- перелік охороняючих від ТЗНОІ характеристик ОЗ з оцінкою повноти віддзеркалення їх інформативними ТДО, що відносяться до видової і сигнальної КІ;

- вимоги по ефективності захисту КІ щодо ОЗ в умовах сектора інформаційного ресурсу, що є на об'єкті.

3. Процедура обґрунтування технології забезпечення безпеки КІ щодо ОЗ передбачає:

- кількісну оцінку значущості ОЗ на базовому (нормативному) показнику технічного рівня ОЗ;

- кількісну оцінку інформативності КІ щодо ОЗ, що застосовується в умовах приховування інформативних ТДО від зловмисників;

- кількісну оцінку ТЕЕ заходів щодо організації і здійснення приховування КІ щодо ОЗ при виділених матеріальних ресурсах на здійснення захисту об'єкту;

- порівняльний аналіз розглянутих варіантів ТЕЕ технології захисту КІ щодо ОЗ прогнозну оцінки інтервалу часу, протягом якого гарантується безпека КІ.

Список літератури

1. Егоров Ф.И. – Задачи защиты информации / Егоров Ф.И., Тискина Е.О., Хорошко В.А. // Захист інформації, №1, 2009. – с.5-12.

2. Тискина Е.О. – Принципи построения систем управления безопасностью информации / Тискина Е.О., Хорошко В.А. // Вісник ДУІКТ, том 7, №3, 2009. – с.284-293.

3. Барткив Н.И. – Количественная оценка эффективности информационного обеспечения управления системой защиты информации / Барткив Н.И., Тискина Е.О., Хорошко В.А. // Захист інформації, №4, 2009. – с.25-29.

4. Кобозева А.А. – Анализ информационной безопасности / Кобозева А.А., Хорошко В.А. – К.: Изд. ГУИКТ, 2009. – 251с.

Представлені загальний підхід і принципи забезпечення захисту інформації від сукупності загроз її безпеки в умовах застосування зловмисником технічних засобів несанкціонованого отримання інформації.

Ключові слова: конфіденційна інформація, система захисту об’єкту, технічні засоби несанкціонованого отримання інформації, технічні демаскуючі ознаки.

Представлены общий подход и принципы обеспечения защиты информации от совокупности угроз ее безопасности в условиях применения злоумышленником технических средств несанкционированного получения информации.

Ключевые слова: конфиденциальная информация, система защиты объекта, технические средства несанкционированного получения информации, технические демаскирующие признаки.

General approach and principles of providing of priv is presented from the aggregate of threats its safety in the conditions of application of hardwares of unauthorized receipt of information a malefactor.

Key words: confidencial information, system for protection of an object, technical means for unauthorized receipt of information, technical disclosuring features.

Надійшла 20.01.2010

УДК 004.683

Печень С.А. (ГУИКТ)

СОВРЕМЕННЫЕ АНТИКРИЗИСНЫЕ МЕРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: БЛОКИРОВКА УТЕЧЕК ИНФОРМАЦИИ, КРИТИЧНЫХ ДЛЯ БИЗНЕС-ПРОЦЕССОВ ПРЕДПРИЯТИЯ

Как показывают современные исследования, чтобы сохранить работу, служащие готовы буквально на все, но если их все-таки уволят, ничто не остановит их от кражи ценной информации, принадлежащей работодателю, причем некоторые сотрудники уже имеют копию такой информации.

Например, в ходе последнего исследования American Management Association и ePolicy Institute 14% из 586 опрошенных сотрудников крупных американских компаний признались

в том, что они отправляли конфиденциальную или потенциально опасную или «неудобную» для их компании информацию лицам, которые не должны были о ней знать [4].

В ходе опроса «Мировая рецессия и ее влияние на рабочую этику» выяснилось, что треть из 600 офисных служащих (с Нью-йоркской Уолл-стрит, лондонского района Канари ворф, где располагаются офисы крупных банков и корпораций, а также из Амстердама, Голландия) подтвердили, что согласны работать 80 часов в неделю, причем четверть опрошенных готова к снижению зарплат при условии, что это позволит им сохранить работу [7]. Тем не менее, все эти работники за спиной у начальства пользуются своими правами доступа к конфиденциальной информации, которую они, не задумываясь, унесут с собой, если их все-таки уволят.

Сокращение – больная тема для опрашиваемых. 56% респондентов признали, что боятся потерять работу. Но если вдруг до них дойдут слухи, что они все-таки попали под сокращение, 46% опрошенных поспешат уйти не с пустыми руками. Они будут смотреть, что есть полезного в корпоративной сети, а если ничего там не обнаружат, то готовы предложить взятку знакомому IT специалисту, чтобы тот нашел для них что-нибудь ценное.

Как утечки повлияют на функционирование бизнес-процессов

При угрозе сокращения 71% опрошенных служащих планируют использовать на новом месте работы конфиденциальные данные прежнего работодателя.

Самое востребованное - это клиентские базы и контактная информация, что является ключевой информацией для функционирования бизнес-процессов поддержки потребителей и предоставления услуг. Утечка таких данных приведет к оттоку клиентской базы и как следствие – уменьшению доходов.

Для маркетинговых бизнес-процессов не менее важна информация о новых тарифах, акциях, планах и предложениях. В случае утечки этих данных конкуренты смогут предложить существующим и потенциальным клиентам более выгодные условия.

Информация о продуктах или услугах, новых разработках, паролях и кодах доступа повлияет на функционирование технологических бизнес-процессов. А это срыв производственных процессов, что приводит к упущенной выгоде, либо к судебным издержкам.

Меньше всего опрошенные служащие «мечтают» украсть базы HR-департамента, договоры и прочие юридические документы.

Нельзя не отметить, что оглашение самого факта утечки может негативно отразится на имидже предприятия.

Каналы утечек

Утечка служебной информации в интернет стала настоящим бедствием для различных компаний. Получив «горячую» конфиденциальную информацию, сотрудники часто стремятся поделиться ей (с умыслом или без оного) используя при этом современные способы коммуникации: электронную почту, Skype, персональные веб-хранилища, instant-messenger и как наиболее простой, доступный и одновременно широковещательный способ - публикация ее в интернете с использованием решений на базе технологии WEB 2.0. В частности, согласно порталу Alexa.com по посещаемости на Украине на первом месте сайт социальных сетей vkontakte.ru, а его ближайший конкурент odnoklassniki.ru на 6 месте [6]. Как следствие повсеместное распространение блогов и социальных сетей заставляет многие компании проводить переоценку системы управления коммуникациями и переориентировку на новые цели и задачи СУИБ [2,8].

Flash-носители – компактный, легкий, дешевый и в тоже время самый незаметный инструмент для кражи больших объемов данных, в качестве альтернативы им применяют фотокамеры, мобильные телефоны/смартфоны, iPod и другие mp3-плееры, CD/DVD, внешние HDD.

Несмотря на то, что мы живем в цифровую эпоху, нельзя не брать в расчет собственную память сотрудников. Так, согласно вышеуказанному исследованию 7% британцев признались, что просто запоминают важную информацию.

Разглашение конфиденциальной информации приводит к прямым материальным убыткам, потере интеллектуальной собственности, снижению репутации организации и уровня доверия клиентов и партнеров. Кроме этого, увеличивается риск финансовой ответственности компании за нарушение государственных норм, регулирующих процессы обработки конфиденциальных данных.

Решения в области DLP. Что такое DLP?

В данных условиях для защиты информации предприятия, сохранения конкурентоспособности и снижения возможного ущерба можно порекомендовать применение DLP-решений и ужесточение политики безопасности предприятия.

Предотвращение утечек (англ. Data Leak Prevention, DLP) - технологии предотвращения утечек конфиденциальной информации из автоматизированной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек. DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется.

Против утечек конфиденциальных данных традиционные методы защиты информации — разграничение доступа, шифрование и др. — практически бессильны. По этой причине применяются решения, опирающиеся на специализированные системы класса DLP, обеспечивающие:

- контроль наиболее распространенных каналов утечек;
- наличие базы для расследования инцидентов безопасности;
- расширение системы разграничения прав доступа к ресурсам до определения правил передачи данных во внешние сети.

Например: Symantec Data Loss Prevention; Websense Data Security Suite; InfoWatch Enterprise Solution.

Использование DLP–решений позволит попутно решить следующие вопросы повышения производительности труда, актуальные не только в кризис[3]:

- сколько часов тратят ваши сотрудники на работу, а сколько – на личные цели;
- какие веб-сайты, программы и приложения занимают лидирующие позиции в списке наиболее злостных непроизводительных «убийц рабочего времени»;
- на что рассчитывают, чего опасаются и что предполагают делать ваши подчиненные в ближайшие время в связи с кризисом;
- какие информационные опасности для вашей компании существуют в настоящий момент.

Отметим, что на практике большое число компаний порой годами использует такие системы только в режиме слежения (аудита), а не блокирования.

Прежде чем рассматривать противодействие утечкам, оценим близкие к ним или смежные по функционалу.

Системы защиты конфиденциальной информации от утечки по техническим каналам служат для обнаружения разного рода жучков, «закладок», устройств прослушивания и т. д. У данных систем похожие названия, но на этом сходство заканчивается — задачи они решают разные. Пожалуй, единственный общий элемент схем внедрения таких систем и DLP-решений лежит в управленческой плоскости. В обоих случаях необходимо определить перечень сведений конфиденциального характера и сформировать процесс отнесения информации к этому разряду.

Существует класс систем слежения за действиями сотрудников, к возможностям которых порой относят и выявление каналов утечки конфиденциальной информации. Обычно функционал таких систем включает тотальное журналирование всех действий пользователя, в том числе открытие им страниц в Интернете, работу с документами, отправку документов на печать, клавиатурные нажатия и т. д.

Безусловно, использование подобных систем может принести определенную пользу в борьбе с утечками данных. Но, во-первых, искать в огромном объеме логов придется силами отдельной группы специально обученных «надзирателей». Во-вторых, это все же постконтроль нарушений — блокировать саму утечку такой продукт не сможет.

Перед системами DLP стоит задача обнаружить, зафиксировать и локализовать утечку, однако необходимо также заблокировать канал утечки, а по возможности и предотвратить. Есть также класс решений по контролю операций с внешними устройствами, самым распространенным примером которых является съемный USB-накопитель. Такие системы нечувствительны по отношению к содержанию. Устройство может быть заблокировано вообще, могут блокироваться попытки записи на него файлов определенного объема или заданного формата. Однако предопределить действия СЗИ в зависимости от содержимого носителя невозможно.

Только несколько процентов наиболее дальновидных компаний увеличивают расходы на безопасность. Остальные вынуждены сокращать расходы, прежде всего на оборудование (42,1% организаций) и программное обеспечение (37,0% организаций). Приостанавливаются проекты без гарантированного результата, прекращается пора масштабных закупок. В этой ситуации возрастает роль консультантов и внедренцев, которые будут **доводить проекты до конца** и обеспечивать эффективность вложений в безопасность.

Согласно заключению Gartner Group : "Рынок систем предотвращения потери данных (data loss prevention - DLP) продолжает демонстрировать значительный рост, несмотря на тяжелые экономические условия во всем мире. В число причин продолжающегося укрепления этого рынка входят все большая зрелость предлагаемых технологий DLP и понимание покупателями того, что эти технологии могут помочь в соблюдении нормативных требований, которые во время кризиса становятся еще более строгими".

Важность ИБ не вызывает сомнений. Половина участников вышеуказанного исследования считает, что защита корпоративных секретов всегда является первоочередной задачей, а 22,7% респондентов заявили, что укрепление ИБ особенно важно в кризисные времена для повышения конкурентоспособности. Вместе с тем, безопасность не должна стать самоцелью. Наоборот, сегодня ИБ должна понимать нужды бизнеса и развиваться с ним в одном направлении.

- В первую очередь стоит пересмотреть перечень корпоративных секретов в изменившихся условиях и отношение к ним.
- Эффективным способом сокращения финансирования без ущерба для безопасности является перераспределение средств между статьями расходов. Более всего в сложившейся ситуации востребованы будут продукты для защиты информации от разворовывания. Также, компании переориентируются с интеграторов широкого профиля на решения целевых задач при помощи профессиональных консультантов по ИБ, предлагающих более качественные услуги за меньшие деньги. Например, применение внутрикорпоративных прокси-серверов на базе ОС Linux с возможностью внесения адресов социальных сетей и внешних файловых хранилищ (rapidshare.de,shareua.ua…) в списки блокировки доступа. Например Squid proxy-сервер.
- При отсутствии финансов на приобретение новых средств ИБ, целесообразно пересмотреть уже существующие решения и более полно использовать их возможности. Например, ограничение круга применения устройств хранения (usb-накопители, cd/dvd-носители …) за счет использования возможностей доменных политик безопасности ОС

Windows, хотя контролируемое использование внешних устройств возможно организовать и за счет утилит сторонних производителей (USB Disabler Pro, DeviceLock…).

•Автоматизация задач, выполнявшихся ранее вручную. К их числу могут быть отнесены анализ защищенности, установка патчей, управление инцидентами, управление политиками безопасности для средств защиты, их обновление, управление конфигурацией, опечатывание USB-портов компьютеров и т.п. Для каждого из этих классов задач на рынке существуют средства защиты, которые в среднесрочной перспективе могут обойтись дешевле стоимости одного сотрудника для компании.

•Запрет использования или ограничение круга применения тех решений, ущерб от которых может превысить «пользу». Например, отказ от использования внешних почтовых ящиков на бесплатных доменах, ICQ с выходом в Интернет, либо замена на внутрикорпоративные решения – например сервер ICQ на базе Linux, как альтернативное решение - расширение существующей функциональности путем применения Microsoft Office Communicator. Однако, в некоторых случаях, от них (ICQ,Skype…) отказываться не стоит – например, организация приема заявок от клиентов службой технической поддержки.

Выделение финансирования целесообразно прежде всего, на ИБ-проекты с быстрой и очевидной отдачей. Особую роль будет играть профессионализм и оперативность внедренцев ИБ-решений.

Список литературы

1. Хорошко В.А., Чекатков А. А. Методы и средства защиты информации/Под. ред. Ю.С. Ковтанюка. - К.:Юниор, 2003.- 504 с.

2. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты.- К.:ООО «ДС», 2001.-688 с.

3. С.А. Печень. Корпоративная безопасность при доступе сотрудников к наиболее популярным ресурсам сети интернет-ДУІКТ, 2008. – с.65-71.

4. Кризис «протекает» в интернет. http://www.finansmag.ru/news/26919

5. 38% of large US companies have full-time email monitoring staff Dept of snooping and personnel. http://www.theregister.co.uk/2009/08/18/email_monitoring/

6. Top Sites in Ukraine. http://alexa.com/topsites/countries/UA

7. Генина.Н. Кризис: инсайдеры вооружаются. C-News. http://www.cnews.ru/news/top/index.shtml?2008/12/01/329882

8. С.А. Печень. Анализ работы существующих ТЕХНОЛОГИЙ защиты информации корпоративных СЕТЕВЫХ ресурсов -ДУІКТ, 2008.

9. HOWTO: Use Group Policy to disable USB, CD-ROM, Floppy Disk and LS-120 drivers. http://support.microsoft.com/kb/555324.

В статье предложено применение DLP-решений и ужесточение политики безопасности предприятия в условиях кризиса для защиты информации предприятия, сохранения конкурентоспособности и снижения возможного ущерба.

Ключевые слова: бизнес-процессы, информационная безопасность, DLP-решения.

В статті запропоновано застосування DLP-рішень і посилювання політики безпеки підприємства в умовах кризи для захисту інформації підприємства, збереження конкурентоспроможності і зниження можливого збитку.

Ключові слова: бізнес-процеси, інформаційна безпека, DLP-рішення.

The given article is devoted to the usage of DLP-decisions and toughening of a security policy of the enterprise in the crisis situation for protection of the information of the enterprise, preservation of competitiveness and decrease in a possible damage.

Key words: business-processes, information security, DLP(data leak prevention)-decisions.

Поступила 26.11.2010