ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
В ЮРИСПРУДЕНЦИИ

Pur-11@yandex.ru

ПОНЯТИЕ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Модель угроз - это физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Модель нарушителя – часть модели угроз, в которой приводится описание потенциальных нарушителей (внутренних и внешних) и их возможностей по реализации угроз.

ПРИМЕР ФРАГМЕНТА ТАБЛИЦЫ, СОДЕРЖАЩЕЙ ОПИСАНИЕ ВЫЯВЛЕННЫХ УГРОЗ ПРИ ПОСТРОЕНИИ МОДЕЛИ УГРОЗ

Угроза	Способ реализации	Уязвимость	Источник	Объект воздействия	Негативные последствия
Угрозы, связанные с преднамеренными или непреднамеренными действиями сотрудников					
У1. Разглашение данных	**Вынос со трудником носителей с персональными данными за пределы контролируемой зоны**	**Возможность подключения неучтённых съемных носи телей.**	**Внутренние нарушители (сотрудники отдела по работе с клиентами)**	**Фрагменты защищаемой информации, содержащей персональные данные**	**Нарушение конфиден-циально сти**
	Отправка персональных данных за пределы локальной сети	**Отсутствие контроля от правляемых сооб щений по элек тронной почте**			

ПРИМЕР ФРАГМЕНТА ТАБЛИЦЫ, СОДЕРЖАЩЕЙ ОПИСАНИЕ ВЫЯВЛЕННЫХ УГРОЗ ПРИ ПОСТРОЕНИИ МОДЕЛИ УГРОЗ (ПРОДОЛЖЕНИЕ)

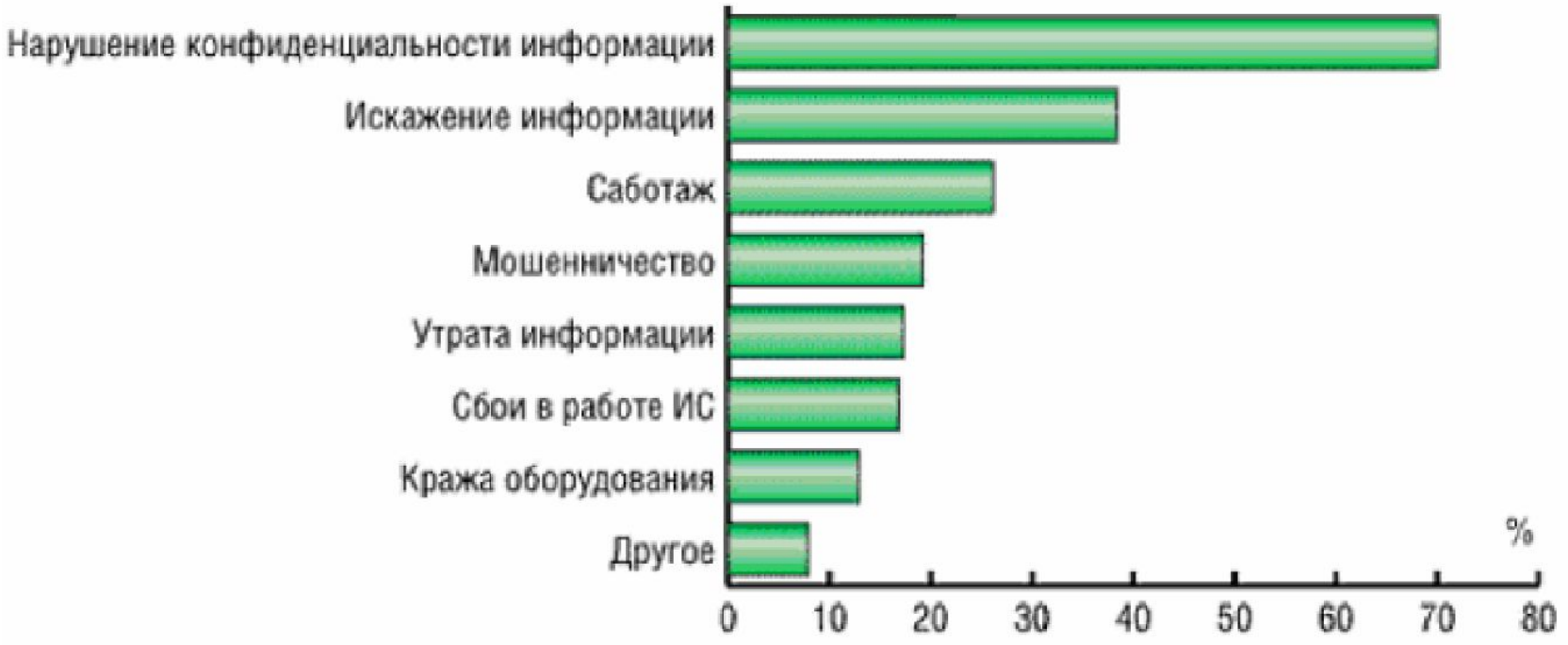
Угроза	Способ реализации	Уязвимость	Источник	Объект воздействия	Негативные последствия
Угрозы, связанные с преднамеренными или непреднамеренными действиями сотрудников					
У2 Угроза заражения вредоносным ПО	**Запуск заражённого файла, полученного по электронной почте**	**Недостатки настройки антивирусной защиты (пользователю доступны функции приостановки защиты на рабочем месте). Незнание пользователями правил безопасности при работе с электронной почтой.**	**Внутренний нарушитель (сотрудники отдела по работе с клиентами)**	**Защищаемая информация на рабочем месте пользователя.**	**Нарушение целостности и конфиденциальности**

КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

1. **По цели воздействия**: нарушение конфиденциальности, целостности, доступности.
2. **По характеру источника угрозы**: субъективные и объективные.
3. **По характеру/природе происхождения**: случайные и преднамеренные (внутренние и внешние)
4. **По характеру воздействия**: активные, пассивные.

КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

ВНУТРЕННИЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



ИДЕНТИФИКАЦИЯ ФАКТОРОВ В ПРОЦЕССЕ АНАЛИЗА УГРОЗ

Напомним (из предыдущей лекции), что независимо от особенностей классификационных систем в процессе анализа угроз для каждой угрозы должны быть *идентифицированы:*

- возможные источники угрозы (см.следующий слайд);
- уязвимости системы, позволяющие реализовать угрозу;
- способы, посредством которых может быть реализована угроза;
- объект воздействия угрозы;
- последствия для информации, ассоциированной с объектом угрозы.

На основании результатов анализа угроз формируется *модель системы защиты информации.*

ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Внешние:

- политика иностранных государств;
- действия разведок и спецслужб;
- экспансия информационных систем в другие государства;
- действия преступных групп;
- стихийные бедствия.

Внутренние:

- противозаконная деятельность различных структур, лиц, групп в области распространения и употребления информации;
- неэффективное регулирование правовых отношений в информационной среде;
- нарушение установленных регламентом сбора, обработки и передачи информации;
- ошибки персонала и пользователей, непреднамеренные и преднамеренные ошибки разработчиков, пользователей; отставание отечественной промышленности;
- отказы и сбои технических систем;неправомерное действие государственных структур.

НЕФОРМАЛЬНАЯ МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Нарушитель – это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Злоумышленник - нарушитель, намеренно идущий на нарушение из корыстных побуждений.

Неформальная модель нарушителя отражает его практические и теоретические возможности, априорные знания, время и место действия и т.п.

НЕФОРМАЛЬНАЯ МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

•Определение конкретных значений характеристик возможных нарушителей в значительной степени субъективно.

•Модель нарушителя, построенная с учетом особенностей конкретной предметной области и технологии обработки информации, может быть представлена перечислением нескольких вариантов его облика.

•Каждый вид нарушителя должен быть охарактеризован значениями характеристик *(см. следующий слайд).*

НЕФОРМАЛЬНАЯ МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

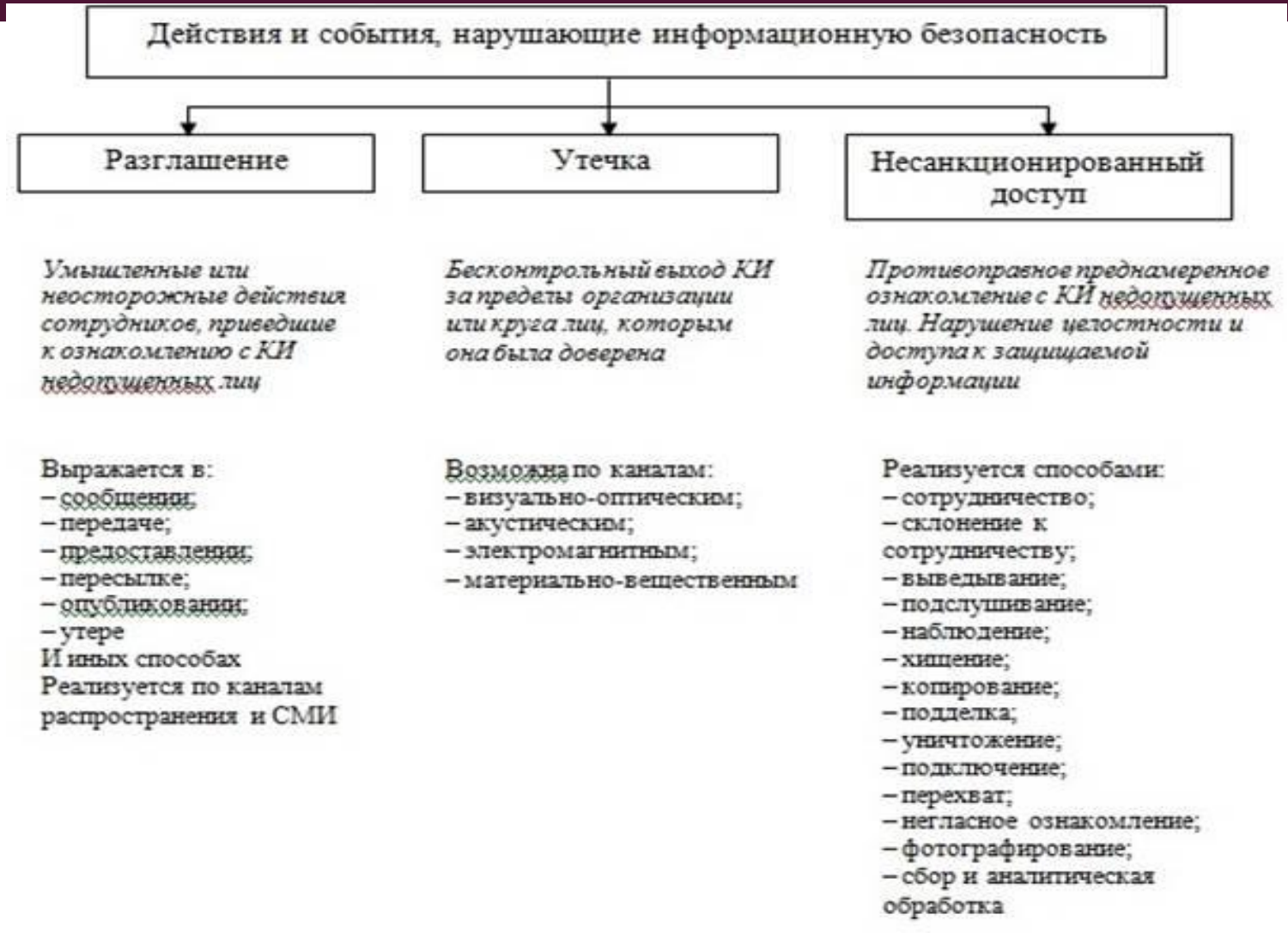
При разработке неформальной модели нарушителя **определяются:**

- предположения о категориях лиц, к которым может принадлежать нарушитель;
- предположения о мотивах действий нарушителя (преследуемых нарушителем целях);
- предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средства);
- ограничения и предположения о характере возможных действий нарушителей. По отношению к информационным ресурсам нарушители могут быть внутренними (из числа персонала) или внешними (посторонними лицами).

КЛАССИФИКАЦИЯ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- по уровню знаний об информационной системе;
- по уровню возможностей (используемым методам и средствам);
- по времени действия;
- по месту действия.

СРЕДСТВА РЕАЛИЗАЦИИ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



ЦЕЛЕВАЯ НАПРАВЛЕННОСТЬ УГРОЗ

Ключевым параметром классификации угроз является их *целевая направленность* (определяемая свойствами информации- конфиденциальность, целостность, доступность, нарушение которых возможно при реализации угрозы).

Угроза нарушения **конфиденциальности** -информация становится известной тому, кто не располагает полномочиями доступа к ней.

Угроза нарушения **целостности** *(см.следующий слайд)* – это угрозы, связанные с вероятностью модификации той или иной информации, хранящейся в информационной системе.

Угроза нарушения **доступности** -создание таких условий, при которых доступ к услуге или информации будет либо заблокирован, либо возможен за время, которое не обеспечит выполнение тех или иных бизнес-целей.

ЦЕЛЕВАЯ НАПРАВЛЕННОСТЬ УГРОЗ

Основные причины нарушения целостности информации.

1. Субъективные

1.1. Преднамеренные.

1.1.1. Вывод из строя оборудования, диверсия (организация пожаров, взрывов, повреждений электропитания и др.).

1.1.2. Непосредственные действия над носителем (хищение, подмена носителей, уничтожение информации).

1.1.3. Информационное воздействие (электромагнитное облучение, ввод в компьютерные системы разрушающих программных средств, воздействие на психику личности и психотропным оружием).

1.2. Непреднамеренные.

1.2.1. Ошибки и отказы обслуживающего персонала, пользователей, разработчиков.

2. Объективные.

2.1. Отказы и полный выход из строя оборудования, программ, систем питания и т.д.

2.2. Сбои (кратковременный выход из строя) аппаратуры, программ, систем питания и т.д.

2.3. Стихийные бедствия (наводнения, землетрясения, ураганы).

2.4. Несчастные случаи (пожары, взрывы, аварии).

2.5. Электромагнитная несовместимость.

КОНТРОЛЬНЫЕ ВОПРОСЫ ЛЕКЦИИ

1. Дайте понятие модели угроз и модели нарушителя.
2. Как могут быть представлены результаты анализа угроз?
3. Приведите классификацию угроз информационной безопасности.
4. Перечислите основные источники угроз информационной безопасности.
5. Кто может являться нарушителем информационной безопасности, а кто злоумышленником?
6. Какие параметры определяются при разработке неформальной модели нарушителя?
7. Кто может быть внутренним нарушителем информационной безопасности?
8. Какие существуют мотивы нарушений информационной безопасности?
9. Приведите классификацию нарушителей информационной безопасности.
10. Перечислите средства реализации угрозы информационной безопасности.
11. Что такое целевая направленность угроз информационной безопасности?
12. В чем заключается угроза нарушения конфиденциальности и целостности?
13. Перечислите основные причины нарушения целостности информации.
14. Что представляет нарушение доступности информации?