Угрозы и нарушители безопасности информации

Содержание лекции

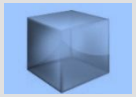
Понятие угрозы безопасности информации

Виды угроз безопасности информации

Источники угроз безопасности информации

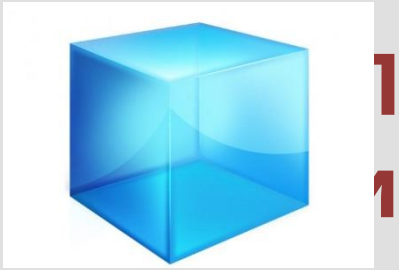
Нарушители безопасности информации

Виды и цели нарушителей



Потенциал и возможности нарушителей

Способы реализации угроз нарушителем



Понятие угрозы безопасности информации

ГОСТ Р 50922-2006

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 50922— 2006

Защита информации

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Издание официальное

БЗ 1—2007/378

Москва
Стандартинформ
2008

Понятие угрозы безопасности информации

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

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 50922— 2006

Защита информации

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Издание официальное

БЗ 1–2007/378

Москва
Стандартинформ
2008

http://docs.cntd.ru

Понятие угрозы безопасности информации

Источник угрозы безопасности информации – субъект (физическое лицо,
материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 50922— 2006

Защита информации

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Издание официальное

БЗ 1–2007/378

Москва
Стандартинформ
2008

http://docs.cntd.ru

Понятие угрозы безопасности информации

Уязвимость (информационной системы) – свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 50922— 2006

Защита информации

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

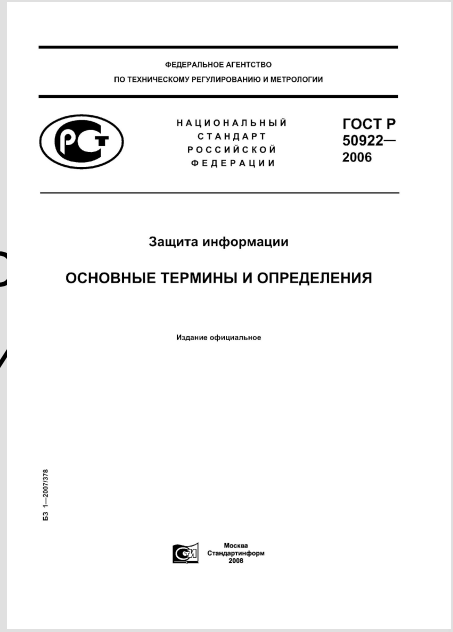
Издание официальное

Москва
Стандартинформ
2008

http://docs.cntd.ru

Понятие угрозы безопасности информации

Фактор, воздействующий на защищаемую информацию – явление, действие или процесс, результатом которо могут быть утечка, искажение, уничтожени защищаемой информации, блокирование доступа к ней.


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 50922— 2006

Защита информации

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Издание официальное

Москва
Стандартинформ
2008

http://docs.cntd.ru

Руководящий документ ФСТЭК России

ФСТЭК России – Федеральная служба по техническому и экспортному контролю

Руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения»

РД ФСТЭК

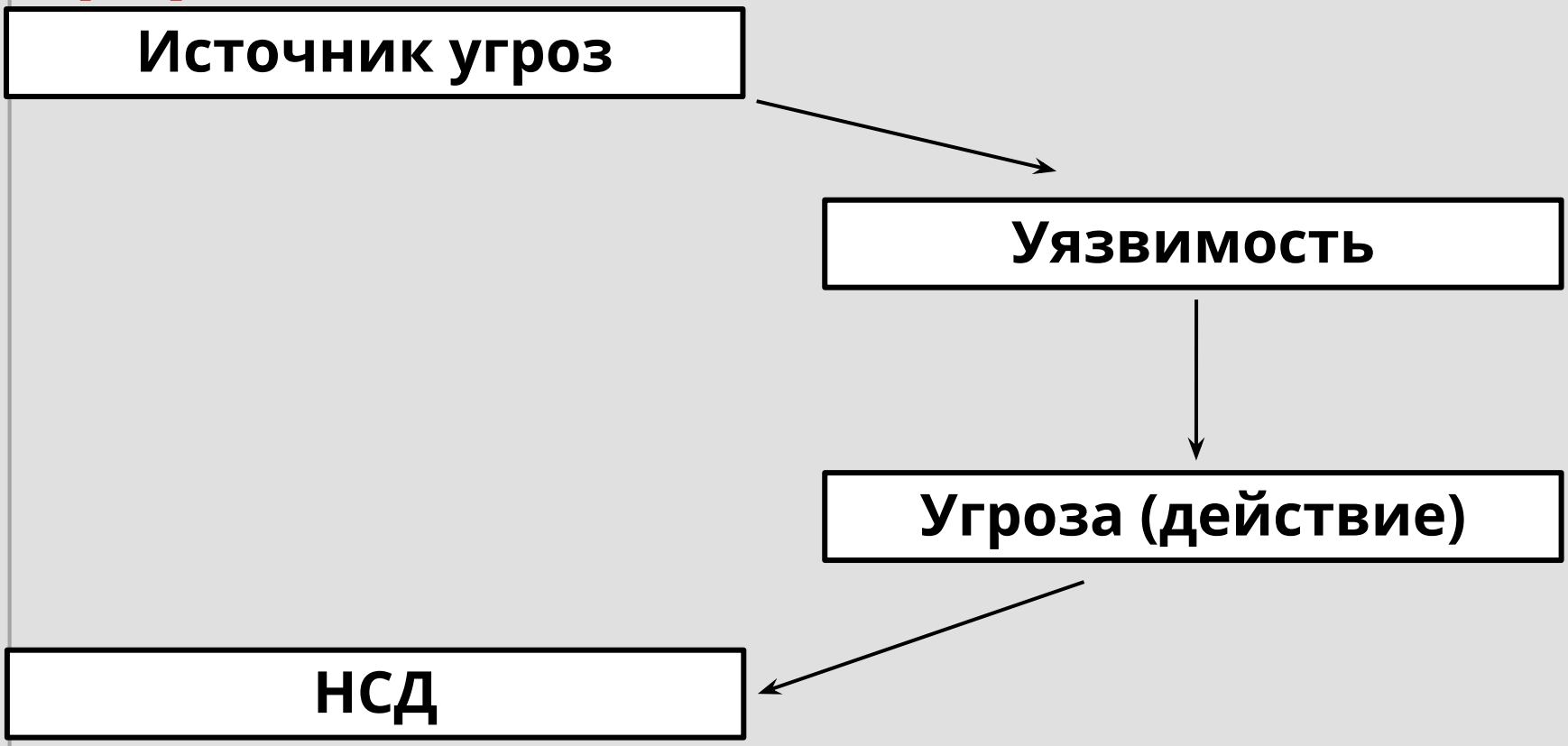
Понятие угрозы безопасности информации

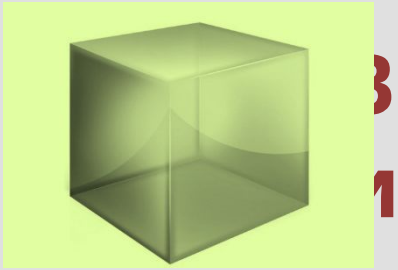
Несанкционированный доступ к информации (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Примечание: под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.

РД ФСТЭК

Понятие угрозы безопасности информации





Виды угроз безопасности информации

Виды угроз безопасности информации

Основные виды угроз безопасности:

- Хищение (копирование информации)
- Уничтожение информации
- Модификация (искажение) информации
- Нарушение доступности (блокирование) информации
- Отрицание подлинности информации
- Навязывание ложной информации

Виды угроз безопасности информации

Классификация угроз ИБ:

- По аспекту информационной безопасности
- По компонентам объекта информатизации
- По способу осуществления
- По расположению источника угроз

Виды угроз безопасности информации

По аспекту информационной безопасности:

- угроза нарушения доступности
- угроза нарушения целостности
- угроза нарушения конфиденциальности

Виды угроз безопасности информации

- Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней
- Угроза нарушения целостности включает в себя любое умышленное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую
- Угроза нарушения доступа к информации возникает всякий раз, когда в результате несанкционированных и (или) непреднамеренных воздействий, блокируется доступ к некоторому информационному ресурсу АС

Виды угроз безопасности информации

По компонентам объекта информатизации, на которые угрозы нацелены:

- данные
- программы
- аппаратура
- поддерживающая инфраструктура

Виды угроз безопасности информации

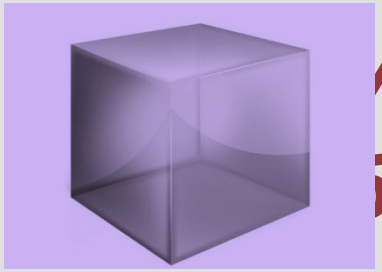
По способу осуществления:

- Случайные действия
- Преднамеренные действия
- Природного характера
- Техногенного характера

Виды угроз безопасности информации

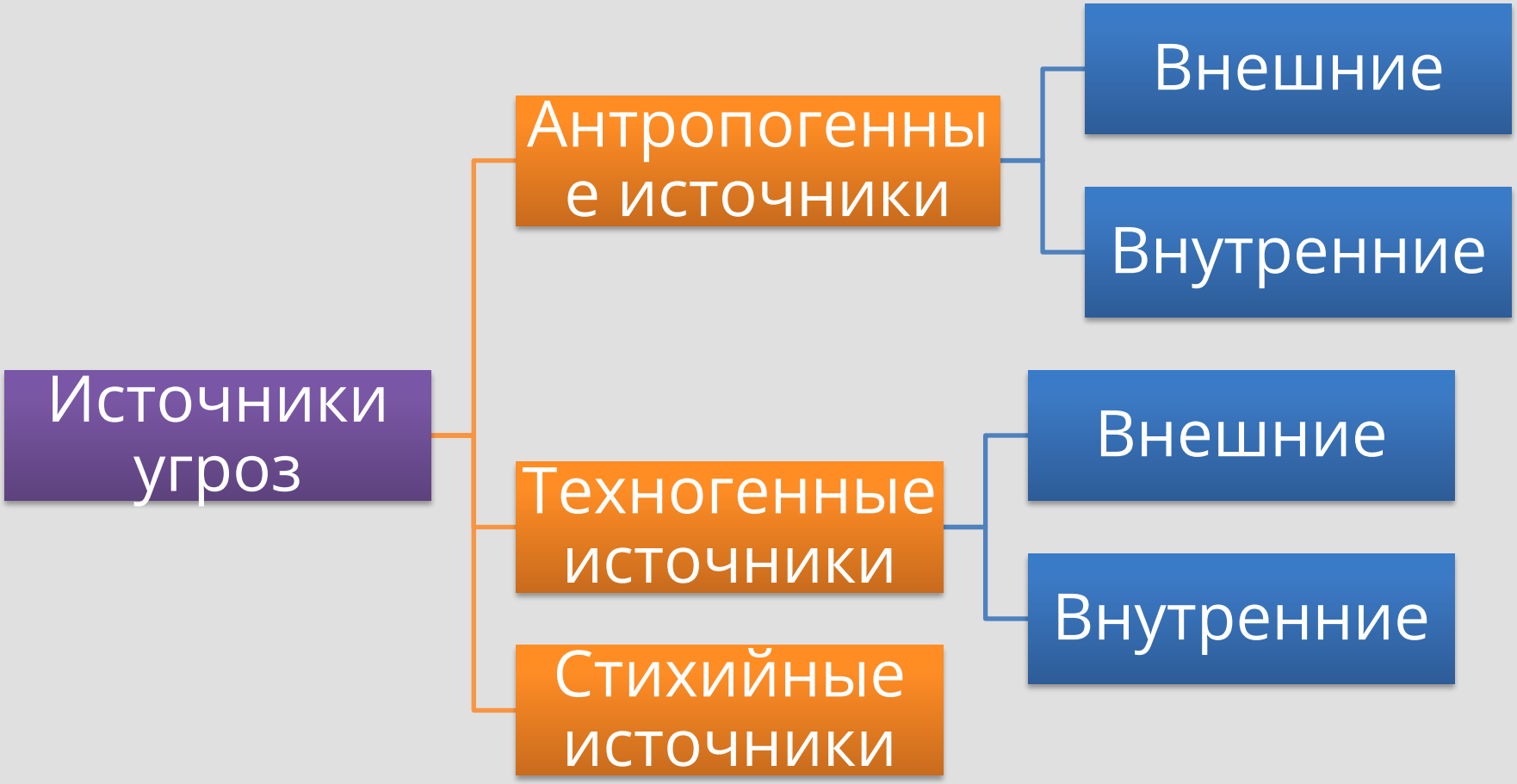
По расположению источника угроз:

- Внутри рассматриваемой АС
- Вне рассматриваемой АС



Источники угроз безопасности информации

Источники угроз безопасности информации



Источники угроз безопасности

Антропогенные источники угроз (внутренние):

- Основной персонал (пользователи)
- Представители служб защиты информации
- Вспомогательный персонал (уборщики, охрана, др.)
- Технический персонал (жизнеобеспечение, эксплуатация)

Источники угроз безопасности

Антропогенные источники угроз (внешние):

- Криминальные структуры
- Потенциальные нарушители, хакеры
- Недобросовестные партнеры
- Технический персонал провайдеров услуг
- Представители надзорных организаций и аварийных служб
- Представители силовых ведомств

Источники угроз безопасности

Техногенные угрозы (внутренние):

- Некачественные средства ОИ
- Некачественные программные средства ОИ
- Вспомогательные средства (охраны, сигнализации, телефонии)
- Другие технические средства

Источники угроз безопасности

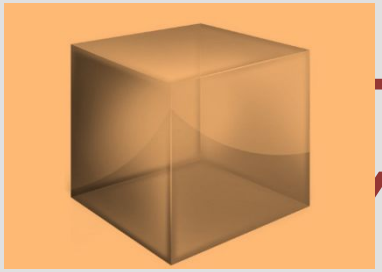
Техногенные угрозы (внешние):

- Средства связи
- Инженерные коммуникации
- Транспорт

Источники угроз безопасности

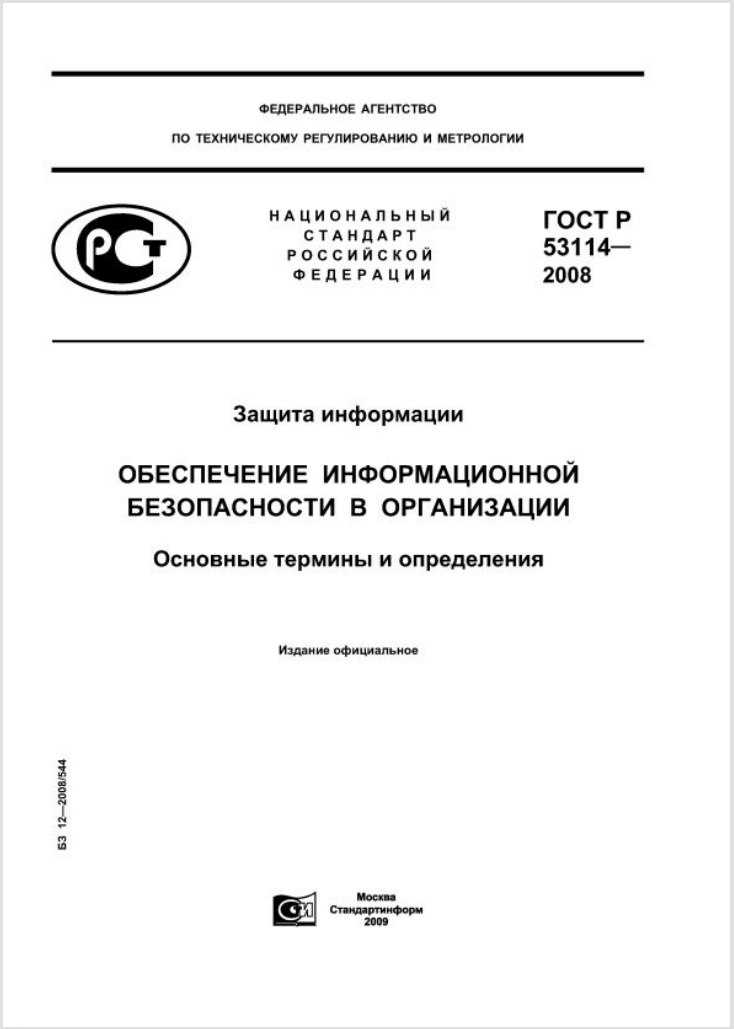
К стихийным источникам относятся:

- Пожары
- Землетрясения
- Наводнения
- Ураганы
- Другие форс-мажорные обстоятельства



Нарушители безопасности информации

ГОСТ Р 53114-2008



ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 53114— 2008

Защита информации

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ

Основные термины и определения

Издание официальное

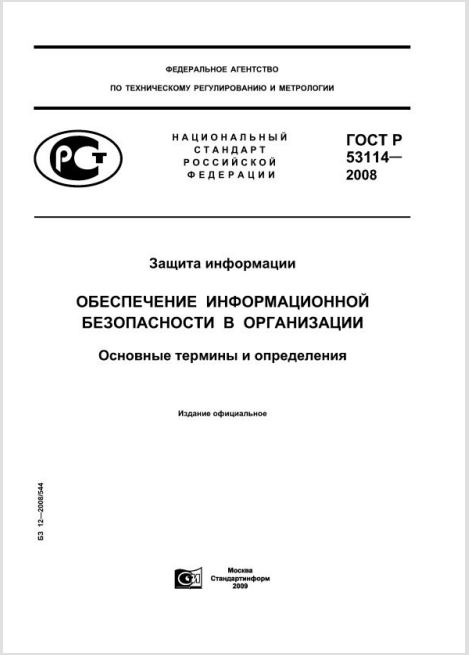
БЗ 12—2008/544

Москва
Стандартинформ
2009

http://docs.cntd.ru

Нарушители безопасности информации

Нарушитель информационной безопасности организации – физическое лицо или логический объект,
случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации.


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 53114— 2008

Защита информации

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ

Основные термины и определения

Издание официальное

Москва
Стандартинформ
2009

http://docs.cntd.ru

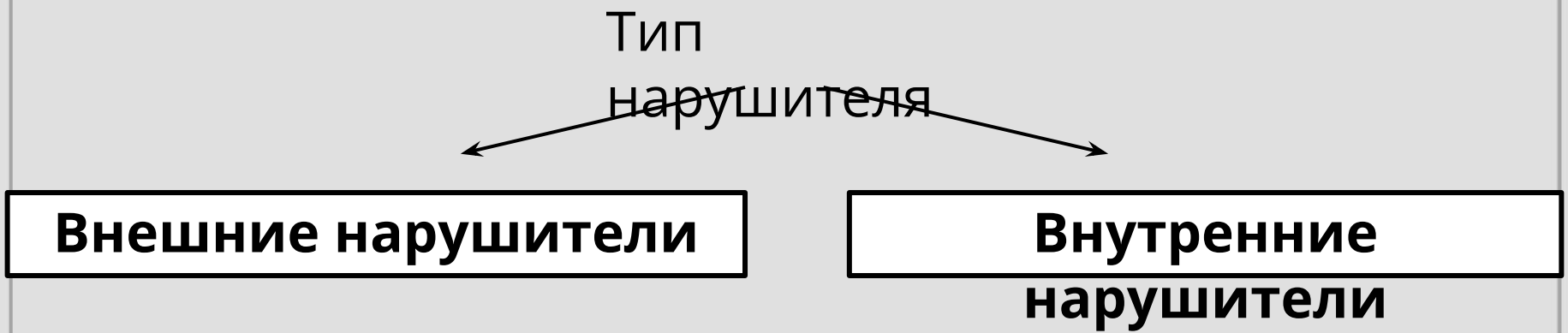
Методика определения угроз безопасности информации в информационных системах

ФСТЭК

fstec.ru

Нарушители безопасности информации

ФСТЭК



Нарушители безопасности информации

ФСТЭК

Тип нарушителя определяется на основе прав доступа субъекта к:

- устройствам ввода/вывода информации
- беспроводным устройствам
- программным, программно-техническим и техническим средствам обработки информации
- съемным машинным носителям информации
- активному и пассивному оборудованию каналов связи
- каналам связи, выходящим за пределы контролируемой зоны

Нарушители безопасности информации

ФСТЭК

Внешние нарушители (тип I) – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы.

Нарушители безопасности информации

Примеры:

- Клиенты
- Приглашённые посетители
- Представители конкурирующих организаций
- Наблюдатели за пределами охраняемой территории

Нарушители безопасности информации

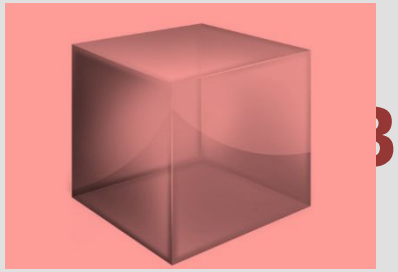
ФСТЭК

Внутренние нарушители (тип II) – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам.

Нарушители безопасности информации

Примеры:

- Операторы информационной системы
- Администраторы вычислительных сетей
- Прикладные и системные программисты
- Технический персонал по обслуживанию зданий



Виды и цели нарушителей

Виды и цели нарушителей

ФСТЭК

1. специальные службы иностранных государств;
2. террористические, экстремистские группировки;
3. преступные группы;
4. внешние субъекты;
5. конкурирующие организации;
6. разработчики, производители, поставщики программно-технических средств;
7. лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ;

Виды и цели нарушителей

ФСТЭК

8. лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора;
9. пользователи информационной системы;
10. администраторы информационной системы и администраторы безопасности;
11. бывшие работники.

Виды и цели нарушителей

ФСТЭК

- Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики;
- Реализация угроз безопасности информации по идеологическим или политическим мотивам;
- Организация террористического акта;
- Причинение имущественного ущерба путем мошенничества или иным преступным путем;
- Дискредитация или дестабилизация деятельности органов государственной власти, организаций;
- Получение конкурентных преимуществ;

Виды и цели нарушителей

ФСТЭК

- Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки;
- Любопытство или желание самореализации;
- Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды;
- Реализация угроз безопасности информации из мести;
- Реализация угроз безопасности информации непреднамеренно из-за неосторожности или неквалифицированных действий.

Виды и цели нарушителей

ФСТЭК

№	Виды нарушителя	Типы нарушителя	Возможные цели (мотивы) реализации угроз безопасности информации
1	Специальные службы иностранных государств	Внешний, внутренний	Нанесение ущерба государству, дестабилизация деятельности органов государственной власти

Виды и цели нарушителей

ФСТЭК

№	Виды нарушителя	Типы нарушителя	Возможные цели (мотивы) реализации угроз безопасности информации
2	Террористи-ческие, экстремистски е группировки	Внешний	Нанесение ущерба государству, дестабилизация деятельности органов государственной власти, совершение террористических актов, идеологические или политические

Виды и цели нарушителей

ФСТЭК

№	Виды нарушителя	Типы нарушителя	Возможные цели (мотивы) реализации угроз безопасности информации
3	Преступные группы (криминальные структуры)	Внешний	Причинение имущественного ущерба, выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды

Виды и цели нарушителей

ФСТЭК

№	Виды нарушителя	Типы нарушителя	Возможные цели (мотивы) реализации угроз безопасности информации
4	Внешние субъекты (физические лица)	Внешний	Идеологические или политические мотивы, причинение имущественного ущерба, выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды, желание самореализации

Виды и цели нарушителей

ФСТЭК

№	Виды нарушителя	Типы нарушителя	Возможные цели (мотивы) реализации угроз безопасности информации
5	Конкурирующие организации	Внешний	Получение конкурентных преимуществ, причинение имущественного ущерба

Виды и цели нарушителей

ФСТЭК

№	Виды нарушителя	Типы нарушителя	Возможные цели (мотивы) реализации угроз безопасности информации
6	Разработчики, производители, поставщики программных, технических и программно-технических средств	Внешний	Причинение имущественного ущерба, внедрение дополнительных возможностей в ПО, непреднамеренные, неосторожные или неквалифицированные действия

Виды и цели нарушителей

ФСТЭК

№	Виды нарушителя	Типы нарушителя	Возможные цели (мотивы) реализации угроз безопасности информации
7	Лица, привлекаемые для установки, наладки, монтажа и других видов работ	Внутренний	Причинение имущественного ущерба, непреднамеренные, неосторожные или неквалифицированные действия

Виды и цели нарушителей

ФСТЭК

№	Виды нарушителя	Типы нарушителя	Возможные цели (мотивы) реализации угроз безопасности информации
8	Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (охранники, уборщики и т.д.)	Внутренний	Причинение имущественного ущерба, непреднамеренные, неосторожные или неквалифицированные действия

Виды и цели нарушителей

ФСТЭК

№	Виды нарушителя	Типы нарушителя	Возможные цели (мотивы) реализации угроз безопасности информации
9	Пользователи информационной системы	Внутренний	Причинение имущественного ущерба, непреднамеренные, неосторожные или неквалифицированные действия, желание самореализации, месть за ранее совершённые действия,

Виды и цели нарушителей

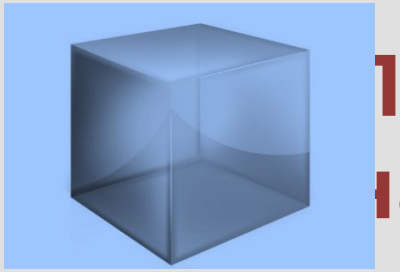
ФСТЭК

№	Виды нарушителя	Типы нарушителя	Возможные цели (мотивы) реализации угроз безопасности информации
10	Администрация информационной системы и администраторы безопасности	Внутренний	Причинение имущественного ущерба, непреднамеренные, неосторожные или неквалифицированные действия, желание самореализации, месть за ранее совершённые действия,

Виды и цели нарушителей

ФСТЭК

№	Виды нарушителя	Типы нарушителя	Возможные цели (мотивы) реализации угроз безопасности информации
11	Бывшие работники (пользователи)	Внешний	Причинение имущественного ущерба, месть за ранее совершённые действия



Потенциал и возможности нарушителей

Потенциал и возможности нарушителей ФСТЭК

- Нарушители с базовым (низким) потенциалом нападения;
- Нарушители с базовым повышенным (средним) потенциалом нападения;
- Нарушители с высоким потенциалом нападения.

Потенциал и возможности нарушителей ФСТЭК

Нарушители с базовым (низким) потенциалом нападения:

- Внешние субъекты (физические лица)
- Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора
- Пользователи информационной системы
- Бывшие работники
- Лица, привлекаемые для установки, наладки, монтажа и других видов работ

Потенциал и возможности нарушителей ФСТЭК

Нарушители с базовым повышенным (средним) потенциалом нападения:

- Террористические, экстремистские группировки
- Преступные группы, криминальные структуры
- Конкурирующие организации
- Разработчики, производители, поставщики программных и технических средств
- Администраторы информационной системы и администраторы безопасности

Потенциал и возможности нарушителей ФСТЭК

Нарушители с высоким потенциалом нападения:

- Специальные службы иностранных государств, блоков государств

Потенциал и возможности нарушителей ФСТЭК

Возможности нарушителей с базовым (низким) потенциалом нападения:

- Получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках
- Получить информацию о методах и средствах реализации угроз безопасности информации или самостоятельно создать методы и реализации атак на информационную систему

Потенциал и возможности нарушителей ФСТЭК

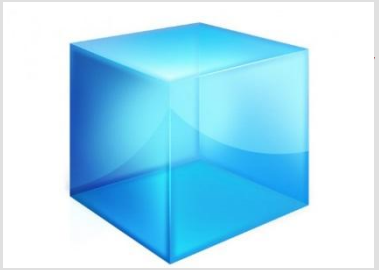
Возможности нарушителей с базовым повышенным (средним) потенциалом нападения:

- Все возможности нарушителей с базовым потенциалом
- Осведомлённость о мерах защиты информации в системе данного типа
- Возможность получить информацию об уязвимостях отдельных компонент информационной системы
- Доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы

Потенциал и возможности нарушителей ФСТЭК

Возможности нарушителей с высоким потенциалом нападения:

- Все возможности нарушителей с базовым и базовым повышенным потенциалом
- Имеют возможность осуществлять НСД
- Имеют возможность получить доступ к ПО чипсетов, системному и прикладному обеспечению
- Имеют возможность получить информацию об уязвимостях и создать методы и средства реализации угроз безопасности информации



пособы реализации угроз арушителем

Способы реализации угроз нарушителем ФСТЭК

Угрозы безопасности информации могут быть реализованы нарушителями за счет:

- НСД и (или) воздействия на объекты на аппаратном уровне;
- НСД и (или) воздействия на объекты на общесистемном уровне;
- НСД и (или) воздействия на объекты на прикладном уровне;
- НСД и (или) воздействия на объекты на сетевом уровне.

Способы реализации угроз нарушителем ФСТЭК

Угрозы безопасности информации могут быть реализованы нарушителями за счет:

- несанкционированного физического доступа и (или) воздействия на линии, (каналы) связи, технические средства, машинные носители информации;
- воздействия на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия).

Способы реализации угроз нарушителем ФСТЭК

Угрозы безопасности информации могут быть реализованы непосредственно за счет:

- доступа к компонентам информационной системы;
- создания условий и средств, обеспечивающих такой доступ;
- доступа или воздействия на обслуживающую инфраструктуру, за которую оператор не отвечает.

Способы реализации угроз нарушителем ФСТЭК

Локальная цель нарушителя, не имеющего доступа к компонентам информационной системы:

- получение доступа к информационной системе;
- получение максимально возможных прав и привилегий при таком доступе.

Способы реализации угроз нарушителем ФСТЭК

Нарушители могут совершать действия, следствием которых является нарушение безопасности информации, преднамеренно (преднамеренные угрозы безопасности информации) или случайно (непреднамеренные угрозы безопасности информации).

Способы реализации угроз нарушителем ФСТЭК

Целенаправленная угроза безопасности информации направлена на интересующую нарушителя информационную систему с заранее известными ему структурно-функциональными характеристиками и особенностями функционирования.

Целенаправленная угроза безопасности информации адаптирована к структурно-функциональным характеристикам информационной системы.

Способы реализации угроз нарушителем ФСТЭК

При подготовке и реализации целенаправленных угроз безопасности информации нарушитель может использовать методы социальной инженерии, которые позволяют ему изучить поведение пользователей и их реакцию на поступающие к ним внешние данные.

Способы реализации угроз нарушителем ФСТЭК

Нецеленаправленная («веерная») угроза безопасности информации не ориентирована на конкретную информационную систему.

Цели:

- НСД
- перехват управления или воздействие на как можно большее количество информационных систем

Способы реализации угроз нарушителем ФСТЭК

Реализация преднамеренных угроз безопасности информации включает:

- сбор информации об информационной системе, ее структурно-функциональных характеристиках, условиях функционирования;
- выбор методов и средств, используемых для реализации угроз безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и условиями функционирования;

Способы реализации угроз нарушителем ФСТЭК

Реализация преднамеренных угроз безопасности информации включает:

- непосредственную реализацию угроз безопасности информации в информационной системе (проникновение в информационную систему, закрепление в информационной системе, реализацию неправомерных действий);
- устранение признаков и следов неправомерных действий в информационной системе.