**«Защита от внутренних угроз на предприятиях связи»**

2008 г.

# **СОДЕРЖАНИЕ**

Введение

1. Самые громкие инсайдерские инциденты в области телекоммуникаций

2. Внутренние нарушители

3. Законы в области защиты от внутренних угроз

3.1. Правовое и нормативное регулирование

3.2. Сертификация по международным стандартам

4. Статистические исследования

5. Методы предотвращения внутренних утечек

Заключение

Список использованной литературы

# **ВВЕДЕНИЕ**

Актуальность темы обусловлена тем, что в связи с массовым характером предоставления услуг связи в базах данных телекоммуникационных компаний могут быть аккумулированы записи миллионов и десятков миллионов граждан. Именно они и нуждаются в наиболее серьезной защите. Как показала практика, в результате пренебрежения опасностью утечки бизнес рискует потратить сотни миллионов долларов на PR-кампании, судебные издержки и новые средства защиты персональной информации клиентов.

Специфика защиты информации в телекоммуникационных компаниях проявляется в характере тех данных, которые необходимо защищать. Вся информация хранится в базах данных, находящихся в IT-инфраструктуре оператора. Кража чревата сразу несколькими негативными последствиями. Во-первых, это может ударить по репутации компании, что проявляется в оттоке существующих клиентов и трудностях в привлечении новых. Во-вторых, фирма нарушает требования закона, что может привести к отзыву лицензии, судебным издержкам, дополнительному ущербу для имиджа.

Целью работы является изучение защиты от внутренних угроз на предприятиях связи.

Задачами работы являются:

- рассмотрение самых громких инсайдерских инцидентов в области телекоммуникаций;

- анализ внутренних нарушителей;

- изучение законов в области защиты от внутренних угроз: правовое и нормативное регулирование и сертификация по международным стандартам;

- изучение статистических исследований;

- рассмотрение методов предотвращения внутренних утечек.

Работа состоит из пяти глав.

В первой главе рассматриваются самые громкие инсайдерские инциденты в области телекоммуникаций, во второй главе рассматриваются внутренние нарушители, в третьей главе анализируются законодательная база в области защиты от внутренних угроз, в четвертой главе рассматриваются статистические исследования, в пятой главе приводятся методы предотвращения внутренних утечек.

В заключении содержатся выводы по проведенному исследованию.

## **Самые громкие инсайдерские инциденты в**

## **области телекоммуникаций**

Реальные инциденты являются наиболее наглядной иллюстрацией всей серьезности угрозы от инсайдеров. Пренебрежение этой опасностью в 2006 г. привело к крупному скандалу в США. Журналисты за $90 купили список входящих и исходящих вызовов бывшего кандидата в президенты США, генерала Уэсли Кларка, и американская общественность с удивлением обнаружила, что телефонные записи, во-первых, вообще не защищены законом, а, во-вторых, очень плохо защищены операторами мобильной связи.

В январе 2007г. информационные агентства сообщили об одной «неочевидной» утечке. В Интернете появилась база данных пользователей мобильной связи от «Корбина телеком»: фамилии, номера телефонов, гарантийные взносы почти 40 тыс. абонентов, в том числе нескольких топ-менеджеров компании. Комментарии «Корбины» в некоторой степени успокоили клиентов. Скорее всего, под видом новой базы, предлагалась информация 4-летней давности. Тогда программист-инсайдер действительно выложил в свободный доступ сведения об абонентах компании, и за это время информация почти полностью потеряла свою актуальность. [1]

В десятку самых громких инсайдерских инцидентов вошла кража клиентской базы японского сотового оператора KDDI. Под угрозой раскрытия информации о крупной утечке данных инсайдеры требовали $90 тыс. у японской корпорации KDDI – второго по величине оператора сотовой связи в стране. Чтобы продемонстрировать обоснованность своих угроз, в мае 2006 г. шантажисты предъявили представителям KDDI компакт-диски и USB-флешки с приватными данными, подбросив их на проходную. Однако менеджмент компании проигнорировал требования преступников и обратился к правоохранительным органам. В течение двух недель полицейские контролировали переговоры шантажистов и KDDI, а потом арестовали подозреваемых. Расследование показало, что в руки шантажистов действительно попала база приватных сведений о 4 млн. клиентов KDDI. Каждая запись базы содержала имя, пол, дату рождения, телефоны, почтовые адреса каждого клиента. Все эти данные идеально подходят для осуществления кражи личности. Топ-менеджмент уверен, что один из служащих специально скопировал сведения и вынес их за пределы компании.

В целом, более 200 работников имели доступ к украденным данным.

Не менее громкий инцидент произошел ближе к России: утечка базы данных белорусского сотового оператора Velcom. Журналисты приобрели текстовый файл с информацией о номерах телефонов и ФИО 2 млн. его абонентов. При этом пресса отмечает, что базы данных Velcom регулярно становятся достоянием общественности: с 2002 г. вышло как минимум шесть вариантов, причем каждый раз информация дополнялась. Между тем базы данных МТС в белорусском Интернете по-прежнему отсутствуют. Столкнувшись с волной критики, Velcom заявила, что белорусские законы не защищают персональные данные граждан, а значит, никаких юридических претензий к Velcom быть не может. Оператор обвинил в утечке банк, которому была передана база данных клиентов «для возможности проверки работниками [банка] правильности указанных реквизитов при оплате услуг связи». После этого Velcom «рассматривает возможность предъявления иска о защите деловой репутации». К чему приведет разбирательство, покажет время, но пока инсайдеры слишком часто уходят от ответственности.

Октябрь 2006 г. Инсайдеры из индийского телекома Acme Tele Power украли результаты инновационных разработок и передали их фирме-конкуренту Lamda Private Limited. По оценкам Ernst & Young, прямые финансовые убытки Acme составили $116 млн. Любопытно, что интеллектуальная собственность «утекла» самым обычным способом – по электронной почте. После этого компания Acme Tele Power собирается вообще перенести свой бизнес из Индии в Австралию. [2]

## **2. внутренние нарушители**

Очень многие организации проводили исследования в сфере внутренних утечек. Наиболее крупные и известные - исследования Uncertainty of Data Breach Detection, проведенного Ponemon Institute [4]; исследования западных аналитиков: CSI/FBI Computer Crime and Security Survey [5]. Таблица 1 иллюстрирует одно из таких исследований.

**Табл. 1. Самые опасные угрозы ИБ по совокупному ущербу в долларах**

|  |  |
| --- | --- |
| *Угрозы* | *Ущерб (в долларах)* |
| Вирусы | $ 15 691 460 |
| Неавторизованный доступ | $ 10 617 000 |
| Кража ноутбуков | $ 6 642 560 |
| Утечка информации | $ 6 034 000 |
| Отказ в обслуживании | $ 2 992 010 |
| Финансовое мошенничество | $ 2 556 900 |
| Злоупотребление сетью или почтовыми инсайдерами | $ 1 849 810 |
| Телеком-мошенничество | $ 1 262 410 |
| Зомби-сети в организации | $ 923 700 |
| Взлом системы извне | $ 758 000 |
| Фишинг (от лица организации) | $ 647 510 |
| Злоупотребление беспроводной сетью | $ 469 010 |
| Злоупотребление интернет-пейджерами инсайдерами | $ 291 510 |
| Злоупотребление публичными веб-приложениями | $ 269 500 |
| Саботаж данных и сетей | $ 260 00 |

Можно добавить только, что в комментариях по объему ущерба аналитики FBI и Института компьютерной безопасности скептически относятся к тому, что респонденты смогли более или менее точно определить объем убытков в связи с утечкой персональных данных или коммерческих секретов. Такие инциденты имеют множество долгосрочных отрицательных последствий. Например, ухудшение общественного мнения, снижение репутации и сокращение клиентской базы. Все это происходит постепенно и занимает недели и месяцы. А для выявления убытков в виде недополученной вследствие утечки прибыли требуется как минимум год. Так что внутренняя структура финансовых потерь из-за угроз ИБ не поддается точному определению.

В целом защита информации в организациях включает в себя [3]:

* совокупность компьютеров, связанных между собой в сеть;
* каналы связи, реализованные произвольными каналами передачи информации, через которые физически реализуется сеть логических связей;
* обмен конфиденциальной информацией внутри сети в строгом соответствии с допустимыми логическими связями
* интегрированная многоуровневая защита от несанкционированного доступа и внешнего воздействия
* жесткое централизованное задание структуры логических связей и разграничение доступа внутри сети
* независимость логической структуры сети от типов каналов передачи информации.

Большинство компаний уже давно построило защиту от внешних угроз, и теперь им требуется защитить тылы. Среди внутренних угроз можно выделить несколько наиболее распространенных способов нанесения ущерба:

* неавторизованный доступ в систему (ПК, сервер, БД);
* неавторизованный поиск/просмотр конфиденциальных данных;
* неавторизованное изменение, уничтожение, манипуляции или отказ доступа к информации, принадлежащей компьютерной системе;
* сохранение или обработка конфиденциальной информации в системе, не предназначенной для этого;
* попытки обойти или взломать систему безопасности или аудита без авторизации (кроме случаев тестирования системы безопасности или подобного исследования);
* другие нарушения правил и процедур внутренней безопасности сети.

Существует несколько путей утечки конфиденциальной информации:

* почтовый сервер (электронная почта);
* веб-сервер (открытые почтовые системы);
* принтер (печать документов);
* FDD, CD, USB drive (копирование на носители). [6]

Прежде чем переходить к аналитическим выкладкам, необходимо ответить на вопрос, что же все-таки называется внутренней угрозой. Важность этого определения усиливается еще и тем, что саботаж — лишь часть внутренних угроз, следует различать саботажников и, например, инсайдеров, «сливающих» конфиденциальную информацию конкурентам.

Корпоративный саботаж — это вредительские по отношению к компании действия, совершенные инсайдерами в силу уязвленного самолюбия, желания отомстить, ярости и любых других эмоциональных причин. Заметим, что под емким термином «инсайдер» понимаются бывшие и нынешние сотрудники предприятия, а также служащие-контрактники.

Корпоративные диверсии всегда совершаются из эмоциональных, порой нерациональных побуждений. Саботажник никогда не руководствуется желанием заработать, не преследует финансовую выгоду. Этим, собственно, саботаж и отличается от других инсайдерских угроз.

Исследование Секретной службы США установило, что в 98% случаев диверсантом является мужчина. Однако эти мотивы представляют собой следствия более ранних событий, которые вывели служащего из равновесия (Табл. 2). По сведениям аналитиков, в большинстве случаев саботажу предшествует неприятный инцидент на работе или серия таких инцидентов.

Табл. 2 События, предшествующие саботажу

|  |  |
| --- | --- |
| Конфликт | 20% |
| Увольнение | 47% |
| Отсутствие повышения | 13% |
| Другие | 20% |

Источник СЕRT

Многие саботажники на момент совершения диверсии являются уже бывшими сотрудниками компании-жертвы, сохранившими доступ к ее информационным ресурсам по каким-то причинам (вероятно, оплошности администратора). Заметим, это почти половина всех случаев.

Как показало исследование CERT, практически все корпоративные диверсанты являются специалистами, так или иначе связанными с информационными технологиями.

Табл. 3 Портрет типичного саботажника

|  |  |
| --- | --- |
| Инженер | 14% |
| Программист | 21% |
| Системный администратор | 38% |
| Специалист по IT | 14% |
| Другое | 13% |

Источник СЕRT

Таким образом, из наиболее достоверных черт саботажника можно выделить всего две: это мужчина, сотрудник технического департамента. Девять из десяти диверсий совершаются людьми, так или иначе связанными с информационными технологиями. По мнению экспертов компании InfoWatch, разработчика систем защиты конфиденциальной информации от инсайдеров, причина такой профессиональной принадлежности кроется в психологических особенностях этих служащих. Подробнее разобраться в проблеме позволят два примера из жизни, наиболее ярко иллюстрирующие типичные черты характера IT-профессионалов.

«Я работал в средней по величине компании, занимающейся разработкой программного обеспечения. При доступе к основным серверам у меня были привилегии администратора. Только чтобы размять свой ум, я обдумывал, как можно использовать этот доступ злонамеренно, и разработал следующий план. Во-первых, взломать систему резервного копирования... Во-вторых, подождать год или дольше. В-третьих, стереть всю информацию на серверах, включая взломанное программное обеспечение для шифрования/дешифрования резервных данных. Таким образом, у предприятия останутся лишь зашифрованные резервные копии (без ключа). В-четвертых, предложить компании купить ключи, которые удалось получить еще на первом шаге. Если фирма откажется, то потеряет годы своей работы. Это, конечно, всего лишь гипотетический план. Я не пытался претворить его в жизнь, поэтому не знаю, сработал бы он или нет…», — Филиэс Купио (Filias Cupio). «Большинство специалистов по информационным технологиям, которых я знаю, даже еще начинающие ребята, сразу же при вступлении в должность первым делом устанавливают программу скрытого управления (rootkit) в корпоративную систему. Это рефлекс. Ребята не хотят никому навредить и не строят вредоносных планов, им просто нужен надежный доступ к системе, чтобы можно было спокойно работать из дома или колледжа», — Бен.

Глубокая психологическая подоплека акта саботажа часто приводит к тому, что рассерженный служащий угрожает начальству или сослуживцам. Иногда он даже делится своими мыслями с кем-то из коллег. Другими словами, информация о готовящейся диверсии есть не только у саботажника. Аналитики подсчитали, что в 31% случаев сведениями о планах диверсанта располагают другие люди. Из них 64% — коллеги, 21% — друзья, 14% — члены семьи, а еще 14% —сообщники.

В 47% случаев диверсанты совершают подготовительные действия (например крадут резервные копии конфиденциальных данных). В 27% — конструируют и проверяют механизм атаки (готовят логическую бомбу в корпоративной сети, дополнительные скрытые входы в систему и т. д). При этом в 37% случаев активность сотрудников можно заметить: из этого количества 67% подготовительных действий заметны в режиме online, 11% — offline, 22% — обоих сразу.

Следует также учесть, что подавляющее большинство атак производится саботажниками в нерабочее время и с помощью удаленного доступа к корпоративной сети. [7]

## **3. Законы в области защиты от внутренних угроз**

### Правовое и нормативное регулирование

Специфика сектора телекоммуникаций (по сравнению с другими отраслями) проявляется и в вопросах нормативного регулирования. Во-первых, компании этой отрасли часто ориентированы на предоставление услуг физическим лицам, а потому аккумулируют в своей корпоративной сети огромные объемы персональных данных абонентов. Отсюда пристальное внимание руководства департаментов ИТ и ИБ к ФЗ «О персональных данных», который предъявляет целый ряд требований к безопасности приватных сведений граждан***.*** Во-вторых, телеком не так давно обзавелся собственным стандартом под названием «Базовый уровень информационной безопасности операторов связи» [8]. Он представляет собой минимальный набор рекомендаций, реализация которых должна гарантировать определенный уровень ИБ коммуникационных услуг, позволяя обеспечить баланс интересов операторов, пользователей и государства. Разработка этого норматива обусловлена развитием телекоммуникационной отрасли: операторы связи вынуждены объединять свои сети, чтобы предоставлять необходимый набор услуг, однако сами операторы не знают, с кем они имеют дело и кому они могут доверять, чтобы избежать угроз ИБ [9]. Некоторые положения этого документа напрямую касаются внутренних рисков ИБ и проблем сохранения персональных данных. Например, оператору рекомендуется «обеспечивать конфиденциальность передаваемой и/или хранимой информации систем управления и автоматизированных систем расчета за услуги связи (биллинга), сведений об абонентах (персональных данных физических лиц) и оказываемых им услугах связи, ставших известными операторам связи в силу исполнения договоров об оказании услуг связи». От компаний требуют вести журналы регистрации событий ИБ и хранить их согласно срокам исковой давности (в России – 3 года). Более того, «для фильтрации потока первичных событий рекомендуется применять технические средства корреляции событий, оптимизирующие записи в журналах инцидентов по информационной безопасности». Нельзя обойти вниманием пункт, который гласит: «Оператору, допустившему утрату баз данных абонентов (клиентов) других (взаимодействующих) операторов, рекомендуется информировать последних об этом в кратчайшие сроки». Таким образом, российский сектор телекоммуникаций постепенно приближается к передовому опыту – в США и ЕС компании уже давно несут ответственность за утечку приватных данных и по закону обязаны поставить пострадавших в известность об утечке. Со временем такая норма должна появиться и в России.

Правда, утверждать, что нормативное регулирование играет определяющую роль в секторе телекоммуникаций, пока нельзя. Тем не менее руководству уже сегодня следовало бы задуматься о соответствии ИТ и ИБ существующим стандартам и законам на тот случай, если надзорные органы начнут наконец действовать. Кроме того, крупные телекоммуникационные компании, чьи акции котируются на биржах, обязаны удовлетворять требованиям фондовых рынков. В России, например, это необязательный Кодекс корпоративного поведения ФСФР (Федеральная служба по финансовым рынкам), в Британии – Объединенный кодекс корпоративного управления (полуобязательный), а в США – закон SOX (Sarbanes-Oxley Act of 2002). ФЗ «О персональных данных» и «Базовый уровень…» представляют непосредственный интерес для российских телекоммуникационных компаний.[10]

ФЗ «О связи» (ст. 46, п. 1) возлагает на оператора такие функции ИБ, как защита сооружений связи, средств связи и передаваемой по ним информации от несанкционированного доступа; обеспечение безопасности функционирования внутренней инфраструктуры оператора связи.

Требования эти необходимо реализовывать в системе функционирования сети связи, контролировать их работоспособность, сопровождать эксплуатацию, готовить и представлять в вышестоящие инстанции статистическую отчетность. Однако из-за отсутствия координирующих нормативных положений единого подхода к обеспечению безопасности информации не существует. Нет общего подхода и к составу подразделений ИТ и ИБ. Это, как правило, зависит от объема выполняемых оператором задач, а функциональные обязанности между ИТ и ИБ распределяются исходя из предыдущего опыта руководителей этих подразделений.

### Сертификация по международным стандартам

Самая известная в мире сертификация – по требованиям стандарта ISO 27001:2005. В России на сегодняшний день официально сертифицировали свои системы управления информационной безопасностью (СУИБ) шесть компаний; четыре из них работают в сфере ИТ. Стандарт ISO/IEC27001:2005, выпущенный British Standards Institute в 2005 г., основан на лучших мировых практиках. Он четко определяет ключевые процессы, которыми необходимо управлять менеджеру, отвечающему за обеспечение ИБ в организации. Согласно этому стандарту, заключительный этап подтверждения эффективности системы ИБ – проведение независимой проверки аккредитованным органом по сертификации. Положительное заключение такого органа свидетельствует об эффективном и корректном обеспечении процессов управления ИБ, о позитивном имидже фирмы, а для ее руководства служит убедительным аргументом, что в ИС предприятия используются современные средства обеспечения ИБ с максимальным уровнем эффективности. Сам процесс проверки внешним органом по сертификации повышает степень доверия руководства к ИБ-подразделениям, являясь показателем качества и профессионализма сотрудников этой службы.

Решение о внедрении СУИБ в организации должно приниматься на самом высоком уровне управления, в идеале – генеральным директором. Без поддержки руководства такие проекты нередко обречены на провал, в лучшем случае – на неэффективное функционирование в условиях неприятия процессов работниками фирмы.

В документе X.sbno из рекомендаций ITU-Т,основанном на «Базовом уровне…», все требования разделены на три вида:

1. В требованиях к политикам определена необходимость зафиксированной (утвержденной) внутренними процедурами предприятия связи политики безопасности, основанной на лучших практиках оценки и управления рисками, отвечающей нуждам деловой деятельности и соответствующей национальному законодательству. Политики безопасности должны быть опубликованы и доведены до сведения персонала оператора связи и внешних участников (клиентов, взаимодействующих операторов, других заинтересованных лиц).
2. В требованиях к функциональности описаны требования только к имеющимся сертифицированным техническим средствам, описываются процедуры журналирования событий.
3. В требованиях к взаимодействию описан порядок идентификации собственных клиентов и других операторов. В подразделе указывается на необходимость наличия круглосуточной службы реагирования на инциденты безопасности (или использования такой службы на правах аутсорсинга).

Существует также требование обеспечения конфиденциальности передаваемой и/или хранимой информации для систем управления и автоматизированных систем расчета за услуги связи (биллинга), сведений об абонентах (персональных данных физических лиц) и оказываемых им услугах связи. При этом оно должно соблюдаться и в том случае, если эта информация стала известна оператору связи в силу исполнения договоров об оказании услуг связи. [11]

## **Статистические исследования**

Одной из самых масштабных и интересных работ в области защиты от внутренних угроз оказалось исследование 275 телекоммуникационных компаний, проведенное аналитическим центром InfoWatch. Согласно его результатам, инсайдерские риски превалируют над внешними угрозами в соотношении 6:4. Проанализируем структуру этих рисков и влияние на них различных факторов: используемых средств защиты информации, нормативного регулирования и др.

Список самых опасных внутренних угроз информационной безопасности (Табл. 4) возглавили нарушение конфиденциальности информации (85%) и искажение информации (64%). Обе эти угрозы можно обобщить понятием «утечка информации».

На третьей–четвертой позициях – мошенничество (49%) и саботаж (41%). Интересно, что в проводившемся общеотраслевом исследовании угроза саботажа почти на 15% опережает риск мошенничества. Видимо, в силу специфики предоставления услуг связи мошенничество признано одной из наиболее опасных угроз.

Табл. 4 Самые опасные угрозы ИБ

|  |  |
| --- | --- |
| Нарушение конфиденциальности информации | 85% |
| Искажение информации | 64% |
| Мошенничество | 49% |
| Саботаж | 41% |
| Утрата информации | 25% |
| Сбои в работе ИС | 18% |
| Кража оборудования | 11% |
| другое | 7% |

Оценивая негативные последствия утечки конфиденциальной информации, респонденты должны были указать две самые нежелательные, на их взгляд, позиции из предложенного списка ( Табл.5). Оказалось, что больше всего они дорожат своей репутацией и общественным мнением (51%), а потеря клиентов (43%) для них страшнее прямых финансовых убытков (36%) – показателя, который лидировал в общеотраслевом исследовании.

Табл. 5 Негативные последствия утечки информации

|  |  |
| --- | --- |
| Удар по репутации и плохое паблисити | 51% |
| Потеря клиентов | 43% |
| Прямые финансовые убытки | 36% |
| Снижение конкурентно способности | 29% |
| Преследование регулирующими или правоохранительными органами | 21% |
| Потеря партнеров | 18% |
| Судебное преследование и юридические издержки | 2% |

Интересно, что лишь 2% респондентов опасаются, что утечка информации повлечет за собой юридические издержки и судебное преследование. Это однозначно свидетельствует о неразвитости правоприменительной практики в России. Напомним, что в феврале 2007 г. в России вступил в силу Федеральный закон «О персональных данных», позволяющий привлечь к ответственности компанию, допустившую их утечку. Однако эксперты InfoWatch сомневаются, что «правильный» закон положит конец незаконному распространению персональных данных. Для того чтобы это осуществилось на практике, должно появиться не одно судебное решение, наказывающее организации, виновные в утечке информации.

Табл. 6 Каналы утечки информации

|  |  |
| --- | --- |
| Мобильные накопители | 85% |
| Электронная почта | 83% |
| Интернет (веб-почта форумы | 81% |
| Интернет пейджеры | 77% |
| Печатающие устройства | 65% |
| Фотопринадлежности | 30% |
| другие | 2% |

Что касается наиболее распространенных каналов утечки информации (Табл.6), то здесь результаты исследования телекоммуникационного сектора почти полностью повторили общеотраслевые результаты исследования экономики.

Одним из самых важных стал вопрос о количестве утечек конфиденциальной информации, допущенных респондентами в 2006 г. (Табл.7). Как и в других отраслях, лидером оказалось безликое «Затрудняюсь ответить»: выяснилось, что почти никто из опрашиваемых не использует специализированные решения для выявления утечек. И все-таки положительные сдвиги есть: если в общеэкономическом исследовании затруднения с ответом возникли у 44,8% респондентов, то в секторе телекоммуникаций уже только у 38%. Вывод: представители телекома лучше осведомлены об утечках, чем компании других секторов, что свидетельствует о более серьезном отношении к проблемам ИБ [10].

Табл. 7 Количество утечек информации

|  |  |
| --- | --- |
| 1-5 утечек | 31% |
| 6-25 утечек | 14% |
| Более 25 утечек | 2% |
| Нет утечек | 15% |
| Затрудняюсь ответить | 38% |

### Степень влияния законов на бизнес предприятий связи

Респондентам предлагалось оценить степень влияния закона на свой бизнес (Табл.8). Оказалось, что сегодня этот закон почти не работает(10): подавляющее большинство опрошенных (58%) определили его влияние как «несильное», а каждый четвертый (24%) заявил, что закон вообще ни на что не влияет. И лишь 18% организаций видят в этом документе серьезный фактор влияния на бизнес. Но в целом в отрасли бытует мнение, что ФЗ «О персональных данных» – беззубый норматив.

Табл. 8 Оценка влияния ФЗ «О персональных данных» на бизнес компании

|  |  |
| --- | --- |
| Сильно влияет | 18% |
| Влияет, но не сильно | 58% |
| Вообще не влияет | 24% |

По мнению экспертов InfoWatch, подавляющее большинство опрошенных операторов реально оценивают закон. Выдвигая общие требования, этот нормативный акт не определяет, как именно операторы обязаны обеспечить конфиденциальность приватных сведений – получается, по собственному разумению. Более того, в ФЗ в явном виде не предусмотрена ответственность за утечку информации для руководства или бизнеса.

И наконец, федеральный орган, уполномоченный следить за выполнением закона (ФСТЭК России), до сих пор не выпустил стандарт безопасности для персональных данных. Поэтому неясно, какие же меры по обеспечению конфиденциальности закон и регулирующие органы считают достаточными. Отсутствует в России и правоприменительная практика в сфере борьбы с утечками. [10]

Стандарт «Базовый уровень информационной безопасности операторов связи» существует пока лишь в виде рекомендаций Международного союза электросвязи и российской Ассоциации документальной электросвязи. Следование им в каждой стране будет зависеть от требований государственного регулирования. Однако российские регуляторы, вероятно, смогут использовать эти рекомендации в качестве лицензионных условий, а некоторые операторы – в качестве условий присоединения к собственной сети связи. Более того, оператор может предоставлять телекоммуникационные услуги с уровнем безопасности, гарантируемым при выполнении «Базового уровня…», а услуги с повышенным уровнем безопасности – на возмездной основе. Другими словами, «Базовый уровень…» имеет все шансы стать драйвером развития ИБ в телекоммуникационном секторе. Это мнение разделяет и большинство респондентов исследования InfoWatch.

Интересны результаты углубленного опроса респондентов: все они слышали о «Базовом уровне…», но 30% признались, что недостаточно хорошо знакомы с его требованиями. Хотя «Базовый уровень…» уже сегодня рекомендует оповещать пострадавших об утечке информации, он все же не фокусирует внимание на внутренних угрозах ИБ. Опрашиваемым было предложено определить необходимость включения в «Базовый уровень…» требований к защите от внутренних угроз, таких, например, как утечка персональных и конфиденциальных данных (Рисунок 4.6). Разработчикам стандарта, вероятно, стоило бы выделить этот источник угроз ИБ для телекоммуникационных компаний.

Табл. 9 Включить ли в «Базовый уровень…» требования к защите от внутренних угроз?

|  |  |
| --- | --- |
| Да, обязательно | 18% |
| Скорее да | 41% |
| Скорее нет | 10% |
| Нет, не нужно | 31% |

### Средства защиты

Наиболее популярными средствами ИБ в телекоммуникационных компаниях (Рисунок 4.7) оказались антивирусы (100%), межсетевые экраны (79%) и контроль доступа (68%).

В целом представители этого сектора используют больше различных продуктов и решений, чем российские компании из других секторов экономики. Между тем некоторые опасения вызывает малочисленность организаций, реализующих защиту от утечки данных, – всего 8%. В среднем по отраслям этот показатель равняется 10,5%.

Табл. 10 Используемые средства ИБ

|  |  |
| --- | --- |
| Антивирусное ПО | 100% |
| Межсетевые экраны | 79% |
| Контроль доступа | 68% |
| Антиспамовое ПО | 44% |
| IDS/IPS | 26% |
| VPN | 17% |
| Защита от утечки данных | 8% |
| Другое | 16% |

Однако, по мнению аналитиков InfoWatch, даже 8% – неплохой показатель для такой новой области, как защита от внутренних угроз ИБ. Если вспомнить, что в 15% компаний вообще не зафиксировано ни одной утечки (Рисунок 4.4), то выходит, что как минимум 7% (15 – 8) из них не допустили утечек, хотя и не использовали никаких средств защиты. Но, скорее всего, такие организации просто не могут отследить, происходят у них утечки или нет.

Что же мешает компаниям внедрять системы защиты от утечек? Из предложенного списка (Рисунок 4.8) каждый респондент мог выбрать одну позицию. Почти каждый третий (30%) главной причиной считает отсутствие стандартов. Причем под стандартами здесь понимаются не только нормативные или рекомендательные акты, но и единое видение системы внутренней безопасности. Так, многие отмечали, что до сих пор не сформирован единый подход к решению проблемы внутренней ИБ. Поэтому компаниям сложно планировать бюджет и выбирать продукты для внедрения. Отсюда еще одна проблема – бюджетные ограничения (22%). Ведь не имея единого представления внутренней ИБ, компания не может планировать свои расходы и заранее выделять деньги на решение проблемы с инсайдерами.

Табл. 11 Препятствия на пути внедрения защиты от утечки

|  |  |
| --- | --- |
| Бюджетные ограничения | 22% |
| Психологические препятствия | 18% |
| Юридические препятствия | 9% |
| Отсутствие технологических решений | 3% |
| Отсутствие стандартов | 30% |
| Нехватка квалифицированного персонала | 15% |
| Затруднюсь ответить | 2% |
| другие | 1% |

Можно сравнить эти результаты с общеотраслевыми. Там лидируют психологические препятствия (25,4%), а отсутствие стандартов (12,2%) лишь на пятом месте. Отсюда вывод: сектор телекоммуникаций подходит к проблеме внутренней ИБ более зрело по сравнению с другими отраслями. Судя по всему, представители сектора ИТ уже преодолели психологический барьер и отчетливо понимают необходимость унификации процесса защиты от внутренних угроз.

**Табл. 12 Наиболее эффективные пути защиты от утечки**

|  |  |
| --- | --- |
| Организационные меры | 27% |
| Внедрение комплексных решений на основе ИТ | 49% |
| Ограничение с внешними сетями | 11% |
| Тренинги сотрудников | 9% |
| Другие | 3% |
| Никакие | 1% |

Следующий вопрос – наиболее эффективные способы защиты от утечек информации (Рисунок 4.9). Речь идет о мерах, которые представляются организациям наиболее адекватными и приемлемыми для решения проблемы внутренней ИБ, но по ряду причин не используются на практике. Безусловный лидер (49%) – комплексные информационные продукты. Эта мера доминирует уже на протяжении трех лет в общеотраслевом исследовании, поэтому можно смело утверждать, что именно в этом направлении будет происходить наибольший рост рынка внутренней ИБ в ближайшие годы.

Табл. 13 Планы по внедрению защиты от утечек информации

|  |  |
| --- | --- |
| Система мониторинга электронной почты | 21% |
| Комплексная система мониторинга сетевых ресурсов | 41% |
| Система мониторинга Интернет- трафика | 20% |
| Система мониторинга рабочих станций | 15% |
| Не планируем | 4% |

Базовым, по мнению экспертов InfoWatch, должно стать комплексное решение на основе ИТ, так как только с его помощью можно реализовать положения политики ИБ на рабочих местах. Вывод экспертов подтверждают планы внедрения средств защиты информации от утечек на ближайшие 2–3 года (Рисунок 4.10). Комплексные решения планирует внедрить 41% респондентов, т.е. почти на 10% больше, чем в других отраслях.

Главная озабоченность в проблеме внутренних нарушителей – отсутствие единого подхода к обеспечению внутренней безопасности. На практике это сильно затрудняет выбор конкретного решения: поставщиков много, каждый из них обладает какими-то плюсами, но, не имея четких критериев, мало в чем пересекается с конкурентами.

### Итоги исследований

Исследование показало, что по сравнению с другими отраслями российские телекоммуникационные компании довольно зрело относятся к проблеме ИБ в целом и защите от внутренних угроз в частности, но и у них есть направления для совершенствования ИБ.

Во-первых, в телекоме все еще низок уровень использования эффективных средств защиты от утечек. Причем среди респондентов бытует мнение, что их компания вообще не допускает утечки, хотя никаких инструментов проверки не использует. [10]

Во-вторых, операторам следует учитывать тенденции ужесточения нормативного регулирования: рекомендации «Базового уровня…» вскоре могут стать обязательными для исполнения. Кроме того, могут появиться новые требования к безопасности приватных сведений в рамках ФЗ «О персональных данных».Но и сейчас оператор нуждается в демонстрации своей способности предоставлять услуги связи, отвечающие установленным требованиям, и хочет продемонстрировать взаимодействующим с ним операторам способность совместно с ними противостоять угрозам ИБ. Поэтому добровольная сертификация довольно распространена уже сегодня. [11]

**5.Методы предотвращения внутренних утечек**

### 

### Административная работа с персоналом

По мнению экспертов компании InfoWatch, наилучшее средство предотвращения корпоративного саботажа — профилактические меры. Прежде всего компаниям нужно проверять рекомендации и места предыдущей работы нанимаемых служащих. Еще один чрезвычайно эффективный метод — регулярные тренинги или семинары, на которых до персонала доводится информация об угрозах IT-безопасности и саботаже как таковом. При таком подходе руководство делает ставку на тех сотрудников, которые взаимодействуют с саботажником в офисе, видят его нервозное поведение, получают угрозы в свой адрес и т. п. О подобных инцидентах следует тут же извещать уполномоченных лиц.

Следующий метод предполагает использование принципа минимальных привилегий и четкого разделения функций. Административных полномочий у обычных офисных служащих быть не должно. Также понятно, что сотрудник, отвечающий за резервные копии, не должен иметь возможности удалить данные в оригинальном источнике. Вдобавок в обязанности этого работника следует вменить информирование начальства в случае, если на резервные копии покусится какой-то другой служащий. Вообще, проблема защиты резервных копий может быть решена созданием их дубликатов. В связи с тем, что в компании, как правило, не так много по-настоящему критических данных, создание нескольких резервных копий представляется целесообразным.

Чрезвычайно важен момент эффективного управления паролями и учетными записями.

Лучшей профилактической мерой можно назвать мониторинг, причем не только пассивный (журналы событий), но и активный (защита ценной информации). В этом случае нанести реальный ущерб компании сможет только топ-менеджер, поскольку у остальных работников, имеющих доступ к цифровым активам фирмы, просто не будет прав на удаление ценной информации. На рынке уже есть специализированные решения для защиты данных от внутренних угроз, в том числе и от корпоративного саботажа. [7]

### 

### InfoWatch Enterprise Solution

Решение InfoWatch Enterprise Solution (IES) поставляется российской компанией InfoWatch, разработчиком систем защиты от инсайдеров. Оно позволяет обеспечить всесторонний контроль над всеми путями утечки конфиденциальных сведений: почтовым каналом и веб-трафиком, коммуникационными ресурсами рабочих станций и т. д. На сегодняшний день IES уже используется правительственными (Минэкономразвития, Таможенная служба), телекоммуникационными (ВымпелКом), финансовыми (Внешторгбанк) и топливно-энергетическими компаниями (ГидроОГК, Транснефть).

Архитектуру IES можно разделить на две части: мониторы, контролирующие сетевой трафик, и мониторы, контролирующие операции пользователя на уровне рабочих станций. Первые устанавливаются в корпоративной сети в качестве шлюзов и фильтруют электронные сообщения и веб-трафик, а вторые развертываются на персональных компьютерах и ноутбуках и отслеживают операции на уровне операционной системы . Сетевые мониторы IWM и IMM также могут быть реализованы в виде аппаратного устройства – InfoWatch Security Appliance. Таким образом, заказчику предлагается на выбор либо программное, либо аппаратное исполнение фильтров почты и веб-трафика. Преимущества такого подхода лучше всего проявляются при защите сложной вычислительной сети, охватывающей территориально распределенные филиалы.

К мониторам уровня рабочей станции относятся Info-Watch Net Monitor (INM) и InfoWatch Device Monitor (IDM). Модуль INM отслеживает операции с файлами (чтение, изменение, копирование, печать и др.), контролирует работу пользователя в Microsoft Office и Adobe Acrobat и тщательно протоколирует все действия с конфиденциальными документами.

Вся эта функциональность логично дополнена возможностями модуля IDM, который контролирует обращение к сменным накопителям, приводам, портам (COM, LPT, USB, FireWire), беспроводным сетям (Wi-Fi, Bluetooth, IrDA) и т. д.

Вдобавок, компоненты INM и IDM в состоянии работать на ноутбуках, при этом администратор безопасности имеет возможность задать специальные политики, действующие на период автономной работы сотрудника. Во время следующего подключения к корпоративной сети мониторы сразу же уведомят офицера безопасности, если пользователь попытался нарушить установленные правила во время удаленной работы.

Все мониторы, входящие в состав IES, способны блокировать утечку в режиме реального времени и сразу же оповещать об инциденте офицера безопасности. Управление решением осуществляется через центральную консоль, которая позволяет настраивать корпоративные политики. Также предусмотрено автоматизированное рабочее место офицера безопасности, с помощью которого специальный служащий может быстро и адекватно реагировать на инциденты. Таким образом, комплексное решение IES адресует все аспекты защиты конфиденциальной информации от инсайдеров.

### Lumigent Entegra и Log Explorer

Продукты компании Lumigent Entegra и Log Explorer служат для пассивной защиты информации, хранящейся в базах данных. Они позволяют осуществлять аудит баз данных и восстанавливать информацию в них.

Продукт Entegra следит за действиями пользователей при работе с базами данных и осуществляет аудит самих баз. Он позволяет определить, кто, когда и как просматривал или изменял записи в базе данных, а также изменял, структуру или права пользователей для доступа к ней. Стоит заметить, что продукт не в состоянии предотвратить какое-либо вредоносное воздействие, он лишь может отправить информацию об этой операции для записи в журнал. Log Explorer ведет избыточный журнал всех произведенных с базой данных транзакций, что позволяет в случае каких-либо проблем произвести анализ и аудит совершенных операций и восстановить потерянные или измененные записи без использования резервной копии. Однако речь о восстановлении на самом деле не идет, Log Explorer позволяет осуществлять откат транзакций. Таким образом, этот модуль не в состоянии предотвратить утечку, но может снизить риски искажения записей.

### PC Acme

Продукт PC Activity Monitor (Acme) позволяет осуществлять пассивный мониторинг операций пользователя на уровне рабочей станции. Решение состоит из двух частей: средства централизованного управления и многочисленные агенты, внедряемые в рабочие станции по всей организации. С помощью первой компоненты продукта можно централизованно распределить агенты по всей корпоративной сети, а потом управлять ими. Агенты представляют собой программные модули, которые очень глубоко внедряются в Windows 2000 или Windows XP. Разработчики сообщают, что агенты располагаются в ядре операционной системы, и пользователю практически нереально нелегально удалить их оттуда или отключить. Сами агенты тщательно протоколируют все действия пользователей: запуск приложений, нажатие клавиш и т. д. Можно сказать, что журнал событий, получающийся на выходе, по степени своей детализации напоминает результаты неусыпного видеонаблюдения за экраном компьютера. Однако получаемый журнал, естественно, представлен в текстовом виде. Центральная консоль управления позволяет собирать запротоколированные данные на один единственный компьютер и анализировать их там. Однако на этом этапе могут возникнуть сложности. Во-первых, офицеру безопасности приходится вручную анализировать сотни тысяч записей о тех или иных системных событиях, чтобы выделить те, которые являются нарушением политики ИТ-безопасности, привели к утечке и т. п. Но даже если офицеру безопасности удастся обнаружить факт утечки, то он все равно уже не сможет ее предотвратить. Таким образом, программа PC Acme подходит для пассивного мониторинга всех действий пользователя на уровне рабочей станции.

### Proofpoint  Messaging Security

Аппаратное решение компании Proofpoint позволяет обеспечить полный контроль над электронной почтой. С помощью этого устройства можно проверить сообщения на вирусы и спам, предотвратить нецелевое использование почтовых ресурсов и утечку конфиденциальной информации в электронных письмах. Защита от утечки конфиденциальных данных построена на базе механизма контентной фильтрации. Если в передаваемом сообщении находится конфиденциальная информация, то продукт способен заблокировать утечку. Решение Proofpoint является классическим примером продукта, предназначенного для защиты одного конкретного канала передачи данных – электронной почты. Такой продукт может быть использован в тех случаях, когда основной функциональностью является фильтрация спама и выявление вирусов, а предотвращение утечек — всего лишь приятное дополнение. [12]

### Как ловят инсайдеров

Пример победы над инсайдерами продемонстрировала в середине февраля 2006 г. российская компания LETA IT-company. Благодаря грамотному подходу к внутренней ИТ-безопасности, фирме удалось обезвредить инсайдера, уличенного в злоупотреблении служебным положением. Как показали результаты внутреннего расследования, один из менеджеров по работе с клиентами пытался проводить контракты на поставку программного обеспечения не через своего законного работодателя, а через им же созданную подставную компанию. Злоупотребление было оперативно и заблаговременно выявлено с помощью InfoWatch Mail Monitor.

## **ЗАКЛЮЧЕНИЕ**

Таким образом, в США и ЕС компании уже давно несут ответственность за утечку приватных данных и по закону обязаны поставить пострадавших в известность об утечке. Надеемся, что со временем такая норма появится и в России. Уже можно отметить положительные тенденции. Число организаций, защитивших себя от утечек, непрерывно растет и еще будет увеличиваться.

Организации начинают хорошо осознавать опасность роста угроз, связанных с собственным персоналом, хотя мало предпринимают необходимых мер для защиты. В списки своих приоритетных задач не все включили обучение и повышение квалификации сотрудников в сфере ИБ, регулярную оценку работы своих поставщиков IT-услуг с целью контроля за соблюдением ими политики ИБ, полагаясь исключительно на доверие. Лишь немногие рассматривают сегодня ИБ как одну из приоритетных задач руководства.

По мере развития бизнес-моделей организаций в направлении децентрализации некоторые функции делегируются внешним подрядчикам, следовательно, все труднее становится контролировать защищенность своей информации и оценивать уровень рисков. Компании могут делегировать выполнение работы, но не должны делегировать ответственность за безопасность.

Недостаточное внимание со стороны высшего руководства, нерегулярное проведение оценки рисков, а также недостаток либо полное отсутствие инвестиций в работы по снижению рисков, связанных с человеческим фактором (некорректное поведение сотрудников, оплошность, нарушение установленных правил или стандартов). Основное внимание по-прежнему уделяется лишь таким внешним угрозам, как вирусы, а серьезность внутренних угроз недооценивается: есть готовность покупать технологические средства (межсетевые экраны, антивирусную защиту и т. п.), но нет желания решать кадровые проблемы безопасности.

Многие инциденты с участием сотрудников остаются не выявленными. По мнению авторов исследований, телекоммуникационные компании могут и должны изменить свой взгляд на ИБ только как на статью расходов на ведение бизнеса: относиться к ней как к одному из способов повышения конкурентоспособности и сохранения стоимостного потенциала компании.

Ряд крупных компаний подпадают под требования различных нормативных актов, которые обязывают защищать приватные сведения. В целом ожидается, что спрос на решения по защите от инсайдеров и утечек будет стабильно расти как минимум в течение ближайших пяти лет.

# **Список ИСПОЛЬЗОВАННОЙ литературы**

1. InfoWatch. Новости. Как непросто определить утечку – Корбина телеком. 2007 г.
2. Сбиба В.Ю, Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. СПб: Питер, 2008.
3. “КНС ИНФОТЕКС” http://home.tula.net/insider/001b.htm.
4. Зенкин, Д. Инсайдеры в 75 раз опаснее хакеров. С-News. Аналитика. http://www.cnews.ru/reviews/index.shtml?2008/10/22/324142.
5. Доля, А. CitCity. Инсайдеры наступают. http://citcity.ru/14874/
6. InfoWatch: Внутренние угрозы: перед лицом общей опасности. http://www.infowatch.ru/threats?chapter=147151398&id=153017335
7. Доля, А. Саботаж в корпоративной среде. http://www.directum-journal.ru/card.aspx?ContentID=1717301.
8. Базовый уровень информационной безопасности операторов связи. [В Интернете] http://www.ccin.ru/treb\_baz\_u.doc.
9. Доля А. Безопасность телекомов. http://citcity.ru/15562
10. Доля А.В. Внутренние угрозы ИБ в телекоммуникациях. 2007 г. http://www.iks-navigator.ru/vision/456848.html.
11. Костров, Д.В. Информационная безопасность в рекомендациях, требованиях, стандартах. 2008 г.

http://www.iks-navigator.ru/vision/2390062.html.

1. Вестник связи: Защита от инсайдеров в телекоммуникационных компаниях.

http://www.vestnik-sviazy.ru/t/e107\_plugins/content/content.php?content.39.

1. Чужой среди своих: протокол заседания круглого стола. Вестник связи. - №7. 2006 r. http://www.vestnik-sviazy.ru/t/e107\_plugins/content/content.php?content.59.