Защита информации

7.1. Введение в информационную безопасность

- Понятие защиты информации;
- Система защиты информации;
- Угрозы информационной безопасности;
- Государственная система информационной безопасности;
- Информация по уровням доступа;
- Законодательство в сфере ИБ.

Понятие защиты информации

Защита информации – комплекс мер, направленных на предотвращение несанкционированного удаления, модификации и воспроизведения информации.

Основные направления защиты информации – охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности.

Потеря информации, может приводить к серьезным экономическим, и временным затратам не ее восстановление.

Искажение информации может приводить к ошибочным решениям со всеми вытекающими экономическими и социальными последствиями.

Несанкционированное воспроизведение, может быть связано с нарушением государственной тайны, прав интеллектуальной собственности (авторских прав, ноухау), коммерческой тайны, конфиденциальности персональных данных с соответствующими негативными последствиями.

Система защиты информации

Безопасная система — использует аппаратные и программные средства, управляет доступом к информации так, что только должным образом авторизованные лица или же действующие от их имени процессы получают право читать, писать, создавать и удалять информацию.

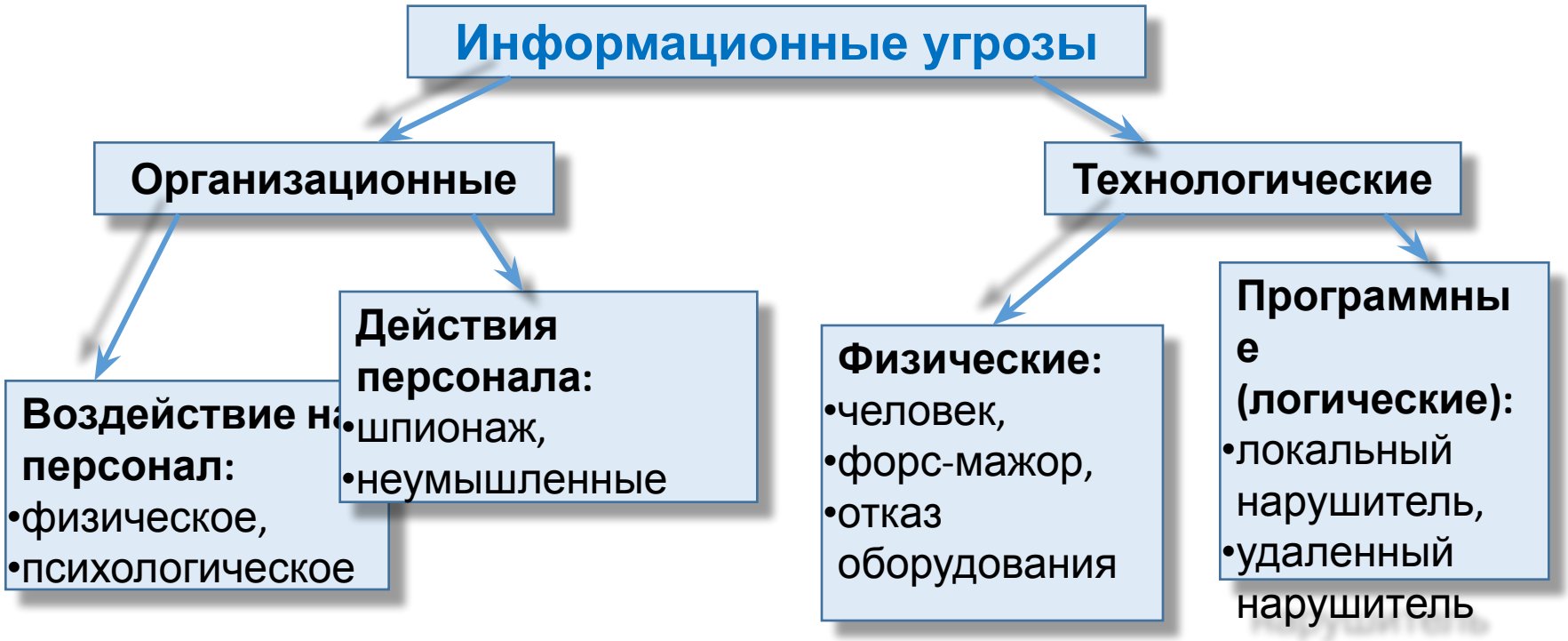
Критерии оценки ИБ:
политика ИБ (активный компонент защиты),
гарантированность (пассивный компонент).

Абсолютно безопасных систем нет, поэтому говорят о надежной системе в смысле «система, которой можно доверять» (как можно доверять человеку). Система считается надежной, если она с использованием достаточных аппаратных и программных средств обеспечивает одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа.

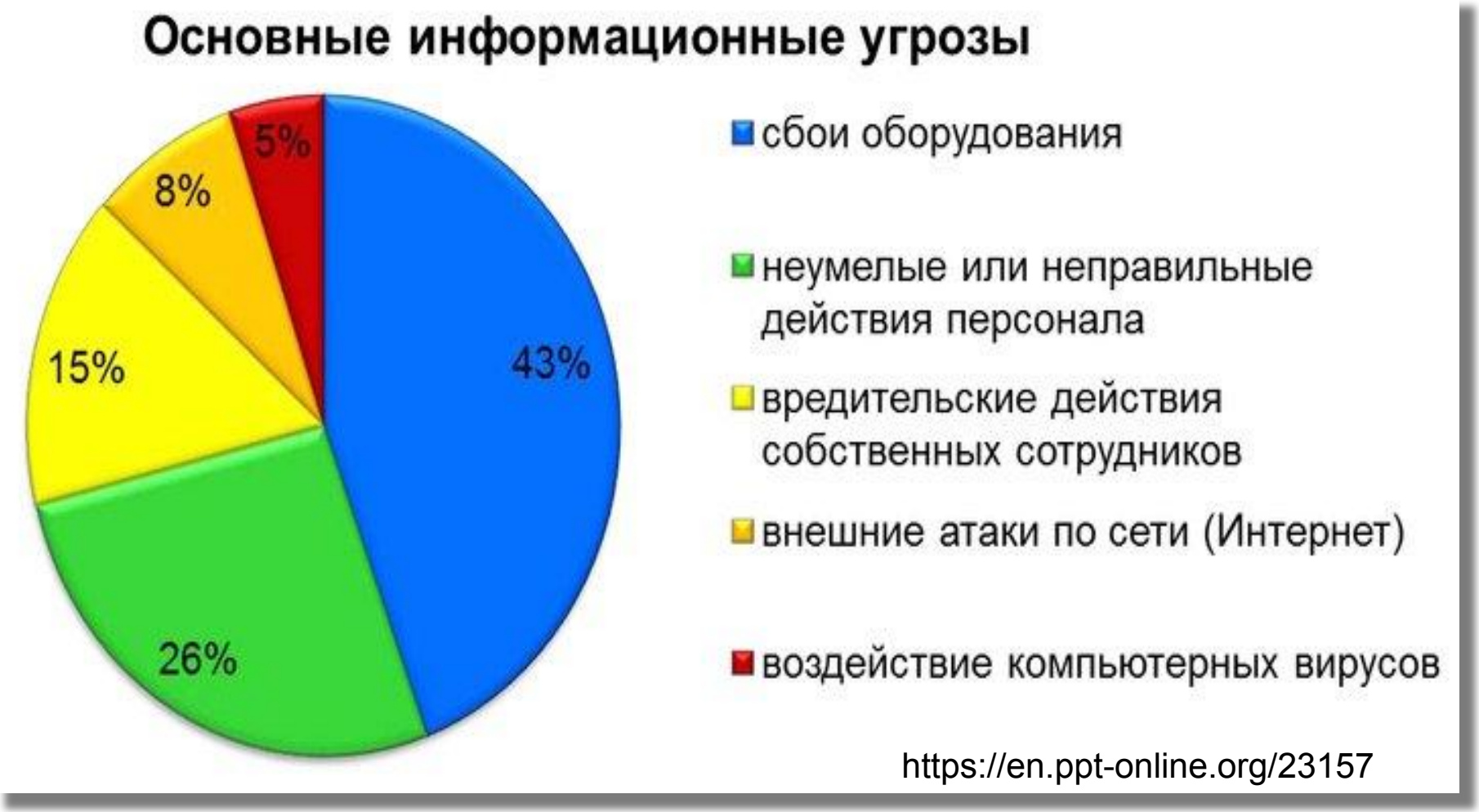
Основные критерии оценки степени защиты информации – это:
Политика безопасности, являясь активным компонентом защиты, включает в себя анализ возможных угроз и выбор соответствующих мер противодействия, отображает тот набор законов, правил и норм поведения, которым пользуется конкретная организация при обработке, защите и распространении информации.
Гарантированность, являясь пассивным элементом защиты, отображает меру доверия, которое может быть оказано архитектуре и реализации системы (другими словами, показывает, насколько корректно выбраны механизмы, обеспечивающие безопасность системы).
Система ИБ должна гарантировать:

- конфиденциальность информации;
- целостность информации;
- доступность информации, когда она нужна.

Угрозы информационной безопасности



Угрозы информационной безопасности



https://en.ppt-online.org/23157

Информация по уровням доступа

С точки зрения права:

1. Информация ***без ограничения*** права доступа;

К такому рода информации, например, относится:

• информация общего пользования, предоставляемая пользователям бесплатно;

• информация о состоянии окружающей природной среды, ее загрязнении (Федеральный закон от 2 мая 1997 г. № 76-ФЗ «Об уничтожении химического оружия»);

• информация в области работ по хранению, перевозке, уничтожению химического оружия (Федеральный закон от 2 мая 1997 г. № 76-ФЗ «Об уничтожении химического оружия», статья 1.2).

Информация, содержащая сведения об обстоятельствах и фактах, представляющих угрозу жизни, здоровью граждан, не подлежит засекречиванию, не может быть отнесена к тайне.

2. Информация ***с ограниченным доступом*** – государственная тайна, служебная тайна, коммерческая тайна (в т. ч. ноухау), банковская тайна, профессиональная тайна и персональные данные, как институт охраны права неприкосновенности частной жизни;

3. Информация, распространение которой ***наносит вред*** интересам общества, законным интересам и правам граждан; – порнография; информация, разжигающая национальную, расовую и другую рознь; пропаганда и призывы к войне, ложная реклама, реклама со скрытыми вставками и т. п. – так называемая «вредная» информация.

4 Объекты интеллектуальной собственности: авторское право, патентное право, средства индивидуализации и т. п. Исключение составляют ноу-хау, которые охраняются в режиме коммерческой тайны

Законодательство в сфере ИБ

Объект защиты	Законодательные и нормативные акты
Национальная безопасность	**Доктрина информационной безопасности Российской Федерации** (утверждена Президентом РФ от 9 сентября 2000 г. № Пр-1895)
Интеллектуальная собственность	**Гражданский кодекс РФ, статья 1274.** Свободное использование произведения в информационных, научных, учебных или культурных целях.
Компьютерная информация	**Уголовный кодекс, статья 272. Неправомерный доступ к компьютерной информации:** 1) штраф в размере до **500 тысяч рублей**; 2) срок лишения свободы до **7 лет**;
Компьютерные сети	**Статья 273. Создание, использование и распространение вредоносных компьютерных программ.** 1) штраф в размере до **200 тысяч рублей**; 2) срок лишения свободы до **7 лет**;
Компьютеры и телекоммуникационные сети	**Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей:** 1) штраф в размере до **200 тысяч рублей**; 2) срок лишения свободы до **5 лет**.

Составы компьютерных преступлений

Составы компьютерных преступлений (т.е. перечень признаков, характеризующих общественно опасное деяние как конкретное преступление) приведены в ***28 главе УК,*** которая называется ***"Преступления в сфере компьютерной информации"*** и содержит три статьи:

- ст. 272 "Неправомерный доступ к компьютерной информации";
- ст. 273 "Создание, использование и распространение вредоносных программ для ЭВМ" ;
- ст. 274 "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети".

Неправомерный доступ к компьютерной информации (ст. 272 УК)

Предусматривает ответственность **за неправомерный доступ к компьютерной информации** (информации на машинном носителе, в ЭВМ или сети ЭВМ), если это повлекло

- *уничтожение,*
- *блокирование,*
- *модификацию либо копирование информации,*
- *нарушение работы вычислительных систем.*

Неправомерный доступ к компьютерной информации (ст. 272 УК)

Преступное деяние состоит в неправомерном доступе к охраняемой законом компьютерной информации, который всегда носит характер совершения определенных действий и может выражаться в проникновении в компьютерную систему путем использования специальных технических или программных средств позволяющих преодолеть установленные системы защиты; незаконного применения действующих паролей или маскировка под видом законного пользователя для проникновения в компьютер, хищения носителей информации, при условии, что были приняты меры их охраны, если это деяние повлекло уничтожение или блокирование информации.

Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК)

Статья предусматривает уголовную ответственность за ***создание программ для ЭВМ или их модификацию***, заведомо *приводящее к несанкционированному уничтожению, блокированию и модификации, либо копированию информации, нарушению работы информационных систем, а равно использование таких программ или машинных носителей с такими программами*.

Статья защищает права владельца компьютерной системы на неприкосновенность находящейся в ней информации.

Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК)

Под созданием вредоносных программам в смысле ст. 273 УК РФ понимаются программы специально разработанные для нарушения нормального функционирования компьютерных программ. Под нормальным функционированием понимается выполнение операций, для которых эти программы предназначены, определенные в документации на программу. Наиболее распространенными видами вредоносных программ являются широко известные **компьютерные вирусы и логические бомбы.**

Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК)

Под использованием программы понимается выпуск в свет, воспроизведение, распространение и иные действия по их введению в оборот. Использование может осуществляться путем записи в память ЭВМ, на материальный носитель, распространения по сетям, либо путем иной передачи другим лицам.

Уголовная ответственность по этой статье возникает уже в результате создания программы, независимо от того использовалась эта программа или нет.

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274. УК)

Статья 274 УК устанавливает ответственность за ***нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети*** лицом, имеющим доступ к ним, *повлекшее уничтожение, блокирование или модификацию охраняемой законом информации, если это деяние причинило существенный вред.*

Статья защищает интерес владельца вычислительной системы относительно ее правильной эксплуатации.

Составы компьютерных преступлений

Предусмотренные составы компьютерных преступлений не охватывают полностью всех видов совершения компьютерных посягательств.

Статьи :

- **146 УК РФ - нарушение авторских и смежных прав ;**
- **147 УК РФ - нарушение изобретательских и патентных прав,**

- дающие возможность уголовного преследования за незаконное использование программного обеспечения.

Составы компьютерных преступлений

Хотя четкого определения компьютерного преступления не существует, их условно можно подразделить на две большие категории:

- **преступления, связанные с вмешательством в работу компьютеров**
- **преступления, использующие компьютеры как необходимые технические средства**.

Вывод: таким образом, компьютерное преступление, *есть противоправные действия, направленные на достижение доступа к хранимой на компьютере информации, имеющей ограниченные права доступа. При этом компьютер может быть как объектом преступления, так и в качестве инструмента преступной деятельности.*

Составы компьютерных преступлений

Целью защиты информации *является гарантирование законных прав различных категорий пользователей на обеспечение возможности разграничения доступа к информации.*

Объекты нападений компьютерных преступлений

1. Компьютеры военных и разведывательных организаций (в шпионских целях).
2. Компании и предприятия бизнеса (промышленный шпионаж).
3. Банки и предприятия бизнеса (профессиональные преступники).
4. Компьютеры любых организаций, особенно правительственных и коммунальных (террористы).
5. Любая компания (мишень для бывших служащих, а университеты – для студентов).
6. Любая организация (с целью разрешения интеллектуальной головоломки, а иногда при выполнении заказов).

Приемы компьютерных преступлений

Изъятие средств вычислительной техники (СВТ) производится с целью получения системных блоков, отдельных винчестеров или других носителей информации, содержащих в памяти установочные данные о клиентах, вкладчиках, кредиторах банка и т.д.

Такие действия проводятся путем хищения, разбоя, вымогательства и сами по себе содержат состав обычных «некомпьютерных» преступлений. Они квалифицируются по ст. 158, 161, 162,163 УК России.

Приемы компьютерных преступлений

Перехват (негласное получение) информации также служит для «снятия» определенных сведений с помощью методов и аппаратуры аудио-, визуального и электромагнитного наблюдения.

Объектами, как правило, являются **каналы связи, телекоммуникационное оборудование, служебные помещения** для проведения конфиденциальных переговоров, **бумажные и магнитные носители** (в том числе и технологические отходы). Это компетенция ст. 138,183 УК.

Приемы компьютерных преступлений

Несанкционированный доступ (НСД) к средствам вычислительной техники - это активные действия по созданию возможности распоряжаться информацией без согласия собственника.

Они могут быть квалифицированы с использованием ст. 183, 272 УК. **НСД** обычно реализуется с использованием следующих основных приемов:

- **«за дураком»** - физическое проникновение в производственные помещения.
- **«за хвост»** - злоумышленник подключается к линии связи законного пользователя и дожидается сигнала, обозначающего «конец работы», перехватывает его на себя, а потом, когда законный пользователь заканчивает активный режим, осуществляет доступ к банковской системе.

Приемы компьютерных преступлений

- **«компьютерный абордаж»** - злоумышленник вручную или с использованием автоматической программы подбирает код (пароль) доступа к КС системе с использованием обычного телефонного аппарата.
- **«неспешный выбор»** - преступник изучает и исследует систему защиты от НСД, ее слабые места, выявляет участки, имеющие ошибки или неудачную логику программного строения, разрывы программ (брешь, люк) и вводит дополнительные команды, разрешающие доступ;
- **«маскарад»** - злоумышленник проникает в компьютерную систему, выдавая себя за законного пользователя с применением его кодов (паролей) и других идентифицирующих шифров;

Приемы компьютерных преступлений

- **«мистификация»** - злоумышленник создает условия, когда законный пользователь осуществляет связь с нелегальным терминалом, будучи абсолютно уверенным в том, что он работаете нужным ему законным абонентом. Формируя правдоподобные ответы на запросы законного пользователя и поддерживая его заблуждения некоторое время, злоумышленник добывает коды (пароли) доступа или отклик на пароль;
- **«аварийный»** - злоумышленник создает условия для возникновения сбоев или других отклонений в работе СВТ. При этом включается особая программа, позволяющая в аварийном режиме получать доступ к наиболее ценным данным. В этом режиме возможно «отключение» всех имеющихся в компьютерной