веб-сервисы вынуждены временно простаивать часами, и даже днями, теряя пользователей и прибыль, вследствие резких всплесков посещаемости, или распределенных атак с помощью ботнетов, направленных на потребление ресурсов сервера обработкой излишнего нежелательного количества запросов и уменьшение полезной пропускной способности интернет-соединения вследствие отдачи лишнего количества трафика.

Цель работы – повышение эффективности распознавания нагрузочных атак в обслуживании веб-серверов с помощью методов интеллектуального анализа данных, выявление закономерностей в распределении запросов, благодаря которым можно более точно отделять периоды атаки от периодов штатной работы.

Каждый веб-сервис имеет уникальное распределение характерных запросов на отдачу контента (тяжелого – большие изображения, медиа-контент, файлы;и легкого –

пользовательские скрипты, стили оформления, небольшие статичные изображения), либо генерацию веб-страниц (нагружающих как сам веб-сервер, так и сервер баз данных), что отражается на структуре входящего и исходящего трафика, имеет уникальный, характерный для него тип нагрузки и распределения процессорного времени и памяти по выполняющимся процессам – вся эта статистика формирует уникальный «отпечаток», который можно использовать как эталон для сравнения и выявления аномалий, критических ситуаций, и причин, их вызывающих.

В ходе работы была проведена реальная DDoS – атака на тестовый кластер серверов, во время которой была собрана подробная статистика запросов к веб-сервису. Информация по каждому запросу (IP адрес, user-agent, тип запроса, время запроса в виде UNIX Timestamp, адрес страницы, и так далее) записывалась в базу данных, после чего анализировалась, визуализировалась, и сравнивалась с аналогичной информацией, накопленной за период штатной работы веб-сервиса.

По визуализации данных были установлены критерии, по которым выборка линейно разделяется: резкий всплеск количества запросов в секунду, изменение распределения по методам HTTP запросов (GET, POST); изменение распределения запросов по типу отдаваемого контента: многократное увеличение количества запросов к генерирующим страницам, завязанным на базу данных, многократное увеличение количества запросов к тяжелой статике (картинкам, элементам оформления), которые эффективно забивают канал трафиком при отдаче; выявлено изменение распределения IP адресов по блокам, т.е. изменение территориального распределения клиентов; изменение распределений идентификационных строк браузеров (user-agent), существенные отклонения от устоявшейся статистики в сторону нормального распределения. Также была выявлена характерная последовательность запросов для легитимных пользователей – при загрузке страницы в определенном порядке загружается статика, скрипты, и оформление, когда атакующие запросы идут подряд и без закономерностей.

Выявленные в ходе работы закономерности и статистику запросов можно использовать как входные данные для различных алгоритмов интеллектуального анализа данных (Datamining), что повысит точность определения нештатных ситуаций и аномалий трафика.

УДК 004.056.52

АВТОМАТИЗИРОВАННОЕ СОЗДАНИЕ СИСТЕМЫ РОЛЕВОГО УПРАВЛЕНИЯ ДОСТУПОМ ДЛЯ ТЕЛЕКОММУНИКАЦИОННОЙ КОМПАНИИ

Н.А. Семенова
(Московский институт электроники и математики национального исследовательского университета «Высшая школа экономики»)
Научный руководитель – д.ф.-м.н., ст.н.с. М.И. Рожков
(Московский институт электроники и математики национального исследовательского университета «Высшая школа экономики»)

Краткое вступление, постановка проблемы. Значительным шагом в унификации механизмов управления доступом в распределенных автоматизированных информационных системах (АИС) является переход к централизованному управлению доступом (ЦУД). Система ЦУД включает в себя единый каталог учетных записей пользователей и прав доступа, назначенных им во всех модулях, а также единый перечень политик безопасности, определяющий правила назначения и отзыва прав доступа во всех управляемых модулях АИС, и обеспечивающий взаимосвязь между фактическими должностными обязанностями сотрудника в текущий момент времени и правами доступа, назначенными соответствующей ему учетной записи пользователя.

Вместе с тем, как отмечается во многих работах по данной тематике, первоначальное проектирование элементов системы ролевого управления доступом является крайне трудоемкой и дорогостоящей задачей, так как требует длительной совместной работы аналитиков информационной безопасности и технических специалистов — администраторов модулей АИС.

Среди особенностей АИС крупных телекоммуникационных компаний можно выделить следующие наиболее важные для реализации в них управления доступом: наличие сложных иерархических организационно-управленческих и организационно-технологических структур, а также существенную текучесть кадров в сфере информатизации.

Таким образом, являются актуальными исследования, направленные на разработку и научное обоснование подходов к моделированию и внедрению системы централизованного ролевого управления доступом в распределенных АИС.

Цель работы. Разработка алгоритма автоматизированного построения системы ролевого управления доступом (алгоритма ПРС) с учетом семантического контекста составляющих ее элементов (учетных записей пользователей, прав доступа и ролей).

Базовые положения исследования. Построение системы ролевого управления доступом осуществляется на основе формальной модели семантически осмысленного ролевого управления доступом (СК-РУД модели) к информационным ресурсам АИС, учитывающей специфику предметной области (семантический контекст) назначения ролей.

Работа алгоритма основана на представлении основных множеств системы ролевого управления доступом в виде решетки формальных понятий.

Промежуточные результаты. Автором разработан алгоритм ПРС, который впервые по сравнению с существующими аналогичными алгоритмами основан на методах формального анализа понятий и учитывает семантический контекст назначения ролей. Алгоритм ПРС по сравнению с аналогичными алгоритмами при построении системы ролевого управления доступом исключает создание ролей, совпадающих по входящим в их состав правам доступа и авторизованным на них учетным записям пользователей, а также строит систему семантически осмысленного ролевого управления доступом, соответствующую определениям и предположениям СК-РУД модели, явно задавая иерархию ролей и правила их автоматического назначения учетных записям пользователей.

Сравнительное тестирование функционала систем ролевого управления доступом, построенных с помощью алгоритмов ORCA и ПРС, в ходе промышленной эксплуатации в АИС ЗАО «К-Директ» позволило сделать вывод, что создание ролевой иерархии с семантическим контекстом при помощи алгоритма ПРС позволяет улучшить существенные функциональные характеристики системы ролевого управления доступом.

Основной результат. Алгоритм ПРС и основанная на нем методика построения системы централизованного семантически осмысленного ролевого управления доступом позволяет формализовать требования к разработке систем ролевого управления доступом с автоматизированным назначением ролей для широкого класса АИС с учетом специфики бизнес-процессов предприятия. Результаты исследования были использованы в ходе реализации проекта по разработке системы ЦУД АИС ЗАО «К-Директ», в котором с применением предложенной автором методики был реализован единый механизм ролевого управления доступом в шести подключаемых модулях АИС.

УДК 004.056

ОПРЕДЕЛЕНИЕ АВТОРСТВА ТЕКСТОВ КОРОТКИХ СООБЩЕНИЙ ПОРТАЛОВ СЕТИ ИНТЕРНЕТ ПРИ ПОМОЩИ МЕТОДОВ МАТЕМАТИЧЕСКОЙ ЛИНГВИСТИКИ

М.Е. Сухопаров
Научный руководитель – д.т.н., доцент И.С. Лебедев

Повсеместное использование ИТКС и сравнительная легкость доступа к ресурсам сети Интернет обуславливают необходимость в контроле над информационными потоками и идентификации возможных направлений информационного воздействия. В связи, с чем встает вопрос о необходимости анализа текстовой информации и установления авторства текста коротких сообщений различных порталов сети Интернет, вследствие недостаточной развитости механизмов идентификации пользователей. Анализ текстовых сообщений комментариев, блогов, а так же борьба с различными проявлениями астротерфинга являются крайне важным для борьбы с процессом искусственного формирования общественного мнения в сети Интернет.

Решаемая научная задача состоит в обосновании и разработке научно-методического аппарата идентификации авторства текстовой информации ($\mathbf{M}_{\text{m}}$), предназначенного для автоматического вычисления информации ($\hat{I}$) о текстах предметной области с минимальной потерей полноты, точности и адекватности ($\Delta I_{\min}$) при обработке I в комплексах вычислительных средств СЗИ, базирующегося на использовании:

- множество моделей $\left(H = \{H | f(q', d')\}\right)$, свойства которых q' и d' имеют функциональную зависимость $f(q', d')$ от свойств $\boldsymbol{Q}'$ представления информации и требуемых свойств $\boldsymbol{D}'$ представления данных в ИС;
- множество методов ($\mathbf{M}$) обеспечивающих отражение текстовой информации $\boldsymbol{T}$в элементы данных $\boldsymbol{O}$ с помощью функции $\boldsymbol{F}$.

Математически указанная задача формулируется следующим образом: найти множество $\mathbf{M} : Q \to Q', D \to D'$, $\forall q'(q' \in Q'), \forall d'(d' \in D')$ такое, что $\exists\left(\hat{I} = \hat{I}\{\mathbf{M}, H, q, q', d, d', \Delta I\}\right)$, при $\left\|I - \hat{I}\right\| \Rightarrow \Delta I_{\min}$. $M : T \xrightarrow{F} O$.

Реализация предлагаемых решений позволит идентифицировать авторов коротких сообщений форумов и блогов сети Интернет во время различных пиар – акций с целью борьбы и контроля над формированием и манипуляцией общественным мнением и другими проявлениями астротерфинга.

УДК 004.623

БЕЗОПАСНОСТЬ АУТЕНТИФИКАЦИИ В ИНТЕРНЕТ СЕРВИСАХ

А.А. Абабков
Научный руководитель – д.т.н., доцент И.С. Лебедев

В работе рассматривается возможные проблемы при аутентификации пользователей в сети Интернет, направления их решения и возможность предотвращения кражи персональных данных.

Цель работы – решение и выявление уязвимостей при аутентификации в сети интернет.

Интернет как вид информационных технологий является местом, где пользователи оставляют свою персональную информацию, которая, в дальнейшем, хранится и

обрабатывается в базах данных. Личная информация пользователей представляет интерес злоумышленников, которые могут использовать личную информацию в корыстных целях. Поэтому стоит говорить именно о безопасности личной информации и о требованиях, предъявляемых при ее обработке. Во избежание несанкционированного доступа, модификации или уничтожения персональных данных, должны разрабатываться высокоэффективные программно-аппаратные комплексы, с учетом современных технологий и нормативно-правовой базы.

Современный Интернет – это место скопления личной информации почти каждого человека. Мировая глобализация привела к тому, что в Интернете зарегистрированы миллионы людей и, так, или иначе, существует реальная угроза хранения и обработки этой информации.

В настоящее время существует реальная угроза с аутентификацией пользователей в различных Интернет сервисах: форумы, социальные сети, почтовые сервисы, что приводит к возможности кражи персональных данных или подмены, модификации личной информации, третьими лицами.

На данный момент почти каждый Интернет сервис предоставляет возможность регистрации пользователя. Он зачастую обязан ввести требуемую информацию ради получения доступа к дополнительным возможностям Интернет сервисов. Но после регистрации пользователь чаще всего не знает, где и как хранится введенная им информация, и что с этой информацией в дальнейшем могут сделать владельцы и администраторы базы данных.

Возникновение данной проблемы обусловлено недостаточно хорошими методами защиты персональных и регистрационных данных: недостаточный уровень шифрования информации, доступ технического персонала к служебной информации, уязвимость в программном коде Интернет сервисов.

Литература

1. Портал PHP, MySQL и другие веб-технологии [Электронный ресурс]. – Режим доступа: http://www.php.su/functions/?md5, своб.
2. Википедия свободная энциклопедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/MD5, своб.
3. Википедия свободная энциклопедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/HTML, своб.
4. Википедия свободная энциклопедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/PHP, своб.
5. Каталог статей для программистов [Электронный ресурс]. – Режим доступа: http://www.smartyit.ru/php/54, своб.

УДК 004.056+004.896

ОЦЕНКА ПРИМЕНИМОСТИ КЛАССИЧЕСКИХ МОДЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ К ЗАДАЧЕ УПРАВЛЕНИЯ РОБОТОТЕХНИЧЕСКИМИ СИСТЕМАМИ

Д.Ю. Басманов

Научный руководитель – к.ф.-м.н., доцент И.И. Комаров

Постановка задачи. Благодаря техническому прогрессу робототехнические системы становятся все доступнее, что делает их более привлекательными для использования в автоматизации задач. Вместе с тем, как это часто бывает с новыми технологиями, информационная безопасность не рассматривается как важный фактор при проектировании

подобных систем. Внедрение решений по обеспечению информационной безопасности постфактум или на завершающих этапах разработки зачастую требует переделки архитектуры системы и больших временных и денежных затрат. Ситуация осложняется тем, что на сегодняшний день не существует стандартов информационной безопасности для робототехнических систем.

Цель работы – провести оценку применимости классических моделей информационной безопасности к задаче управления робототехническими системами.

Базовые положения исследования. Защита информации в общем случае подразделяется на обеспечение конфиденциальности, целостности и доступности. До сих пор в русскоязычной и зарубежной литературе в основном рассматривались вопросы отказоустойчивости. Существует ряд классических моделей информационной безопасности, часть которых посвящена другим аспектам: обеспечение конфиденциальности информации (например, модель Белла-ЛаПадула) и целостности данных (модель Кларка-Вилсона). У этих моделей есть свои ограничения по применению. Робототехнические системы также имеют ряд особенностей, которые могут потребовать защиты других параметров управления, таких как непрерывность или скрытность, что необходимо учитывать применяя модели из других отраслей. Например, для кооперативных робототехнических систем важна непрерывность коммуникаций, иначе роботы не смогут взаимодействовать друг с другом. С другой стороны, разглашение третьим лицам информации о состоянии батареи или боезапаса в случае с военными роботами может представлять большую угрозу. Кроме того, робототехнические системы с обучением могут значительно менять свое дельнейшее поведение в зависимости от информации, которая может поступать из специфических источников: визуальные жесты, голосовые команды, тактильные датчики и т.п.

Основные результаты. В данной работе рассмотрены характеристики и ограничения классических моделей информационной безопасности. Проанализированы особенности робототехнических систем и выявлены важные направления защиты. Проведена оценка применимости классических моделей информационной безопасности к задаче управления робототехническими системами. Найдены полезные модели в области распределенных вычислений.

УДК 004.773.2

ВЫЯВЛЕНИЕ ПОТЕНЦИАЛЬНЫХ УЯЗВИМОСТЕЙ СИСТЕМЫ НА ОСНОВАНИИ АНАЛИЗА ОБРАЩЕНИЙ К АППАРАТНЫМ РЕСУРСАМ

Р.Ш. Ишкин
Научный руководитель – д.т.н., доцент И.С. Лебедев

В работе рассматривается возможные способы выявления потенциальных уязвимостей систем с применением анализа обращений к аппаратным ресурсам.

Цель работы – повышение точности выявления потенциальных уязвимостей систем.

Целью взлома системы является получение неограниченных прав доступа. Одним из видов взлома компьютера является взлом с помощью установленного программного.

В большинстве программ, предусмотрены функции безопасности. Проблема в том, что многие механизмы, разработанные для защиты, сами являются программами и, следовательно, могут также иметь уязвимости. При ошибках в программном обеспечении убытки исчисляются миллионами, что иногда приводит к необратимым и даже фатальным последствиям.

Множество используемых современных операционных систем поддерживают расширяемость с помощью динамически загружаемых драйверов устройств и модулей, что существенно усложняет задачу обеспечения информационной безопасности.

Взлом программного обеспечения всегда является нетривиальной задачей. Сначала нужно понять, какую задачу решает фрагмент кода. Часто это можно сделать только по результатам работы. Иногда программный код можно разделить на несколько фрагментов и изучить их отдельно. Либо предназначение программного кода определяется с помощью некорректных входных данных. Этот код можно дизассемблировать или декомпилировать. После чего появляется возможность с его помощью можно изучить проект программы и архитектурные проблемы.

Учитывая вышесказанное, представляются актуальными вопросы исследования низкоуровневых обращений программного обеспечения к аппаратным ресурсам определенной системы, а также разработки методологии и определения уязвимостей на примере реализации алгоритма, выполненного посредством языка Си (дефакто являючимся основой большинства современных высокоуровневых языков) и Java (как одного из наиболее используемых кроссплатформенных языков), с последующим дизассемблированием и систематизацией результатов анализа на основании этих данных.

Литература

1. Касперски К., Рокко Е. Искусство дизассемблирования. – СПб: БХВ-Петербург, 2008. – 896 с.
2. Хогланд Г., Мак-Гроу Г. Взлом программного обеспечения – анализ и использования кода. – М.: Изд. дом «Вильяме», 2005. – 400 с.
3. Пирогов В. Ассемблер и дизассемблирование. – СПб: БХВ-Петербург, 2006. – 464 с.
4. Википедия свободная энциклопедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Дизассемблер, своб.
5. Википедия свободная энциклопедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Взлом_программного_обеспечения, своб.
6. Википедия свободная энциклопедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Обратная_разработка,http://ru.wikipedia.org/wiki/Обратная_инженерия, своб.
7. Часто задаваемые вопросы по дизассемблеру IDA Pro[Электронный ресурс]. – Режим доступа: http://cracklab.narod.ru/doc/ida_faq.htm, своб.

УДК 004.773.2

ДОПОЛНИТЕЛЬНЫЕ ПАРАМЕТРЫ СЕТЕВОЙ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ НАПРАВЛЕННЫЕ НА РЕШЕНИЕ ПРОБЛЕМЫ ФОРМИРОВАНИЕ ОБЩЕСТВЕННОГО МНЕНИЯ В СЕТИ ИНТЕРНЕТ

П.С. Кламбоцкий
Научный руководитель – д.т.н., доцент И.С. Лебедев

В работе рассматривается возможности по дополнительным параметрам идентификации пользователей в сети интернет направленные на решение проблемы формирование общественного мнения.

Цель работы – решение проблемы формирования общественного мнения в сети Интернет.

Интернет как вид информационных технологий оказывает наиболее значительное влияние на формирование общественного мнения в современном обществе и создает новую информационную сферу. Эти условия создают специфическую коммуникационную среду,

которая находит свое отражение в различных Интернет-сообществах (форумы), таких как социальные сети, блоги, микроблоги и т.д. Поэтому стоит говорить именно о влиянии особенностей коммуникационной среды на процесс формирования общественного мнения. Интернет способствует развитию двухступенчатой модели коммуникации с обратной связью. Это создает характер личного участия человека в решении социально значимых проблем, что также влияет на повышение активности интернет-взаимодействия и формирование на его основе общественного мнения.

Интернет и коммуникационная среда имеют значительное объединяющее и организующее свойство, что может говорить о влиянии их не только на процесс формирования, но также и на процесс реализации общественного мнения.

В настоящее время существует большая проблема с идентификацией пользователей на форумах, что приводит к возможности выражать одним пользователем своего мнения (возможно заведомо неверного или ложного) от разных лиц, формируя тем самым массовость и единства мнения у многих людей путем написания сообщений от разных лиц. Тем самым происходит формирование массовости и единство мнения. Обычно это происходит путем развития мысли от сообщения к сообщению и склонение остальных пользователей, просматривающих сообщения, к своей точке зрения.

Возникновение данной проблемы обусловлено недостатком технологии идентификации пользователей на информационных площадках и форумах, что дает возможность для регистрации одному пользователю сколь угодное количество аккаунтов.

Литература

1. Гавра Д.П. Формирование общественного мнения: ценностный аспект. – СПб, 1995. – 62 с.
2. Крыштановский А.О. Анализ социологических данных. – М.: Изд. дом ГУ-ВШЭ, 2006. – 281 с.
3. Горшков М.К. Общественное мнение. – М.: Политиздат, 1988. – 382 с.
4. Википедия свободная энциклопедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Общественное_мнение, своб.
5. «ПСИ-ФАКТОР» – Центр практической психологии [Электронный ресурс]. – Режим доступа: http://psyfactor.org/forum1.htm, своб.
6. Территория твоего развития [Электронный ресурс]. – Режим доступа: http://www.brainity.ru/society/trends/11995/, своб.
7. Википедия свободная энциклопедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Аутентификация, своб.
8. Архив полезных статей Интернета [Электронный ресурс]. – Режим доступа: http://webarticles.net.ru/articles/internet/identification_user.php, своб.
9. ИВП «Прогресс» Обеспечение безопасности объектов [Электронный ресурс]. – Режим доступа: http://sio.su/down_a4ud_407_def.aspx, своб.

УДК 004.056

ПРОГНОЗИРОВАНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е.В. Козлова
Научный руководитель – д.т.н., профессор И.А. Зикратов

Методы прогнозирования различного рода процессов находят свое применение во многих областях науки.

Доктрина информационной безопасности Российской Федерации, в частности, ставит задачу совершенствования форм, методов и средств выявления, оценки и прогнозирования

угроз информационной безопасности страны как безотлагательную [1]. Однако формализация подхода к прогнозированию такого вида угроз не осуществлена и по сей день.

Прогнозирование информационных угроз в настоящее время реализовано в качестве предположений о тех видах атак, которые вероятно будут актуальны или возникнут в новых формах проявления в ближайшем будущем. Прогноз также осуществляется в виде анализа динамики техпроцессов, которые существуют на данный момент, и предположения о сохранении выделенного тренда.

Вместе с тем существует необходимость осуществления прогноза с нахождением причинно-следственных связей, зависимостей, а также моделирования повторяющихся циклов реализации информационных угроз. Эту задачу позволяют решить средства статистического анализа.

Для фирмы в частности это поможет планировать затраты на обеспечение безопасности и контролировать обновление пакетов программ защиты информации. В критические периоды времени это позволит диверсифицировать силы, направленные на обеспечение информационной безопасности, и избежать многих проблем (юридических, финансовых), а также поддержать собственную репутацию.

В результате такой подход может быть использован для целей поддержания непрерывности ведения бизнеса.

Таким образом, необходимость заблаговременного принятия решений при проектировании и обслуживании средств защиты информационной системы актуализирует проблему, поставленную в рамках данного исследования.

Целью работы является прогнозирование возможных угроз информационной безопасности на конкретную дату, а также поиск взаимосвязей.

Задачей данного исследования будет построение формализованной математической модели прогнозирования угроз информационной безопасности, а также выработка методики принятия решений.

Исследование будет заключаться в анализе статистических данных реализованных угроз и их прогнозирование на основе полученной математической модели.

Источником информации для целей данного исследования будут являться данные, предоставляемые в обзорах, отчетах различных организаций и порталов.

Следующие методы предлагается использовать для целей исследования [2]:

- корреляционно-регрессионный анализ;
- анализ тренда;
- прогнозирование временных рядов;
- моделирование сезонных колебаний.

В результате исследования должен быть выработан некий метод, позволяющий на основе входных данных проанализировать взаимосвязи и сделать практические выводы из выполненного прогноза.

Этот метод будет включать: анализ основных угроз безопасности, подбор статистических данных, анализ взаимосвязей, построение значимой модели, прогноз развития и принятие решений по результатам анализа.

Этот подход позволит с установленной степенью вероятности говорить о том, что на конкретную дату или за конкретный промежуток времени ожидается наступление или усиление влияния конкретных угроз безопасности.

В настоящее время открыто публикуемые данные достаточно тяжело систематизировать. Прерывистость этих данных порой также не позволяют создать однородный массив за выбранный период времени.

Все это делает сбор статистической систематизированной информации ключевым для целей исследования.

Первые результаты анализа на основе части массива той статистической информации, которую на данный момент удалось найти и систематизировать, первично позволяют

говорить о наличии взаимосвязи между исследуемыми показателями, а также об обоснованности дальнейших исследований.

Литература

1. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) // Российская газета. – 28.09.2000. – № 187.
2. Елисеева И.И., Юзбашев М.М. Общая теория статистики. Учебник / Под ред. И.И. Елисеевой. – 5-е изд., перераб. и доп. – М.: Финансы и статистика, 2004. – 656 с.

УДК 004.02

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ РОБОТОТЕХНИЧЕСКИХ КОМПЛЕКСОВ

П.А. Кузьмич, И.С. Пантюхин, Е.Н. Коваль, А.С. Сучков
Научный руководитель – д.т.н., профессор И.А. Зикратов

В связи с ростом области применения информационных систем, в том числе с применением робототехнических комплексов, вопрос расследования инцидентов информационной безопасности, применительно к ним, становится все более актуальным.

Необходимость расследования инцидентов отражена в большинстве международных стандартов, в том числе ISO\IEC 27001-2005, ISO\IEC TR 18044.

Особенность расследования инцидентов в системах, где составной частью является робототехнический комплекс, заключается в том, что в большинстве случаев такие устройства не содержат надлежащей встроенной системы фиксации событий, а если таковая система есть – то получить сведения в полном объеме и надлежащем виде крайне сложно.

Важным аспектом расследования инцидентов информационной безопасности в робототехнических системах также является необходимость использования комплексного подхода, включая исследование каналов связи между составными частями комплекса. Это становится все более актуально в связи с развитием технологий управления роботами через общедоступные сети, в том числе Интернет.

Такие сложности возникают в подавляющем большинстве из-за отсутствия документации, содержащей информацию о внутреннем строении, а также из-за отсутствия возможности идентифицировать составляющие комплекс части.

Отсутствие документации даже при возможности идентифицировать управляющие элементы системы объясняется также и нежеланием разработчиков сообщать информацию о внутренней логике работы своего комплекса.

Несмотря на данные сложности исследование таких систем необходимо и возможно.

Безусловно, исследуя неизвестную систему, выполнить в полном объеме принцип сохранения объекта исследования в неизменном состоянии не удастся, поскольку поиск способов подключения к изучаемой системе может быть проведен только экспериментальным путем.

Тем не менее, большинство реализаций программно-аппаратных комплексов реализуются с применением одних и тех же технологий, схожего программного обеспечения (операционной системы), взаимодействуют по стандартным (или схожим) протоколам и программируются через стандартные типы шин (JTAG, RS232, USB и т.д.)

В связи с этим процесс исследования целесообразно разделить на несколько основных этапов, а именно:

Визуальное изучение объекта исследования с целью установления используемых компонент (платформы, микропроцессора, носителей памяти), их типов и интерфейсов подключения;

Разработка и доработка методики с учетом полученных результатов и проверка (в том числе повторная) опытным путем;

Сбор полученной информации и формулировка ответов на поставленные исследованием вопросы.

В общем случае приемлема следующая модель взаимодействия (рисунок).

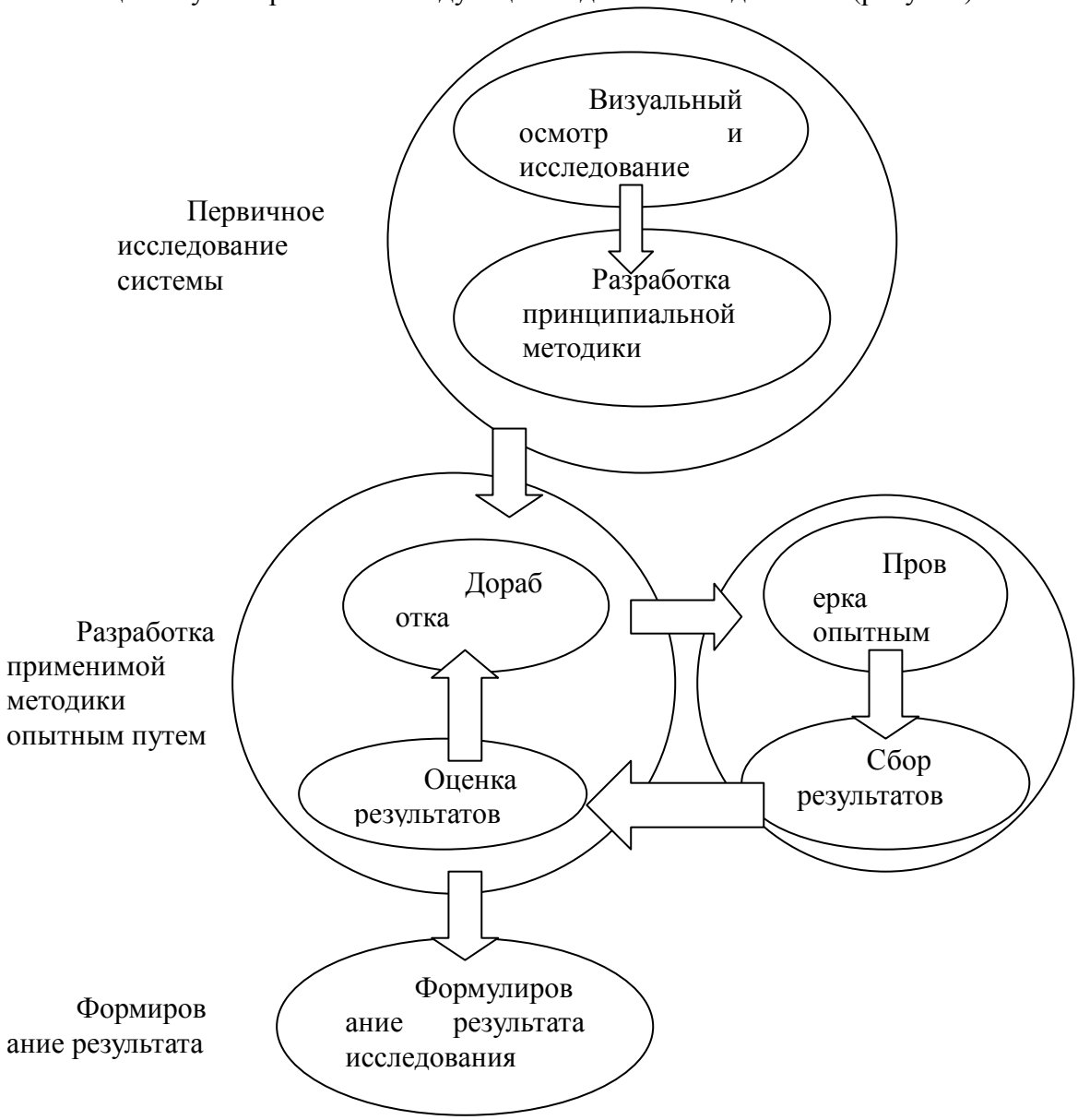

Рисунок. Модель взаимодействия

Также стоит отметить, что формирование новой методики может быть выполнено на основе аналогичной методики, разработанной ранее. Подведение в конце исследования не только положительных результатов, но и отрицательных, позволит избежать многих ошибок при производстве последующих исследований.

УДК 004.056+91:004

АНАЛИЗ ТЕКУЩЕГО СОСТОЯНИЯ БЕЗОПАСНОСТИ ГЕОИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Л.Д. Ястребов
Научный руководитель – к.т.н., доцент А.Г. Карманов

Введение. Географическая информационная система (ГИС) – современная компьютерная технология для картографирования и анализа объектов реального мира, происходящих и прогнозируемых событий и явлений. ГИС дает человеку наиболее естественное и понятное отображение пространственных данных.

В настоящее время использование ГИС уже давно вышло за пределы военных и промышленных ведомств, и теперь геоинформационные технологии все чаще и чаще применяются в повседневной жизни.

Основные понятия. Согласно ГОСТ Р 52438-2005, ГИС – это информационная система, оперирующая пространственными данными. Однако для современных ГИС это определение можно несколько уточнить. Далее под ГИС будем понимать специализированную ИС, предназначенную для работы на интегрированной основе с геопространственными и различными по содержанию семантическими данными. В свою очередь под геопространственными данными (геоданными) мы будем понимать данные об объектах и явлениях, которые представлены в координатно-временной форме.

С точки зрения защиты данных ГИС удобно классифицировать по признаку доступности этих данных. Можно выделить три основных категории ГИС по признаку доступности геоданных: сетевая, персональная и Интернет-ГИС.

Под сетевой ГИС будем понимать систему, функционирующую в масштабе предприятия и предназначенную для обеспечения совместного доступа к геоданным. Основным атрибутом сетевой ГИС является наличие ГИС-сервера или серверов со специализированным программным обеспечением для хранения геоданных, к которым обращаются пользователи.

Под персональной ГИС будем понимать систему, функционирующую на одном компьютере и предназначенную для решения задач, не требующих привлечения сетевых технологий. Этот класс разделяется на два подкласса: ГИС массового использования и настольная ГИС.

ГИС массового использования рассчитана на свободную продажу и не может содержать каких-либо секретных данных. Кроме того, она должна обеспечивать надежную защиту от повторного использования данных, которое могло бы быть причиной убытков владельцев ГИС. Примерами таких ГИС являются электронные атласы, картографические справочники, навигаторы и другие.

Настольная ГИС может представлять собой элемент корпоративной ГИС для решения каких-либо прикладных задач. Они могут использоваться в небольших компаниях, занимающихся обработкой и анализом геоданных, полученных с помощью других ГИС. Обычно такие компании не создают первоначальные данные, а покупают их у поставщиков. В этом случае поставщикам необходимо защищать продаваемые данные от возможности несанкционированного использования и тиражирования.

Интернет ГИС – это система, выполняющая основные манипуляции с геоданными (в том числе и хранение данных) на специализированном картографическом Интернет сервере и предоставляющая эти данные пользователям по протоколу, совместимому с HTTP.

Вопросы безопасности. Как правило, разработчики ГИС, а также различные компании и ассоциации, занимающиеся проблемами ГИС, наибольшее внимание уделяют вопросам

расширения функциональности и области использования своих продуктов, увеличению эффективности расчетов и вычислительной мощности. Однако вопросам, связанным с информационной безопасностью ГИС, не уделяется необходимого внимания. Хотя следует помнить, что зачастую в ГИС может содержаться информация, представляющая коммерческую или государственную тайну.

Наиболее масштабная работа, связанная с проблемой безопасности ГИС, была проведена и опубликована Л.К. Бабенко и другими авторами в книге «Защита данных геоинформационных систем» [1]. На основании модели угроз был проведен анализ и сделаны рекомендации по повышению безопасности ГИС разных типов.

Так, для персональной ГИС массового использования, в качестве стратегии защиты предлагается уделять минимальное внимание защите самой программы, что позволит удешевить ее, но в то же время уделить максимальное внимание защите данных, что позволит защитить коммерческие и имущественные интересы разработчика и поставщика данных. В качестве мер защиты предлагается скрывать некоторые объекты и целиком убирать координаты объектов.

Для персональной настольной ГИС рекомендуется криптографическая защита данных, а также использование приложений, умеющих напрямую читать шифрованные данные. Рассматривается три разных способа шифрования: функции шифрования встраиваются в прикладное ПО, обеспечиваются на уровне ОС или же предоставляются сторонними разработчиками. При этом проводится обзор алгоритмов шифрования DES, IDEA, ГОСТ 28147-89.

Для сетевых и Интернет ГИС рекомендуется максимально защищать сервера от несанкционированного доступа, изменения и удержания данных, предоставление пользователям только тех данных, повторное использование которых в коммерческих продуктах исключается. Подробно описаны методы, с помощью которых можно повысить защищенность серверов, такие как модернизация программного обеспечения, использование узкоспециализированных серверов, удаление лишних приложений, ограничение использования скриптов и другие.

Заключение. Особенность рассмотренных методов защиты в том, что ГИС рассматривается как набор разрозненных компонентов и различные методики повышения безопасности предлагаются для этих отдельных компонентов с точки зрения пользователя и администратора ГИС.

Защита отдельных компонентов, несомненно, важна, но также необходимо рассматривать вопросы защищенности самого геоинформационного ПО с точки зрения разработчика системы, так как только на этапе проектирования внутренней структуры системы есть возможность органично предусмотреть действие многочисленных угроз информационной безопасности.

Литература

1. Бабенко Л.К., Макаревич О.Б., Журкин И.Г., Басан А.С. Защита данных геоинформационных систем. – М.: Гелиос АРВ, 2010. – 336 с.
2. Лурье И.К. Геоинформационное картографирование: история становления ГК [Электронный ресурс]. – Режим доступа: http://www.lomonosov-fund.ru/enc/ru/encyclopedia:0133948. – Загл. с экрана.

УДК 342.721

АНАЛИЗ ИЗМЕНЕНИЙ РОССИЙСКОГО ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

А.А. Старков
Научный руководитель – к.т.н., доцент А.В. Птицын

Введение и постановка проблемы. 1 ноября 2012 года постановлением Правительства РФ №1119 были утверждены Требования к защите персональных данных при их обработке в информационных системах персональных данных, которые отменили Постановление Правительства №781 от 17 ноября 2008 года «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных». Постановлением определены категории информационных систем, три типа актуальных угроз безопасности персональных данных, а также четыре уровня защищенности персональных данных с конкретизацией требований к ним. Несмотря на то что новый нормативно-правовой акт призван искоренить все недостатки предыдущего, к законодателю остался ряд вопросов по содержанию некоторых из его положений.

Целью работы является анализ новых требований законодательства в области защиты персональных данных, обзор видоизмененной классификации информационных систем и актуальных угроз, а также выработка собственных предложений по совершенствованию законодательства в данной сфере.

Базовые положения исследования. В ходе анализа вышеупомянутого законодательного акта было выявлено некоторое количество его «белых пятен», исправление которых может позволить контролирующим органам однозначно регламентировать алгоритм своей работы при проведении проверок операторов персональных данных, а операторам более ответственным образом подойти к исполнению требований закона. Новые требования не соответствуют последней редакции закона «О персональных данных», в них не предложены методы и способы нейтрализации угроз, есть некоторые вопросы по терминологии документа, кроме того полноценное функционирование Требований возможно только после принятия соответствующих актов ФСБ и ФСТЭК. В связи с этим автором выработаны конкретные предложения по совершенствованию существующего документа.

Результаты исследования. В результате анализа Требований к защите персональных данных при их обработке в информационных системах персональных данных автором был выдвинут ряд предложений по совершенствованию законодательства в этой сфере. На сегодняшний день требуется разработка отраслевых моделей угроз, а также состава и содержания организационных и технических мер по обеспечению безопасности персональных данных. Кроме того, в документе отсутствуют требования по защите от ПЭМИН, разработка которых также необходимо произвести в ближайшее время. Наконец, в связи с тем, что вместо классов информационных систем персональных данных требования теперь задаются уровнем защищенности последних, требуются дополнительные работы от операторов по определению уровней защищенности персональных данных, так как с выходом Требований «закон трех» по сути остался вне правового поля.

УДК 004.912

ОЦЕНКА ТОНАЛЬНОСТИ ТЕКСТОВОЙ ИНФОРМАЦИИ, АНАЛИЗ И СРАВНЕНИЕ ЭФФЕКТИВНОСТИ АЛГОРИТМОВ

А.Е. Красильников
Научный руководитель – к.ф.-м.н., доцент И.И. Комаров

Задача анализа тональности текстовой информации, генерируемой в сети Интернет, является частью задачи обеспечения информационной безопасности. Она крайне важна для успешной работы любых организаций и структур.

Целью работы являлось разработка и создание программного продукта, выполняющего анализ тональности текстовой информации несколькими методами, сравнение его с существующими образцами и изучение возможности улучшения результатов для выбранных методов. В качестве рабочих выбраны: метод с использованием лингвистического словаря и наивный байесовский классификатор.

Анализ тональности текста, реализуемый с помощью тонального словаря, состоит из нескольких этапов. Сначала отрабатывает отдельный лингвистический модуль, автоматически производящий анализ текста, лемматизацию всей лексики, отношения между словами. Затем слова размечаются по заранее подготовленным словарным спискам тональной лексики. Каждому слову приписывается значение, указывающие на силу тональности. Если слово не нашлось в списках тональной лексики, то оно считается нейтральным. Анализируется каждое слово в предложении, затем идет построение биграмм, происходит анализ тональности предложения с учетом полученных данных, тональность предложения равняется среднему арифметическому тональностей его составляющих.

Наивный байесовский классификатор – вероятностный классификатор, основанный на теореме Байеса и (наивном) предположении о статистической независимости случайных величин.

$$P(C \mid F_1,\ldots,F_2) = \frac{\mathrm{P}(C)\,\mathrm{P}(F1,\ldots,F2 \mid C)}{\mathrm{P}(F1,\ldots,F2)}.$$

Основное достоинство данного классификатора заключается в низкой вычислительной сложности, а также в оптимальности, при условии действительной независимости признаков.

Оба метода используют для обучения и работы часть открытого тонального словаря проекта MPQA (Multi-PerspectiveQuestionAnswering).

Традиционно эффективность задачи классификации текста формулируется в терминах точности и полноты.

Точность – отношение числа правильно отнесенных текстов к определенному классу, к числу всех текстов, отнесенных к этому классу.

Полнота – отношение числа правильно отнесенных текстов класса 1 к числу текстов класса выбранного в коллекции.

Для оценки эффективности работы реализованных алгоритмов был проведен анализ выборки, состоящей из 30 текстов различной тематики. Для сравнения с существующими решениями, были использованы открытые проекты PythonNLTK и анализатор проекта Brandlisten. В основе работы обоих анализаторов лежит Наивный байесовский классификатор.

Таблица. Наивный байесовский классификатор

	Точность	Полнота
PythonNLTK	0,9	1
Brandlisten	0,25	0,25
Метод, использующий тональный словарь	0,6	0,6

	Точность	Полнота
Наивный байесовский классификатор	0,8	0,9

Исходя, из результатов можно сделать вывод: эффективность работы анализатора с использованием наивный байесовского классификатора выше, чем у метода, основанного только на использовании тонального словаря, однако ниже чем у классификатора в проекте PythonNLTK. Добиться повышения эффективности работы созданного анализатора возможно увеличением обучающей выборки, а также совместным использованием нескольких методов анализа тональности.

УДК 026.06

МЕТОДЫ И СРЕДСТВА КЛОНИРОВАНИЯ RFID-МЕТОК

Р.А. Юрьева
Научный руководитель – к.ф.-м.н., доцент А.Б. Левина

Краткое вступление, постановка проблемы. Доступные методы для защиты RFID-меток от клонирования ограничены. В частности, криптографические подходы, предложенные в литературе не могут быть использованы с популярными существующими стандартными метками, поскольку они требуют изменений в интегральной схеме чипа, и существующие меры детектирования клонирования плохо работают в условиях ограниченной видимости.

Цель работы. Аналитический обзор существующих методов и средств клонирования содержимого RFID-меток и способов защиты от несанкционированного клонирования.

Базовые положения исследования. Представленный метод позволяет использовать перезаписываемую память метки. К ID-метки добавляется хаотическое случайное число, которое меняется каждый раз, когда метку «прочитывают». Обозначают это число тайным, так как это тайна от всех, кто не имеет доступа к метке, а также, потому что это число может быть понято как одноразовый пароль. Централизованная серверная система выдает эти «тайные» числа и отслеживает, какие числа, на каких метках для обнаружения ошибок синхронизации.

Промежуточные результаты. Каждый раз, когда метка «прочитывается» индикатор сначала проверяет статический идентификатор метки. Если это число является верным, индикатор затем сравнивает метку с синхронизированным «тайным» числом, что хранится для данного тега. Если эти числа совпадают, то тег проходит проверку, в противном случае происходит сигнал тревоги. После проверки, индикатор создает новый синхронизированный «секрет».

Практические результаты. Обнаружение клонированных RFID-меток – важная задача, для обеспечения безопасности коммерческих приложений RFID, поскольку она не требует более затратных алгоритмов шифрования. Предложенный способ представляет собой хаотически синхронизированный метод «секретов» для обнаружения атак на RFID-метки и их клонирования, чтобы точно определить различные теги с тем же ID. Представленный метод требует лишь небольшого количества перезаписи памяти для написания случайного числа в теге, но обеспечивает значительное повышение уровня безопасности для систем, которые используют незащищенные теги.