ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

ВИТИ МИФИ НИЯУ

Угрозы информационным системам. Факторы, приводящие к информационным потерям.

Угрозы информационным системам. Факторы, приводящие к информационным потерям.

1. ***Введение.***
2. ***Осуществление угроз информационным ресурсам.***
3. ***Факторы, приводящие к информационным потерям.***
4. ***Виды угроз информации.***
5. ***Источники возникновения угроз.***

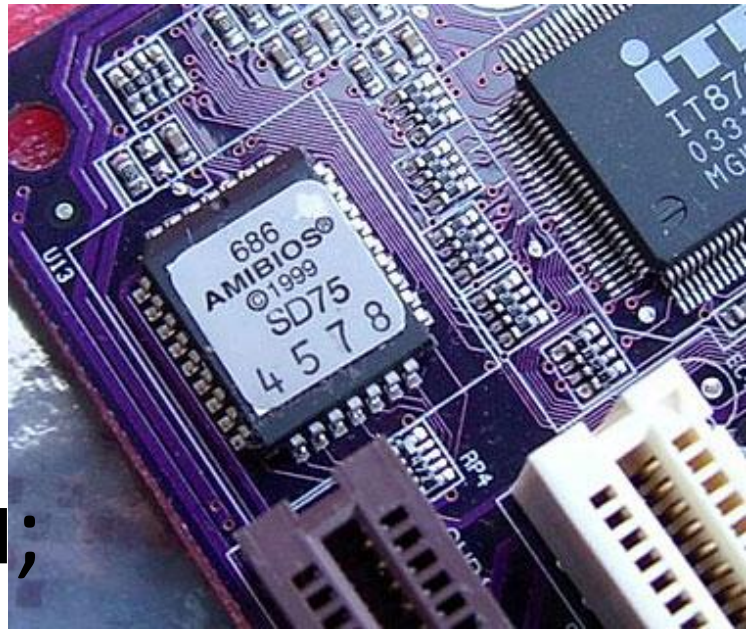
УГРОЗА БЕЗОПАСНОСТИ

- реальные или потенциально возможные действия или условия, приводящие к овладению, хищению, искажению, изменению или уничтожению информации в информационной системе, а также к прямым материальным убыткам за счет воздействия на материальные ресурсы

Классификация угроз безопасности

1. по воздействию на основные характеристики ИС;
2. по природе возникновения;
3. по ориентации.

КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ПО ВОЗДЕЙСТВИЮ НА ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ИС



- отказ в обслуживании;
- нарушение целостности (модификация);
- нарушение конфиденциальности.

КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ПО ПРИРОДЕ ВОЗНИКНОВЕНИЯ

- стихийные бедствия;
- несчастные случаи (чрезвычайные происшествия);
- различного рода ошибки или злоупотребления;
- сбои и отказы оборудования и др.

КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ПО ОРИЕНТАЦИИ

- угрозы персоналу;
- материальным и финансовым ресурсам и информации, как составным элементам информационной системы.

Требования к информационным системам

1. Готовность.
2. Надежность.
3. Конфиденциальнос

ГОТОВНОСТЬ

- способность информационной системы обеспечить законным пользователям условия доступа к ресурсам в соответствии принятым режимом работы.

НАДЕЖНОСТЬ

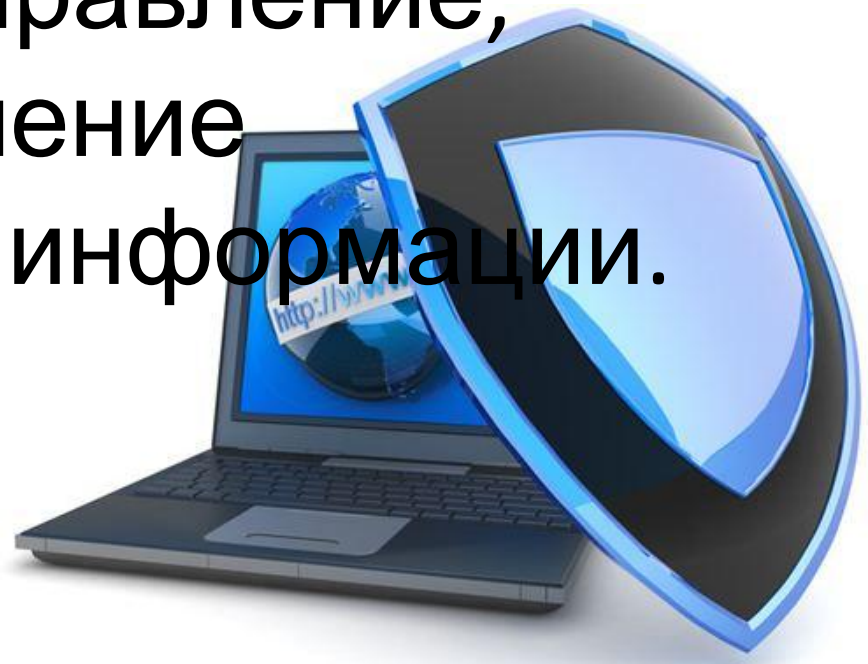
- способность системы обеспечивать целостность и сохранность информации ее законных пользовате.

КОНФИДЕНЦИАЛЬНОСТЬ

- способность системы обеспечивать информационные потребности только законным пользователя интересов.

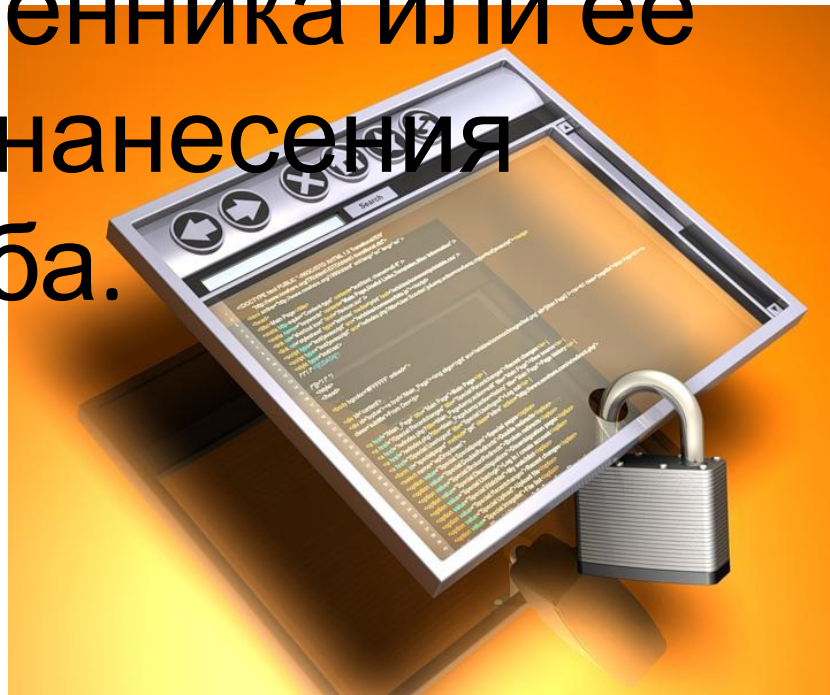
ПОЛИТИКА БЕЗОПАСНОСТИ

- набор законов, правил и практического опыта, на основе которых строится управление, защита и распределение конфиденциальной информации.



УГРОЗЫ ИНФОРМАЦИОННЫМ РЕСУРСАМ

- овладение конфиденциальной информацией, ее модификация в интересах злоумышленника или ее разрушении с целью нанесения материального ущерба.



Осуществление угроз информационным ресурсам

может быть произведено:

1) методами, использующими психологические особенности людей;

2) через имеющиеся агентурные источники в органах государственного управления, коммерческих структур, имеющих возможность получения конфиденциальной информации;

3) путем подкупа лиц, непосредственно работающих на предприятии или структурах, непосредственно связанных с его деятельностью;

Осуществление угроз информационным ресурсам

4) путем перехвата информации, циркулирующей в средствах и системах связи и вычислительной техники, с помощью технических средств разведки и съема информации, несанкционированного доступа к информации и преднамеренных программно-математических воздействий на нее в процессе обработки и хранения;

5) путем подслушивания конфиденциальных переговоров, ведущихся в служебных помещениях, служебном и личном автотранспорте, на квартирах и дачах;

Осуществление угроз информационным ресурсам

6) через переговорные процессы с иностранными или отечественными фирмами, используя неосторожное обращение с информацией;

7) через инициативных лиц из числа сотрудников, которые хотят заработать деньги и улучшить свое благосостояние или проявляют инициативу по другим
или материальным причинам.

Факторы, приводящие к информационным потерям

1. Несчастные случаи.
2. Кража и преднамеренная порча материальных средств.
3. Аварии, выход из строя аппаратуры, программ и баз данных.
4. Ошибки накопления, хранения, передачи и использования информации.
5. Ошибки эксплуатации.
6. Концептуальные ошибки и ошибки внедрения.
7. Злонамеренные действия в нематер[illegible]
8. Болтливость и разглашение.
9. Причины социального характера.
10. Промышленный шпионаж.

Несчастные случаи

Несчастные случаи вызывают частичный или полный вывод из строя оборудования или информационного ресурса.

Причинами этого могут быть:

— пожары, взрывы, аварии;

— удары, столкновения, падения;

— воздействия агрессивных химических или физических сред;

— поломка элементов машин различного характера: механического, электрического, электронного и электромагнитного;

— последствия природных явлений (наводнения, бури, молнии, град, оползни, землетрясения и т. д.).

Кража и преднамеренная порча материальных средств

Воруют, главным образом, небольшие по габаритам аппаратные средства (мониторы, процессорные блоки, клавиатуру, принтеры, модемы, кабели и оргтехнику), информационные носители (диски, дискеты, ленты, магнитные карты и др.) и различное другое имущество (документация, комплектующие и др.).
Посягательства и вредительские действия проявляются в самых различных формах: явные (например, оставленная отвертка внутри печатающего устройства, в корпусе вентилятора процессора) или скрытые (например, вредные химические вещества в помещениях и аппаратуре).

Аварии и выход из строя аппаратуры, программ и баз данных

Остановка или нарушение деятельности информационных центров не такие уж редкие события, а продолжительность этих состояний в основном небольшая. Но иногда, между тем, прямые и косвенные последствия этих действий могут быть весьма значительными.

Последствия этих действий к тому же не могут быть заранее предусмотрены и оценены.

Ошибки хранения, накопления, передачи и использования информации

Эти ошибки связаны с человеческим фактором, будь-то при использовании традиционных носителей информации или при диалоговом обмене в режиме удаленного доступа.

При диалоговом режиме дополнительно прибавляются ошибки восприятия, чтения, интерпретации содержания и соблюдения правил.

Ошибки хранения, накопления, передачи и использования информации

Ошибки передачи зависят от используемой техники. Они могут быть *простыми* при использовании средств почтовой связи и *чисто техническими* (телепередача). В обоих случаях могут быть потери, ошибки неумения, оплошности, наличие помех, сбои и искажения отдельных букв или сообщений. Ошибки подобного рода оцениваются как потери предприятия. И хотя их трудно определить и оценить, но учитывать необходимо

Ошибки эксплуатации

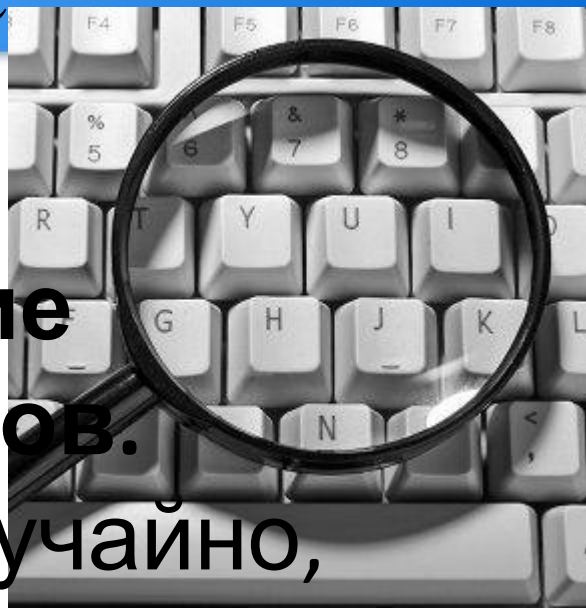
1) нарушение защиты;
2) переполнение файлов;
3) ошибки языка управления данными;
4) ошибки при подготовке и вводе информации;
5) ошибки операционной системы;
6) ошибки программы;
7) аппаратные ошибки;
8) ошибочное толкование инструкций;
9) пропуск операций.

Концептуальные ошибки и ошибки внедрения

Концептуальные ошибки могут иметь драматические последствия в процессе эксплуатации информационной системы.

Ошибки внедрения бывают в основном менее опасными и достаточно легко устранимыми.

Злонамеренные действия в нематериальной сфере



Мошенничество и хищение информационных ресурсов.
Нередко все начинается случайно, часто с небольшого правонарушения. Мошенничество часто совершается в корыстных целях, по договоренности с третьими лицами (сотрудничество).

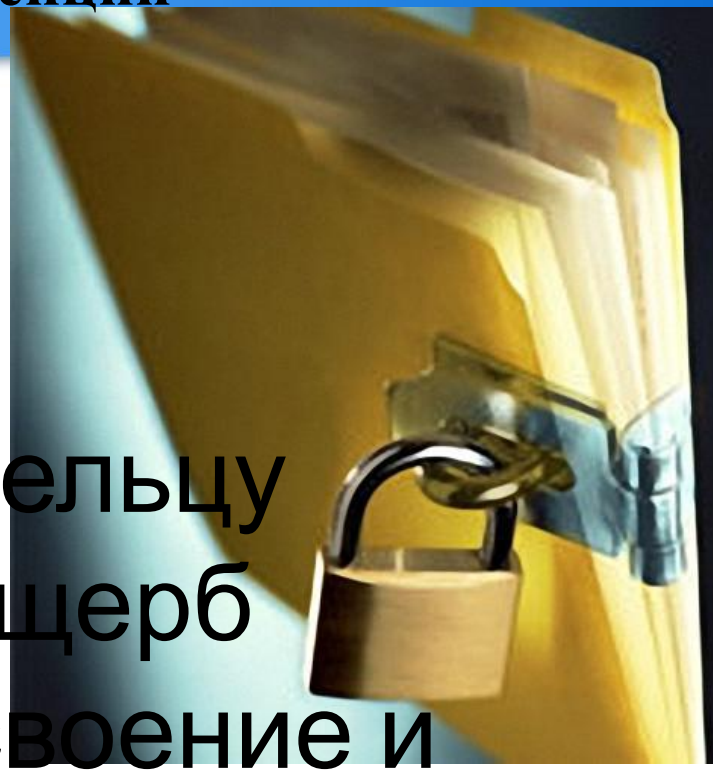
Болтливость и разглашение

Эти действия, последствия которых не поддаются учету, относятся к числу трудно контролируемых и могут находиться в рамках от простого, наивного хвастовства до промышленного шпионажа в коммерческой деятельности.

Причины социального характера

Увольнение сотрудников, забастовки и другие действия персонала, приводящие к производственным потерям и неукомплектованности рабочих мест. Опасность этих действий существует почти всегда.

Промышленный шпионаж, как форма недобросовестной конкуренции



— это наносящие владельцу коммерческой тайны ущерб незаконный сбор, присвоение и передача сведений, составляющих коммерческую тайну.

Виды угроз информации

1. Угроза раскрытия.
2. Угроза целостност
3. Угроза отказа в обслуживании.

Угроза раскрытия

– информация становится известной тому, кому не следовало бы ее знать. В терминах компьютерной безопасности угроза раскрытия имеет место всякий раз, когда получен доступ к некоторой конфиденциальной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда вместо слова "раскрытие" используются термины "кража", "утечка"

Угроза целостности

– любое умышленное изменение (модификацию или даже удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую. Обычно считается, что **угрозе раскрытия** подвержены в большей степени государственные структуры, а **угрозе целостности** - деловые или коммерческие.

Угроза отказа в обслуживании

– возникает всякий раз, когда в результате некоторых действий блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным, так чтобы запрашиваемый ресурс никогда не был получен, или оно может вызвать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В таких случаях говорят, что ресурс исчерпан.

Источники возникновения угроз

1. Вход в систему.
2. Подсистемы связи.
3. Процессор.
4. Персонал.
5. Накопители.

ВХОД В СИСТЕМУ

– неправильная идентификация и аутентификация

ПОДСИСТЕМЫ СВЯЗИ

– подключение записывающих и следящих устройств;

- электромагнитное излучение;
- телефонные подслушивающие устройства;
- взаимные помехи;
- неправильные соединения;
- перекрестные соединения;
- вставка неразрешенных сообщений;
- удаление текущих сообщений;
- несанкционированный доступ к сообщениям;

ПРОЦЕССОР

- неисправность защитных цепей;
- распространение опасного программного обеспечения;
- сбой в защитных функциях программы;
- неправильное управление доступом.

ПЕРСОНАЛ

- замена санкционированного программного обеспечения на несанкционированное;
- разглашение защитных мер;
- отключение защитных устройств в аппаратном обеспечении;
- использование автономных программ;
- отключение защитных функций в программном обеспечении;
- незаконный доступ к системе.

НАКОПИТЕЛИ

- кража;
- незаконное копирование;
- несанкционированный доступ;
- разрушение или удаление.

Благодарим за внимание!