DOI: 10.17117/no.2014.01.033

Поступило в редакцию: 03.11.2014

<http://ucom.ru/doc/no.2014.01.033.pdf>

vka@mil.ru

Нечай А.А., Минухина Л.С., Котиков П.Е. Финансовые риски при утечке информации

Nechay A.A., Minuhina L.S., Kotikov P.E.
Financial risks of information leakage

Статья посвящена актуальному экономическому вопросу финансовых рисков при потере информации. Сегодня информация играет большую роль в жизни любой компании или государственной организации, чем пару десятков лет назад. Ценным является также рассмотрение возможных рисков, угроз и их классификации, а также технологических путей несанкционированного доступа

Ключевые слова: финансовые риск, утечка информации, угрозы информации, классификация угроз, несанкционированный доступ, утечка конфиденциальной информации

Нечай Александр Анатольевич

Преподаватель

Военно-космическая академия им. А.Ф. Можайского
г. Санкт-Петербург, ул. Ждановская, 13

Минухина Лариса Сергеевна

Курсант

Военно-космическая академия им. А.Ф. Можайского
г. Санкт-Петербург, ул. Ждановская, 13

Котиков Павел Евгеньевич

Кандидат технических наук, доцент

Военно-космическая академия им. А.Ф. Можайского
г. Санкт-Петербург, ул. Ждановская, 13

The article is devoted to the economic, financial and o risks of information loss. Today, information plays a much greater role in the life of any company or government organization than a couple of decades ago. Valuable is also the consideration of possible risks, threats and their classification, as well as technological ways unauthorized access

Key words: financial risk, leakage of information, threat information, classification of threats, unauthorized access, leakage of confidential information

Nechay Alexander Anatolievich

Teacher

Military space Academy Alexander Mozhaisky
St. Petersburg, Zhdanov st., 13

Minuhina Larisa Sergievna

Cadet

Military space Academy Alexander Mozhaisky
St. Petersburg, Zhdanov st., 13

Kotikov Pavel Evgenievich

Candidate of Technical Sciences, associate Professor

Military space Academy Alexander Mozhaisky
St. Petersburg, Zhdanov st., 13

Сегодня информация играет большую роль в жизни любой компании или государственной организации, чем пару десятков лет назад. Кто владеет информацией, тот владеет миром, а кто владеет чужой информацией, тот гораздо лучше подготовлен к конкурентной борьбе, чем его соперники.

Чем чреваты сегодня утечки конфиденциальной информации для тех, кто их допускает?

Внедрение новых информационных технологий ставит современные компании в зависимость от информационной системы, а переход на электронные носители информации приводит к необходимости уделять пристальное

внимание вопросу информационной безопасности. Любое вмешательство в работу информационной системы: кража, уничтожение или несанкционированный доступ к данным может привести к значительным убыткам компании, а иногда и к ее полной ликвидации, особенно если эти данные касаются ее коммерческих тайн или ноу-хау.

Обеспокоенность внутренними угрозами информационной безопасности обоснована. Госструктуры и представители бизнес-сектора ставят на первое место утечку информации далеко не случайно, так как негативные последствия этого инцидента очевидны: прямые финансовые убытки, удар по репутации, потеря клиентов. Сравнение индексов обеспокоенности внутренними и внешними угрозами ИБ показывает, что именно инсайдерские риски преобладают в списке наиболее опасных угроз. Более того, наибольший рейтинг опасности приходится на утечку конфиденциальной информации.

Согласно данным портала информационной безопасности Content Security степень опасности внутренних и внешних угроз такова:

- разглашение (излишняя болтливость сотрудников) – 32%;
- несанкционированный доступ путем подкупа и склонения к сотрудничеству со стороны конкурентов и преступных группировок – 24%;
- отсутствие в фирме надлежащего контроля и жестких условий обеспечения информационной безопасности – 14%;
- традиционный обмен производственным опытом – 12%;
- бесконтрольное использование информационных систем – 10%;
- наличие предпосылок возникновения среди сотрудников конфликтных ситуаций, связанных с отсутствием высокой трудовой дисциплины, психологической несовместимостью, случайным подбором кадров, слабой работой кадров по сплочению коллектива – 8%.

Наиболее актуальными и значимыми, как это ни печально, оказываются угрозы, источником которых выступают пользователи системы и ее обслуживающий персонал, то есть сотрудники компаний. Такая тенденция подтверждается не только различными исследованиями крупнейших аудиторских компаний, но и отмечается в ежегодных докладах МВД России, посвященных правонарушениям в сфере информационной безопасности.

Нельзя сказать, что проблема утечек информации появилась совсем недавно – такие вещи, как промышленный шпионаж, переманивание ценных специалистов вместе с их наработками и знаниями и другие подобные действия известны уже достаточно давно.

Каким образом можно оценить возможный ущерб от утечки конфиденциальных данных?

Для начала необходимо свериться со списком возможных источников ущерба:

- Упущенная выгода в результате испорченного имиджа;
- Штрафы со стороны регуляторов;
- Компенсации по судебным искам;
- Снижение котировок акций (для акционерных компаний) в результате попадания на рынок инсайдерской информации;

– Прямые убытки: стоимость разработки технологических решений, стоимость проигранных в результате утечек данных тендеров и т.д.

Каждая утечка информации «ставит галочку» напротив как минимум одного из перечисленных выше пунктов, наиболее серьезные же утечки способны «преподнести» компании весь этот список. Соответственно, общая сумма ущерба от каждой конкретной утечки информации складывается из «цены» каждого источника ущерба.

Конечно, не для всех перечисленных пунктов подсчитать возможную стоимость ущерба достаточно просто.

Если, к примеру, штрафы со стороны регуляторов или стоимость технологических разработок подсчитать не так уж сложно, то предсказать, как поведет себя рынок ценных бумаг в ответ на обнародованные инсайдерами документы, или сколько клиентов отвернутся от компании в результате ухудшившейся репутации, практически невозможно. Поэтому в своих оценках лучше не придерживаться оптимистической позиции «все обойдется», а закладывать в «бюджет» утечки максимально возможную сумму ущерба.

К сожалению, достоверных исследований, которые показывали бы среднюю стоимость утечки информации в России, пока нет, однако можно ориентироваться на данные для других стран, которые вряд ли будут существенно отличаться.

Так, согласно исследованиям Ponemon Institute, средняя стоимость утечки информации для фирм в Великобритании в 2008 г. составила 1,7 млн. фунтов, то есть почти 80 миллионов российских рублей.

Еще одна цифра: в среднем убытки при потере служебного ноутбука составляют почти 50 тыс. долларов – такие данные были получены после опроса представителей 29 организаций, которые пережили 138 отдельных случаев потери ноутбуков их постоянными или временными сотрудниками, пишет Ру-форматор со ссылкой на PCWorld. Такая сумма получена с помощью учета семи различных факторов: цены самого ноутбука, определения потерянных данных, экспертизы и расследования обстоятельств потери, сообщения об утечке данных и действий по смягчению последствий инцидента, потери интеллектуальной собственности, потери производительности, а также других юридических и нормативных затрат.

Эксперты также подсчитали, что чем быстрее компания реагирует на утрату компьютера, тем меньшие потери она несет.

Если потерю ноутбука удалось обнаружить в тот же день, то затраты могут составить в среднем лишь 8 950 долларов. Спустя неделю они могут достичь уже 115 849 долларов.

Шифрование данных приводит к существенному снижению финансовых потерь при утрате компьютера.

Так, если информация на жестком диске ноутбука была зашифрована, потеря обходится в 37 443 долларов, если нет, – то в 56 165 долларов.

Наконец, финансовые потери напрямую зависят от того, какую должность в компании занимает человек, потерявший компьютер или лишившийся его в результате кражи.

Наибольшей ценностью обладает ноутбук не высшего должностного лица компании, а директора или менеджера. Потеря ноутбука топ-менеджером обходится в среднем в 28 449 долларов, но если его потеряли директор или менеджер, сумма возрастает до 60 781 долларов и 61 040 долларов соответственно. Это свидетельствует о высоком уровне риска для корпоративных сетей, потому что доступ к сайтам для взрослых, поиск работы на подозрительных ресурсах и другие виды нецелевого использования рабочих ноутбуков могут привести к серьезным утечкам информации, а иногда и к проникновению вредоносного ПО в сеть организации.

Для чего оценивать возможный ущерб от утечек информации?

Прежде всего, для того, чтобы понять, какую цену в действительности имеет конфиденциальная информация, которой обладает организация, а также оценить выгоду от внедрения средств защиты от утечек информации (например, DLP-систем – от английского Data Leak Prevention, предотвращение утечек данных). Выгода, конечно же, есть, когда стоимость возможных утечек хотя бы в 2 раза превышает стоимость внедрения подобной системы. Как показывает практика, для подавляющего большинства компаний внедрение DLP-системы действительно целесообразно.

Защита от внутренних угроз.

Ни для кого не секрет, что в среднем 82 % угроз информационным ресурсам компаний исходят от действий собственных сотрудников, совершаемых ими либо по неосторожности, либо преднамеренно. По прогнозам экспертов, опасность внутренних угроз имеет тенденцию к росту и является по-прежнему одной из самых злободневных проблем. В условиях жесткой конкурентной обстановки особенно актуальной является задача по сохранению конфиденциальности данных.

Ошибочно отправленное электронное письмо, сообщение ICQ или выводимые на печать документы могут содержать конфиденциальные сведения, не предназначенные для посторонних лиц. Коммерческая или служебная тайна, персональные данные клиентов, партнеров или сотрудников, а также иные виды защищаемой информации могут попасть в руки к третьим лицам и нанести бизнесу непоправимый ущерб. Необходимо своевременно принять меры для предотвращения рисков, связанных с утечкой конфиденциальной информации.

Возможные риски:

– Финансовые риски – результатом утечки конфиденциальных данных может быть ситуация, когда коммерческая тайна становится известной третьим лицам. В случае попадания такой информации в руки конкурентов существует высокая вероятность финансовых потерь, нередко приводящих к банкротству компании.

– Правовые риски – бесконтрольный выход конфиденциального документа за пределы корпоративной сети может стать предметом пристального внимания со стороны регулирующих органов. Судебные иски и штрафные санкции за нарушение норм законодательства, регулирующих защиту персо-

нальных данных и иных видов конфиденциальной информации, не является редким явлением.

– Репутационные риски - утечка конфиденциальных данных может получить широкую огласку в СМИ и привести к разрушению имиджа компании в глазах ее клиентов и партнеров, став причиной серьезного финансового ущерба.

Для обеспечения защиты от утечек информации должна быть предусмотрена DLP-система.

DLP-системы (от англ. Data Loss Prevention) – программные или программно-аппаратные средства, предназначенные для защиты от утечек по сетевым и локальным каналам. Передаваемые данные анализируются на предмет их конфиденциальности и распределяются по определенным категориям (общедоступная информация, персональные данные, коммерческая тайна, интеллектуальная собственность и др.). Если в информационном потоке детектируются данные конфиденциального характера, DLP-система выполняет одно из следующих действий: разрешает их передачу, блокирует или отправляет на дополнительную проверку специалисту по безопасности в неоднозначных случаях.

DLP-системы охватывают широкий комплекс коммуникационных каналов, позволяя отслеживать электронную почту, службы мгновенных сообщений и иной интернет-трафик, принтеры, Bluetooth-устройства, USB-устройства и другие внешние носители.

Существующие DLP-системы различаются набором функциональных возможностей.

Во-первых, DLP-системы могут быть активными (обнаруживают и блокируют утечку данных) и пассивными (обнаруживают утечку данных и высылают оповещение об инциденте). В настоящее время акцентируется внимание на активных DLP-системах, основная задача которых – предотвращение утечки данных в режиме реального времени, а не выявление ее постфактум. Для таких DLP-систем можно при желании настроить режим мониторинга, позволяющий не вмешиваться в бизнес-процессы и направлять сообщение об инциденте специалисту по безопасности.

Во-вторых, DLP-системы могут решать ряд дополнительных задач, связанных с контролем действий сотрудников, их рабочего времени и использования корпоративных ресурсов.

Весомый плюс DLP-систем заключается в том, что они позволяют сохранять непрерывность бизнес-процессов, практически не влияя на работу конечных пользователей. Благодаря всем вышеперечисленным возможностям DLP-системы в настоящий момент – одно из самых востребованных решений для обеспечения информационной безопасности бизнеса.

Правильное внедрение и настройка DLP-системы – отдельный сложный вопрос. Здесь невозможно обойтись без грамотного консалтинга. Высококвалифицированные специалисты компании «Инфозащита» помогут с выбором решения, соответствующего специфике Вашего предприятия.

Современный рынок DLP – один из самых быстрорастущих, что ярко демонстрирует высокий спрос на подобные системы защиты. Разработчики DLP-решений постоянно развивают и совершенствуют новые эффективные технологии для борьбы с утечками данных.

Угрозы информационной безопасности. Классификация угроз

Построение надежной защиты информационной системе организации невозможно без предварительного анализа возможных угроз безопасности системы.

Под угрозой безопасности информации понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Угрозами информационной безопасности называются потенциальные источники нежелательных событий, которые могут нанести ущерб ресурсам информационной системы.

Все угрозы безопасности, направленные против программных и технических средств информационной системы, в конечном итоге оказывают влияние на безопасность информационных ресурсов и приводят к нарушению основных свойств хранимой и обрабатываемой информации.

Угрозы информационной безопасности различают по следующим основным признакам:

По характеру возмущающих воздействий на систему угрозы разделяются на случайные или непреднамеренные и умышленные.

Источником непреднамеренных угроз могут быть выход из строя аппаратных средств, неправильные действия работников информационной системы или ее пользователей, непреднамеренные ошибки в программном обеспечении и т.д. Такие угрозы следует держать во внимании, так как ущерб от них может быть значительным.

Умышленные угрозы в отличие от случайных преследуют цель нанесения ущерба управляемой системе или пользователям. Это делается нередко ради получения личной выгоды. Человека, пытающегося нарушить работу информационной системы или получить несанкционированный доступ к информации, обычно называют взломщиком, а иногда «компьютерным пиратом» (хакером).

По характеру нанесенного ущерба умышленные угрозы подразделяют на пассивные и активные.

Пассивные угрозы направлены в основном на несанкционированное использование информационных ресурсов ИС, не оказывая при этом влияния на ее функционирование. Например, несанкционированный доступ к базам данных, прослушивание каналов связи и т.д.

Утечка конфиденциальной информации – это бесконтрольный выход конфиденциальной информации за пределы ИС или круга лиц, которым она была доверена по службе или стала известна в процессе работы. Эта утечка может быть следствием:

– разглашения конфиденциальной информации;

- ухода информации по различным, главным образом техническим, каналам;
- несанкционированного доступа к конфиденциальной информации различными способами.

Разглашение информации ее владельцем или обладателем есть умышленные или неосторожные действия должностных лиц и пользователей, которым соответствующие сведения в установленном порядке были доверены по службе или по работе, приведшие к ознакомлению с ним лиц, не допущенных к этим сведениям.

Возможен бесконтрольный уход конфиденциальной информации по визуально-оптическим, акустическим, электромагнитным и другим каналам.

Несанкционированный доступ – это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям.

Наиболее распространенными путями несанкционированного доступа к информации являются:

- перехват электронных излучений;
- принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей;
- применение подслушивающих устройств (закладок);
- дистанционное фотографирование;
- перехват акустических излучений и восстановление текста принтера;
- чтение остаточной информации в памяти системы после выполнения санкционированных запросов;
- копирование носителей информации с преодолением мер защиты;
- маскировка под зарегистрированного пользователя;
- маскировка под запросы системы;
- использование программных ловушек;
- использование недостатков языков программирования и операционных систем;
- незаконное подключение к аппаратуре и линиям связи специально разработанных аппаратных средств, обеспечивающих доступ к информации;
- злоумышленный вывод из строя механизмов защиты;
- расшифровка специальными программами зашифрованной информации;
- информационные инфекции.

Перечисленные пути несанкционированного доступа требуют достаточно больших технических знаний и соответствующих аппаратных или программных разработок со стороны взломщика. Например, используются технические каналы утечки – это физические пути от источника конфиденциальной информации к злоумышленнику, посредством которых возможно получение охраняемых сведений.

Однако есть и достаточно примитивные пути несанкционированного доступа:

- хищение носителей информации и документальных отходов;

- инициативное сотрудничество;
- склонение к сотрудничеству со стороны взломщика;
- выпытывание;
- подслушивание;
- наблюдение и другие пути.

Любые способы утечки конфиденциальной информации могут привести к значительному материальному и моральному ущербу как для организации, где функционирует ИС, так и для ее пользователей.

Довольно большая часть причин и условий, создающих предпосылки и возможность неправомерного овладения конфиденциальной информацией, возникает из-за элементарных недоработок руководителей организаций и их сотрудников.

Например, к причинам и условиям, создающим предпосылки для утечки коммерческих секретов, могут относиться:

- недостаточное знание работниками организации правил защиты конфиденциальной информации и непонимание необходимости их тщательного соблюдения;
- использование неаттестованных технических средств обработки конфиденциальной информации;
- слабый контроль за соблюдением правил защиты информации правовыми, организационными и инженерно-техническими мерами;
- текучесть кадров, в том числе владеющих сведениями, составляющими коммерческую тайну;
- организационные недоработки, в результате которых виновниками утечки информации являются сотрудники.

Большинство из перечисленных технических путей несанкционированного доступа поддаются надежной блокировке при правильно разработанной и реализуемой на практике системе обеспечения безопасности. Но борьба с информационными инфекциями представляет значительные трудности, так как существует и постоянно разрабатывается огромное множество вредоносных программ, цель которых – порча информации в базах данных и программном обеспечении компьютеров. Большое число разновидностей этих программ не позволяет разработать постоянных и надежных средств защиты против них.

Список литературы:

1. Николаева Т.П. Основы информационной экономики. СПб.: ЛЕКС СТАР, 2001. С. 128.
2. Федеральный закон «Об информации, информатизации и защите информации» от 25 января 1995 года № 24-ФЗ.
3. Федеральный закон Российской Федерации "О государственной тайне" от 21 июля 1993 года N 5485-1.
4. Федеральный закон Российской Федерации «О коммерческой тайне» от 29 июля 2004 г. N 98-ФЗ.
5. Ильин А.И., Волков В.П. Экономика предприятия. М.: Новое знание, 2003. С. 677.
6. Нечай А.А. Выявление недеklarированных возможностей аппаратно-программного обеспечения // Экономика и социум. 2014. № 1-2 (10). С. 457-460.
7. Лохвицкий В.А., Калинин С.В., Нечай А.А. Подход к построению системы автоматизированной интеграции информации в базу данных для её своевременной актуализации // Мир современной науки. 2014. № 2 (24). С. 8-12.

References:

1. Nikolaeva T.P. *Basis of the information economy*. SPB.: LEX STAR, 2001. P. 128.
2. Federal law "On information, Informatization and protection of information" dated January 25, 1995 № 24-FZ.
3. Federal law of the Russian Federation "On state secrets" dated July 21, 1993 N 5485-1.
4. Federal law of the Russian Federation "On commercial secrets" dated 29 July 2004, № 98-FZ.
5. Ilyin A.I., Volkov V.P. *Business Economics*. M.: New knowledge, 2003. P. 677.
6. Nechay A.A. *Detection of undeclared capabilities of the device-but-software // Economy and society*. 2014. № 1-2 (10). Pp. 457-460.
7. Lohvitski C.A., Kalinichenko S.C., Nechay A.A. *Approach to building a system for automated integration of data into a database for its timely update // the World of modern science*. 2014. № 2 (24). Pp. 8-12.

© 2014, Нечай А.А., Минухина Л.С., Котиков П.Е.
Финансовые риски при утечке информации

© 2014, Nechay A.A., Minuhina L.S., Kotikov P.E.
Financial risks of information leakage