Способы хищения информации в банках и методы борьбы с этим явлением

Е.В. Лола
Заместитель Председателя Правления -
Руководитель Службы внутреннего контроля
ОАО КБ «Стройкредит»

Содержание

1. Риски хищения информации в банках

2. Основные каналы распространения конфиденциальной информации

3. Стратегия борьбы с хищением конфиденциальной информации

4. Общие методы снижения рисков распространения конфиденциальной информации

5. Роль Службы внутреннего контроля при организации работы по борьбе с хищением информации

1. Риски хищения информации в банках

В наше время информация – товар на рынке. Владение ценной информацией порождает риски ее хищения:

- ***Финансовые*** – хищение данных банковских карт, ключевой информации и паролей для взаимодействия с Банком России*, системами денежных переводов и мгновенных платежей, получение информации о планируемых продуктах, хищение «базы клиентов» с целью переманивания

- ***Юридические*** – хищение конфиденциальной информации – нарушение банковской тайны*, Закона о персональных данных*

- ***Репутационные*** – с одной стороны, их сложно оценить, однако они могут привести к оттоку клиентов

* применительно к Российскому законодательству

2. Основные каналы распространения конфиденциальной информации

Инсайдерские

- Копирование на внешние носители - магнитные, оптические, флэш (в т.ч. мобильные телефоны, плееры, фотоаппараты)
- Интернет – электронная почта, мгновенные сообщения (ICQ, MSN, jabber…), веб-сайты – файлообменники (RapidShare, DepositFiles), подключение к удаленным компьютерам (например, домашнему), инициирование соединений для удалённого доступа к локальной сети организации извне с целью дальнейшего вывода доступной информации и/или взлома информационных систем
- Установка (или использование имеющихся) дополнительных устройств: Проводной или сотовый МОДЕМ (бесконтрольное подключение к удаленным компьютерам, сетям, Интернету), Адаптер беспроводной связи Wi-Fi или BlueTooth (бесконтрольное подключение к близлежащим беспроводным сетям, например точка доступа, организованная в припаркованном автомобиле)

Основные каналы распространения конфиденциальной информации

Инсайдерские *(продолжение)*

- Фото-, видеосъёмка (бумажных документов, содержимого мониторов, вводимых паролей для доступа к закрытой информации – как ручная, так и скрытая автоматизированная)
- Кража носителей резервной информации, «рабочих» жестких дисков, установка внутренних устройств-«жучков» (вовлечение сотрудников ИТ-службы)
- Факс (бесконтрольная отправка копий документов),
  Телефон (голосовая передача значительных объёмов информации)
- Вынос бумажных документов, копий
- Несанкционированный доступ к информации (с помощью взлома ПО, методов социальной инженерии, получения доступа к чужим компьютерам и закрытым информационным ресурсам) и дальнейшее использование вышеуказанных каналов

Основные каналы распространения конфиденциальной информации

Инсайдерские

Внешние угрозы

Внешние угрозы

- Кража переносных компьютеров и внешних носителей
- Вредоносное ПО (шпионское ПО, троянский конь)
- Социальная инженерия (воздействие на психологию сотрудников с целью выманивания паролей, запуска ими специально подготовленных программ),
- Визуальный «съём» информации (с мониторов, бумажных документов)
- Съём информации с вышедших из эксплуатации носителей, выброшенных документов
- Хакерские атаки, «взлом» сетей

Основные каналы распространения конфиденциальной информации

Инсайдерские

Внешние угрозы

Основные каналы утечек, I полугодие 2008 года

Источник: InfoWatch, 2008

3. Стратегия борьбы с хищением конфиденциальной информации

Организационные меры

Технические меры

Организационные меры - ввод в действие (с ознакомлением всех сотрудников под роспись) актуальной Политики информационной безопасности (ИБ):

- Внешние носители – полный запрет личных носителей, ограничение использования по принципу необходимости, строгий учёт используемых носителей, назначение ответственных за ИБ в каждом подразделении
- Интернет - регламентация получения доступа, использования и контроля использования ресурсов сети Интернет, регламентация использования корпоративной электронной почты, запрет использования внешних сервисов электронной почты
- Дополнительные устройства - регламентация отключения неиспользуемых устройств, запрет/контроль самостоятельной установки/подключения дополнительных устройств

3. Стратегия борьбы с хищением конфиденциальной информации

Организационные меры (продолжение)

- Запрет/контроль использования фото- и видеотехники, личных мобильных телефонов, переносных компьютеров; контроль помещений (например, видеонаблюдение)
- Регламентация учета, хранения и использования, а также контроль за перемещением всех накопителей информации, регламентация контроля за средствами вычислительной техники (СВТ) при обслуживании, уборке помещений и т.п.
- Утвержденные ограничения использования факсов, модемов, политика учета использования телефонной связи
(*пример:* полный запрет личных мобильных телефонов в ряде Российских банков)

3. Стратегия борьбы с хищением конфиденциальной информации

Организационные меры (продолжение)

- Строгий контроль оборота конфиденциальных документов с помощью введения режима «коммерческой тайны» в соответствии с Законом о Коммерческой Тайне* (недостаточность *только* «соглашения о конфиденциальности», присутствующего в большинстве организаций), мотивация сотрудников

- Разграничение полномочий пользователей информационных систем; ведение и контроль журналов доступа к критичным ресурсам; ввод в действие частных политик безопасности для всех операционных систем, программных комплексов, коммуникационного оборудования, использование сегментации сетей

* применительно к Российскому законодательству

Стратегия борьбы с хищением конфиденциальной информации

Технические меры – в соответствии с утвержденной Политикой ИБ внедрение соответствующих технических ограничений:

- Внешние носители – аппаратное и/или программное ограничение использования на рабочих станциях, обязательное шифрование на используемых внешних носителях, автоматизированный контроль использования внешних носителей (специальное ПО)
- Разграничение доступа к ресурсам сети Интернет (предоставление доступа только к необходимым ресурсам, либо разграничение специальным ПО), контроль использования, исключение взаимодействия сети Интернет с внутренней сетью организации (выделенные компьютеры, либо терминальный доступ)
- Отключение неиспользуемых устройств, аппаратное (либо программное) отключение возможности подключения дополнительных устройств, постоянный контроль конфигураций компьютеров

Стратегия борьбы с хищением конфиденциальной информации

Технические меры (продолжение)

- Контроль проноса личных устройств в организацию (металлодетекторы, контроль багажа), хранение личных мобильных телефонов, фото и видеотехники вне рабочих мест, контроль помещений (видеонаблюдение)
- Хранение резервных носителей в безопасных хранилищах, контроль доступа в помещения (видеонаблюдение), опечатывание СВТ («стикеры», пломбы), контроль за их сохранностью
- Техническое ограничение/контроль использования факсов, модемов (на офисных АТС); учет/аудиозапись использования телефонной связи, исключение возможности использования личных мобильных телефонов (покрытие стен/окон, генераторы помех)
- Контроль использования копировальной техники (установка на открытых пространствах, видеонаблюдение)
- Разграничение доступа пользователей информационных систем, адекватная настройка систем безопасности операционных систем, программных комплексов, коммуникационного оборудования; своевременное обновление систем безопасности; использование систем обнаружения/предотвращения вторжений

Стратегия борьбы с хищением конфиденциальной информации

Организационные меры

Технические меры

Снижение рисков внешних угроз – использование специальных технических средств, а также уже упомянутых методов:

- Регламентация использования переносных компьютеров и внешних носителей информации, обязательное шифрование всей критически важной информации
- Внедрение системы антивирусного ПО, исключение взаимодействия сети Интернет с внутренней сетью организации
- Вовлечение всех сотрудников в процесс обеспечения ИБ (ознакомление с документами, тренинги, назначение ответственных за ИБ), мотивация сотрудников

Стратегия борьбы с хищением конфиденциальной информации

Организационные меры

Технические меры

Снижение рисков внешних угроз (продолжение)

- Правильная расстановка СВТ, мебели, использование защитных экранов, тонированных стёкол
- Регламентация жизненного цикла, в т.ч. утилизации носителей информации (цифровых, бумажных)
- Настройка систем безопасности операционных систем, программных комплексов, коммуникационного оборудования в соответствии с утвержденными требованиями; своевременное обновление систем безопасности; использование систем обнаружения/предотвращения вторжений

4. Общие методы снижения рисков распространения конфиденциальной информации

- Внедрение системы менеджмента информационной безопасности на базе международных (или локальных) стандартов (ISO 27001, СТО БР ИББС 1.0*)
- Регулярный пересмотр Политики информационной безопасности
- Использование современных технологий – операционных систем, СУБД, программных комплексов (устаревшее ПО – часто невозможно ограничить доступ ко всей базе данных)
- Регулярный аудит прав доступа пользователей ЛВС, организация контроля за действиями сотрудников ИТ-служб

* применительно к Российскому законодательству

5. Роль Службы внутреннего контроля при организации работы по борьбе с хищением информации

3 модели организации работы информационных систем:

- *Самостоятельное существование ИТ-Службы*
  (отсутствие Службы ИБ, либо подчиненность Службы ИБ ИТ-Директору)

  Практически полное отсутствие системы внутреннего контроля
  Конфликт интересов организации работы ИТ и обеспечения ИБ

- *Независимое существование ИТ-Службы и Служба ИБ*

  Одностороннее влияние на ИТ-Службу со стороны Службы ИБ
  Недостаточность четкого распределения функций
  Зачастую фрагментарный подход к обеспечению ИБ
  Отсутствие оценки деятельности Службы ИБ, необходимости/достаточности принятых мер

- ***Наличие ИТ-аудита*** *(наряду со Службой ИБ и ИТ-Службой)*

  Независимая оценка работы как ИТ-Службы, так и Службы ИБ
  Разрешение вопросов между ИТ-Службой и Службой ИБ

Роль Службы внутреннего контроля при организации работы по борьбе с хищением информации

Предпочтительно создание в составе СВК **Отдела информационного аудита** (ОИА). Независимый подход и отсутствие заинтересованности (в отличие от Служб ИБ, ИТ-служб) позволяет Отделу информационного аудита СВК адекватно оценить как сами информационные риски, так и применяемые в организации методы по снижению этих рисков. Силами ОИА будет регулярно проводиться:

- Аудит нормативной базы в области защиты информации и организации работы ИТ-систем
- Оценка системы внутреннего контроля и выявление рисков в организации работы информационных систем и обеспечения ИБ, оценка целесообразности выбора конкретных мер защиты
- Аудит информационных систем на соответствие утвержденным стандартам
- Вынесение предложений по внесению изменений в нормативную базу, улучшению системы внутреннего контроля

Роль Службы внутреннего контроля при организации работы по борьбе с хищением информации

Требования к ИТ-аудиторам

ИТ-аудитор должен иметь техническое образование, опыт работы в ИТ-службах и/или Службах ИБ. Как преимущество должны расцениваться опыт работы в области аудита информационных систем, навыки программирования, знание законодательства в области защиты информации, международных и локальных стандартов организации работы информационных систем и стандартов информационной безопасности, **банковских технологий, технологий работы платежных систем, бухгалтерского учёта**, наличие профессиональных сертификатов.

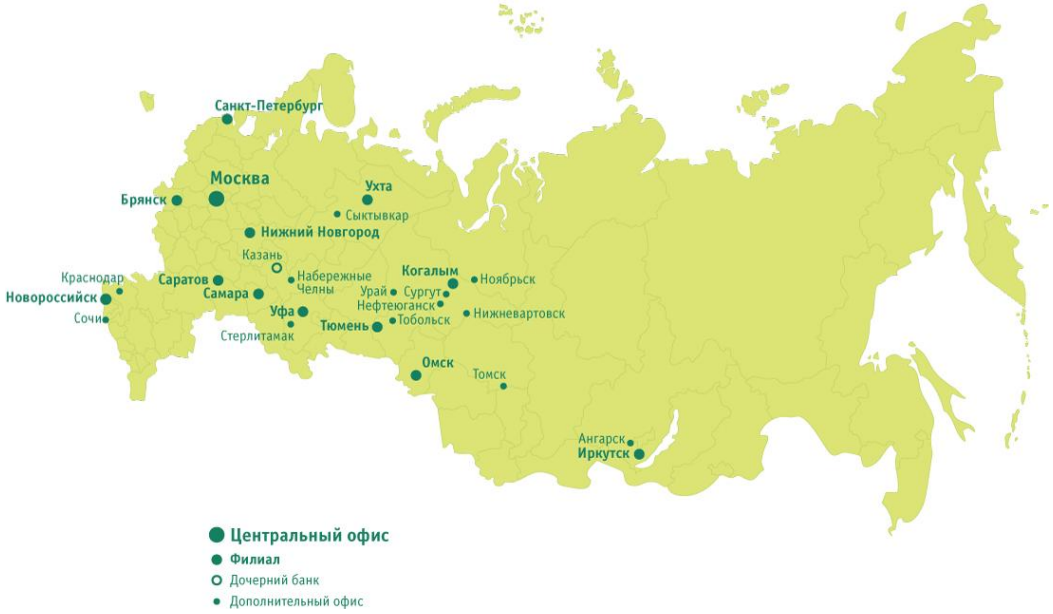
При наличии указанных знаний целесообразно привлечение ИТ-аудитора к большинству «финансовых» проверок СВК, что, в ряде случаев, позволит поднять их на качественно новый уровень. ИТ-аудитором может быть автоматизирована часть рутинной работы финансовых аудиторов.

Роль Службы внутреннего контроля при организации работы по борьбе с хищением информации

В случае **отсутствия возможности создания ОИА** (обычно по финансовым причинам, либо из-за недостаточного уровня зрелости организации) наиболее оправданным вариантом выглядит привлечение сторонних консультантов для создания (оценки существующей) системы менеджмента информационной безопасности и **разработки** (доработки) **нормативной базы**.

При наличии актуальной нормативной базы, разработанной (доработанной) независимыми консультантами, возможен аудит организации работы информационных систем и обеспечения ИБ на соответствие утвержденным стандартам существующими силами СВК.

Вопросы



Евгений Валерьевич Лола

Заместитель Председателя Правления –
Руководитель Службы внутреннего контроля
ОАО КБ «Стройкредит»