Информационная безопасность

Security

Разработал Дубаков А.А.

Понятие ИБ

- **ИБ-Защищенность информации** и **поддерживающей инфраструктуры** от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести **неприемлемый ущерб** субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.
- **Защита информации** – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Цель ИБ

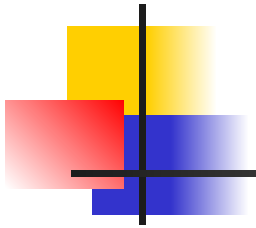
- Цель мероприятий в области **информационной безопасности** – защитить **интересы субъектов информационных отношений**. Интересы эти многообразны, но все они концентрируются вокруг трех основных аспектов:
  - **доступность**;
  - **целостность**;
  - **конфиденциальность**

Три кита

- **Доступность** – это возможность за приемлемое время получить требуемую информационную услугу.
- **Целостностью** - актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.
- **Конфиденциальность** – это защита от несанкционированного доступа к информации

Понятие ИБ

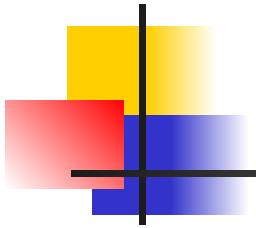
- "Компьютерная безопасность" (как эквивалент или заменитель ИБ) слишком узкий подход
- Компьютеры – только одна из составляющих информационных систем
- Безопасность определяется всей совокупностью составляющих и, в первую очередь, самым слабым звеном, которым в подавляющем большинстве случаев оказывается человек (записавший, например, свой пароль на "горчичнике", прилепленном к монитору).



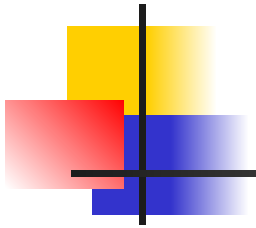
- ИБ зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал.

«Неприемлемый ущерб»

- Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда **стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба**. Значит, с чем-то приходится мириться и **защищаться следует только от того, с чем смириться никак нельзя**



- **Угроза** – это потенциальная возможность определенным образом нарушить информационную безопасность.
- Попытка реализации угрозы называется **атакой**, а тот, кто предпринимает такую попытку, – **злоумышленником** (malicious)
- Потенциальные злоумышленники называются **источниками угрозы**.



- Чаще всего угроза является следствием наличия **уязвимых** мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Классификация угроз

- **по аспекту информационной безопасности** (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;
- **по компонентам информационных систем**, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- **по способу осуществления** (случайные/преднамеренные действия природного/техногенного характера);
- **по расположению источника угроз** (внутри/вне рассматриваемой ИС).

Угрозы доступности

- Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются **непреднамеренные ошибки** штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.
- По некоторым данным, до 65% потерь – следствие непреднамеренных ошибок.
- Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе.
- Очевидно, самый радикальный способ борьбы с непреднамеренными ошибками – **максимальная автоматизация и строгий контроль**

Другие угрозы доступности

- **отказ пользователей**;
- **внутренний отказ** информационной системы;
- **отказ поддерживающей инфраструктуры**.

Отказ пользователей

- Нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);
- Невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);
- Невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Внутренние отказы

- Отступление (случайное или умышленное) от установленных правил эксплуатации;
- Выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);
- Ошибки при (пере)конфигурировании системы;
- Отказы программного и аппаратного обеспечения;
- Разрушение данных;
- Разрушение или повреждение аппаратуры.

Отказ поддерживающей инфраструктуры

- Нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
- Разрушение или повреждение помещений;
- Невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

"обиженные" сотрудники

- Весьма опасны так называемые **"обиженные" сотрудники** – нынешние и бывшие. Как правило, они стремятся нанести вред организации-"обидчику", например:
  - испортить оборудование;
  - встроить логическую бомбу, которая со временем разрушит программы и/или данные;
  - удалить данные.
- Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

стихийные бедствия

- **стихийные бедствия** и события, воспринимаемые как стихийные бедствия,– грозы, пожары, наводнения, землетрясения, ураганы.
- По статистике, на долю огня, воды и тому подобных "злоумышленников" (среди которых самый опасный – перебой электропитания) приходится 13% потерь, нанесенных информационным системам

Вредоносное программное обеспечение

- Вредоносная функция;
- Способ распространения;
- Внешнее представление.
- Т.н. "бомбы" предназначаются для:
  - внедрения другого вредоносного ПО;
  - получения контроля над атакуемой системой;
  - агрессивного потребления ресурсов;
  - изменения или разрушения программ и/или данных.

По механизму распространения различают:

- **вирусы** – код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;
- **"черви"** – код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы).

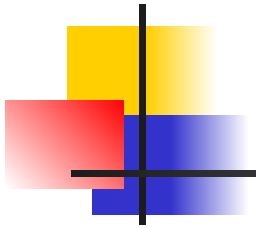
Основные угрозы целостности

- **Статическая целостность**
  - **ввести неверные данные;**
  - **изменить данные.**
- **Динамическая целостность**
  - **нарушение атомарности транзакций,**
  - **переупорядочение,**
  - **кража,**
  - **дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т. п.).**
- **Соответствующие действия в сетевой среде называются активным прослушиванием.**

Основные угрозы конфиденциальности

- Служебная информация (пароли)
- Предметная информация
  - Перехват данных - Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например на кабельную сеть, может кто угодно, так что эту угрозу нужно принимать во внимание по отношению не только к внешним, но и к внутренним коммуникациям
  - Маскарад-представление за другого
  - Злоупотребление полномочиями
- Откуда берутся базы данных налогоплательщиков

- Первый шаг при построении системы **ИБ** организации – ранжирование и детализация аспектов: **доступность**, **целостность**, **конфиденциальность**
- **Важность** проблематики ИБ объясняется двумя основными причинами:
  - ценностью накопленных информационных ресурсов;
  - критической зависимостью от информационных технологий.
- Разрушение важной информации, кража конфиденциальных данных, перерыв в работе вследствие отказа – все это выливается в крупные материальные потери, наносит **ущерб** репутации организации. Проблемы с системами управления или медицинскими системами угрожают здоровью и жизни людей.



- Подтверждением **сложности** проблематики ИБ является параллельный (и довольно быстрый) **рост затрат** на защитные мероприятия и количества **нарушений** ИБ в сочетании с ростом среднего ущерба от каждого нарушения. (Последнее обстоятельство - еще один довод в пользу важности ИБ.)

Четыре **уровня** мер

- законодательного;
- административного (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
- процедурного (меры безопасности, ориентированные на людей);
- программно-технического.

Две группы мер

- **меры ограничительной направленности**, для создания и поддержания в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности (назовем их);
- **направляющие и координирующие меры**, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры созидательной направленности).

Закон "Об информации, информатизации и защите информации"

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Законодательный уровень

- Правовые акты и стандарты
  - Необходимо всячески подчеркивать важность проблемы ИБ; сконцентрировать ресурсы на важнейших направлениях исследований; скоординировать образовательную деятельность; создать и поддерживать негативное отношение к нарушителям ИБ – все это функции законодательного уровня

Российская ситуация

- Российские правовые акты в большинстве своем имеют ограничительную направленность. **Лицензирование** и **сертификация** не обеспечивают безопасности. К тому же в законах не предусмотрена ответственность государственных органов за нарушения ИБ.
- Реальность такова, что в России в деле обеспечения ИБ на помощь государства рассчитывать не приходится. (Кто переходит на зеленый сигнал светофора).

Оранжевая книга

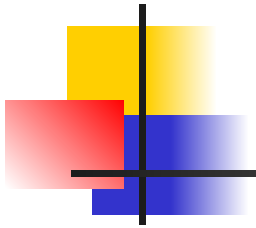
- абсолютно безопасных систем не существует, это абстракция. Есть смысл оценивать лишь степень доверия, которое можно оказать той или иной системе.
- "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

Элементы политики безопасности

- произвольное управление доступом
  - **метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. (может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа к объекту)**
- безопасность повторного использования объектов
  - **для областей оперативной памяти и дисковых блоков и магнитных носителей в целом**
- метки безопасности
  - **Метка субъекта описывает его благонадежность, метка объекта – степень конфиденциальности содержащейся в нем информации.**
- принудительное управление доступом
  - **Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. Смысл сформулированного правила понятен – читать можно только то, что положено.**

Классы безопасности ОК

- **В "Оранжевой книге" определяется четыре уровня доверия – D, C, B и A**
- Уровень D предназначен для систем, признанных неудовлетворительными
- Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием степени доверия.



- уровень С – произвольное управление доступом;
- уровень В – принудительное управление доступом;
- уровень А – верифицируемая безопасность.

рекомендации **X.800**

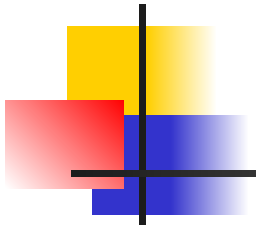
- Рекомендации X.800 весьма глубоко трактуют вопросы защиты **сетевых конфигураций** и предлагают развитый набор сервисов и **механизмов безопасности**.
  - Сервисы безопасности
  - Сетевые механизмы безопасности
  - Администрирование средств безопасности

Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"

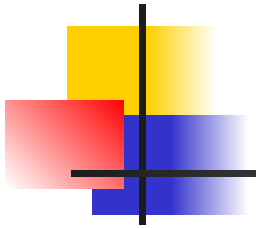
- идентификация и аутентификация;
- **защита данных пользователя**;
- **защита функций безопасности** (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);
- **управление безопасностью** (требования этого класса относятся к управлению атрибутами и параметрами безопасности);
- **аудит безопасности** (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);
- **доступ к объекту оценки**;
- **приватность** (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);
- **использование ресурсов** (требования к доступности информации);
- **криптографическая поддержка** (управление ключами);
- **связь** (аутентификация сторон, участвующих в обмене данными);
- **доверенный маршрут/канал** (для связи с сервисами безопасности).

Административный уровень

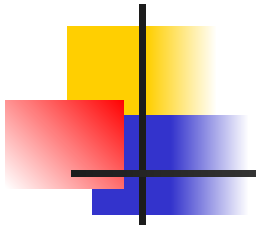
- Главная задача мер административного уровня – сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.
- Основой программы является **политика безопасности**, отражающая подход организации к защите своих информационных активов.
- Разработка политики и **программы безопасности** начинается с **анализа рисков**, первым этапом которого, в свою очередь, является ознакомление с наиболее распространенными **угрозами**



- Главные угрозы – внутренняя сложность ИС, непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.
- На втором месте по размеру ущерба стоят кражи и подлоги.
- Реальную опасность представляют пожары и другие аварии поддерживающей инфраструктуры.



- Необходимым условием для построения надежной, экономичной защиты является рассмотрение **жизненного цикла** ИС и синхронизация с ним мер безопасности. Этапы жизненного цикла:
  - инициация;
  - закупка;
  - установка;
  - эксплуатация;
  - выведение из эксплуатации.



- Безопасность невозможно добавить к системе; ее нужно закладывать с самого начала и поддерживать до конца.

Процедурный уровень

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

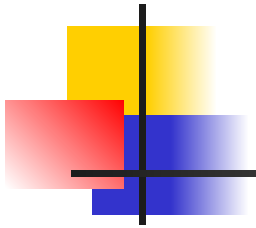
Принципы безопасности

- непрерывность защиты в пространстве и времени;
- разделение обязанностей;
- минимизация привилегий.

Текущие работы

- Необходимо регулярно осуществлять:
  - поддержку пользователей;
  - поддержку программного обеспечения;
  - конфигурационное управление;
  - резервное копирование;
  - управление носителями;
  - документирование;
  - регламентные работы.

Программно-технические меры



- Программно-технические меры, то есть меры, направленные на контроль компьютерных сущностей – оборудования, программ и/или данных, образуют последний и самый важный рубеж информационной безопасности.

Меры безопасности

- **превентивные**, препятствующие нарушениям ИБ;
- меры **обнаружения** нарушений;
- **локализующие**, сужающие зону воздействия нарушений;
- меры по **выявлению нарушителя**;
- меры **восстановления** режима безопасности.

Сервисы безопасности

- **идентификация** и **аутентификация**;
- **управление доступом**;
- **протоколирование** и **аудит**;
- **шифрование**;
- **контроль целостности**;
- **экранирование**;
- **анализ защищенности**;
- обеспечение **отказоустойчивости**;
- обеспечение **безопасного восстановления**;
- **туннелирование**;
- **управление**.