Введение в информационную безопасность

Доронина Лариса Алексеевна, к. э.н., доцент

Безопасность информационная

- 1) комплекс организационно-технических мероприятий, обеспечивающих целостность данных и конфиденциальность информации в сочетании с ее доступностью для всех авторизованных пользователей
- 2) показатель, отражающий статус защищенности информационной системы

Почему важно защищать информацию?

- Информация и поддерживающие ее информационные системы и сети являются ценными производственными ресурсами организации.
- Их доступность, целостность и конфиденциальность необходимы для нормальной деятельности организации.

Пример 1. Из "Стандарта Банка России..."

- 5.9. ...Собственник должен знать, что он должен защищать. Собственник должен знать и уметь выделять (идентифицировать) наиболее важный для его бизнеса информационный актив (ресурс)

Информационная безопасность подразумевает:

- - обеспечение конфиденциальности - информация доступна только тем, кто имеет на то соответствующее право;
  - обеспечение целостности - защищается точность и полнота информации, а также методов ее обработки;
  - доступность - гарантируется, что авторизованные пользователи, когда нужно, имеют возможность получить доступ к информации

Иллюзии ИБ

- **Иллюзия 1: информационная безопасность = компьютерной безопасности**

Иллюзия 2: информационная безопасность – это только борьба с преступниками

- - защита информационных ресурсов организации от иных видов угрозы, таких как природные явления (наводнение, пожар) или же техногенные катастрофы (отключение электроэнергии);
  - обеспечение долговременной сохранности целостных и аутентичных информации и документов, подлежащих длительному и постоянному хранению,
- - защита юридических, имущественных и иных прав организации, ее сотрудников и клиентов путем соблюдения установленных норм и правил делопроизводства и документооборота.
- - обеспечение сохранности и быстрого доступа к информации, которая необходима для быстрого восстановления деятельности организации в случае непредвиденных обстоятельств. Этот вид деятельности требует защиты иного круга информационных ресурсов, часто - на таких носителях, для использования которых не **требуются технические средства.**

Особенности информационных ресурсов

- 1. Электронные документы и информация хранятся в компьютерных системах и сетях (отв. ИТ- службы)
  2. За бумажные документы главным образом отвечает служба документационного обеспечения управления (отв. Служба ДОУ)

- 3. Наиболее ценная и важная информация хранится в головах сотрудников. Как говорят американцы, руководитель организации всегда должен помнить, что 65% информации ежедневно вечером покидает офис фирмы и может утром не вернуться, - или, хуже того, перебежать к конкурентам

Самое слабое звено в обеспечении информационной безопасности

- Уязвимость любой системы оценивается по наиболее слабому звену, а это часто кадры
- **Из исследовательского отчета фирмы "Эрнст и Янг":**
  6. Люди остаются самым слабым звеном в обеспечении информационной безопасности.
  Инвестиции в технологии немногого стоят, если не обучать сотрудников тому, что и как делать. Этот факт еще раз подтверждают несколько недавних инцидентов, получивших большой общественный резонанс, при расследовании которых в конечном итоге выяснилось, что их причиной стали не технические уязвимости, а человеческие ошибки.
  На технологии делается настолько большой упор, что о "человеческой" составляющей информационной безопасности часто забывают. Результаты опроса 2012 г. подтверждают, что во многих компаниях эта проблема остается нерешенной

Пример. Из "Стандарта Банка России...":

- 5.4. Наибольшими возможностями для нанесения ущерба организации БС РФ обладает ее собственный персонал.
- В этом случае содержанием деятельности злоумышленника является нецелевое использование предоставленного контроля над информационными активами, а также сокрытие следов своей деятельности.
- Внешний злоумышленник, скорее да, чем нет, может иметь сообщника(ов) внутри организации

Вывод

- - все принимаемые на работу сотрудники должны проверяться
- - следует поощрять бдительность на рабочих местах и предусмотреть способы, при помощи которых сотрудники могли бы сообщать о подозрительной деятельности.

Исследования Секретной Службой США (USSS) и Университетом Карнеги - Меллона

- Были проанализированы 23 киберпреступления, совершенных в период с 2002 по 2012 г. сотрудниками банков и финансовых организаций США, причем ряд преступников согласился дать интервью и объяснить мотивы своих действий.
- В отчете под названием "Угроза изнутри: незаконная компьютерная активность в банковском и финансовом секторах" в качестве главного вывода отмечается, что преступникам, как правило, не потребовались какие-то особые знания и навыки.
- Для "взлома" систем использовались не столько недостатки оборудования и программного обеспечения, сколько отсутствие должной дисциплины и контроля на рабочих местах. Большинство преступлений было совершено ради наживы, но в четверти случаев основным мотивом была месть - как правило, за увольнение

- По данным "Глобального обследования состояния информационной безопасности - 2012", подготовленного компанией PricewaterhouseCoopers, сотрудники и бывшие сотрудники компаний являются виновниками 50% всех инцидентов информационной безопасности.
- В 2013 г. этот показатель составлял 69%.

Кроме кнута должен быть и пряник

- Пример. Из "Стандарта Банка России...":
  5.11. Соблюдение политики ИБ в значительной степени является элементом корпоративной этики, поэтому на уровень ИБ в организации серьезное влияние оказывают отношения как в коллективе, так и между коллективом и собственником или менеджментом организации, представляющим интересы собственника.
- ..Понимая, что наиболее критичным элементом безопасности организации является ее персонал, собственник должен всемерно поощрять решение проблемы ИБ

Для уменьшения уровня угрозы перехода сотрудников к конкурентам необходимо

- 1) снижать заинтересованность сотрудников в смене места работы, для чего:
  - следить за средними уровнями зарплаты на рынке труда и не допускать заметного отставания уровня зарплаты ключевых сотрудников от средних уровней;
  - следить за тем, чтобы у сотрудников всегда была ясная перспектива профессионального роста и/или роста зарплаты;
  - не забывать о моральном поощрении сотрудников, о создании хорошего климата в коллективе.

- - развивать корпоративную культуру, включающую лояльность к своей организации, 2) избегать ситуаций, когда сотрудник становится незаменим; своевременно готовить кадровый резерв
- 3) подробно и тщательно описывать деловые процессы и операции на всех участках, оформляя эти описания в виде внутренних нормативных документов - инструкций по выполнению операций.

Пример

- В декабре 2007 г. все заместители генерального директора и ряд ведущих сотрудников ОАО "Пермэнергосбыт" после проведения аукциона по продаже 49% акций АО блокировали работу компании (ушли на больничный или в отпуска). Им принадлежали ЭЦП, дающие доступ к банкам, к работе на оптовом рынке. Была парализована работа серверной, ключи от которой были "утеряны". После ее вскрытия обнаружилась пропажа 44 дисков, на которых была база данных по всем потребителям г. Перми

Выводы

- - в отношении электронных документов необходимо соблюдать все требования к документообороту, включая:
  - строгий учет документов, включение электронных документов в номенклатуру дел;
  - установление сроков хранения;
  - долговременное хранение электронных документов с сохранением их целостности и аутентичности;
  - проведение экспертизы ценности и уничтожения электронных документов по истечении сроков хранения в строгом соответствии с законодательством;
  - разработать и внедрить планы действий на случай чрезвычайных ситуаций, которые включали бы в себя и планы защиты важнейших документов организации - как электронных, так и бумажных;
  - важно обеспечение единой политики управления доступом к документам организации на всех видах носителей;
  - необходимо сохранение корпоративной памяти организации в виде документов на всех видах носителей: ее истории, опыта успехов и неудач
- - обязательна защита конфиденциальной информации и персональных данных.

  - распространение на электронные документы правил работы службы ДОУ

Другие проблемы защиты

- Учет электронных документов
- Электронная почта

Пример

- 16 мая 2005 г. одна из крупнейших инвестиционных компаний мира Morgan Stanley судом США признана виновной в мошенничестве. Штраф, наложенный на компанию, является самым крупным в истории - 1,4 млрд долл. Главная причина привлечения компании к ответственности - неспособность представить в суд свою электронную переписку.

Пример

- Всемирный совет автоспорта в сентябре 2007 г. принял решение об исключении команды "Формулы-1" "Макларен" из Кубка конструкторов этого года и оштрафовал на 100 млн долл. за то, что главный конструктор команды был уличен в нелегальном владении секретной технической документацией "Феррари".
- Компания собиралась подавать апелляцию, однако отказалась от этого, сообщив в официальном пресс-релизе:
- *"К нашему сожалению и удивлению, из содержания электронных писем, о существовании которых ранее не было известно, стало ясно, что доступ к информации не ограничивался одним человеком, хотя это никоим образом не было санкционировано командой"*

Сохранение важнейших документов организации

- К важнейшим относят те документы и материалы - на всех видах носителей (необязательно подлинники), которые потребуются немедленно, в первые минуты, часы и дни после чрезвычайного происшествия, а также те, безвозвратная утрата или повреждение которых подрывает (по юридическим, нормативным и эксплуатационным причинам) возможность организации продолжать свою деятельность (п. 7.1 ГОСТ Р ИСО 15489-1-2007)

Другие важнейшие документы

- Списки телефонов и адресов сотрудников компании, списки поставщиков, способных в случае необходимости предоставить помещения и оборудование, необходимое для восстановления деятельности, и т.п.
- Персональные данные. В Соединенных Штатах основательно защищаются только финансовые и медицинские персональные данные, но наказания за нарушения следуют весьма серьезные

- Спасибо за внимание!