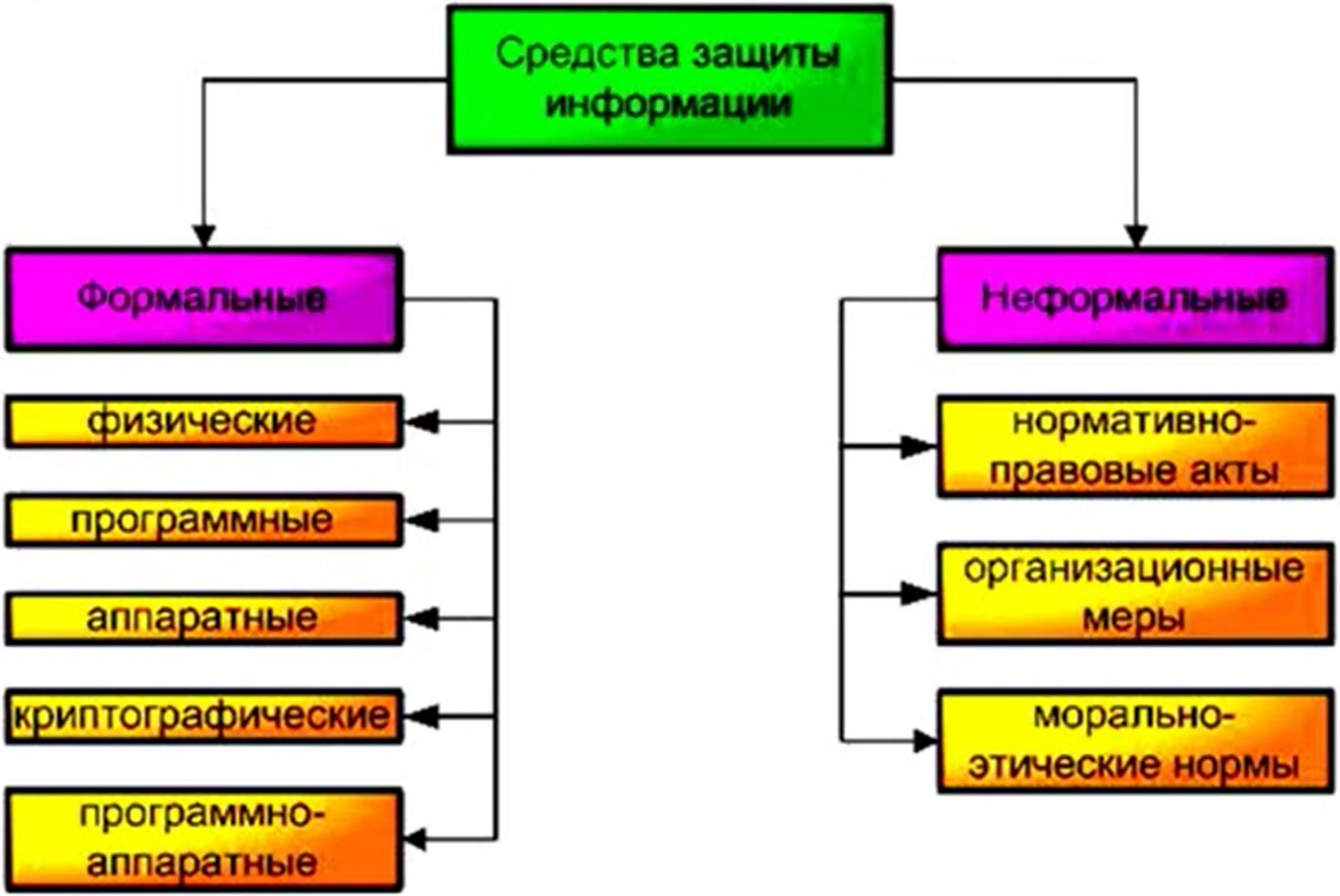
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Лекция 2. Основные понятия и угрозы информационной безопасности

Понятие информационной безопасности

Под ***информационной безопасностью*** понимается защищённость 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.


Средства защиты информации
Формальные
физические
программные
аппаратные
криптографические
программно-аппаратные
Неформальные
нормативно-правовые акты
организационные меры
морально-этические нормы

Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

Из этого положения можно вывести два важных следствия:

- Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может **существенно различаться**.
- Информационная безопасность **не сводится исключительно к защите от несанкционированного доступа** к информации, это принципиально более широкое понятие.

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.

Основные составляющие информационной безопасности

Доступность – это возможность за приемлемое время получить требуемую информационную услугу.

Целостность – актуальность и непротиворечивость информации, её защищенность от разрушения и несанкционированного изменения.

Конфиденциальность – это защита от несанкционированного доступа к информации.

Целостность подразделяется на статическую, понимаемую как неизменность информационных объектов, и динамическую, относящуюся к корректному выполнению сложных действий (транзакций).

Основные угрозы информационной безопасности

Угроза - это потенциальная возможность определённым образом нарушить информационную безопасность.

Попытка реализации *угрозы* называется ***атакой***, а тот, кто предпринимает такую попытку, - ***злоумышленником***.

Потенциальные *злоумышленники* называются ***источниками угрозы***.

Чаще всего *угроза* является следствием наличия ***уязвимых мест*** в защите информационных систем.

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется ***окном опасности***, ассоциированным с данным *уязвимым* местом.

Угрозы можно классифицировать по нескольким критериям:

- 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).

Вредоносное программное обеспечение

Грани *вредоносного ПО*:

- вредоносная функция;
- способ распространения;
- внешнее представление.

Часть, осуществляющую разрушительную функцию, называют ***"бомбой"***. Обычно *"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:

вирус - код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;

"червь" - код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение.

ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» содержится следующее определение:

«Программный вирус - это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах».

Спам.

Всего за несколько лет спам из незначительного раздражающего фактора превратился в одну из серьёзнейших угроз безопасности:

- электронная почта в последнее время стала главным каналом распространения вредоносных программ;
- спам отнимает массу времени на просмотр и последующее удаление сообщений, вызывает у сотрудников чувство психологического дискомфорта;
- как частные лица, так и организации становятся жертвами мошеннических схем, реализуемых спамерами (зачастую подобного рода события потерпевшие стараются не разглашать);
- вместе со спамом нередко удаляется важная корреспонденция, что может привести к потере клиентов, срыву контрактов и другим неприятным последствиям; опасность потери корреспонденции особенно возрастает при использовании чёрных списков RBL и других «грубых» методов фильтрации спама.

Каналы утечки информации и способы их ликвидации

Типичная ситуация, но чем она грозит при неумелой политике информационной безопасности:

- Документ создан, и счастливый сотрудник, после долгой работы над ним отошел на обед. В это время злоумышленник осуществил несанкционированный доступ к персональному компьютеру сотрудника и подменил или уничтожил документ.
- Документ создан, сотрудник положил его в папку на файловом сервере корпоративной сети и пошел домой. В это время его конкурент по карьерной лестнице или недоброжелатель, добравшись до сервера, подменил или уничтожил документ.
- Документ создан, сотрудник положил его в папку на файловом сервере корпоративной сети. Произошла атака на корпоративную сеть компании со стороны сети Интернет и все базы данных и другие материалы уничтожены.
- Документ создан и отправлен по электронной почте или отправлен на *ftp* сервер в головной офис. При передаче документа произошёл его перехват и подмена.
- Документ создан, переписан на диск или «флэшку» и отправлен с курьером в головной офис. Курьер за день очень устал и забыл папку с диском в метро.
- Документ создан, обработан и содержится где-то на диске какого-то компьютера. Компьютер списывается, и новый владелец находит в скрытых файлах годовой финансовый отчёт. Он его продаёт конкуренту.
- По сети или через обмен дисками или флэш-носителями компьютер сотрудника или сервер сети был заражён вирусом, что повлекло за собой уничтожение баз данных и другой важной информации.

Каналы утечки информации и способы их ликвидации

Персональный компьютер.

- шифрование с достаточной длиной ключа;
- системы защиты, блокирующие загрузку компьютера до предъявления электронного идентификатора;
- антивирусная защита персональных ресурсов.

Корпоративная сеть.

- межсетевые экраны;
- шифрование;
- антивирусная защита.

Сети питания и другие каналы.

- помехоподавляющие фильтры
- мероприятия, направленные на невозможность использования технических средств снятия информации.

Уничтожение информации.

- уничтожители информации на магнитных носителях
- специальные информационные сейфы с источником бесперебойного питания.

Комплексный подход.