

**КЛАССИФИКАЦИЯ УГРОЗ И
ИСТОЧНИКОВ
ДЕСТАБИЛИЗИРУЮЩИХ
ВОЗДЕЙСТВИЙ НА
ИНФОРМАЦИЮ.**

Выполнил: Яшин М.А.
Группа 20501

Угроза – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и (или) целостности информации.

Классификация:

- 1) Угрозы конфиденциальности:
 - а) хищение (копирование) информации либо хищение средств обработки и хранения
 - б) утрата - неумышленная потеря носителя или средства обработки
- 2) Угрозы целостности
 - а) модификация - изменение содержания информации
 - б) уничтожение (информации или средств её обработки)
 - в) отрицание подлинности
 - г) навязывание ложной информации (дезинформация)
- 3) Угрозы доступности
 - а) блокирование
 - б) уничтожение информации и средств её обработки

По типу источника угроз:

Источники угроз делят на 3 группы:

- 1) Антропогенные
- 2) Техногенные
- 3) Стихийные

Все кроме стихийных делятся на внешние и внутренние

Антропогенные внешние:

- криминальные структуры,
- хакеры,
- недобросовестные партнеры,
- технический персонал поставщиков услуг связи,
- представители надзорных организаций,
- аварийных служб и представители силовых структур.

Антропогенные внутренние:

- основной персонал (пользователи, программисты, разработчики),
- вспомогательный персонал (уборщики и охрана),
- технический персонал.

Техногенные внешние:

- ▣ средства связи,
- ▣ сеть инженерных коммуникаций (водоснабжение, вентиляция),
- ▣ транспорт

Техногенные внутренние:

- некачественные технические средства обработки информации,
- некачественные программные средства обработки,
- вспомогательные средства (системы пожарноохранной сигнализации)

Источники дестабилизирующего воздействия на информацию:

- Люди
- Технические средства отображения (фиксации), хранения, обработки, воспроизведения, передачи информации, средства связи;
- Системы обеспечения функционирования технических средств отображения, хранения, обработки, воспроизведения и передачи информации;
- Технологические процессы отдельных категорий промышленных объектов;
- Природные явления.

- ❖ Виды дестабилизирующих воздействий на защищаемую информацию можно разбить на две группы: внешние и внутренние, каждая из которых, в свою очередь, делится на умышленные и случайные, которые могут быть явными и скрытыми.
- ❖ Метод дестабилизирующего воздействия в ГОСТе назван фактором!!! Факторы, воздействующие на защищаемую информацию и подлежащие учету при организации защиты информации, по признаку отношения к природе возникновения делят на классы:
 - объективные;
 - субъективные.

По отношению к объекту информатизации факторы, воздействующие на защищаемую информацию, подразделяют на внутренние и внешние.

Объективные факторы:

1. Внутренние факторы

- Передача сигналов по проводным линиям связи.
- Передача сигналов по оптико-волоконным линиям связи.
- Излучения сигналов, функционально присущих ОИ.
 - Излучения акустических сигналов.
 - Излучения неречевых сигналов.
 - Излучения речевых сигналов.
 - Электромагнитные излучения и поля.
 - Излучения в радиодиапазоне.
 - Излучения в оптическом диапазоне.
- Паразитное электромагнитное излучение.
- Наводки.
 - Наводки в электрических цепях ТС, имеющих выход за пределы ОИ.
 - Наводки в линиях связи.
 - Наводки в цепях электропитания.
 - Наводки в цепях заземления.
 - Наводки на ТС, провода, кабели и иные токопроводящие коммуникации и конструкции, гальванически не связанные с ТС ОИ, вызванные побочными и (или) паразитными электромагнитными излучениями, несущими информацию.
- Акустоэлектрические преобразования в элементах ТС ОИ.
- Дефекты, сбои, отказы, аварии ТС и систем ОИ.
- Дефекты, сбои и отказы программного обеспечения ОИ.

1. Внешние факторы

- Явления техногенного характера.
 - Непреднамеренные электромагнитные облучения ОИ.
 - Радиационные облучения ОИ.
 - Сбои, отказы и аварии систем обеспечения ОИ.
- Природные явления, стихийные бедствия.
 - Термические факторы (пожары и т. д.).
 - Климатические факторы (наводнения и т. д.).
 - Механические факторы (землетрясения и т. д.).
 - Электромагнитные факторы (грозовые разряды и т. д.).
 - Биологические факторы (микробы, грызуны и т. д.).

Субъективные факторы.

1. Внутренние факторы:

- Разглашение защищаемой информации лицами, имеющими к ней право доступа.
 - Разглашение информации лицам, не имеющим права доступа к защищаемой информации.
 - Передача информации по открытым линиям связи.
 - Обработка информации на незащищенных ТС обработки информации.
 - Опубликование информации в открытой печати и других средствах массовой информации.
 - Копирование информации на незарегистрированный носитель информации.
 - Передача носителя информации лицу, не имеющему права доступа к ней.
 - Утрата носителя с информацией.
- Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации.
 - Несанкционированное изменение информации.
- Несанкционированный доступ к защищаемой информации.
 - Подключение к техническим средствам и системам ОИ.
 - Использование закладочных устройств.
 - Хищение носителя защищаемой информации.
 - Нарушение функционирования ТС обработки информации.
- Неправильное организационное обеспечение защиты информации.
- Ошибки обслуживающего персонала ОИ.

1. Внешние факторы

- Доступ к защищаемой информации с применением технических средств.
 - Доступ к защищаемой информации с применением технических средств разведки.
 - Доступ к защищаемой информации с применением средств визуально-оптической разведки.
 - Доступ к защищаемой информации с использованием эффекта «высокочастотного навязывания».
- Несанкционированный доступ к защищаемой информации.
- Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку.
- Действия криминальных групп и отдельных

Виды воздействия	Способы дестабилизирующего воздействия	Результат воздействия на информацию
1. Со стороны людей		
Непосредственное воздействие на носители защищаемой информации	<ul style="list-style-type: none"> - физическое разрушение; - создание аварийных ситуаций для носителей; - удаление информации с носителей; - создание искусственных магнитных полей для размагничивания носителей; - внесение фальсифицированной информации в носители. 	Уничтожение, искажение, блокирование
Несанкционированное распространение конфиденциальной информации	<ul style="list-style-type: none"> - словесная передача (сообщение) информации; - передача копий(снимков) носителей информации; - показ носителей информации; - ввод информации в вычислительные сети; - опубликование информации в открытой печати; - использование информации в публичных выступлениях. 	разглашение
Вывод из строя технических средств (ТС) при работе с информацией и средств связи	<ul style="list-style-type: none"> - неправильный монтаж ТС; - поломка(разрушение) ТС. В т.ч. разрыв (повреждение) кабельных линий связи; - создание аварийных ситуаций для ТС; - отключение ТС от сетей питания; - вывод из строя систем обеспечения функционирования ТС; - вмонтирование в ЭВМ разрушающих радио и программных закладок. 	Уничтожение, искажение, блокирование
Нарушение режима работы ТС и технологии обработки информации	<ul style="list-style-type: none"> - повреждение отдельных элементов ТС; - нарушение правил эксплуатации ТС; - внесение изменений в порядок обработки информации; - заражение программ обработки информации вредоносными вирусами; - выдача неправильных программных команд; - превышение расчетного числа запросов; - создание помех в радиозфире с помощью дополнительного звукового или шумового фона; - передача ложных сигналов; - подключение подавляющих фильтров в информационные цепи, цепи питания и заземления; - нарушение, изменение режима работы систем обеспечения функционирования ТС. 	Уничтожение, искажение, блокирование
Вывод из строя и нарушение режима работы систем обеспечения функционирования ТС	<ul style="list-style-type: none"> - неправильный монтаж систем; - поломка, разрушение систем или их элементов; - создание аварийных ситуаций для систем; - отключения систем от источников питания; - нарушение правил эксплуатации систем. 	Уничтожение, искажение, блокирование

2. Со стороны технических средств при работе с информацией и средств связи

Выход ТС из строя	<p>-техническая поломка, авария (без вмешательства людей);</p> <ul style="list-style-type: none">- возгорание, затопление(без вмешательства людей);- выход из строя систем обеспечения функционирования ТС;- воздействие природных явлений;- воздействие измененной структуры окружающего магнитного поля;- заражение программ обработки носителя информации, в том числе размагничивание магнитного слоя диска(ленты) из-за осыпания магнитного порошка.	Уничтожение, искажение, блокирование
Создание электромагнит-ных излучений	<ul style="list-style-type: none">- запись электромагнитных излучений.	Хищение

3. Со стороны систем обеспечения функционирования ТС при работе с информацией

Выход систем из строя	<ul style="list-style-type: none">- техническая поломка, авария(без вмешательства людей);- возгорание, затопление(без вмешательства людей);- выход из строя источников питания;- воздействие природных явлений.	Уничтожение, искажение, блокирование
Сбои в работе систем	<ul style="list-style-type: none">- появление технических неисправностей элементов систем;- воздействие природных явлений;- нарушение режима работы источников питания.	Уничтожение. Искажение, блокирование

4. Со стороны технологических процессов отдельных промышленных объектов

Изменение структуры окружающей среды	<ul style="list-style-type: none">- изменение естественного радиационного фона окружающей среды при функционировании объектов ядерной энергетики;- изменение естественного химического состава окружающей среды при функционировании объектов химической промышленности;- изменения локальной структуры магнитного поля из-за деятельности объектов радиоэлектроники и изготовлению некоторых видов вооружения и военной техники.	Хищение
--------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------

5. Со стороны природных явлений

<p>Землетрясение, наводнение, ураган (смерч), шторм, оползни, лавины, извержения вулканов</p>	<ul style="list-style-type: none">- разрушение (поломка), затопление, сожжение носителей информации, ТС работы с информацией, кабельных средств связи, систем обеспечения функционирования ТС;- нарушение режима работы ТС и систем обеспечения функционирования ТС;- нарушение технологии обработки.	<p>Потеря, уничтожение, искажение, блокирование, хищение</p>
<p>Гроза, дождь, снег, перепады температуры и влажности воздуха. Магнитные бури</p>		