ISSN 2223–2966

Научно-практический журнал

Scientific and practical journal

**СОВРЕМЕННАЯ НАУКА:
АКТУАЛЬНЫЕ ПРОБЛЕМЫ ТЕОРИИ И ПРАКТИКИ**

ЕСТЕСТВЕННЫЕ И
ТЕХНИЧЕСКИЕ НАУКИ

№ 10/11–2012 (октябрь/ноябрь)

Учредитель журнала
Общество с ограниченной
ответственностью
«НАУЧНЫЕ ТЕХНОЛОГИИ»

В НОМЕРЕ:

МАТЕРИАЛЫ
V МН-ПК
“ИНФОРМАЦИОННЫЕ
ТЕХНОЛОГИИ В НАУКЕ,
БИЗНЕСЕ И ОБРАЗОВАНИИ”

Часть 2

Издатель: Общество с ограниченной ответственностью
«Научные технологии»
Адрес редакции и издателя:
109443, Москва,
Волгоградский пр–т, 116–1–10
Тел/факс: 8(495) 755–1913
E–mail: redaktor@nauteh–journal.ru
http: //www.nauteh–journal.ru
http: //www.vipstd.ru/nauteh

Журнал зарегистрирован Федеральной службой по надзору
в сфере массовых коммуникаций, связи
и охраны культурного наследия.
Свидетельство о регистрации
ПИ № ФС 77–44912 от 04.05.2011 г.

Журнал издается с 2011 года

Редакция:
Главный редактор
А.В. Царегородцев
Выпускающий редактор
Ю.Б. Миндлин
Корректор
Е.В. Михайлова
Верстка
Д.М. Замятин

*Подписной индекс издания
в каталоге агентства "Почта России"* — 80016

В течение года можно произвести подписку
на журнал непосредственно в редакции

Журнал отпечатан в типографии
ООО "КОПИ–ПРИНТ"
тел./факс: (495) 973–8296
Подписано в печать 30.11.2012 г.
Формат 84×108 1/16
Печать цифровая
Заказ № 0000
Тираж 2000 экз.

СОДЕРЖАНИЕ

CONTENTS

ЗАЩИТА ИНФОРМАЦИИ

№ 10/11-2012 (октябрь/ноябрь)

CONTENTS

ЗАЩИТА ИНФОРМАЦИИ

РЕШЕНИЕ ЗАДАЧИ ПРОГНОЗИРОВАНИЯ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ БЕЗОПАСНОСТИ НА ПРИМЕРЕ ПРЕСТУПЛЕНИЙ ЭКОНОМИЧЕСКОЙ НАПРАВЛЕННОСТИ

Бекетнова Юлия Михайловна
НИЯУ МИФИ, Москва, аспирант
beketnova@mail.ru

В современных условиях одним из перспективных направлений развития информационной безопасности является проблема оценки рисков. В частности, моделирование преступной активности субъектов финансовой и информационной безопасности позволит своевременно выявлять наиболее уязвимые участки, а также перераспределять усилия, направленные на противодействие угрозам безопасности. Так, прогнозирование преступлений экономической направленности может использоваться в качестве дополнительного инструмента при поддержке принятия управленческих решений в целях наиболее эффективного использования кадровых, экономических, технических и других ресурсов.

В настоящей статье приведен пример построения авторегрессионной модели преступлений экономической направленности и сделан прогноз совершения таких преступлений в будущем.

Данные для проведения анализа, а именно, статистические данные по преступлениям экономической направленности за период с января 2003 года по март 2012 года, были взяты из официальной статистики МВД России (Рис.1).

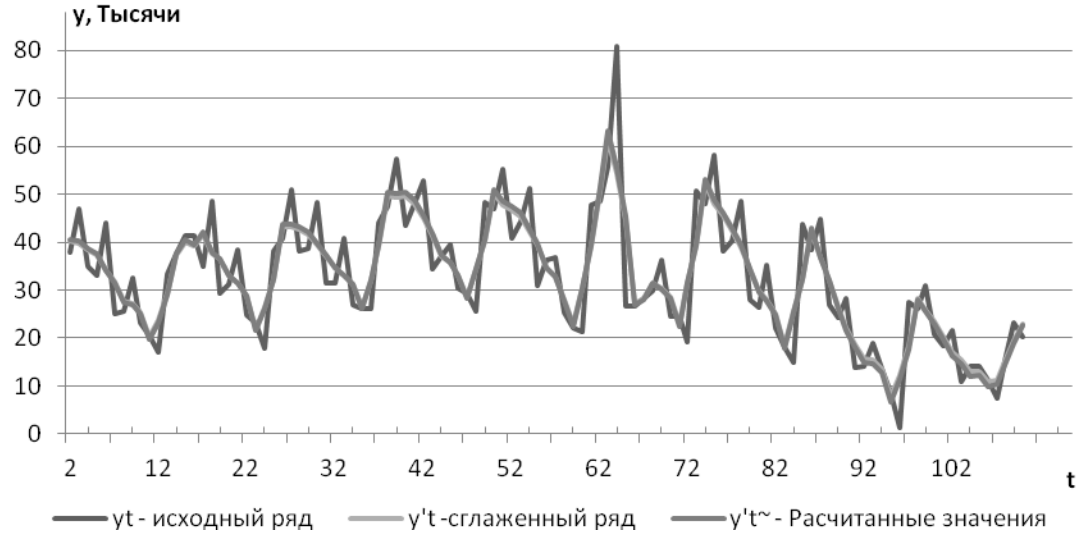

Рис. 1. Регрессионная модель преступлений экономической направленности

При анализе графика (рис.1), была замечена сезонность совершаемых преступлений, пик которой приходится на весенне-летний период времени.

Было принято решение о необходимости применения сглаживания ряда (как метода выявления тренда) перед непосредственным анализом методом линейной регрессии с авторегрессионной составляющей. Сглаживание проводилось методом скользящей средней.

Полученное уравнение регрессии имеет вид:

$$\tilde{y}'_1 = -1587.73 + 1.05 y'_{t-1}$$

График, построенный на основании рассчитанных значений, буквально повторяет данные со сглаженными значениями и довольно точно отражает исходные данные. Далее была проведена математическая проверка полученных значений на адекватность, по результатам которой можно заключить, что на основании выявленной регрессионной модели, представляется возможным осуществить прогноз на несколько периодов вперед.

Прогнозирование условно можно разделить на два этапа: построение точечного прогноза и нахождение границ (доверительного интервала) для интервального прогноза.

Интервальный прогноз осуществляется путем нахождения границ прогноза:

$y'_{n+k} \pm U_k$ – граница прогноза,

где y'_{n+k} – точечный прогноз величины *y*, а U_k – величина отклонения от точечного значения, соответствующая исследуемой точке y'_{n-1+k} и заданному уровню вероятности.

Величина U_k для линейной модели рассчитывается по формуле:

$$U_k = S_\sigma t_\lambda \sqrt{\frac{1}{n} + \frac{\left(y'_{n-1+k} - \overline{y}_{n-1}\right)^2}{\sum_{t=2}^{n}\left(y'_{t-1} - \overline{y}_{n-1}\right)^2}}$$

где t_λ - табличное значение *t*-критерия Стьюдента для заданной вероятности попадания прогнозируемой величины внутрь доверительного интервала.

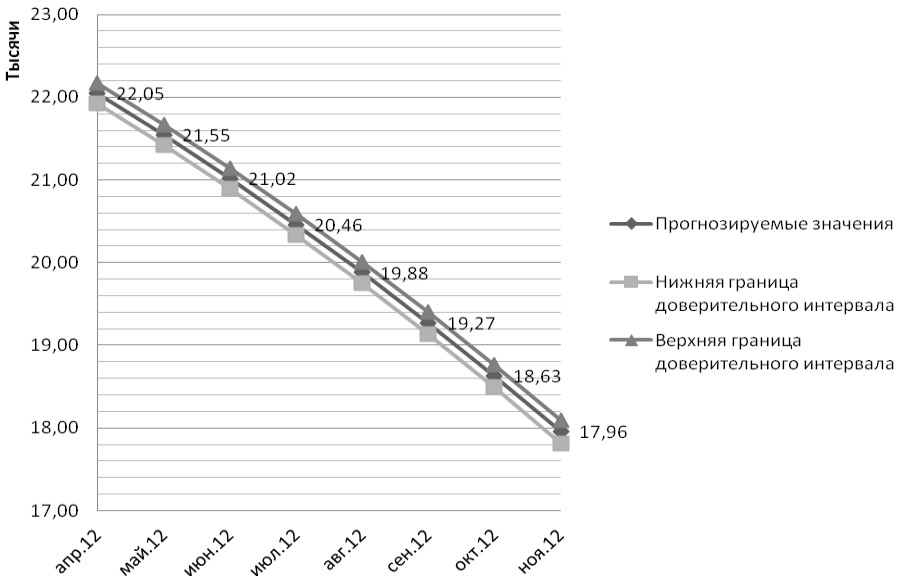

Рис. 2. Прогноз преступлений экономической направленности

Таким образом, для построения прогноза необходимо для каждого периода прогноза определить точечный прогноз y'_{n+k} и величину отклонния от точечного значения U_k.

На основе данных был построен график, изображенный на рисунке 2.

По графику можно видеть, что количество преступлений поддается цикличности. Прогнозные значения на ближайшие 8 месяцев подтверждают цикличность. Количество преступлений экономической направленности в этом периоде будет снижаться.

Данный прогноз составлен на основании общей тенденции за 9 лет. Он отражает общую тенденцию за этот период и теряет актуальность с каждым последующим прогнозным значением.

Список источников

1. Дрейпер Н., Смит Г. Прикладной регрессионный анализ. Множественная регрессия 3-е издание/ Смит, Дрейпер - М.: Диалектика, 2007.

2. Мещеряков В. В. Задачи по статистике и регрессионному анализу/ В. В. Мещеряков - М.: Диалог-МИФИ, 2009.

АНАЛИЗ ПРОБЛЕМ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ ГИБРИДНОЙ ОБЛАЧНОЙ АРХИТЕКТУРЫ

Ермошкин Григорий Николаевич
Финансовый университет при Правительстве РФ, Москва, аспирант
ermoshkin_nn@mail.ru

Аннотация. В статье будет проведен анализ гибридных систем и освещены их проблемы и достоинства, предпринята попытка разрешить часть вопросов в данной сфере.

Ключевые слова: информационная безопасность, гибридная облачная архитектура, оценка рисков.

Введение

Все больше организаций выбирают облачные системы. И беря в учет преимущества этих систем это вполне понятно. Однако любая такая система имеет ряд врожденных недостатков, способных перевесить все достоинства.

Основными рисками можно считать потерю контроля, недостаток безопасности, доступности данных, а так же вероятные финансовые потери которые это может повлечь.

Использование частного облака способно решить большинство проблем, но его развертывание и обслуживание дорого стоит. Публичное облако намного экономичней в короткой перспективе, но влечет за собой высокие риски. Гибридное облако потенциально способно разрешить данное противоречие. Но, к сожалению, здесь следует отметить недостаток изученности данных систем и отсутствие достаточной информации для построения системы способной сбалансировать преимущества и риски.

В данной статье предпринята попытка разрешить часть вопросов в данной сфере. Будет проведен анализ гибридных систем и освещены проблемы и достоинства.

Гибридная архитектура содержит две основных части: частную и публичную. Каждая из них имеет достоинства и недостатки. Достоинства и недостатки гибридных систем можно представить в двух измерениях: наследственные и уникальные. Наследственные преимущества и риски происходят напрямую из частного и публичного сегментов. Уникальные происходят из особенностей комбинации этих двух частей. Большинство наследственных преимуществ связанны с частным облаком; в то же время основные риски проистекают от публичного облака.

Основным преимуществом гибридного облака является возможность сбалансировать наследственные достоинства и риски, относительная простота и скорость развертывания.

Важнейшие риски это безопасность, разрозненный контроль и настройка, доступность и законодательные аспекты.

Правильная стратегия применения гибридной модели направлена на максимизацию преимуществ и минимизацию рисков, эффективное поддержание и улучшение баланса на протяжении жизненного цикла – в соответствии с состоянием организации.

Провайдеры публичных облачных вычислений указывают на достоинства, такие как скорость и простота развертывания. Однако забывают упомянуть риски связанные с использованием этой модели. Проблемы безопасности, потеря контроля, недостаток производительности, доступность и законодательные аспекты. Хотя, гибридная модель подразумевает баланс между рисками и преимуществами, организация должна быть осторожна в принятии этой модели, тщательно оценив свое положение.

Понимание основных особенностей модели позволяет принять правильное решение и эффективно управлять рисками.

Облачная модель предоставляет услуги информационных технологий по требованию через сеть. Частное облако представляет модель, в которой сетевая инфраструктура и услуги являются собственностью организации и распространяются внутри. Это наиболее удачный вариант, но требующий наибольших начальных вложений. Публичное облако является точной противоположностью. В данной модели услуги и поддерживающая их инфраструктура находятся во владении внешнего провайдера. Доступ к сервисам осуществляется через интернет. Но, при всех недостатках эта модель достаточно экономична – в короткой перспективе (например, как временное решение перед переходом к частному облаку).

В гибридном облаке часть сервисов находится внутри организации, в то время как другая часть располагается у внешнего провайдера. Внутренние

сервисы доступны через внутреннюю сеть организации, внешние - через внешнюю сеть, например интернет. Пользователь обычно взаимодействует с внешними сервисами через web интерфейс.

1. Преимущества использования гибридных облаков

Большинство преимуществ являются наследованными от частного облака. Однако публичные облака также имеют ряд достоинств.

Список преимуществ гибридных систем:

- Сбалансированность: данная модель имеет потенциальную возможность достигнуть баланса между риском и достоинствами. Менеджеры должны принимать положительные особенности и минимизировать недостатки.
- Подобие: Принятие облачной модели подобно аутсорсингу. Это одинаково верно и для частного, и для публичного облаков, т.о., менеджеры способны использовать существующий опыт для быстрого перехода.
- Скорость: Облачная архитектура и сервисы могут быть развернуты относительно быстро. Публичное облако специально создано для быстрого развертывания. Существует ряд готовых решений частных облаков.
- Простота: Облачные сервисы могут быть развернуты без особых затрат. Принятие нового готового к использованию облачного решения просто. Это, однако, не касается переноса сервисов.
- Снижение расходов.
- Масштабируемость: ресурсы могут, масштабированы в зависимости от потребностей.
- Оплата: пользователь платит лишь за ресурсы, которые потребляет.

2. Риски использования гибридных облаков

Следует учитывать следующие риски гибридных облачных систем:

- Неверный баланс: неправильное соотношение частей способно повлечь различные риски.
- Потеря контроля: поддержание контроля данных и сервисов крайне важно. Полный контроль возможен лишь в частном сегменте.
- Ограниченная настройка: потеря контроля означает ограниченность или невозможность настройки.
- Безопасность: Открытость публичного облака ведет к серьезным проблемам безопасности. Ценные данные могут быть скомпромитированны.

- Доступность: сетевая природа сервисов приводит к риску потери доступа, что может привести к остановке работы организации.
- Законность: т.к. публичное облако физически может находиться в любой точке мира, то данные могут оказаться в регионе без законодательной защиты.

Заключение

Результаты проведенного в работе анализа могут быть использованы при разработке модели оценки рисков распределенных систем облачной архитектуры, которую можно будет использовать в ходе аудита информационной безопасности для повышения эффективности процедур менеджмента риска облачных систем.

Список источников

1. "Risk Management in Cloud Computing" By Sri Prakash, Technology Risk Management Consultant, E-Com Canada Inc. Fri, April 15, 2011.

2. "The future of IT outsourcing and cloud computing" PwC study, November, 2011.

3. http://csrc.nist.gov/groups/SNS/cloud-computing/

4. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Joint Task Force Transformation Initiative, NIST Special Publication 800-37, Revision 1, <URL:http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-l.pdf>.

5. Steve Elky. An Introduction to Information System Risk Management -SANS Institute, 2007.

ИССЛЕДОВАНИЕ В НИЯУ МИФИ ПРИМИТИВНОСТИ НЕОТРИЦАТЕЛЬНЫХ МАТРИЦ

Когос Константин Григорьевич
НИЯУ МИФИ, Москва, аспирант
k.kogos@mail.ru

Кяжин Сергей Николаевич
НИЯУ МИФИ, Москва, студент
s.kyazhin@kaf42.ru

Фомичев Владимир Михайлович
Финансовый университет при Правительстве РФ, Москва, профессор
fomichev@nm.ru

Введение

В системах шифрования и идентификации к криптографическим функциям векторных пространств предъявляется требование совершенности, то есть зависимости каждой координатной функции от всех переменных [1]. Обобщениями свойства совершенности являются строгий лавинный критерий, критерии распространения, свойство «бент». Изучение совершенности криптографических функций — актуальная задача, так как в криптосистемах функции выбираются не случайно, а из отображений с рядом заданных свойств.

Из соображений простоты реализации совершенная функция строится в виде композиции нескольких функций с относительно слабыми перемешивающими свойствами, при этом важно, чтобы совершенная композиции содержала небольшое число перемножаемых функций. Например, так строятся подстановки итеративных блочных шифров, где важной характеристикой простоты реализации является число раундов шифрования.

1. Примитивность графов и неотрицательных матриц

Для оценки свойства совершенности используется математический аппарат матриц и графов.

Матрицу M над полем действительных чисел называют положительной (неотрицательной), если положительны (неотрицательны) все её элементы, обозначают: $M>0$ ($M\geq 0$). Квадратную 0,1-матрицу M называют примитивной, если $M^t>0$ при некотором натуральном t. Наименьшее натуральное γ, при котором $M^\gamma>0$, называется экспонентом (показателем примитивности) матрицы M, обозначается exp$M$.

Равносильным образом рассматривают n-вершинный орграф Г, матрица смежности вершин которого равна M. Орграф Г и матрица M одновременно примитивны или не примитивны, в случае примитивности их экспоненты равны. Связь между графами и неотрицательными матрицами основана на теореме [2]: пусть $M^t=(m_{ij}^{(t)})$, тогда число путей длины t из i в j в графе Г равно $m_{ij}^{(t)}$, $i,j\in\{1,\ldots,n\}$.

Известен универсальный критерий примитивности орграфа Г [3, с.226]. Если $C_1,\ldots,C_k$ есть все простые контуры орграфа Г длин $l_1,\ldots,l_k$ соответственно, то сильно связный орграф Г примитивен $\Leftrightarrow \gcd(l_1,\ldots,l_k)=1$. При использовании критерия могут быть полезны таблицы примитивных наборов натуральных чисел, свойства которых описаны в [4].

Абсолютная оценка экспонента примитивной матрицы M порядка n (орграфа Г) дана Виландтом [5]: $\exp M\leq n^2-2n+2$.

При $n>2$ описаны примитивные орграфы [6], на которых (и только на них) достигается абсолютная оценка Виландта. Они представляют собойгамильтонов контур, к которому добавлена дуга (i,j), где вершины i,j расположены на контуре на расстоянии 2, $i,j\in\{1,\ldots,n\}$. Множество этих изоморфных орграфов, названных графами Виландта, состоит из $n!$ изоморфных графов. Для орграфов Г, отличных от графов Виландта, при нечетном $n>3$ верна достижимая оценка: $\exp\Gamma\leq n^2-3n+4$.

Оценки экспонентов для других классов матриц и графов даны в обзорной статье [7].

2. Исследования в НИЯУ МИФИ

Исследования примитивности графов и неотрицательных матриц активно проводятся, в основном начиная с 2011 года, под руководством профессора Фомичева В.М. студентами 4-го и 5-го курсов (Когос К.Г., Коренева А.М., Кяжин С.Н.). Результаты исследований докладывались на конференциях, в том числе, на международных (научная сессия в НИЯУ МИФИ, EUROCRYPT'12, SIBECRYPT в 2011-12 гг.), составили основу нескольких УИРов, 3 дипломных проектов и

более 10 публикаций в материалах конференций и в ведущих математических журналах России.

Исследования проводятся по следующим направлениям:

- систематизация результатов, подготовка обобщающих обзоров [7];
- уточнение диаметров и экспонентов частных классов графов [6,9];
- исследование алгебраических и теоретико-числовых свойств множеств, связанных со свойством примитивности графов и матриц, построение алгоритмов распознавания указанных свойств, оценка вычислительной сложности алгоритмов [4,8];
- разработка приложений к решению криптографических задач [9].

Развиваются некоторые перспективные направления исследований:

- примитивность в частичной полугруппе разноразмерных матриц;
- локальная примитивность графов и матриц.

3. О приложениях теории примитивности графов и матриц

Приложения возможны к широкому классу коммуникаций, построенных с помощью бинарного отношения на множестве объектов.

Пример 1. Транспортная система коммуникаций. Вершинами орграфа являются n городов, ребра графа соответствуют непосредственным путям между городами. Пусть из i-го города стартует автоколонна машин i-го цвета, $i=1,\ldots,n$, (в колонне достаточно много машин), разделяясь на части по путям, выходящим из каждого города, и путь по любому одному ребру машины преодолевают за 1 день. С помощью свойств примитивности можно оценить количество дней, после которых во всех городах одновременно окажутся машины всех цветов.

Пример 2. Коммуникации преступного мира. Расследуется дело группы n преступников, в целом разобщенной, но между некоторыми членами группы (соседями) имеются связи (дуги графа). В начале i-й преступник располагает i-м аргументом для создания ложного, но правдоподобного алиби, $i=1,\ldots,n$. В первый час он передает всем соседям этот аргумент и ежечасно каждый преступник передает соседям весь набор аргументов, который он получил в предыдущий час. Набор менее чем из n аргументов считается ненадежным и преступником не запоминается. Считается, что дело станет нераскрываемым, когда одновременно все преступники получат все n аргументов. Оценив экспонент графа, можно оценить время, которое имеется у правоохранительных органов на раскрытие преступления.

Список источников

1. Фомичев В.М. Методы дискретной математики в криптологии. // В. М. Фомичев. — М.: Диалог-МИФИ, 2010 — 424 с.

2. Берж К. Теория графов и её применение. М.: ИЛ, 1962г. — 320с.

3. Сачков В.Н., Тараканов В.Е. Комбинаторика неотрицательных матриц. — М.: ТВП, 2000. — 448 с.

4. Кяжин С.Н., Фомичев В.М. О примитивных наборах натуральных чисел // Прикладная дискретная математика, №2(16), 2012.

5. Wielandt H. Unzerlegbare nicht negative Matrizen // Math. Zeitschr. 1950. No. 52. P. 642-648.

6. Фомичев В.М. Оценки экспонентов примитивных графов // Прикладная дискретная математика, №2(12), 2011.

7. Когос К.Г., Фомичев В.М. Положительные свойства неотрицательных матриц // Прикладная дискретная математика, №4(18), 2012.

8. Кяжин С.Н., Фомичев В.М. Алгоритмы анализа примитивности ориентированных графов // Безопасность информационных технологий, №1, 2012.

9. Коренева А.М., Фомичев В.М. Об одном обобщении блочных шифров Фейстеля // Прикладная дискретная математика, №3(17), 2012.

ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ В СФЕРЕ ЭЛЕКТРОННОЙ КОММЕРЦИИ (НА ПРИМЕРЕ ИНТЕРНЕТ-АУКЦИОНА)

Солодков Денис Сергеевич
Тимохов Сергей Дмитриевич
Российский университет дружбы народов, Москва, студенты

Кравченко Николай Юрьевич
Финансовый университет при Правительстве РФ, Москва,
ст. преподаватель
d.solodkov@yandex.ru, greytim95@rambler.ru

Введение

Темп роста аудитории пользователей Интернета во всем мире, стимулирует развитие экономической деятельности, активные участники которой стремятся увеличить свой доход, используя всемирную глобальную сеть как торговую площадку. Такая экономическая активность, получившая название «электронная коммерция», призвана упростить процедуру купли-продажи товаров и услуг, как для продавцов, так и для покупателей. Примерами «электронной коммерции» можно назвать продажу рекламного места на популярных веб-ресурсах, создание интернет-магазинов, интернет-аукционов и других информационных систем.

В настоящее время интернет-аукционы (далее ИА) – это динамично развивающаяся область электронной коммерции, в которой теоретическая база и сама технология разработки таких информационных систем слабо систематизированы и формализованы.

1. Основные положения проектирования информационной системы интернет-аукциона

Целью данной статьи является изложение основных принципов построения информационных систем ИА и выработка практических советов.

ИА – это сфера электронной коммерции, в основе которой лежат принципы традиционных аукционных торгов.

Самым известным и посещаемым (свыше 88 миллионов активных пользователей) ИА в мире является eBay (www.ebay.com), позиционирующий себя как интернет-аукцион общего профиля, построенный по принципу C2C (consumer to consumer), что означает, что в роли продавцов и покупателей выступают частные лица.

2. Обеспечение безопасности информационной системы интернет-аукционов и ее участников

При разработке любого веб-приложения в сфере электронной коммерции, в том числе интернет-аукциона, необходимо предусмотреть механизмы защиты как самого веб-приложения, так и его участников. Статистика уязвимостей по типу приложений показывает, что наиболее проблемными в этом плане являются web-приложения, доля обнаруженных уязвимостей в которых превышает 40% от общего числа.

Межсайтовое выполнение сценариев (Cross-site Scripting, XSS) - наличие уязвимости Cross-site Scripting позволяет атакующему передать серверу исполняемый код, который будет перенаправлен браузеру пользователя.

Утечка информации (Information Leakage) – эти уязвимости возникают в ситуациях, когда сервер публикует важную информацию, например, комментарии разработчиков или сообщения об ошибках.

Внедрение операторов SQL (SQL Injection) - эти атаки направлены на Web-серверы, создающие SQL запросы на основе данных, вводимых пользователем.

Недостаточная защита данных при их передаче на транспортном уровне (Insufficient Transport Layer Protection) – эта уязвимость позволяет перехватывать данные, передаваемые, например, по HTTP вместо HTTPS.

Идентификация приложений (Web Server/Application Fingerprinting) – определение версий приложений, которое используется злоумышленниками для получения информации об используемых сервером и клиентом операционных системах, Web-северах и браузерах.

Расщепление HTTP-запроса (HTTP Response Splitting) – данная уязвимость позволяет злоумышленнику посылать серверу специальным образом сформированный запрос, ответ на который интерпретируется целью атаки как два разных ответа.

Необходимо оснастить веб-приложение продуманной и эффективной системой защиты от взлома, которая поддерживалась бы в актуальном состоянии. Тем самым обеспечивается безопасность не только самой системы от возможности ее копирования, изменения и уничтожения, но и личных данных ее участников и финансовых операций между ними.

Также информационная система должна иметь свои собственные механизмы по защите участников системы от мошенников. Эти механизмы должны проверять надежность другой стороны и тем самым снижать риски, основанные на недобросовестности участников системы.

Возможными механизмами могут быть:

- система рейтинговой оценки, суть которой сводится к выставлению участниками системы друг другу оценок после совершения сделки купли-продажи;
- проверка продавцов и покупателей на реальность телефонных номеров, почтовых адресов, и т.д. вплоть до проверки паспортных данных;
- проверка участников системы на наличие средств на банковском счете при регистрации и/или вводе ставки для обеспечения финансовых гарантий;
- система штрафов (может быть привязана к системе рейтинговой оценки), которая позволит наказывать участников, которые не выполнили свои обязательства по продаже или покупке;
- система возмещения убытков, которая будет предусматривать выплату оговоренной суммы пострадавшей стороне.

Для обеспечения гарантий оплаты товара\услуги покупателем владелец интернет-аукциона может взять на себя обязательство посредничества при проведении операции с денежными средствами через банковский счет или кошелек электронных денег интернет-аукциона.

Заключение

Обеспечение безопасности своего веб-ресурса – необходимое условие разработки информационной системы ИА. Кроме того, защищенность системы повышает доверие со стороны целевой аудитории, следовательно, способствует получению дополнительных конкурентных преимуществ.

Список источников

1. Данные официального сайта eBay (www.ebayinc.com).

2. Данные сайта www.alexa.com, занимающимся составлением рейтингов веб-ресурсов.

3. Источник описаний уязвимостей - проект по защите информации www.protectme.ru.

СИСТЕМНЫЙ АНАЛИЗ И ПРОГНОЗИРОВАНИЕ КРЕДИТНЫХ РЕЙТИНГОВ КОММЕРЧЕСКИХ ОРГАНИЗАЦИЙ НА ОСНОВЕ ИНТЕГРАЛЬНЫХ ОЦЕНОК В ИНТЕРЕСАХ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ФИНАНСОВОМУ МОНИТОРИНГУ

Шарапов Алексей Викторович
ООО «Эйс-трейд», Москва, зам. ген. директора
a.sharapov@me.com

Оценка качества и степени надежности компании нужны во многих отраслях человеческой деятельности. Чаще всего такие оценки нужны инвестиционным и банковским организациям, например, для расчета ставки займа или стоимости облигаций. Оценкой обычно занимаются рейтинговые агентства, определяющие экспертным путем значение от 0 до 22, где 0 – это компании в состоянии дефолта, а 22 – это сверхнадежные эмитенты. Исторически вместо чисел используются буквенные значения (D, C, CC- … AAA).

При расчете такого рейтинга берутся во внимание динамика финансовых показателей компании и рейтинг государства, оцениваются политические, рыночные и другие риски, потенциально влияющие на будущее финансовое состояние компании.

При всех несомненных положительных качествах таких оценок, у них есть и недостатки. В первую очередь это стоимость и время исследования. Кроме того, несмотря на высокую репутацию и профессионализм крупнейших рейтинговых агентств, у экспертной оценки есть недостаток – человеческий фактор.

При создании исходной матрицы данных анализировалось множество финансовых показателей – кредитный рейтинг у S&P, дивидендная доходность (Trailing Annual Dividend Yield), отношение долга к собственному капиталу (debt to equity), прибыльность (profit margin (%) ttm), Return on equity, Return on Assets, Operating Margin % ttm, debt to GDP, jobless rate, Total Cash per share, Revenue per share.

Однако наиболее эффективным оказался следующий набор характеристик. В нем присутствуют основные финансовые показатели организаций, опи-

сывающие уровень долговой нагрузки, прибыльности и эффективности работы менеджмента.

Таблица 1

Название компании	Страна	Рейтинг	Trailing A	debt to equ	profit marg	Return on (	Return on A
Chevron	США	15	3,1	7,79	11,55	21,59	11,27
ExxonMobil Corp.	США	22	2,3	9,2800	9,4712	29,0200	9,4800
OAO Gazprom	Россия	14	5,92	17,4100	26,3300	16,3500	8,9300
Shell Oil Co.	Нидерланд	20	5	18,5200	5,5200	15,2900	7,1100
Occidental Petroleum	США	14	2,5	19,2700	26,1300	16,8900	10,41
JSC Gazprom Neft	Россия	13	4,1	27,8900	12,1400	26,5	12,95
EOG Resources, Inc.	США	16	0,6	37,5600	13,6600	10,8600	5,17
BP PLC	Великобри	17	4,5	42,0600	4,5800	15,9000	4,9700
Total	Франция	20	4,5	46,2100	6,1700	16,2400	8,8200
Devon Energy Corpora	США	15	1,3	47,71	24,9	11,23	6,19
Noble Energy	США	13	0,1	57,0700	17,5000	9,9200	4,04
ConocoPhillips	США	17	4,69	58,0500	3,2700	20,3100	9,9400
China Petroleum & Che	Китай	18	3	58,7800	2,1600	11,9700	4,8000
Anadarko Petroleum Corp	США	13	0,5	69,7100	-9,9100	-5,75	1,75
Chesapeake Energy Cor	США	10	1,3	73,6300	18,6900	13,8500	4,1700
Helix Energy Solutions Gr	США	11	0	74,3100	9,5500	9,5700	4,44
Questar Corporation	США	15	3,1	125,8700	19,0100	19,7300	6,91
Forest Oil Corporation	США	9	0	278,5300	-68,4400	-40,8400	4,97
Cheniere Energy	США	12	0	471,19	-88,9400	-634,3700	0,2800

В анализе принимали участие компании только из одной нефтяной отрасли для исключения ошибок, связанных с различием отраслей.

Как мы видим, основной вклад дают первая, вторая и отчасти третья компонента.

Таблица 2

	ГК1	ГК2	ГК3
Дивидентная доходность	0,435278839	0,499845248	-0,107317061
долг к собственному капиталу	-0,39228603	0,559901288	-0,395243411
Доля прибыли (%) ttm	0,524588486	-0,026167844	0,505124136
Рентабельность собственного капитала	0,427133193	-0,458878025	-0,750406251
Рентабельность активов	0,446103305	0,474775187	-0,11834593

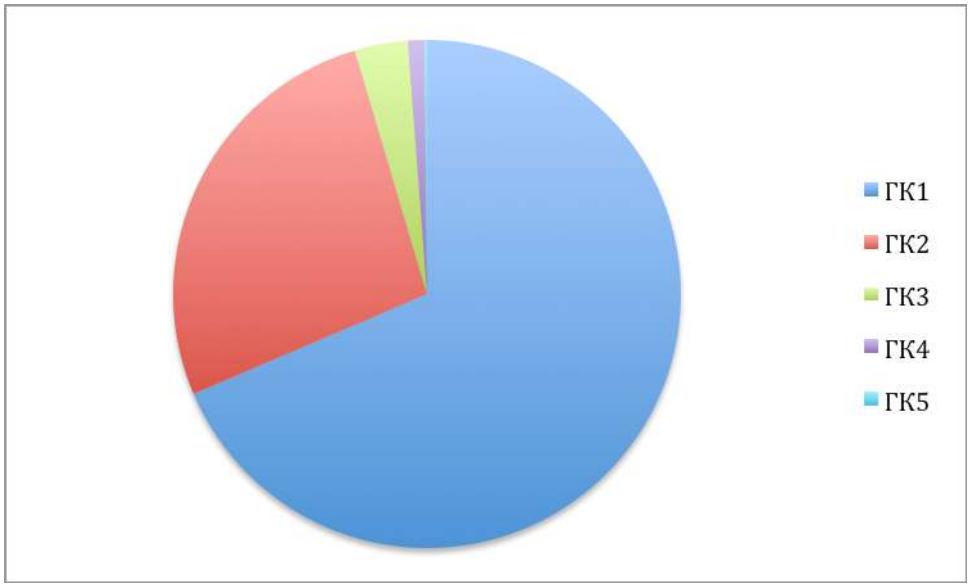

Рис. 1. Вклад главных компонент в общую дисперсию

Первая главная компонента характеризует общий интегральный показатель успешности компании.

Вторая главная компонента характеризует ???

В качестве меры эффективности интегральной оценки компаний брались кредитные рейтинги агентства Standart&Poors. Буквенные рейтинги представлялись в численном виде (числа от 1 до 22, где 1 – это дефолтный рейтинг D, а 22 – рейтинг максимальной надежности AAA).

Таблица 3

	PC2	Рейтинг S&P
Chevron	-1,121931	-15
ExxonMobil Corp.	-1,192716	-22
OAO Gazprom	-1,042932	-14
Shell Oil Co.	-1,0721	-20
Occidental Petroleum	-1,070968	-14
JSC Gazprom Neft	-0,95607	-13
EOG Resources, Inc.	-1,06751	-16
BP PLC	-0,976229	-17
Total	-0,871633	-20
Devon Energy Corporation	-0,976602	-15
Noble Energy	-0,974375	-13
ConocoPhillips	-0,781277	-17
China Petroleum & Chemical Corp	-0,884955	-18
Anadarko Petroleum Corporation	-0,850906	-13
Chesapeake Energy Corp.	-0,856395	-10
Helix Energy Solutions Group Inc.	-0,849078	-11
Questar Corporation	-0,447983	-15
Forest Oil Corporation	0,736544	-9
Cheniere Energy	4,181139	-12

Как мы видим, лучшей компанией считается ExxonMobil, как по интегральной оценке методом главных компонент, так и согласно рейтингу Standart&Poors.

Худшие результаты получили фактически преддефолтные компании Forest Oil и Cheniere Energy с рейтингами B+ и BB+ соответственно.

Совпадая по ряду позиций, вместе с тем, анализируя весь список компаний, можно увидеть различия между интегральный подходом к оценке и экспертными оценками Standart&Poors.

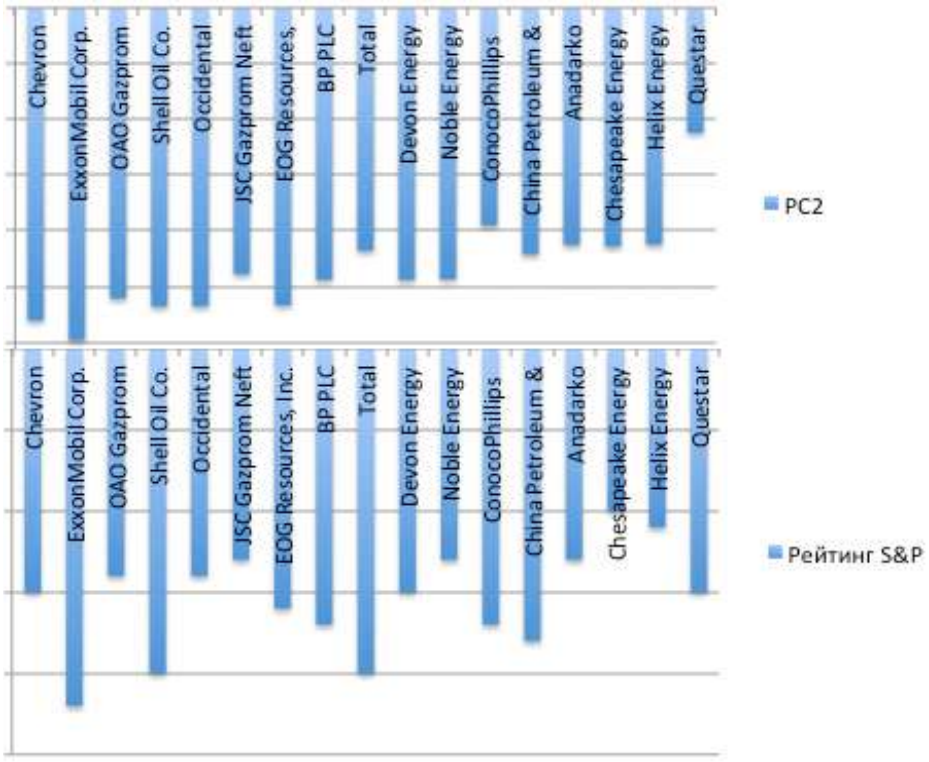

Рис. 2

Различия объясняются несколькими факторами:

- Рейтинг S&P обычно не может быть выше рейтинга страны, поэтому кредитный рейтинг Газпрома, например, не может быть выше BBB (рейтинга России).
- Существуют факторы, прямо не касающиеся финансовых показателей компании – так, например, Chesapeake Energy имеет относительно низкий рейтинг S&P из-за скандалов в руководстве компании.
- Ряд компаний может иметь преимущество, если высока вероятность того, что в случае неприятностей они получат помощь со стороны государства (например, Газпром или China Petrolium).

СОВРЕМЕННАЯ КРИПТОЛОГИЯ: EUROCRYPT 2012 И SIBECRYPT 2012. НАУЧНАЯ ПРОБЛЕМАТИКА И ЛИЧНЫЕ ВПЕЧАТЛЕНИЯ

Коренева Алиса Михайловна
Компания Pointlane, Москва, ведущий специалист отдела ИБ
alisa.koreneva@gmail.com

Криптология – наука, которая еще совсем недавно была открыта только спецслужбам, в наши дни доступна для изучения каждому человеку, имеющему к ней интерес. Возможности криптологии широко используются во многих современных приложениях – шифрование личных данных на носителях и при передаче информации по каналам связи, криптовалюта, системы аутентификации, сертификаты для организации доверенной переписки по электронной почте. Не удивительно, что интерес молодых специалистов к данной науке растет. В настоящее время конференции по криптологии ежегодно проходят в Европе, Америке, Азии и России. В 2012 году мне довелось выступить с докладами на международной конференции Eurocrypt (Англия, Кембридж) и на российской конференции Sibecrypt (Иркутск) в рамках темы научной работы «Криптографические свойства блочных шифров регистрового типа, построенных на основе обобщения раундовой функции Фейстеля» [1,2].

Цель научного исследования – развить математический аппарат анализа блочных шифров на основе регистров сдвига произвольной длины, обобщающих шифры Фейстеля. Шифры Фейстеля позволяют обеспечить ряд хороших криптографических свойств, в том числе, инволютивность алгоритма шифрования – полезное технологическое свойство шифрующих подстановок, при котором зашифрование и расшифрование реализуются одним и тем же алгоритмом [3]. Увеличение длины базового регистра позволяет рассчитывать на улучшение некоторых характеристик шифра. Например, использование регистра сдвига большей длины дает возможность увеличить размер входного блока данных без существенного усложнения реализации алгоритма, что актуально для шифрования больших объемов информации, а также предоставляет разработчику богатое множество вариантов при построении раундовой функции и ключевого расписания.

В ходе исследований блочных шифров регистрового типа доказан критерий инволютивности и оценены перемешивающие свойства. В математическом плане исследования относятся в основном к теории графов: получены новые результаты в виде оценок экспонентов и диаметров определенного класса ориентированных графов, моделирующих перемешивание данных регистровыми блочными шифрами [2,4,5].

Результаты исследований были представлены в рамках конференций – европейской и российской. Несмотря на различие в масштабах интересно сравнение этих научных форумов: обе конференции похожи по своей структуре и атмосфере. Но есть и существенные различия, особенно в научных направлениях: работы на Eurocrypt 2012 посвящены математическому аппарату эллиптических кривых, разработке протоколов, анализу асимметричных криптоалгоритмов. Выступление с докладом про симметричные блочные шифры выглядело там довольно необычно, но, тем не менее, было одобрено со стороны председателей и участников конференции.

Участников на Eurocrypt было в десятки раз больше, чем на Sibecrypt. Это во многом связано с тем, что западные ВУЗы широко финансируют участие студентов и аспирантов в подобных мероприятиях, чем мотивируют молодых людей к научной деятельности. Также в рамках Eurocrypt состоялись интересные личные знакомства с видными учеными: У. Диффи, Б. Пренелем, А. Шамиром и др.

На Sibecrypt 2012 доклад также был одобрен председателем Оргкомитета. Научная проблематика докладов, представленных на Sibecrypt, была в меньшей степени связана с развитием асимметричной криптографии или ее математического аппарата. Однако на конференции выступил молодой ученый из Канады (российского происхождения), что можно расценить как наличие интереса к российской криптографической конференции. Благодаря прекрасным способностям организаторов и крайне дружественной обстановке пребывание на Sibecrypt было очень приятным. Российскую конференцию во многом отличает по-домашнему теплая атмосфера, а сибирская природа просто несравненна по своей красоте.

Обобщая бесценный личный опыт участия в Eurocrypt и Sibecrypt, стоит отметить, что результатом можно считать совершенствование собственных знаний, знакомство и общение с уникальными людьми, выступление перед крупной аудиторией.

Такого рода опыт доступен каждому из нас – молодых ученых, студентов и аспирантов российских ВУЗов, которые, занимаясь различными исследованиями, успешно развиваются в современных научных направлениях. К сожа-

лению, часто случается, что молодому человеку не хватает времени, терпения или определенных условий, и он перестает заниматься своей научной работой, теряет к ней интерес, расставляет другие приоритеты в жизни. Чтобы избежать больших потерь в научных кадрах, необходимо продумать меры морального и материального стимулирования перспективных молодых ученых со стороны заинтересованных организаций. Сделать это надо пока еще не поздно, пока нашей стране есть чем гордиться.

Студентам и молодым ученым не стоит упускать свой шанс или просто ждать, как проходит время. Все-таки есть возможность проявить себя и продемонстрировать свои личные достижения. Помните, что в научном обществе Вас окружают единомышленники, люди с которыми не трудно завести знакомство и с которыми есть большое количество тем для общения.

Хотелось бы пожелать успехов каждому, кто работает или начинает работать в области научных исследований. Безусловно, это большой человеческий труд, но ведь нет ничего сильнее, чем желание целеустремленного человека. Каждый из нас заслуживает своей личной победы.

Список источников

1. Alisa Koreneva and Vladimir Fomichev One Little Cipher Story [Электронный ресурс]: Rump Session EuroCrypt 2012. – Режим доступа к статье: http://www.cs.bris.ac.uk/eurocrypt2012/Rump/koreneva.pdf

2. А.М. Коренева, В.М. Фомичев. Об одном обобщении блочных шифров Фейстеля // Томский государств. университет. Прикладная дискретная математика, №3 (17), 2012. – С. 34-40.

3. Фомичев В.М. Методы дискретной математики в криптологии. - М.: Диалог-МИФИ, 2010. – 424 с.

4. Коренева А.М. Систематизация теоретико-графовых моделей в криптологии // М.: НИЯУ МИФИ. Безопасность информационных технологий. – 2011. – №3. – С. 47-49.

5. Коренева А.М. Применение теоретико-графового подхода для определения значения экспонента матрицы существенной зависимости // М.: НИЯУ МИФИ. Безопасность информационных технологий. – 2011. –№4. – С. 126-129.

АНАЛИЗ ИНФОРМАЦИОННОЙ И ФИНАНСОВОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ ДЕНЕГ И ПРОБЛЕМА ПРОТИВОДЕЙСТВИЯ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ПРЕСТУПНЫХ ДОХОДОВ И ФИНАНСИРОВАНИЯ ТЕРРОРИЗМА

Корнев Иван Александрович
Федеральная служба по финансовому мониторингу, Москва
ведущий специалист-эксперт
kornev.ivan@gmail.com

С развитием информационных технологий и сети Интернет наличие интернет-магазинов и услуг становятся обыденностью. Вместе с тем с привычными способами оплаты с помощью наличных денежных средств, банковских счетов и карт появились электронные деньги. Электронные кошельки набирают всё большую популярность с увеличением товаров и услуг, которые можно оплатить с помощью них.

Какими же преимуществами обладают электронные деньги? Основным является низкая стоимость транзакций, особенно внутренних (в рамках одной системы с кошелька на кошелек), что делает возможным применение электронных денег для осуществления микроплатежей, для чего обычные безналичные средства малоприменимы.

Кроме того электронные деньги обеспечивают анонимность их использования, сравнимую с наличными денежными средствами, а также очень простое вхождение в систему. Вам не нужно идти в банк, заключать какие либо договора, предоставлять документы, и т. д. Обзавестись собственным кошельком и получать или отправлять платежи можно практически мгновенно, не вставая из-за компьютера.

Еще одно преимущество электронных денег в том, что почти все операции с ними происходят в режиме он-лайн, и занимают очень мало времени. Переводы средств с одного кошелька на другой происходят практически мгновенно, время совершения внешних платежей определяется только скоростью работы платежной системы.

Но наряду с преимуществами электронных денег существуют и недостатки, такие как незащищенность их государством, то есть государство не дает

никаких гарантий сохранения их платежеспособности. Поэтому электронные деньги в первую очередь платежное, а не накопительное средство.

Кроме того электронные деньги существуют только в рамках той системы, в которой они эмитированы, и они не являются общепринятым платежным средством, обязательным к приему. Из-за этого все платежи, которые вы можете совершить при помощи ваших электронных денег, сводятся к тому набору, который предоставляет вам оператор системы, произвольные платежи в рамках системы невозможны.

Также перевод средств из одной системы электронных денег в другую может быть достаточно неудобной и дорогостоящей операцией, подобный перевод обходится существенно дороже, чем перевод внутри системы. [1]

Кроме того электронные деньги можно использовать и для незаконной деятельности, поскольку имеется возможность создавать неидентифицированные электронные кошельки, что позволяет анонимно перечислять и получать денежные средства, которые, например, в последствии можно использовать для подготовки террористических актов.

Хоть и возможности неидентифицированных кошельков и ограничены, их достаточно для финансирования отдельных мероприятий, для которых не нужно больших расходов. А зачислить на кошелек можно практически с любого терминала до 15 тысяч рублей, и при наличии достаточного количества кошельков собрать требуемую сумму на теракт не составляет труда.

Также существует вероятность, что системы электронных денег могут быть внедрены в сферу розничных платежей лишь с преступной целью: отмывания «грязных денег», уклонения от уплаты налогов или незаконной организации азартных игр (электронная лотерея, тотализатор и т. д.).

Да и так ли безопасны электронные деньги? От мошенничества в сфере электронных платежей нужны не менее серьезные меры безопасности, чем при защите банковских.

Существует разные методы защиты, начиная с ввода паролей и файлов ключей, заканчивая сертификатами и электронно-цифровой подписью. Чем сложнее методы и надежнее системы, тем они дороже и сложнее в использовании. Поэтому различные платежные системы используют свой набор методов для обеспечения безопасности проводимых операций.

Кроме технических и физических методов защиты существуют необходимые правила, при соблюдении которых риск обмана уменьшается. Обычно у каждой системы есть свои типовые правила, с которыми клиент знакомится при регистрации в ней.

Но также не нужно забывать и про безопасность персонального компьютера, с которого происходит вход и управление электронным кошельком. Если компьютер «заражен», то мер безопасности, предусмотренных платежной системой, может не хватить для сохранности ваших электронных денег.

До недавнего времени в России не были закреплены нормативно ни определение электронных денег, ни порядок их регулирования и контроля. Осенью этого года вступил в силу Федеральный закон Российской Федерации от 27 июня 2011 г. N 161-ФЗ «О национальной платежной системе», в котором были даны определение электронных денежных средств, а также порядок регулирования этого сегмента.

В связи с принятием данного закона в целый ряд нормативно-правовых актов были внесены изменения, которые накладывают некоторые обязательства на платежные системы по изменению организационно-правовой формы, получению лицензий, ограничению остатка электронных денежных средств и другие.

Но достаточно ли этих изменений для увеличения безопасности электронных денег, возможности мониторинга и контроля движения электронных денежных средств? Это ещё предстоит узнать, поскольку после вступления закона в силу организациям предоставлено время на преобразование и изменение, с целью соответствия нормам законодательства.

Список источников

1. Электронные деньги, URL: http://www.support.it-oskol.ru/e-money.htm

УПРАВЛЕНИЕ ДОСТУПОМ В ИНФОРМАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Царегородцев Анатолий Валерьевич
д.т.н., профессор,
Финансовый университет при Правительстве РФ

Коростелев Антон Андреевич
аспирант,
Московский государственный институт электроники и математики
Национальный исследовательский университет
«Высшая школа экономики»

Введение

Управление доступом – обширная функция, которая включает в себя доступ требований для пользователей или системных администраторов (привилегированных пользователей), которые работают с сетью, системой или приложениями. Управление доступом в организации следует рассматривать согласно ее политики доступа и стандартов, принятых фирмой.

В модели облачных вычислений, где пользователи имеют доступ к облачным услугам с любого конечного устройства, имеющего доступ в Internet, роль сетевого контроля доступа значительно уменьшается. Причина в том, что стандартный контроль доступа сети фокусируется на защите ресурсов от несанкционированного доступа, основанного на атрибутах конечных устройств, которые в большинстве случаев неполноценны, не уникальны для различных пользователей и могут привести к неточной оценке. В облачных вычислениях сетевой контроль доступа проявляется в виде политики облачных брандмауэров.

В отличие от сетевого управления доступом, пользовательскому контролю доступа должно уделяться большее внимание в облачных вычислениях, так как это связано с идентификацией пользователя для доступа к ресурсам в облаках. Пользовательское управление доступом включает в себя строгую авторизацию, технологию единого входа (SSO), управление привилегиями, запись и мониторинг ресурсов облачных вычислений, играющих значительную роль в защите конфиденциальности и целостности информации в облачных вычислениях.

1. Контроль доступа SaaS

В модели поставки SaaS, CSP (криптопровайдер) отвечает за управление всеми аспектами инфраструктуры сети, сервера и приложений. В такой модели, где приложение поставляется как услуга для конечных пользователей, обычно через web-браузер сетеориентированные системы контроля становятся менее уместны и заменяются контролем доступа пользователя, например, при авторизации используются одноразовые пароли. Таким образом, следует обратить внимание на контроль доступа пользователей (авторизация, объединение, управление привилегиями, деинициализация и т.д.) для защиты информации, хранящейся в SaaS. Например, управление доступом в Salesforce.com организовано с помощью набора фильтров, которые поначалу кажутся простыми, однако это впечатление обманчиво. Каждый из фильтров применим к группам или классам пользовательских учетных записей.

1. Права класса пользователей на просмотр таблицы, объекта или функциональной области определяются профилями.

2. Права класса пользователей на просмотр столбца таблицы (атрибута объекта) определяются профилями.

3. Права класса пользователей на просмотр записи (строки или экземпляра) определяются ролями.

4. Типы записей определяют, каким профилям разрешено просматривать отдельные ячейки внутри записи, и могут использоваться для ограничения доступа практически к любой функции или классу объекта.

Эти фильтры имеют модификаторы, позволяющие делегировать права и расширять зону доступа для привилегированных пользователей. Впрочем, для большинства пользователей возможностей, предоставляемых механизмами фильтрации, оказывается вполне достаточно. Иногда это даже вызывает у них недовольство. Блокировки и фильтрации можно осуществлять в контексте текущего состояния и в зависимости от конкретных потребностей бизнеса. Таким образом, система позволяет задавать исключения при определении схемы совместного использования данных как на индивидуальном, так и на групповом уровне.

2. Контроль доступа PaaS

В модели PaaS, CSP отвечает за управление контролем доступа к инфраструктуре сети, серверов и платформенных приложений. Однако, клиенты отвечает за контроль доступа приложений, развернутых на PaaS платформе. Контроль доступа приложений проявляется как управление доступом конечного пользователя, что включает резервирование и аутентификацию пользователя.

3. Контроль доступа IaaS

В модели поставки IsaS, клиенты полностью несут ответственность в области управления всеми аспектами контроля доступа к их ресурсам на облаке. Доступ к виртуальным серверам, виртуальной сети, виртуальному хранилищу и приложениям, размещенным на IsaS платформе, должен быть разработан и организован клиентами.

В поставочной модели IsaS управление контролем доступа подразделяется на 2 вида:

- Контроль доступа на уровне инфраструктуры CSP (Управление контролем доступа к сети, размещению и управление приложениями, которые принадлежат и контролируются CSP);
- Контроль доступа на уровне виртуального клиента (Управление контролем доступа к вашему виртуальному серверу (виртуальной машине или VM), виртуальному хранилищу, виртуальным сетям и приложениям, размещенным на виртуальных серверах).

Принимая во внимание следующие аспекты в управлении контролем доступа инфраструктуры в облаке, как правило, рассматривается: сетевой контроль доступа, виртуальный контроль доступа к серверу, станцию управления облаком, web-консоль.

Заключение

Контроль доступа это важнейшая функция управления безопасностью в облачных моделях SPI (SaaS, PaaS, IaaS) и стандартной модели развертывания облака (публичная, частная и гибридная). Управление доступом является важным аспектом для защиты информации в информационных системах, построенных на основе облачных вычислений и может выступать основным средс-

твом управления безопасностью при отсутствии шифрования и других средств управления данными.

На данный момент возможности управления доступом, предлагаемые CPS, не являются достаточными для корпоративных клиентов по ряду причин:

- механизмы контроля доступа, нормы и процессы не стандартизированы посредством CSP. Для эффективного управления доступом к виртуальной облачной инфраструктуре клиентам необходимо предпринимать дополнительные усилия для понимания CSP параметров контроля доступа и их настройки;
- отсутствие единой стандартизации делает очень сложным управление доступом для нескольких облаков. Например, поддержка SAML не осуществляется с любого из главных CSP;
- контроль за доступом пользователя к ресурсам облака осуществляется на низком уровне. Контроль доступа с CSP обычно поддерживает управление на сетевом уровне, кроме управления доступом пользователей. Доступ пользователей относится к вопросам аутентификации. На мой взгляд, следует предложить гибкий контроль доступа, основанный на принципах наименьших привилегий и разделения обязанностей (например, консоль-менеджер, менеджер сетевого доступа, хост-менеджер).

С точки зрения корпоративных клиентов управление доступом это основной процесс обеспечения безопасности для защиты конфиденциальности, целостности и доступности информации, расположенной в облаке. Надежная программа управления доступом должна включать в себя резервное копирование, время деинициализации, гибкую аутентификацию, управление привилегиями, учет использования ресурсов, аудит и поддержка соответствующего управления. Клиенты облака должны понимать CSP-специфичные особенности контроля доступа для сетей, систем и приложений.

Список источников

1. Tim Mather, Subra Kumaraswamy, Shahed Latif. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance // O'Reilly Media, Incorporated, 2009.

УЯЗВИМОСТИ СИСТЕМ МОБИЛЬНЫХ ПЛАТЕЖЕЙ

Лагутина Евгения Алексеевна
НИЯУ МИФИ, студент
la.evgeniya@gmail.com

В настоящее время существенно возрастает роль и интенсивность использования мобильных платежей, что обусловлено рядом объективных причин.

Электронные платежи являются выгодной альтернативой традиционным способам оплаты товаров и услуг. Причем можно предположить, что мобильные платежи (схема оплаты, в которой хотя бы один этап транзакции осуществляется с помощью мобильного устройства) в ближайшем будущем будут наиболее востребованными среди существующих способов оплаты. Это обусловлено доступностью мобильных устройств и широкими возможностями реализации приложений, предоставляющих клиенту доступ к его счету.

Следовательно, ввиду популяризации мобильных платежей их безопасность приобретает ключевое значение, и первым шагом проектирования мобильной платежной системы должен быть анализ угроз безопасности, возникновение которых возможно на всех уровнях реализации.

В данной статье проводится анализ существующих уязвимостей, которые необходимо закрыть в процессе создания системы мобильных платежей.

Любая система мобильных платежей представляет собой совокупность объектов, которые могут взаимодействовать по двум основным схемам: удаленного платежа (Remote M-Payment System) и бесконтактного платежа (Proximity Payment Systems). В зависимости от выбора схемы определяется набор технологий, использование которых возможно для передачи данных.

Очевидно, что для обеспечения стойкости системы мобильных платежей, необходимо рассмотреть защищенность использованных при ее построении стандартов, технологий, протоколов и платформ.

Таким образом, все уязвимости можно разделить согласно уровню их реализации: нижний уровень – протокол GSM, операционная система, технология передачи (RFID) и уровень программного обеспечения. Рассмотрим уязвимости нижнего уровня.

Уязвимости протокола GSM

Безопасность системы GSM основана на разделении секрета мобильной станцией и её базовой приёмопередающей станцией, для чего используются следующие три алгоритма:

- алгоритм аутентификации A3;
- алгоритм генерации ключа A8;
- алгоритм шифрования A5.

1) Алгоритмы A3 и A8

Для исключения несанкционированного использования ресурсов системы связи вводятся механизмы аутентификации. У каждого подвижного абонента есть стандартный модуль подлинности абонента (SIM-карта), которая содержит алгоритм аутентификации (A3), и генерации сеансового ключа (A8). В настоящее время известны следующие стандартной реализацией алгоритма A3/A8 является COMP128. Хотя существуют альтернативы COMP128, но этот протокол по-прежнему поддерживается в подавляющем большинстве сетей GSM.

Можно выделить следующие проблемы безопасности:

- Активные атаки — злоумышленник исполняет роль сетевого элемента.
- Небезопасная передача ключевой информации: аутентификационные данные передаются в явном виде внутри и между сетями.
- Односторонняя аутентификация: обеспечивается только аутентификация пользователя для сети, нет средств аутентификации сети для пользователя.
- Слабые алгоритмы шифрования. Длина ключа слишком мала, в то время как скорости вычислений растут

2) Алгоритм шифрования A5 реализуется в самой мобильной станции, а не в SIM-карте, и зависит от производителей оборудования базовых и мобильных станций.

В настоящее время используется модификация A5/3, базой для которой служит алгоритм KASUMI, утвержденный для использования в качестве ядра для алгоритмов конфиденциальности и целостности информации. В настоящее время данный поточный шифр обеспечивает требуемую криптостойкость.

Уязвимости технологии передачи (RFID)

В качестве одного из возможных сценариев реализации уязвимости технологии RFID можно рассмотреть следующий: при потере телефона любой человек, нашедший данное устройство, имеет возможность (при наличии необходи-

мого оборудования) скопировать смарт-карту, содержащую идентификационные данные пользователя. Таким образом, очевидно, могут быть осуществлены операции, инициированные не законным владельцем телефона, а злоумышленником.

Уязвимости ОС (на примере Google Android)

Одной из последних уязвимостей, обнаруженных в Android-смартфонах, является следующая: уязвимость позволяет любому приложению, имеющему разрешение на доступ в интернет, собирать и передавать личные данные пользователя, в том числе данные СМС: номера телефонов и зашифрованный текст сообщений.

Помимо программы, собирающей для HTC пользовательские данные, в новых прошивках также присутствует приложение, не только имеющее доступ ко всей вышеперечисленной информации, но и способное предоставить её любому неавторизованному пользователю по запросу на локальный порт, при этом не требуется никаких специальных разрешений, кроме доступа в интернет (это разрешение, помимо всего прочего, позволит передать полученные данные куда и кому угодно).

Таким образом, получили список уязвимостей нижнего уровня, которые могут нанести ущерб безопасности создаваемой нами системы. Соответственно, данный список дает возможность при реализации системы мобильных платежей предотвратить несанкционированный доступ к конфиденциальной информации посредством перечисленных уязвимостей.

Список источников

1. Security Issues in Mobile Payment Systems. Shivani Agarwal , Mitesh Khapra , Bernard Menezes , Nirav Uchat.

2. Анастасия Мясникова. Реализация алгоритма A5/3 (GSM). URL: ftp://cs.usu.edu.ru/crypto/A5_3/ReadMe.htm

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ В НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЕ РОССИИ

Никитина Виктория Леонидовна
НИЯУ МИФИ, Москва, зам. зав. кафедрой кибербезопасности
op50@mail.ru

Актуальность, новизна, цель и практическая значимость работы обусловлены проблемами реализации Федерального закона от 27 июня 2011 года N 161-ФЗ "О национальной платежной системе" [1], который преследует триединую задачу: уход от иностранной разведки российских финансовых транзакций – усиление национального финансового мониторинга в интересах противодействия легализации (отмывания) доходов, полученных преступным путем, и финансированию терроризма – уменьшение массы наличных денежных средств.

Основные положения нормативного обеспечения защиты информации при осуществлении переводов денежных средств в национальной платежной системе России приведены в анализируемом ниже Положении Центрального банка России от 9 июня 2012 г. N 382-П

Анализируемое «Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» по состоянию на 21 августа 2012 года в целом соответствует требованиям, предъявляемым к подзаконным нормативно-правовым актам. Однако, после вступления России во Всемирную торговую организацию (далее - ВТО) Федеральный закон от 27 июня 2011 года N 161-ФЗ "О национальной платежной системе" и, следовательно, анализируемое Положение требуют дополнений по обязательствам России перед ВТО. В частности, согласно терминологии ВТО банковские операции относятся к банковским услугам. После присоединения к ВТО к оказанию таких банковских услуг в России будут допущены иностранцы из стран – членов ВТО на предусмотренных условиях. Россия присоединилась к ВТО 22 августа 2012 года путем ратификации соответствующих международных соглашений. После ратификации эти тексты стали частью международных со-

глашений России, которые, как известно, имеют бóльшую силу, нежели любые внутренние российские законы. В случае противоречия между этими текстами и внутренними российскими законами в силу ч. 4 ст. 15 Конституции РФ применяться должны будут первые. После вступления России в ВТО в отношении оказания иностранными лицами из членов ВТО финансовых услуг в России / применительно к получателям в России и из России будут действовать правила согласно принятым на себя Россией обязательствам. Кроме того, российские субъекты получат право входить на иностранные рынки финансовых услуг, причем с учетом тех обязательств, которые взяли на себя соответствующие члены ВТО.

В связи с получением Россией статуса члена ВТО для нее начали действовать десятки документов ВТО (как международные соглашения, образующие правовую основу ВТО, так и локальные документы органов ВТО). Важнейший из них — Генеральное соглашение о торговле услугами (General Agreement on Trade in Services), GATS (ГАТС). Сюда же следует отнести Международные стандарты ISO 13335, ISO 13569 (банковские и финансовые услуги), ISO 17799/ BS 7799-2, », COBIT, серию стандартов ИСО/МЭК 27000 и др.

Необходимо отметить следующие резервы доработки Положения:

1. Целесообразно дополнить п.1.1. Положения ссылкой на «Положение о защите информации в платежной системе», утвержденное Постановлением Правительства РФ от 13 июля 2012 № 584;

2. Положение не содержит ссылки на ранее принятый Стандарт Банка России СТО БР ИББС-1.0-2010 «ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ» без соблюдения которого, как отметил В. Лукацкий, крайне трудно выполнять требования Федерального закона от 27 июля 2006 г. N 152-ФЗ “О персональных данных”, которым после 1 января 2011 года должны соответствовать все системы, обрабатывающие персональные данные. Проблема выполнения технических требований, вытекающих из этого закона ускорила процесс принятия кредитными организациями данного стандарта. Обсуждая вопрос внедрения СТО БР ИББС, стоит упомянуть и об Указании Банка России от 09.06.2012 N 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств», в котором установлены формы отчетности по обеспечению защиты информации при осуществлении переводов денежных средств 3 категорий операторов: платежных систем; услуг платежной инфраструктуры; по переводу денежных средств.

3. В соответствии с п. 2.9.1.Положения «В случае если оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры применяют СКЗИ российского производителя, указанные СКЗИ должны иметь сертификаты уполномоченного государственного органа». Однако, никак не урегулирован вопрос применения СКЗИ нероссийского производства. В Приложении 2 приведен перечень требований к СКЗИ без учета происхождения. Например, если длина ключей для симметричных СКЗИ, предназначенных для защиты финансовых транзакций составляет свыше 56 бит, то при наличии нотификации ФСБ, ввозятся такие СКЗИ, что фактически является разрешением и на эксплуатацию. Поэтому получается так, что в НПС могут применяться любые СКЗИ.

4. На оператора платежной системы возлагается большая работа по реагированию на инциденты, разработке методик анализа и реагирования, информирование операторов по переводу и операторов инфраструктуры о выявленных инцидентах и т.д. Оценка соответствия требованиям по ИБ проводится самостоятельно или с приглашением внешних организаций в соответствие с методикой, приведенной в приложении к Положению. При этом никак не урегулирован вопрос о наличии лицензии на техническую защиту конфиденциальной информмции у такой организации в соответствии с Постановлением Правительства РФ от 03.02.2012 г №79 "О лицензировании деятельности по технической защите конфиденциальной информации".

5. Перечень отмеченных замечаний не является исчерпывающим. Отдельного анализа требуют Приложения к анализируемому Положению. Особенно это относится к Приложению 1, которое содержит спорные утверждения из области многомерных экспертных оценок и не соотносится с международными моделями уровней зрелости организаций. Отмеченные замечания требуют дальнейшего анализа и доработки.

Список источников

1. Федеральный закон от 27 июня 2011 года N 161-ФЗ "О национальной платежной системе". "Российская газета" от 30 июня 2011 г. N 139.

МОНИТОРИНГ СЕТИ НА ФИЗИЧЕСКОМ УРОВНЕ

Романов Сергей Андреевич
КНИТУ-КАИ, Казань, студент
rsa5325@yandex.ru

Аннотация. В статье рассматриваются проблемы мониторинга сети: причины, способы мониторинга, способы борьбы с несанкционированным мониторингом сетей.

Применение на практике

Причины применения мониторинга за сетью.

Например, сеть состоит из трех компьютеров a, b и c. На компьютере a запущен сетевой анализатор, и вы можете наблюдать не только входящий/исходящий трафик на компьютере a, но и данные, проходящие между компьютерами b и c. Это типовая ситуация при работе с сетевыми анализаторами, системами учета трафика и мониторинга сетевого контента. В принципе, вы можете запустить эти программы на каждом компьютере, но это довольно неудобно, поскольку у вас перед глазами не будет всей полноты картины.

Способы мониторинга Ethernet

Мониторинг с помощью хабов

Из-за достаточно низкой стоимости в небольших сетях чаще используются хабы нежели коммутаторы, что позволяет использовать их особенность ретрансляции поступающих данных на все порты в promiscuous мониторинге. Помимо этого некоторые виды хабов могут не позволить вести полноценный мониторинг своего сегмента сети.

1) Компьютер, подключенный к хабу

Любой компьютер, подключенный к хабу, может использоваться для мониторинга, поскольку хаб передает принятые/переданные данные от маршрутизатора на все порты. Достаточно лишь отключить на компьютере фильтрацию данных, направляемых по другим IP-адресам. Также отметим, что возможен мониторинг обмена между локальными ПК.

2) Хаб между маршрутизатором и коммутатором

Есть возможность наблюдать данные, передаваемые и получаемые из Интернета, но данные, которыми обмениваются локальные компьютеры внутри ЛВС, вам недоступны.

3) Мониторинг локальной сети без коммутатора

Топология малых компьютерных сетей предусматривает совмещение маршрутизатора и коммутатора, к которому подключаются остальные компьютеры (терминалы). Для мониторинга всех данных, передаваемых или принимаемых из Интернета, можно установить хаб между внешней сетью и маршрутизатором, тогда можно будет узнать даже передаваемые скрытым путем данные. Важно отметить, что программа сетевого мониторинга не сможет различать трафик от разных рабочих станций до тех пор, пока у этих рабочих станций, находящихся за маршрутизатором, не будет трассируемых ip-адресов. Если у них нет трассируемых ip-адресов, то все пакеты будут иметь один ip-адрес – это публичный ip-адрес вашей сети. Компьютер для мониторинга должен быть абсолютно пассивным и не передавать данных в сеть, то есть интерфейс должен только принимать данные. Этого можно достичь путем назначения достичь путем назначения сетевой карте нетрассируемого IP-адреса.

Мониторинг с помощью коммутаторов

Для сетевого мониторинга подходил управляемый коммутатор с поддержкой зеркалирвания портов. Функция зеркалирования позволяет перенаправлять трафик с любых портов на один определенный порт коммутатора.

Есть два типичных способа зеркалирования портов:

1) Использование коммутатора с зеркалированием портов

Главный коммутатор обладает способностью зеркалировать порты на определенный порт. Подключаем компьютер к «зеркальному» порту, на который производится перенаправление трафика с ЛВС. Причем, можно зеркалировать трафик не с одного, а с нескольких портов коммутатора.

2) Использование неконтролируемых коммутаторов в сети

При использовании в сети неконтролируемых коммутаторов, не поддрживающих зеркалирование портов, невозможно подключить к ним контролируемый коммутатор. Максимально возможное в данном случае: подключиться к коммутатору, подключенному к Интернету (они, чаще всего, поддерживают зеркалирование портов) и перехватывать трафик между ЛВС и сетью Интернет. Но будет недоступна информация, передаваемая внутри ЛВС между рабочими станциями. Некоторые коммутаторы, не поддерживающие зерклирование пор-

тов, могут быть использованы для мониторинга в режиме "promiscuous", но в таком случае в результате реализации arp флуда" или arp спуффинга, коммутатор начинает рассылать пакеты по всем портам

Рекомендации по выбору конфигурации сети:

1) Использование отдельного терминала для мониторинга. Мониторинг сети является задачей, требующей больших ресурсов, при обработке данных и трафика, что создает большую нагрузку на процессор. В связи с этим рекомендуется выполнять эту задачу на отдельном компьютере.

2) Использование вместо хабов, ретранслирующих данные на все порты, управляемых коммутаторов, транслирующих трафик на отдельный порт, что снижает нагрузку в сети и риск несанкционированного мониторинга.

Удаленный мониторинг

Способы удаленного мониторинга:

1) Использование программ для удаленного доступа позволяет, которые получили широкое распространение в виду простоты их использования (microsoft remote desktop connection и terminal services, TeamViewer

2) Использование удаленных сетевых модулей. Подключившись к одному или к нескольким удаленным агентам из одного центра, администратор видит в своей программе мониторинга весь трафик с удаленных машин в режиме реального времени. Что дает одновременное подключение сразу ко многим удаленным модулям и возможность анализировать/сохранять данные на вашем компьютере.

Способ мониторинга на базе двух сетевых карт.

На внешней сетевой карте настраивается режим «promiscuous». Promiscuous mode или promisc mode — так называемый «неразборчивый» режим, в котором сетевая плата позволяет принимать все пакеты независимо от того, кому они адресованы. По умолчанию сетевое оборудование игнорирует трафик, адресованный не ему путем сравнения заголовков пакетов. В более широком смысле режим promiscuous также означает прозрачность сети с определенной точки наблюдения, но при этом не подразумевается обязательного перевода адаптеров в данный режим. В современном оборудовании и программном обеспечении часто реализованы и другие способы мониторинга для достижения полной видимости всех сетевых процессов.

Список источников

1. Техника и философия хакерских атак. М.: СОЛОН-Р, 1999, ISBN 5-93455-015-2

2. Лаем Куин, Ричард Рассел Fast Ethernet, bhv, Киев, 1998. ISBN 5-7315-0014-2 (англ: ISBN 0-471-16998-6)

3. Техника сетевых атак. М.: СОЛОН-Р, 2001, ISBN 5-93455-078-0

ПОДХОДЫ К ЗАЩИТЕ ЦЕЛЕВЫХ СИСТЕМ ОТ AET

Макеев Сергей Александрович
Финансовый университет при Правительстве РФ, Москва, студент
kzo-101@mail.ru

Актуальность

На сегодняшний день каждая организация имеет свою корпоративную сеть, в которой циркулирует информация разной степени важности, представляющая интерес для злоумышленника. Для обеспечения защиты корпоративных сетей от угроз строится многоуровневая система защиты, включающая в себя периметровые межсетевые экраны и VPN-коммутаторы, системы предотвращения вторжений. Такой подход к построению системы имеет право на жизнь, однако в 2010 компания Stonesoft объявила об открытии абсолютно новой категории угроз сетевой безопасности – динамических техниках обхода Advanced Evasion Techniques (AET). [1]

Техники AET предоставляют злоумышленникам своего рода мастер-ключ для доступа к любой целевой системе, например, к корпоративным ERP- и CRM-приложениям, SCADA-системам, путем обхода современных систем сетевой безопасности. В результате атаки компании могут понести значительный финансовый или репутационный ущерб. Весьма характерный пример последнего времени (2010) – в трояне ZeuS, созданном для кражи банковских данных и шпионажа, были заложены техники AET [2].

В статье приводится рассмотрение понятия динамических техник обхода, а также предложение по созданию комплексного решения обнаружения и отражения вторжений.

Методы обнаружения и предотвращения вторжений

Под системой предотвращения вторжений (СПВ, IPS) понимается программная или аппаратная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них.

Сетевые СПВ осуществляют сбор и анализ сетевых пакетов, на основании которых проводится обнаружение. Сенсоры таких систем могут быть распре-

делены по элементам сети. В данной статье рассматриваются именно сетевые СПВ.

Выделяют два основных подхода к обнаружению — обнаружение сигнатур (signature detection, misuse detection), обнаружение аномалий (anomaly detection) и гибридный подход. Основные методы обхода СПВ: сбивание с толку; фрагментация; шифрование; перегрузка. [3]

Классический подход к безопасности сети неспособен динамически выявить новые атаки. В статичных методах сигнатурного или шаблонного обнаружения уже недостаточно простого «отпечатка».

Специфика техник обхода

Статья «Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection» об атаках против сетевых систем обнаружения вторжений появилась в 1997 г. Согласно статье, техники обхода есть средство доставки любого «полезного груза» до целевой системы без ее обнаружения средствами сетевой защиты (СПВ).

Необходимо отметить, что большинство техник обхода используют мягкие требования к интерпретации работы протоколов и обычно не нарушают стандартов RFC, поэтому модули разбора протоколов их также не распознают. Примером известных техник обхода являются: IP fragmentation, MSRPC encryption, TCP segmentation, MSRPC fragmentation, SMB fragmentation, TCP TIME_WAIT, IP random options и др. [4]

Динамические техники обхода (АЕТ) – это развитие традиционных техник обхода, которые базируются на следующих принципах: [1]

- объединение нескольких способов обхода, которые действуют на различных уровнях сетевого взаимодействия;
- использование не декларированных и редко используемых свойств протокола;
- возможность изменить комбинацию техник обхода во время атаки;
- продуманное построение атак.

Для маскировки «полезного груза» АЕТ используют слабые места протоколов, а также невысокие ограничения по безопасности при сетевой коммуникации. Так можно внедрять пакеты данных, которые кажутся безвредными для СПВ и проявляют себя как атака только при их интерпретации целевой системой.

Эксперты из компании Stonesoft с конца 2010 года выявили 147 различных видов АЕТ. [1]

Подходы к созданию систем предотвращения вторжений

Большинство современных средств защиты лишь приближается к тому, чтобы максимально быстро закрывать уязвимости. Для реального комплексного подхода необходимо детектировать атаку по контентному содержанию пакетов и анализу используемых эксплойтов.

Для защиты целевых систем от применения АЕТ необходимо скорректировать принципы построения СПВ:

1) нормализация IP/TCP-трафика;
2) наблюдение и анализ на всех уровнях протоколов;
3) восстановление фрагментированных IP-пакетов до их анализа;
4) обнаружение, основанное на изучении трафика на уровне приложений модели OSI;
5) статистический анализ данных;
6) возможность обучения и самообучения (встроенные тесты на проникновение).

Наиболее существенная защита против АЕТ – это нормализация протоколов. СПВ должна инспектировать и анализировать весь сетевой трафик по набору сигнатур, чтобы любая незнакомая и потенциально опасная последовательность данных могла быть легко идентифицирована, а ее распространение по сети – своевременно предотвращено. Однако это очень сложный процесс, и если нормализация протоколов не будет в полной мере реализована, эксплойты смогут «пройти» через систему безопасности.

Выводы

Динамическим техникам обхода сложно противодействовать именно потому, что они комбинированные и имеют большую вероятность успеха, в отличие от одиночных применений.

Для динамических угроз сетевой безопасности системы защиты необходимо постоянно обновлять, чтобы не отставать от процесса совершенствования угроз. Для этого чрезвычайно важно проводить детальный анализ методов нападения и понимать, какие уязвимости системы эксплуатировались.

Список источников

1. Multilayer Traffic Normalization and Data Stream Based Inspection: Essential Design Principles of the Stonesoft IPS. Whitepaper. – 2012.

2. Тараканов Д. За кем охотится ZeuS. http://www.securelist.com/ ru/analysis/208050628/Za_kem_okhotitsya_ZeuS. – 2010.

3. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студ. учреждений высш. проф. образования / В.В.Платонов. — М.: Издательский центр «Академия», 2013. — 336 с. (Сер. Бакалавриат).

4. Network Intrusion: The Advanced IPS Evasion Techniques. http://basicnetworkingconcepts.blogspot.ru/2011/02/network-intrusion-advanced-ips-evasion.html. - 2011.

ИССЛЕДОВАНИЕ И РАЗРАБОТКА МЕТОДОВ КОМБИНИРОВАННОГО АНАЛИЗА КРУПНЫХ ГЕТЕРОГЕННЫХ ИНФОРМАЦИОННЫХ МАССИВОВ ФИНАНСОВО-ЭКОНОМИЧЕСКОЙ ИНФОРМАЦИИ В ЦЕЛЯХ ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ ОТМЫВАНИЯ ПРЕСТУПНЫХ ДОХОДОВ И ФИНАНСИРОВАНИЯ ТЕРРОРИЗМА НА ФОНДОВОМ РЫНКЕ

Чукова Дарья Ильинична
НИЯУ МИФИ, Москва, аспирант
DIChukova@mephi.ru

Проблема отмывания денег и финансирования терроризма содержит в себе ряд глобальных угроз, как на мировом, так и на национальном уровне. Отсутствие должного внимания к этой проблеме может повлечь за собой целый ряд последствий, таких как: значительное повышение уровня преступности, стремительный рост уровня коррупции, проблемы в функционировании финансовой системы, инфляцию и многое другое.

Со временем методы отмывания денег становятся все более изощренными, что требует постоянного совершенствования системы противодействия отмыванию денег. Поэтому анализ финансово-экономической информации с целью выявления инцидентов отмывания денег является актуальной задачей.

Наиболее привычным инструментом для отмывания денег всегда считались банки, однако, во время кризиса ситуация несколько изменилась. Компаниям, работающим на фондовом рынке, стало достаточно легко обосновывать происхождение значительной части доходов клиентов за счет стремительной изменчивости цен. Это можно подтвердить, оценив Российский индекс волатильности (характеризует степень колебания цен активов, отражает, насколько высоки отклонения ценовых изменений относительно общей тенденции) за 2008-2010 года.

В сентябре–декабре 2008 года индекс волатильности принимал экстремально высокие значения. Максимальное значение было достигнуто 21 ноября 2008 года, оно составило 200,5%.

В начале 2009 года ситуация на российском фондовом рынке оставалась напряженной. Российский индекс волатильности в этот период показывал сильные колебания – от 60% до 100%.

В марте 2009 года началось восстановление российского рынка акций, значение индекса волатильности постепенно снижалось. Данная тенденция сохранилась до конца апреля 2010 года – постепенный рост рынка сопровождался снижением уровня волатильности.

Помимо нестабильной ситуации на фондовом рынке, использованию именно этой сферы для отмывания денег способствовало то, что получить брокерскую лицензию намного дешевле и проще, чем банковскую. Во время кризиса минимальное требование к размеру собственных средств профучастника составляло 5 миллионов рублей, тогда как минимальное требование к капиталу банка - 90 миллионов рублей.

В связи с этим, брокерские компании все чаще стали подозреваться в нарушении законодательства в части противодействия отмывания денег и финансирования терроризма.

Цель исследовательской работы - формирование критериев подозрительности участников фондового рынка, методом их анализа в терминах теории распознавания образов. Для этого используется информация Федеральной службы по финансовым рынкам об аннулировании лицензий профессионального участника рынка ценных бумаг на осуществление брокерской деятельности, дилерской деятельности и деятельности по управлению ценными бумагами. Рассматриваются случаи аннулирования брокерских лицензий в 2008-2010 годах за нарушения законодательства противодействия легализации (отмывания) доходов, полученных преступным путем, и финансированию терроризма.

В результате работы планируется получить численные показатели, отражающие степень надежности участника фондового рынка, а также оценить риски наличия существенных нарушений в деятельности организации, которые могут повлечь за собой аннулирование лицензий профессионального участника рынка ценных бумаг на осуществление брокерской деятельности, дилерской деятельности и деятельности по управлению ценными бумагами.

Результаты, которые планируется получить, могут быть применены в Федеральной службе по финансовому мониторингу для выявления инцидентов отмывания преступных доходов и финансирования терроризма участниками фондового рынке.

Список источников

1. Комментарий Руководителя ФСФР России В.Д. Миловидова газете “Коммерсант” о создании биржей РТС индекса волатильности российского рынка // Коммерсант. 2010. 8 декабря.

2. Фомин Я.А., «Распознавание образов. Теория и применение» М.; изд. «Фазис», 2012.

ИЕРАРХИЧЕСКАЯ СТРУКТУРА КОМПЛЕКСА МОДЕЛЕЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОРГАНИЗАЦИИ

Яхонтов Иван Владимирович
Финансовый университет при Правительстве РФ, Москва, аспирант

Введение

Насколько важна любая информация, относящаяся к бизнесу понятно многим. Пользуясь собранной и обработанной информацией, можно успешно конкурировать на своем рынке и захватывать новые. Информация помогает в поиске партнеров и способствует четкому определению позиции по отношению к ним.

Кроме того, при переходе к рыночной экономике информация становится товаром и должна поэтому подчиняться специфическим законам товарно-рыночных отношений. В этих условиях проблема защиты информации весьма актуальна и для организаций любой формы собственности.

Вопросы безопасности - важная часть концепции внедрения новых информационных технологий во все сферы жизни общества. Широкомасштабное использование вычислительной техники и телекоммуникационных систем в рамках территориально-распределенной сети, переход на этой основе к безбумажной технологии, увеличение объемов обрабатываемой информации и расширение круга пользователей приводят к качественно новым возможностям несанкционированного доступа к ресурсам и данным информационной системы, к их высокой уязвимости.

Системный подход обеспечивает адекватную многоуровневую защиту информации, рассматриваемую как комплекс организационно-правовых и технических мероприятий. Кроме того, при реализации механизмов защиты должны использоваться передовые, научно обоснованные технологии защиты, обеспечивающие требуемый уровень безопасности, приемлемость для пользователей и возможность наращивания и модификации СЗИ в дальнейшем.

Следовательно, при моделировании информационной системы (ИС) предприятия необходимо учитывать угрозы защиты информации и методы противодействия угрозам. Для этого следует разработать модель системы защиты информации, отвечающую определенным требованиям в зависимости от пот-

ребностей ИС. Для этого разумно будет использовать системный подход, анализ существующих систем и их недостатки.

Анализ подходов к моделированию систем защиты информации показал, что ни одна из представленных моделей не удовлетворяет в полной мере основным критериям. Таким образом, анализ моделей средств защиты информации показывает, что ни один из подходов в полной мере не отвечает предъявляемым требованиям. Модели в основном используются на этапе эксплуатации и сопровождения. Также некоторые модели используются и на этапе проектирования ИС, но только для получения частных оценок уровня защищенности ИС.

Разработка комплекса моделей

Для решения всех задач поставленных перед разрабатываемой моделью СЗИ организации, предлагается реализовывать её в виде комплекса моделей. Архитектура разработанного комплекса моделей представляет собой иерархическую структуру, отображенную на рисунке 1.

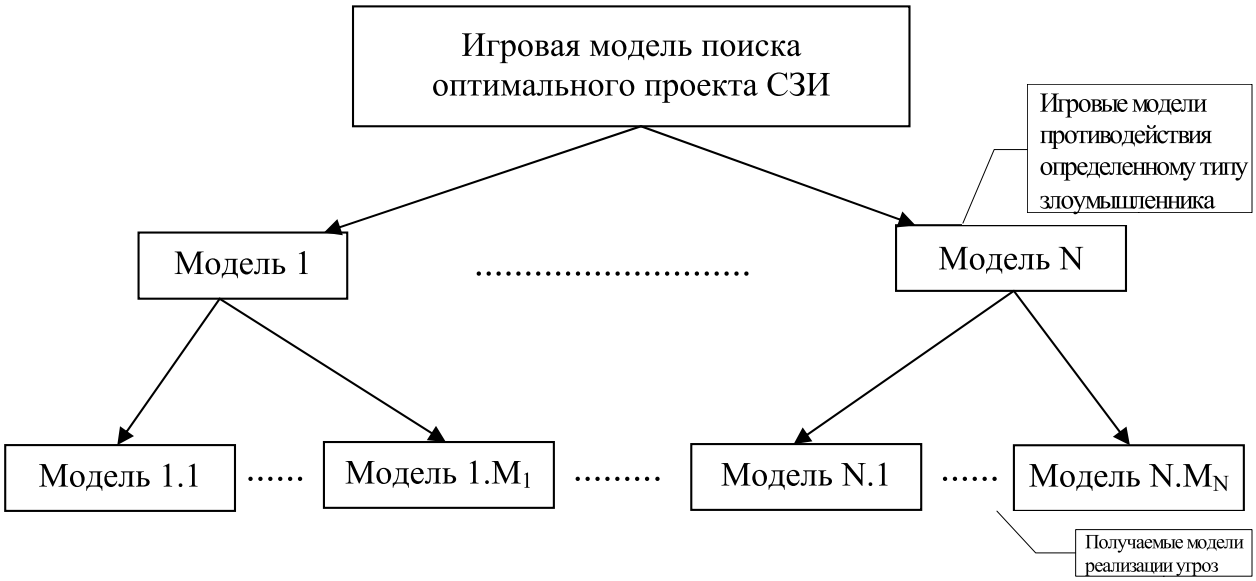

Рис. 1. Иерархическая структура комплекса моделей

Во главе иерархии находится игровая модель поиска оптимального проекта. Исходными данными для данной модели являются показатели обобщенных рисков при противодействии определенному типу злоумышленника и вероятности атаки со стороны того или иного типа злоумышленника. Вероятности атаки должны быть определены отдельно, а показатели обобщенных рисков

поставляют модели, лежащие на среднем уровне иерархии - игровые модели противостояния определенному типу злоумышленника, для которых, в свою очередь, исходными данными являются риски, связанные с реализацией злоумышленником той или иной угрозы, и вероятности того, что злоумышленник будет пытаться осуществить именно эту угрозу. Вероятности нацеленности злоумышленника на реализацию угрозы определяются отдельно, а значения рисков поставляются моделями низшего уровня - полумарковскими моделями реализации угроз.

Разработка модели злоумышленника

Модель исследования оптимальности проекта системы защиты информации предполагает построение модели злоумышленника. Как известно злоумышленники могут быть разных типов. Они могут быть внутренними и внешними, они могут отличаться по уровню подготовки, по уровню оснащения, по целям, которые они перед собой ставят и т.д. Следовательно, необходимо разработать модель злоумышленника, которая формально описывала бы все разнообразие существующих типов злоумышленников.

В рамках описанного комплекса моделей для исследования оптимальности проекта системы защиты информации – модель злоумышленника представляет собой множество

$M=\{\{T\}, \{M^{param}\}, P_k\}$,

где: {T} - множество угроз доступных злоумышленнику. При этом элемент T из множества {T} представляет собой следующее

T;={Pт, {VI}, {E}},

где: Pт - вероятность выбора данной угрозы злоумышленником для эксплуатации; {VI} - множество уязвимостей системы защит информации, причем элемент Vlj из множества {VI} представляет собой следующее

$Vlj = \{P_{init}, S_{param}\}$,

где: P_{init} - вероятность инициализации; S_{param} - множество требований к злоумышленнику. {E} — множество переходов между уязвимостями защиты информации, причем элемент Ej из множества {E} представляет собой следующее

$Ei=\{ P_i^{перех}, P_i^{усп}, \mu_i, \sigma_i \}$,

где: $P_i^{перех}$ - вероятность выбора пути по данному переходу; $P_i^{усп}$ - вероятность успеха; μ_i, σ_i - параметры логнормального закона распределения вероятности пребывания в предыдущем состоянии при выборе пути по данному переходу; S_{param} - множество требований к злоумышленнику. $\{M_{param}\}$ - множество

параметров злоумышленника; P_k — вероятность столкновения системы защиты именно с данным типом злоумышленника.

Заключение

В статье приведен сравнительный анализ различных моделей СЗИ, выявлены основные плюсы и минусы каждой. Представлены рекомендации по созданию архитектуры СЗИ. Даны рекомендации по созданию модели действий злоумышленника для получения оценки эффективности СЗИ и поиска возможных путей ее улучшения.

Список источников

1. Герасименко В.А, Малюк А.А. Основы защиты информации / В.А. Герасименко, А.А. Малюк - М.: Московский Государственный Инженерно-физический институт (технический университет), 1997.

2. Кельтон В., Лоу А. Имитационное моделирование. Классика CS. / Пер. с англ. / В. Кельтон, А. Лоу - 3-е изд. - СПб.: Питер; Киев: Издательская группа BHV, 2004. 847 с.

3. Арьков П.А. Подход к проектированию системы защиты информации автоматизированной системы // XI Региональная конференция молодых исследователей Волгоградской области: тезисы докладов / ВГТУ Волгоград 2006, с. 198.

СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ В ОБЛАЧНЫХ ТЕХНОЛОГИЯХ

Д.Г. Лобанова, Д.А. Диканева, Е.И.Качуров
Финансовый университет при Правительстве РФ, Москва, студенты
lobanova.dana@yandex.ru ,dasha.dikanyova@gmail.com

Аннотация. Специфические уязвимости облачных систем и методы их устранения. Факторы, затрудняющие защиту облачных сред. Факторы, которые необходимо учитывать при разработке адаптивных СПВ, необходимые функции. Возможные способы их модернизации.

Введение

Почему же именно облачные технологии так актуальны на сегодняшний день? Можно ожидать, что в скором времени IT трансформируется в сервис на подобии электричества, дав при этом мощнейший потенциал для инновационного развития. Поэтому ведущие компании-разработчики программного обеспечения направили свои усилия на создание средств защиты сред облачных вычислений. И одним из решений этой задачи могут стать адаптивные системы предотвращения вторжений в облачных системах.

Основные проблемы безопасности облачных вычислений

Ниже приведена классификация и описание основных проблем безопасности, которые возникают в облачной инфраструктуре. Мы определили следующие виды угроз для облака:

1. Неправомерное и нечестное использование облачных технологий
2. Небезопасные программные интерфейсы (API)
3. Внутренние нарушители
4. Уязвимости в облачных технологиях
5. Потеря или утечка данных
6. Кража персональных данных
7. Неправомерный доступ к сервису

Одним из факторов, затрудняющих защиту облачных сред, можно считать отсутствие:

- зрелых стандартов, классифицирующих облачные среды и регламентирующих их взаимодействие с другими системами;
- или недостаточный функционал защиты информации в интерфейсах прикладного программирования (API),
- устоявшейся практики реализации в облачных средах действующих ИБ-стандартов;
- организационной и технической возможности контроля состояния защищенности информации у клиентов.

Факторы, которые необходимо учитывать при разработке адаптивных систем

1. Ответственность.
2. Полнота контроля трафика.
3. Гибкость подхода: возможность модификации списка угроз.
4. Полнота видения/структура СПВ:
   a) уровень 1 – сеть
   b) уровень 2 – существующая инфраструктура.
   c) уровень 3 – развитие инфраструктуры.

Функции СПВ.

- Защита периметра облачной среды от сетевых атак.
- Поддержка согласованных функций обеспечения информационной безопасности в гибридных инфраструктурах: физической, виртуальной и облачной.
- Обеспечение эффективности эксплуатации благодаря поддержке согласованного адресного пространства между существующей физической и расширенной облачной инфраструктурой
- Сокращение общего времени развертывания полнофункциональной виртуальной машины за счет автоматического выделения IP-адресов быстро развертываемым виртуальным машинам.
- Унифицированные средства управления и мониторинга физических, виртуальных и облачных рабочих процессов.

Заключение

Переход на облачные вычисления обещает заманчивые возможности, как для компаний, предоставляющих интернет-услуги, так и для предприятий, активно использующих ИТ в своей работе. Сделав ставку на облачные вычисления, предприятия могут обеспечить себе экономию средств, гибкость и свободный выбор вычислительных мощностей. Возможности разрабатываемой интеллектуальной СПВ на облачные вычисления позволят повысить уровень информационной безопасности как имеющихся, так и перспективных корпоративных инфраструктур, интегрирующих облачные среды.

Список источников

1. http://blog.i-oblako.ru/
2. http://www.bureausolomatina.com/node/96
3. http://www.itland.com.ua/products/sect.php?SECTION_ID=291
4. http://www.pcweek.ru/security/article/detail.php?ID=139185

МОДЕЛЬ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ДЛЯ ПОДДЕРЖКИ СЛЕДСТВЕННОГО ПРОЦЕССА

Деева Наталия Владимировна
Гродненский государственный университет имени Янки Купалы,
Республика Беларусь

Аннотация. Предлагается модель автоматизированной системы для поддержки следственного процесса. Рассматриваются типы уголовно-процессуальных документов, алгоритмы обработки и построение объектной модели их текстов.

Ключевые слова: следственный процесс, контент-анализ, информационная модель следственного процесса, объектная модель текста.

Введение

Сегодня преступные сообщества имеют в своём арсенале развитую базу инструментальных средств, использующую информационные технологии, что позволяет им иметь актуальную информацию и быстро принимать решения. В связи с этим, от специалиста, ведущего следственный процесс, требуется быстрое реагирование и оперативный анализ огромного количества информации.

В данной работе делается попытка создания модели системы мониторинга, контроля и анализа информационных потоков следственного процесса. Такая система должна взять на себя функции первого помощника следователя или группы следователей, работающих по некоторому уголовному делу. Одной из важных функций такой системы является оперативный обмен информацией между различными подразделениями управления внутренних дел и другими государственными органами полномочными предоставлять требуемую в процессе расследования информацию.

Большая часть информации, которой владеет следователь на различных этапах работы – это обычный текст на естественном языке. Особенно важной, в связи с этим, задачей является задача обработки естественно-языкового текста и выделение из него содержательной картины текста.

Документальное обеспечение следственного процесса

В ходе работы над уголовным делом следователь создаёт и обрабатывает огромное количество документов, составляющие тома уголовных дел, которые затем передаются в суд или в архив, в случае закрытия дела по какой-либо причине.

Процесс расследования полностью отображается на множестве уголовно-процессуальных документов дела. Все документы можно разделить на два класса: по ходу расследования и по сути расследования [1]. К первому классу отнесём такие документы, как направления, запросы, сообщения, назначения и т.д. Во второй класс выделим протоколы, объяснения, ответы на запросы, рапорты и заявления.

Информация, находящаяся в протоколах наиболее полно отражает как процесс расследования, так и содержательную часть, расследуемого преступления, составляя при этом информационную модель следственного процесса.

На этапе анализа документального обеспечения следственного процесса выделим следующие задачи:

1. Создание единой системы документооборота.
2. Контент-анализ текстов документов.
3. Построение информационной модели следственного процесса.
4. Реализация модуля поддержки принятия решений для эксперта-криминалиста.

Единая система документооборота

Во время работы над делом следователь руководствуется базой нормативных актов, которые представлены в специализированных кодексах (Трудовой, Уголовный, Гражданский, Налоговый и др.). И одной из важных составляющих единой системы документооборота является наличие актуальной нормативно-правовой базы.

Большинство экспертиз по делу проводятся в различных подразделениях внутренних дел или других государственных организациях (ГАИ, МЧС и т.д.) Для проведения такой экспертизы следователь делает соответствующий запрос и ждёт ответа на него. В единой системе документооборота предлагается упростить и ускорить процесс обмена информацией в виде электронных запросов и ответов, с автоматизированной поддержкой их создания, отправки и получения.

Для повышения эффективности работы следователя предлагается использовать единую базу граждан страны, лиц прибывающих на территории страны в данный момент (информация Таможенных и Пограничных служб), базу работающей части населения (информация Налоговой службы), базу транспортных средств (информация ГАИ), базу средств связи (базы операторов электросвязи и мобильных устройств) и т.д. Поиск информации в базах предлагается возложить на специального робота, который может работать, используя методы чёткого или эвристического поиска. Таким образом, следователя можно частично освободить от трудоёмкой и рутиной бумажной работы и предоставить ему актуальную и оперативную информацию.

Контент-анализ текстов документов

Наиболее информативными в плане содержания картины преступления, являются различного рода протоколы.

Как правило, все протоколы имеют следующую структуру:

1. Постоянный сегмент (юридическая формулировка) – права и обязанности субъекта, различного рода статические формулировки.
2. Процессуальный сегмент – заголовок, информация о следователе и субъектах протокола, информация о самом протоколе.
3. Содержательный сегмент – содержание протокола, например, рассказ свидетеля, вопросно-ответная часть, описательная часть места преступления.

Содержательный сегмент в свою очередь может быть разбит на части, в зависимости от типа протокола. Например, в протоколе допроса выделяется два типа сегмента: вопросно-ответный и повествовательный.

Проанализировав содержание частей протокола можно выделить методы и алгоритмы их обработки.

Так, постоянные сегменты могут выступать в качестве маркеров для выделения других частей протокола. А их содержание, например, права и обязанности субъектов протокола, а также ссылки на статьи кодексов могут храниться в виде специальных гиперссылок на соответствующие объекты информационно-нормативной базы.

Процессуальные сегменты содержат информацию о субъектах протокола, а также о самом протоколе. Так как эта информация достаточно формализована, то предлагается использовать специальные шаблоны, в которые лишь подставлять необходимые ссылки на объекты информационной модели следственного процесса.

Содержательные сегменты представляют собой неформализованный текст, как правило, повествование на естественном языке. Такие сегменты предлагается анализировать на морфо-синтаксическом уровне. Это наиболее сложный и интересный для исследования сегмент.

Для анализа повествовательных текстов предлагается использовать следующую схему:

1. Нормализация повествовательного сегмента
2. Синтаксический анализ сегмента (выделение предложений).
3. Морфологический анализ отдельного предложения (определение характеристик для каждого слова).
4. Синтаксический анализ предложения:
5. Построение объектной модели предложения:
6. Построение объектной модели сегмента (выделение сущностей и их связей).

Информационная модель следственного процесса

В результате анализа текстов протоколов получаем набор ссылок на сущности с уже определёнными свойствами. Моделью представления таких сущностей предлагается выбрать фреймы. Фрейм представляет собой не одну конкретную ситуацию (предмет или состояние), а наиболее характерные, основные моменты ряда близких ситуаций, принадлежащих одному классу. Причем, составляющие фрейма могут быть определены или не определены (так называемые, терминалы), что позволяет наиболее точно представлять модели реального мира. С другой стороны, каждое предложение, как правило, описывает одно или несколько событий, или один или несколько фактов. Такие события и факты будем отражать в виде семантической сети фреймов. Смысловой портрет текста – это набор событий и фактов, упорядоченных во времени. А объектная модель предложения – это семантическая сеть связных фреймов.

Каждое событие характеризуется местом и временем, а также набором объектов и субъектов, принимающих участие в событии. На базе выделенных событий, фактов, субъектов и объектов события строим объектную модель предложения. Построение объектной модели происходит на базе согласованного набора объектных моделей предложений некоторой части документа. Которые в свою очередь позволяют создать объектную модель протокола, а набор таких объектных моделей – обобщенную модель дела.

Заключение

На основании документов дела формируется информационная модель следственного процесса, которая отражает как содержательную картину преступления, так и документационные потоки уголовно-процессуальных документов. Что позволяет управлять следственным процессом на разных уровнях и этапах расследования, а также оперативно получать информацию всем членам следственной группы. Кроме того, построенная информационная модель следственного процесса позволяет проводить временные и пространственные срезы, а также находить несоответствия в показаниях или других

Требования к оформлению рукописей статей, направляемых для публикации в журнале

Для публикации научных работ в выпусках серий научно–практического журнала "Современная наука: актуальные проблемы теории и практики" принимаются статьи на русском языке. Статья должна соответствовать научным требованиям и общему направлению серии журнала, быть интересной достаточно широкому кругу российской и зарубежной научной общественности.

Материал, предлагаемый для публикации, должен быть оригинальным, не опубликованным ранее в других печатных изданиях, написан в контексте современной научной литературы, и содержать очевидный элемент создания нового знания. Представленные статьи проходят проверку в программе "Антиплагиат".

За точность воспроизведения дат, имен, цитат, формул, цифр несет ответственность автор.

Редакционная коллегия оставляет за собой право на редактирование статей без изменения научного содержания авторского варианта.

Научно–практический журнал "Современная наука: актуальные проблемы теории и практики" проводит независимое (внутреннее) рецензирование.

Правила оформления текста.

- Текст статьи набирается через 1,5 интервала в текстовом редакторе Word для Windows с расширением ".doc", или ".rtf", шрифт 14 Times New Roman.
- Перед заглавием статьи указывается шифр согласно универсальной десятичной классификации (УДК).
- Рисунки и таблицы в статью не вставляются, а даются отдельными файлами.
- Единицы измерения в статье следует выражать в Международной системе единиц (СИ).
- Все таблицы в тексте должны иметь названия и сквозную нумерацию. Сокращения слов в таблицах не допускается.
- Литературные источники, использованные в статье, должны быть представлены общим списком в ее конце. Ссылки на упомянутую литературу в тексте обязательны и даются в квадратных скобках. Нумерация источников идет в последовательности упоминания в тексте.
- Список литературы составляется в соответствии с ГОСТ 7.1–2003.
- Ссылки на неопубликованные работы не допускаются.

Правила написания математических формул.

- В статье следует приводить лишь самые главные, итоговые формулы.
- Математические формулы нужно набирать, точно размещая знаки, цифры, буквы.
- Все использованные в формуле символы следует расшифровывать.

Правила оформления графики.

- Растровые форматы: рисунки и фотографии, сканируемые или подготовленные в Photoshop, Paintbrush, Corel Photopaint, должны иметь разрешение не менее 300 dpi, формата TIF, без LZW уплотнения, CMYK.
- Векторные форматы: рисунки, выполненные в программе CorelDraw 5.0–11.0, должны иметь толщину линий не менее 0,2 мм, текст в них может быть набран шрифтом Times New Roman или Arial. Не рекомендуется конвертировать графику из CorelDraw в растровые форматы. Встроенные – 300 dpi, формата TIF, без LZW уплотнения, CMYK.

По вопросам публикации следует обращаться к шеф–редактору научно–практического журнала "Современная наука: актуальные проблемы теории и практики" (e–mail: redaktor@nauteh–journal.ru).