Причины, профилактика и методы противодействия инсайдерской деятельности

Кабанов Артем Сергеевич,
доцент кафедры «Компьютерная безопасность»
Национального исследовательского университета
«Высшая школа экономики»,
кандидат технических наук, доцент

kabanov_as@mail.ru

Лось Алексей Борисович,
доцент кафедры «Компьютерная безопасность»
Национального исследовательского университета
«Высшая школа экономики»,
кандидат технических наук, доцент

alos@hse.ru

В статье рассматриваются проблемы защиты информации от внутреннего нарушителя, которые, по оценкам специалистов, в последнее время приобретают все больший размах. Обоснована актуальность данной проблемы, исследованы причины и методы инсайдерской деятельности, включая методы воздействия на персонал организации. Рассмотрены подробная классификация инсайдеров, их психологические типы, мотивация их деятельности, а также подробный анализ возможного ущерба. Предложены варианты противодействия инсайду. Сформулированы основные выводы и рекомендации.

Ключевые слова: *инсайдер, инсайдерская информация, причины и профилактика инсайда, внутренний нарушитель, противодействие внутреннему нарушителю.*

Reasons, Prevention and Methods of Counteraction of Insider Activity

Kabanov Artem S.,
Assistant Professor of the Department "Computer Security"
of the National Research University
"Higher School of Economics",
Candidate of Technical Sciences, Assistant Professor

Los Aleksey B.,
Assistant Professor of the Department "Computer Security"
of the National Research University
"Higher School of Economics",
Candidate of Technical Sciences, Assistant Professor

The article investigates the problem of protecting information against the offender, which, according to experts, in recent time are becoming more and more popular. The urgency of this problem analyzes the causes and methods of insider activity, including methods of influence on the staff of the organization. Reviewed in detail the classification of insiders, their psychological types, the motivation for their activity, as well as a detailed analysis of possible damage. Proposed options for dealing with the insider, the main conclusions and recommendations.

Key words: *insider, insider information, causes and prevention of insider trading, the inner penetrator, the inner opposition to the offender.*

Введение

В последнее время в мире произошли существенные изменения в характере документооборота, большинство документов стали электронными. Данное обстоятельство упростило работу с информацией в части обработки, хранения и передачи. Однако открыло дополнительные возможности для деятельности различного рода злоумышленников, в том числе внутренних. Кардинально изменились типы и характер внутренних угроз, возросла вероятность потери информации, и, как итог, увеличилась вероятность нанесения ущерба организациям. Наиболее подвержены внутренним угрозам крупные организации, имеющие распределенную инфраструктуру. Как показывает практика, количество персонала и вычислительной техники организации прямо пропорционально скорости и объемам утечки информации. Учитывая значительное количество и разнообразие каналов утечки информации

(использование электронных носителей информации, мобильных устройств и т. д.), можно сказать, что обеспечение информационной безопасности организации, в том числе от внутреннего нарушителя, является весьма сложной задачей и, несомненно, является актуальной[1].

По мнению ведущих аналитических агентств (*InfoWatch* и т. д.), более 70 % всех инцидентов информационной безопасности являются внутренними, что подтверждает актуальность затронутой в статье проблемы. Сформулируем основные определения.

Инсайдер (англ. *insider*) — член какой-либо группы людей, имеющей доступ к информации, не доступной широкой публике. Термин используется в контексте, связанном с конфиденциальной, скрытой или какой-либо другой информацией или знаниями ограниченного распространения. Инсайдер — это член группы, обладающий информацией, имеющейся только у этой группы[2].

Инсайдерская информация (англ. *Insider information*) — существенная, публично не раскрытая информация, которая в случае раскрытия способна повлиять на состояние дел организации[3].

Мотивация и виды инсайдеров

Эксперты выделяют следующие основные причины инсайдерской деятельности:

1.Корысть — главная причина инсайдерской деятельности. Здесь уместно процитировать авторов книги «Безопасный аутсорсинг» М. Пауэра и Р. Тропа, которые писали: «По мере роста ценности данных, накопленных организацией, у посторонних лиц возрастает интерес к их получению, присвоению и ненадлежащему использованию»[4]. Следует отметить, что источником информации для «посторонних лиц» чаще всего являются не каналы связи и не устройства несанкционированного съема информации, а непосредственно работники организации — жертвы, у которых организуется хищение ценных данных. Под термином «корысть» в данном случае понимается не только прямое получение денег, но и любые другие выгоды, которые может получить в данной ситуации обладающий нужной информацией сотрудник: повышение собственной значимости и авторитета, назначение на более высокую должность или получение более высокооплачиваемой работы[5].

2.Чувство личной неприязни или просто попытка доставить неприятности работодателю, коллеге является серьезным мотивом для противоправных действий с информацией. Например, увольняемый администратор уничтожает все файлы на сервере и т. д.

3.Шантаж. Например, работника организации заставляют незаконно передать информацию под страхом расправы над семьей и т. д.

4.Некомпетентность и халатность работников. При отсутствии контроля и реакций на инциденты безопасности персонал организации постепенно перестает выполнять инструкции. В результате возникают ошибочные действия пользователей с непредсказуемыми последствиями.

Рассмотрим наиболее известные классификации инсайдеров.

Компания IDC (*International Data Corporation* — международная исследовательская и консалтинговая компания, занимающаяся изучением мирового рынка информационных технологий и телекоммуникаций) — предлагает делить нарушителей на четыре категории: граждане, нарушители, отступники, предатели[6].

Граждане — сотрудники, лояльно относящиеся к организации. Они практически никогда не нарушают корпоративную политику и, по сути, не являются угрозой для внутренней безопасности.

Нарушители являются основной массой сотрудников организации. Данные сотрудники позволяют себе «небольшие» вольности, такие как: работа с персональной электронной почтой, игра в компьютерные игры и т. д. Действия нарушителей создают угрозу безопасности, но возникающие в результате этого инциденты являются случайными.

Отступники — сотрудники, злоупотребляющие своими привилегиями, такими как до-

[1] National Business-Perm // URL: https://issuu.com/nb-perm/docs/ nb2012

[2] Инсайдерские угрозы // URL: http://www.mirash.ru/doki16.html

[3] Раскрытие информации как базовый принцип функционирования рынка ценных бумаг // URL: http://www.studfiles.ru/preview/2839475/

[4] Психологические причины инсайда // URL: http://insideinform.ru/page/psihologicheskie-prichiny-insajda

[5] Равилов Д. Методы классификации внутренних нарушителей // URL: http://infocom.uz/2009/12/16/metodyi-klassifikatsii-vnutrennih-narushiteley/

[6] Там же.

ступ в сеть Internet и т.д. Например, самовольно устанавливают P2P-клиенты и другие аналогичные сервисы и в дальнейшем используют их для передачи корпоративной информации заинтересованным в ней внешним адресатам. Отступники являются серьезной внутренней угрозой для организации.

Предатели — самый коварный и осторожный вид внутренних нарушителей. В данную категорию входят сотрудники, умышленно и регулярно ставящие под угрозу конфиденциальную информацию организации. Как правило, данные действия совершаются за материальное вознаграждение со стороны заинтересованных лиц. Данный вид нарушителей достаточно сложно выявить, поскольку они совершают противоправные действия продуманно и осторожно[7].

Данная классификация является простой и понятной, однако не дает полного представления об инсайдерах. В ней не затронуты такие важные поведенческие аспекты, как мотивация, последовательность действий, методы и цели инсайдеров. К тому же не совсем четко прослеживается взаимосвязь между классификацией нарушителей и проблемой обеспечения целостности и конфиденциальности информации. Компания *InfoWatch* предложила метод классификации инсайдеров, сосредоточив внимание на защите данных от утечек, искажения и уничтожения. Инсайдеры разделены на шесть типов: халатный, манипулируемый, обиженный, нелояльный, подрабатывающий и внедренный[8].

Халатные инсайдеры — самый распространенный вид внутренних нарушителей. В данную категорию обычно попадают среднестатистические сотрудники организации, обладающие невысоким уровнем компьютерной грамотности, а также рассеянные и невнимательные сотрудники. Все нарушения данной категории инсайдеров в части конфиденциальности информации ничем не мотивированы и не преследуют каких-либо целей. Они нарушают правила хранения и работы с конфиденциальной информацией, мотивируя свои действия только лучшими побуждениями. Угрозы, создаваемые ими, носят незлонамеренный, неправленный характер, например, сотрудники пытаются унести информацию с целью поработать дома, теряют носители информации и т. д.

Манипулируемые инсайдеры в большинстве своем являются жертвами социальной инженерии. По мнению многих экспертов, именно социальная инженерия сегодня является одной из самых острых проблем безопасности информационных систем[9].

Обиженные нарушители — сотрудники, стремящиеся нанести урон организации, преследуя свои личные цели. Как правило, нарушителями движет обида, возникшая из-за недостаточной оценки их роли, например, отказ в выделении корпоративных статусных атрибутов: автомобиля, корпоративного телефона, низкая зарплата, маленькая должность и т. д.

Нелояльные инсайдеры — сотрудники, планирующие в ближайшее время сменить место работы. Именно эти сотрудники попадают под подозрение в первую очередь, если речь заходит о внутренних угрозах. Как показывает практика, семь из десяти сотрудников при увольнении забирают с собой часть доступной им информации, будь то база клиентов или же документы. Чаще всего доступ к закрытой информации нарушители получают, имитируя производственную необходимость, что в свою очередь может привести к их разоблачению. В некоторых случаях данная информация является залогом комфортного увольнения с полагающейся компенсацией и рекомендательными письмами[10].

Нелояльные и обиженные инсайдеры могут легко превратиться в мотивированных извне[11].

Подрабатывающие инсайдеры — сотрудники, решившие дополнительно заработать.

Внедренные инсайдеры — к данному типу нарушителей относятся сотрудники, устраивающиеся на работу только с целью получения доступа к конкретной информации для ее похищения, удаления или искажения. Например, системному администратору крупной компании поступает очень выгодное предложение о переходе на другую работу.

---

7 Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. СПб: Питер, 2008.

8 Инсайдерские угрозы в России // URL: http://www.securitylab.ru/ analytics/368176.php#_Toc221433879

9 Кабанов А.С., Суроев А.В., Лось А.Б. Методы социальной инженерии в сфере информационной безопасности и противодействие им // Российский следователь. 2015. № 18.

10 Равилов Д. Указ. соч.

11 Инсайдерские угрозы в России...

Ему предлагают более высокую зарплату, гибкий график работы, медицинскую страховку, покрывающую все виды лечения. Администратор, не задумываясь, пишет заявление об увольнении. В это время в службу по работе с персоналом данной компании поступает превосходное резюме аналогичного специалиста с рекомендательными письмами и высокой квалификацией. Разумеется, в данной ситуации организация принимает его на работу. В результате, пока старый администратор сдает дела, новый уже получает доступ к конфиденциальной информации и передает ее заказчику. После этого агентство, предложившее новую работу администратору, и новый специалист исчезают, организация остается без корпоративных секретов, а системный администратор — без работы[12].

Подрабатывающие и внедренные инсайдеры — самый расчетливый и неуловимый тип.

Нетехнические методы профилактики и противодействия инсайдерской деятельности

В чистом виде технические решения не всегда эффективны в борьбе с инсайдерской деятельностью, поэтому активно используют организационные и организационно-технические методы.

Организационные методы охватывают широкий спектр методов противодействия инсайдерской деятельности и представляют собой набор политик безопасности организации. В зависимости от типов информации (секретная, конфиденциальная и т. д.), с которой работает организация, разрабатывается конкретный набор процедур.

В политике безопасности, с которой каждый сотрудник в обязательном порядке должен ознакомиться, должны быть изложены положения по обеспечению режима конфиденциальности информации. Целесообразно проинформировать сотрудников о последствиях утечки информации и ответственности за нарушения установленного режима.

Значительную роль в защите от инсайдерской деятельности играет работа с персоналом. Противодействие инсайду осуществляется на следующих основных этапах работы с персоналом:

1. При приеме на работу. В данном случае основная цель — это предупреждение трудоустройства внедряемого агента или сотрудника, который может стать инсайдером в силу своих психологических или других характеристик. Например, вследствие обстоятельств на работе (снижение зарплаты и т. д.) и личных обстоятельств (долги и т. д.)[13].

2. В процессе работы. С.И. Журин в работе «Автоматизированная система предупреждения совершения преступлений как составная часть системы безопасности важного государственного объекта» предложил следующую концепцию противодействия инсайду:

1) создание условий невозможности совершения преступления:

— информационно (система организационно-технических мер);

— физически (система физической защиты);

— психологически (система управления персоналом);

— организационно (система разграничения полномочий и т. д.);

— юридически (система санкций);

— технологически (система защиты от аварий):

2) создание системы мониторинга информации о сотрудниках и прогнозирования совершения преступлений;

3) создание системы психологической и должностной коррекции;

4) создание системы внутреннего аудита;

5) наличие системы внешнего аудита.

3. При увольнении. В данном случае основные задачи: анализ знаний сотрудника, сферы его дальнейшей работы, корректировка системы защиты и работа с увольняемым сотрудником (наблюдение и т. д.).

Рассмотрим основные нетехнические способы профилактики и противодействия инсайдерской деятельности.

Работа с кадрами включает в себя[14]:

1. Оценку благонадежности кандидатов. Сюда входит: анализ личного дела и трудовой книжки, заполнение различных анкет, проверка данных об образовании, сбор данных о личных качествах среди бывших коллег, проверка

[12] Равилов Д. Указ. соч.

[13] Журин С.И. Инсайдер: основная характеристика и комплексность противодействия // URL: http://pvti.ru/data/file/bit/bit_4_2011_34.pdf

[14] Кохен Ф. Нетехнические методы противодействия инсайдерским угрозам // URL: http://www.securitylab.ru/analytics/473402.php

на склонность к мошенничеству, испытательный срок. Неотъемлемыми этапами являются собеседования:

с сотрудником кадровой службы для проверки данных;

с сотрудником службы безопасности для сравнения имеющегося досье с информацией, полученной из других источников;

со специалистом по предполагаемому направлению работы на предмет соответствия требованиям к профессиональным качествам.

В особых случаях, например при назначении на высокопоставленные должности, можно применить проверку на полиграфе, но это требует привлечения грамотных специалистов в данной области и соответствующих знаний нормативно-правовой базы[15].

2. Анализ психологических типов работников. В ряде случаев для систематизации типов сотрудников руководствуются идеями Карла Густава Юнга. Он высказал мысль о том, что поведение человека не является случайным, а поддается анализу и, следовательно, классификации. По его мнению, различия в поведении определяются базовыми психическими функциями, свойственными человеку на протяжении всей его жизни. В своей работе «Психологические типы» К. Юнг выделил различные типы людей в соответствии с индивидуальными способами восприятия и оценки информации. В частности, он предложил три пары полярных шкал, описывающих психические процессы восприятия и обработки информации: **«экстраверсия — интроверсия», «сенсорика — интуиция», «мышление — эмоции»**[16].

Шкала «экстраверсия (**E**) — интроверсия (**I**)» описывает предпочтения человека в отношении используемых установок. Карл Юнг предложил различать две основные установки человека: установку на внешний мир, мир окружающих вещей (экстраверсию) и установку на внутренний мир собственных мыслей, переживаний, представлений (интроверсию).

Шкала «сенсорика (**S**) — интуиция (**N**)» описывает предпочитаемые человеком пути сбора информации. Существует два разных способа восприятия действительности: путь ощущений (сенсорика) и интуиции.

Шкала «мышление (**T**) — эмоции/чувства (**F**)» характеризует процессы принятия человеком решений. Концепция Карла Юнга предполагает наличие двух основных предпочтений в отношении принятия решений или вынесения суждений: путь, опирающийся на логику, объективное и беспристрастное мышление, и путь, строящийся на основе субъективной системы ценностей, личных пристрастий и чувств.

К. Бриггс и И. Бриггс-Майерс добавили еще одну шкалу — **«оценка — восприятие»** — и разработали опросник MBTI (Myers-Briggs Type Indicator) для диагностики психологического типа личности[17].

Шкала «оценка (**J**) — восприятие (**P**)» описывает предпочитаемый человеком способ взаимодействия с внешним миром. Согласно К. Бриггс, существует еще одна пара установок: установка на оценку информации и установка на восприятие информации. Эта пара определяет, какой из двух функций (функцией сбора информации или функцией принятия решений) человек пользуется при общении с внешним миром.

В итоге комбинации предпочтений по каждой шкале позволяют выделить 16 различных психологических типов личности, каждый из которых для удобства обозначается формулой, включающей названия наиболее выраженных признаков.

Например, тип ESTP — экстровертированный (**E**), предпочитающий получать информацию об окружающем мире при помощи своих органов чувств (**S**), ориентированный на мышление (**T**), склонный занимать созерцательную позицию (P). Кроме того, существуют и другие, менее распространенные, но заслуживающие внимания характеристики психологических типов. Например, ESTJ — администратор, ISTJ — инспектор, ESTP — маршал, ESFJ — энтузиаст и т. д. Разумеется, подобные названия не могут адекватно заменить формулу психологического типа, а в ряде случаев его чрезмерно общий характер и вовсе ведет к игнорированию важных различий, искажению представлений о человеке, но тем не менее указанные названия весьма распространены и популярны.

Ряд исследований показывает, что роль нарушителя более свойственна типам ESTP, ESFP,

[15] Там же.

[16] Дрозд А.В. Психология на службе ИБ. Психотипы. Защита информации // INSIDE. 2014. № 6.

[17] Там же.

то есть вероятность того, что представитель данного типа окажется инсайдером, значительно выше, чем у других указанных типов[18].

3. Прикрепление наставника. В ходе испытательного срока опытный сотрудник может помочь недавно принятому на работу коллеге быстрее адаптироваться к внутренним требованиям организации, объективно оценить отношение кандидата к порученному делу и грамотно довести до сведения руководства возникшие затруднения и проблемы.

4. Повышение лояльности сотрудников.

В связи с кризисом и возникающей волной сокращений многие сотрудники организации боятся увольнений, что часто приводит к появлению негативных настроений в трудовом коллективе. Если оставить данную проблему без внимания, то вероятность возникновения инсайдерских угроз резко возрастет[19].

Существуют различные способы повышения лояльности, как материальные, так и нематериальные. Для создания атмосферы доверия руководству необходимо:

строго выполнять все условия договора;

обеспечить справедливое вознаграждение сотрудника за проделанную работу (выплата процентов с прибыли от проектов и т. д.);

создать комфортные условия труда;

обеспечить профессиональный и карьерный рост;

проводить мероприятия для объединения коллектива (team-building);

понимать, что ограничения (технические или организационные) существенно влияют на рабочий процесс и моральное состояние персонала.

Технические методы противодействия инсайдерской деятельности

При использовании технических методов основной задачей службы безопасности является своевременная и обоснованная оценка возможных угроз. Важно также соблюдать баланс «цена — качество — производительность», который позволит использовать ресурсы, выделенные на средства защиты, с максимальной эффективностью, не снижая производительность труда сотрудников излишним контролем и техническими ограничениями.

Наиболее распространены следующие источники угроз инсайдерской деятельности и методы противодействия им[20].

1. Мобильные устройства (ноутбуки, смартфоны и т. д.). Варианты противодействия могут быть следующие:

а) физическое отключение всех интерфейсов (Usb-портов и т. д.);

б) программное блокирование интерфейсов (*Device Lock* и т. д.);

в) использование специализированного терминального программного обеспечения, которое будет работать с данными исключительно на сервере;

г) подавление сигналов или создание высокочастотных помех.

2. Средства мгновенного обмена сообщениями *(Instant messenger, IM).*

В данном случае предотвратить утечку можно двумя способами:

а) блокировка всего исходящего трафика на шлюзе (если имеется);

б) запрет на использование средств IM.

Указанные способы, разумеется, имеют свои слабые стороны и зачастую просто неприменимы, например, когда общение с клиентами / партнерами происходит с использованием ICQ и т. д. В этом случае можно уменьшить число сотрудников, которые имеют доступ к IM, тем самым сузив круг подозреваемых в случае утечки информации. Весьма полезной окажется централизованное архивирование трафика. Но если используется шифрование — выявить факт утечки будет сложно.

3. Использование Web-технологий. Наиболее распространенными способами противодействия являются:

а) блокировка всех сайтов, за исключением необходимых для работы;

б) мониторинг HTTP-трафика.

В первом случае на шлюзе устанавливается специальное программное обеспечение, которое по спискам доступа (или даже без них) разрешает тем или иным пользователям доступ к определенным сайтам.

Мониторинг HTTP-трафика подразумевает использование систем ILD&P *(Information*

---

[18] Дин Д. Типы личности в состоянии стресса // URL: http://ru.laser.ru/socion/references/dean/index.html

[19] Репин М. Причины возникновения инсайда и борьба с ними. Методы повышения лояльности сотрудников // URL: http://www.univermvd.ru/files/other-files/Диссертация2015.pdf

[20] Инсайдеры: теория противодействия // URL: http://www.gfs-team.ru/articles/read/142

Leakage Detection and Prevention) или, как их еще называют, DLP *(Data Leak Prevention)*, которые представляют собой комплекс программных решений для мониторинга потоков информации и предотвращения утечек. Традиционно выделяются три класса подобных решений:

мониторинг и фильтрация почтового/IM/Web-трафика;

слежка за действиями пользователя, в том числе и над определенными типами документов;

решения, предусматривающие более глобальный подход к проблеме, в которых реализован мониторинг всех возможных каналов передачи, хранения и обработки данных, а также централизованное управление для руководителя службы безопасности.

Таким образом, использование указанных средств может не только помочь в расследовании, но и предотвратить утечку информации. Например, инсайдер неосторожно вел переписку со своим заказчиком, и, благодаря проведенному морфологическому анализу текста почтового трафика, сработала система контроля.

4. Кража оборудования. Хищение является проблемой организационно-технического характера. Рекомендации следующие:

а) учет всех вносимых / выносимых предметов;

б) использование камер наблюдения.

Возникают следующие проблемы. Во-первых, вынести краденый жесткий диск или ноутбук из любого здания можно в обход контрольного пункта, а во-вторых, камеры наблюдения если и помогут, то вполне возможно будет уже поздно. Очевидно, что для решения данной проблемы необходимо шифрование конфиденциальной информации.

Рассмотрим основные **методы и средства выявления инсайдеров** и их деятельности.

В зависимости от направления вредоносной деятельности инсайдеров применяются следующие комплексы средств и систем :

1. Для противодействия **кражам** применяются:

DLP-система — контроль периферийных устройств: вывод документов на печать, на внешние носители, на сетевые средства и др.;

Security Information and Event Management — комплекс, состоящий из устройств, устанавливаемых на различных частях компьютерной системы с целью мониторинга и анализа активности пользователей (SIEM-система). Комплекс включает модули сбора информации от устройств и блок анализа аномальной активности пользователей (например, увеличение числа обращений к определенным документам, попытки подбора паролей и т. д.);

2. Для противодействия **шпионажу** применяются:

honeypot (пер. с англ. — «горшочек с медом», представляет собой муляж какой-либо части компьютерной системы), *honeytoken* (в отличие от *honeypot*, не предполагает наличие аппаратной части) — при активном поиске конфиденциальных данных нарушитель может найти, например, файл со специально подготовленной парой логин-пароль, вымышленными персональными данными, служебной информацией. Использование такого файла расценивается как инсайдерская деятельность;

DLP-система: факты наличия шпионажа могут быть выявлены средствами корпоративной компьютерной системы;

SIEM-система: выявление аномалий в работе пользователей — увеличений числа обращений к определенным документам и т. д.;

3. Для предотвращения **случайных, непреднамеренных** действий применяются:

SIEM-система: выявление отклонений от заданных режимов работы;

DLP-системы выявляют передачу конфиденциальных данных, отправленных по ошибке.

SIEM-системы из-за значительной стоимости подходят большим распределенным компаниям (более 1000 ПЭВМ и множество средств защиты информации). Для малых и средних коммерческих структур оптимальным средством для предотвращения инсайдерских угроз является внедрение DLP-систем, а также периодический контроль действий сотрудников как способ выявления аномального поведения.

Выводы

1. Лучший способ минимизации рисков инсайда — правильный подбор персонала.

2. Существенное влияние на противодействие инсайду оказывает повышение лояльности сотрудников и сплочение коллектива.

3. Для эффективной борьбы с инсайдом необходима система комплексных мер, включаю-

щая в себя как организационные, так и технические меры.

4. В настоящее время имеется достаточно широкий комплекс мер противодействия инсайду, поэтому эффективность мер в значительной мере зависит от внимания руководства к данной проблеме и профессионализма службы безопасности.

Литература

1. Кабанов А.С., Суроев А.В., Лось А.Б. Методы социальной инженерии в сфере информационной безопасности и противодействие им // Российский следователь. 2015. № 18.
2. National Business-Perm // URL: https://issuu.com/nb-perm/docs/ nb2012
3. Инсайдерские угрозы // URL: http://www.mirash.ru/ doki16.html
4. Раскрытие информации как базовый принцип функционирования рынка ценных бумаг. Служебная (инсайдерская) информация // URL: http://www.studfiles.ru/preview/2839475/
5. Психологические причины инсайда // URL: http://insideinform.ru /page /psihologicheskie- prichiny-insajda
6. Равилов Д. Методы классификации внутренних нарушителей // URL: http://infocom.uz/2009/12/16/metodyi-klassifikatsii-vnutrennih-narushiteley/
7. Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. СПб.: Питер, 2008.
8. Инсайдерские угрозы в России // URL: http://www. securitylab.ru/ analytics/368176.php#_Toc221433879
9. Журин С.И. Инсайдер: основная характеристика и комплексность противодействия // URL: http://pvti.ru/data/file/bit/bit_4_2011_34.pdf
10. Журин С.И. Автоматизированная система предупреждения совершения преступлений как составная часть системы безопасности важного государственного объекта. М.: МИФИ, 2000. 130 с.
11. Кохен Ф. Нетехнические методы противодействия инсайдерским угрозам // URL: http://www.securitylab.ru/analytics/473402.php
12. Дрозд А.В. Психология на службе ИБ. Психотипы. Защита информации // INSIDE. 2014. № 6.
13. Дин Д. Типы личности в состоянии стресса // URL: http://ru.laser.ru/socion/references/dean/index.html
14. Репин М. Причины возникновения инсайда и борьба с ними. Методы повышения лояльности сотрудников // URL: http://www.univermvd.ru/files/other-files/Диссертация2015.pdf
15. Инсайдеры: теория противодействия // URL: http://www.gfs-team.ru/articles/read/142
16. Веденеев В.С., Бычков И.В. Средства поиска инсайдеров в корпоративных информационных системах // URL: http://pvti.ru/ data/file/bit/2014-1/part_2.pdf