

## **Модуль 3**

# **Организационные и технические меры защиты персональных данных**

Тема 3.1. Угрозы безопасности персональных данных

# Угрозы безопасности информации

Методика оценки угроз безопасности информации  
(Утверждена ФСТЭК России 5 февраля 2021 г.)



Банк данных угроз безопасности информации  
<https://bdu.fstec.ru/>



# Методика оценки угроз безопасности информации (Утверждена ФСТЭК России 5 февраля 2021 г.)



Методика определяет порядок и содержание работ по определению угроз безопасности информации, реализация (возникновение) которых возможна в информационных системах, автоматизированных системах управления, информационно-телекоммуникационных сетях, информационно-телекоммуникационных инфраструктурах центров обработки данных и облачных инфраструктурах (далее – системы и сети), а также по разработке моделей угроз безопасности информации систем и сетей.

Отменяет

Методику определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных  
(Утверждена Заместителем директора ФСТЭК России  
14 февраля 2008 г.)

## Область действия

### По дате создания:

- Вновь создаваемые системы, решение о создании которых принято после 5 февраля 2021 г.
- Уже эксплуатируемые системы, при модернизации

Модели угроз, разработанные и утвержденные ДО 5-го февраля 2021-го года продолжают действовать и подлежат изменению только при модернизации/развитии

Системы и сети, созданные или модернизированные ПОСЛЕ 5-го февраля 2021-го года, должны соответствовать новой методике оценки угроз

## Область действия

### По виду систем:

- Государственные информационные системы и муниципальные информационные системы (ГИС и МИС)
- Информационные системы персональных данных (ИСПДн)
- Значимые объекты критической информационной инфраструктуры (ЗОКИИ)
- ИС управления производством, используемым организациями оборонно-промышленного комплекса
- Автоматизированные системы управления технологическим процессом (АСУ ТП)

**Действие методики не распространяется на:**

- Моделирование угроз системам, в которых для защиты принято решение использовать средства криптографической защиты информации (СКЗИ)
- Моделирование угроз, связанных с техническими каналами утечки информации
- Неантропогенные угрозы (вызванные не нарушителями)
- На не системы и не сети (например, на программное обеспечение)

# Основные понятия и определения

- **Угроза безопасности информации** - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.
- **Уязвимость** - недостаток (слабость) программного (программно-технического) средства или системы и сети в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.
- **Граница оценки угроз безопасности информации** - совокупность информационных ресурсов и компонентов систем и сетей, в пределах которой обеспечивается защита информации (безопасность) в соответствии с едиными правилами и процедурами, а также контроль за реализованными мерами защиты информации (обеспечения безопасности).

# Основные понятия и определения

- **Оператор** - лицо, осуществляющее деятельность по эксплуатации систем и сетей, в том числе по обработке содержащейся в них информации.
- **Пользователь** - лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в системе или сети и использующее результаты ее функционирования.
- **Поставщик услуг** - лицо, предоставляющее оператору и (или) владельцу на основании договора или ином законном основании услуги по использованию своих вычислительных ресурсов, программного обеспечения, средств хранения или передачи информации.



# Основные понятия и определения



**Основные (критические) процессы (бизнес-процессы)** - управленческие, организационные, технологические, производственные, финансово-экономические и иные основные процессы (бизнес-процессы), выполняемые владельцем информации, оператором в рамках реализации функций (полномочий) или осуществления основных видов деятельности, нарушение и (или) прекращение которых может привести к возникновению рисков (ущербу).

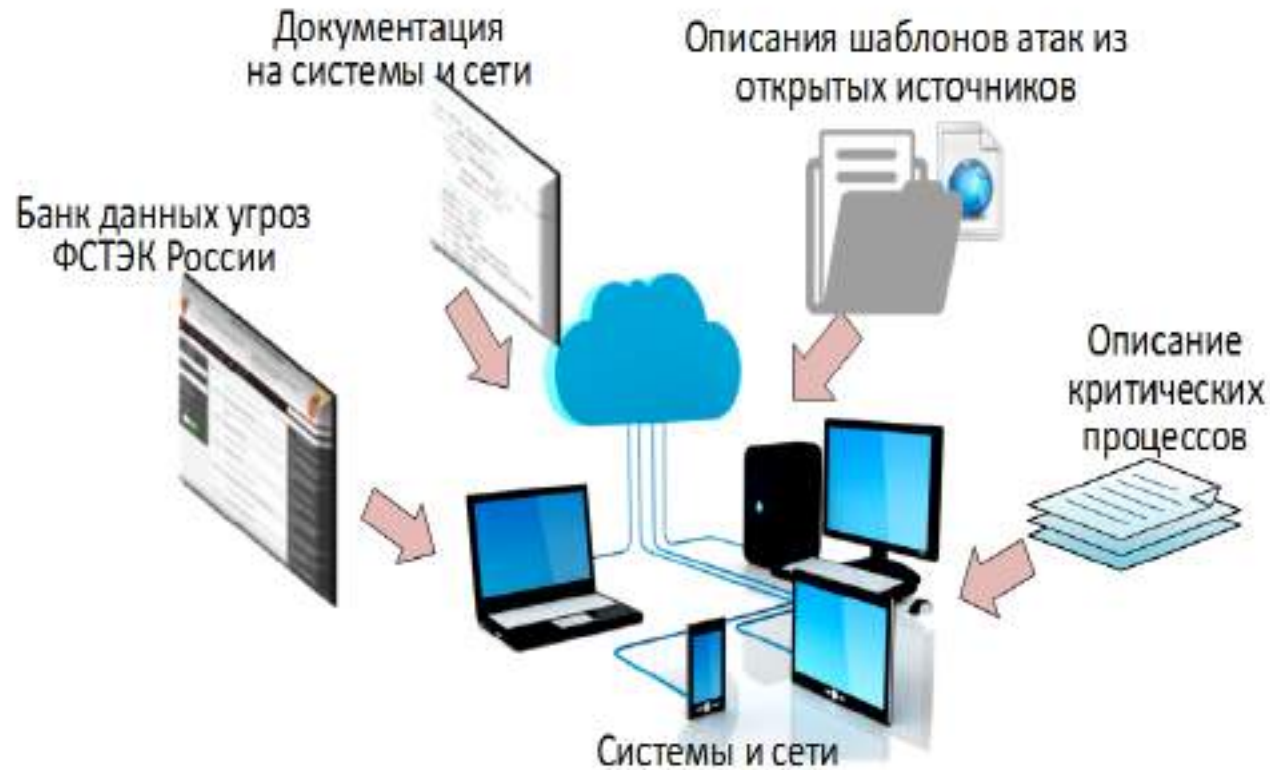


**Возможности нарушителя** - мера усилий нарушителя для реализации угрозы безопасности информации, выраженная в показателях компетентности, оснащенности ресурсами и мотивации нарушителя.

# Исходные данные для оценки угроз безопасности

- ☐ Перечень угроз из Банка данных угроз безопасности информации (БДУ ФСТЭК [bdu.fstec.ru](http://bdu.fstec.ru))
- ☐ Описание векторов (шаблонов) компьютерных атак (CAPEC, ATT&CK, OWASP и т.д.)
- ☐ Документация на системы и сети
- ☐ Договоры, соглашения или иные документы, содержащие условия использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг
- ☐ НПА по создаваемым системам
- ☐ Описание критических процессов
- ☐ Результаты оценки рисков

# Исходные данные для оценки угроз безопасности



# Экспертная группа

**В интересах снижения субъективных факторов при оценке угроз безопасности информации рекомендуется создавать экспертную группу.**

В состав экспертной группы для оценки угроз безопасности информации рекомендуется включать экспертов от:

- ☐ подразделения по защите информации (обеспечения информационной безопасности);
- ☐ подразделения, ответственного за цифровую трансформацию (ИТ-специалистов);
- ☐ подразделения, ответственного за эксплуатацию сетей связи;
- ☐ подразделения, ответственного за эксплуатацию автоматизированных систем управления;
- ☐ подразделений обладателя информации или оператора, ответственного за выполнение основных (критических) процессов (бизнес-процессов).



# Этапы оценки угроз безопасности информации



**Этап 1.** Определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации

**Этап 2.** Определение возможных объектов воздействия угроз безопасности информации

**Этап 3.** Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности

# Этапы оценки угроз безопасности информации

## Этап 1. Определение негативных последствий

Анализ документации систем и сетей и иных исходных данных

Определение негативных последствий  
от реализации угроз

## Этап 2. Определение объектов воздействия

Анализ документации систем и сетей и иных исходных данных

Инвентаризация систем и сетей

Определение групп информационных ресурсов  
и компонентов систем и сетей

## Этап 3. Оценка возможности реализации угроз и их актуальности

Определение источников угроз

Оценка способов реализации угроз

Оценка актуальности угроз

## Этап 1. Определение негативных последствий от реализации (возникновения) угроз безопасности информации

На основе анализа исходных данных определяются событие или группа событий, наступление которых в результате реализации (возникновения) угроз безопасности информации может привести к:

а) нарушению прав граждан;

б) возникновению ущерба в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности государства;

в) возникновению финансовых, производственных, репутационных или иных рисков (видов ущерба) для обладателя информации, оператора.

Событие или группа событий определяются применительно к нарушению основных (критических) процессов (бизнес-процессов), выполнение которых обеспечивают системы и сети, и применительно к нарушению безопасности информации, содержащейся в системах и сетях.

## Этап 1. Определение негативных последствий от реализации (возникновения) угроз безопасности информации

### Пример:

- 1) если оператор обрабатывает персональные данные граждан, которые в соответствии с Федеральным законом «О персональных данных» подлежат обязательной защите, одним из возможных негативных последствий от реализации угроз безопасности информации является нарушение конфиденциальности персональных данных, в результате которого будут нарушены права субъектов персональных данных и соответствующие законодательные акты;
- 2) если оператор обеспечивает транспортировку нефти, одним из возможных негативных последствий от реализации угроз безопасности информации является разлив нефти из нефтепровода, повлекший наступление экологического ущерба;
- 3) если оператор предоставляет услуги связи, одним из возможных негативных последствий от реализации угроз безопасности информации является непредоставление услуг связи абонентам, повлекшее наступление ущерба в социальной сфере;
- 4) для оператора по переводу денежных средств одним из возможных негативных последствий от реализации угроз безопасности информации является хищение денежных средств, в результате которого возможны финансовые и репутационные риски.



# Этап 1. Определение негативных последствий от реализации (возникновения) угроз безопасности информации

Где взять еще примеры ущерба и последствий?

- Приложение № 4 Методики оценки угроз

42

Приложение 4  
к Методике оценки угроз  
безопасности информации

Виды рисков (ущерба) и типовые негативные последствия от  
реализации угроз безопасности информации

Таблица 4.1

| №  | Виды<br>риска (ущерба)                                                                            | Возможные типовые негативные<br>последствия                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----|---------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| У1 | Ущерб физическому лицу                                                                            | Угроза жизни или здоровью.<br>Унижение достоинства личности.<br>Нарушение свободы, личной неприкосновенности.<br>Нарушение неприкосновенности частной жизни.<br>Нарушение личной, семейной тайны, утрата чести и доброго имени.<br>Нарушение тайны переписки, телефонных переговоров, иных сообщений.<br>Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах.<br>Финансовый, иной материальный ущерб физическому лицу.<br>Нарушение конфиденциальности (утечка) персональных данных.<br>«Травля» гражданина в сети «Интернет».<br>Результативные персональные данные граждан                                                                                                                          |
| У2 | Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью | Нарушение законодательства Российской Федерации.<br>Потери (исчезновение) денежных средств.<br>Недополучение ожидаемой (прогнозируемой) прибыли.<br>Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций.<br>Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств).<br>Нарушение платного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса.<br>Срыв запланированной сделки с партнером.<br>Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. |

## Этап 2. Определение возможных объектов воздействия угроз безопасности информации

На основе анализа исходных данных и результатов инвентаризации систем и сетей определяются следующие группы информационных ресурсов и компонентов систем и сетей, которые могут являться объектами воздействия:

Обеспечивающие  
системы

### **Программные средства**

(системное и прикладное программное обеспечение, включая серверы приложений, веб-приложений, системы управления базами данных, системы виртуализации)

### **Информация, содержащаяся в системе**

(защищаемая информация, персональные данные, информация о конфигурации систем и сетей, данные телеметрии, сведения о событиях безопасности и др.)

Пользователи и  
интерфейсы  
взаимодействия

Средства защиты  
информации

Машинные носители

Телекоммуникационное  
оборудование

### **Программно-аппаратные средства обработки и хранения информации**

(автоматизированные рабочие места, серверы, включая промышленные, средства отображения информации, программируемые логические контроллеры, производственное, технологическое оборудование)

## Этап 2. Определение возможных объектов воздействия угроз безопасности информации

Уровни архитектуры систем и сетей, на которых определяются объекты воздействия



## Этап 2. Определение возможных объектов воздействия угроз безопасности информации

Пример распределения границ при оценке угроз безопасности информации между оператором и поставщиком услуг



## Этап 2. Определение возможных объектов воздействия угроз безопасности информации

### Пример:

- 1) разглашение персональных данных и (или) их модификация возможны в результате несанкционированного доступа к базе данных, в которой эта информация хранится;
- 2) разлив нефти из нефтепровода возможен в результате несанкционированного доступа к программируемому логическому контроллеру, обеспечивающему управление задвижками нефтепровода, и подмены хранящихся в нем значений;
- 3) непредоставление услуг связи абонентам возможно в результате отказа в обслуживании маршрутизатора уровня ядра сети;
- 4) нарушение электроснабжения потребителей возможно в результате несанкционированного доступа к программируемому логическому контроллеру, управляющему выключателем, с целью подачи ложных команд на его отключение;
- 5) хищение денежных средств у оператора по переводу денежных средств возможно в результате подмены (модификации) информации, содержащейся в электронных сообщениях.

## Этап 3. Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности

На основе анализа исходных данных, а также результатов оценки возможных целей реализации нарушителями угроз безопасности информации определяются виды нарушителей, актуальных для систем и сетей:

### Основные виды нарушителей:

- ☐ специальные службы иностранных государств;
- ☐ террористические, экстремистские группировки;
- ☐ преступные группы (криминальные структуры);
- ☐ отдельные физические лица (хакеры);
- ☐ конкурирующие организации;
- ☐ разработчики программных, программно-аппаратных средств;
- ☐ лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;
- ☐ поставщики услуг связи, вычислительных услуг;
- ☐ лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;
- ☐ лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.);
- ☐ авторизованные пользователи систем и сетей;
- ☐ системные администраторы и администраторы безопасности;
- ☐ бывшие (уволенные) работники (пользователи).



## Этап 3. Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности

### Нарушители могут быть:

- ❑ внешние нарушители – нарушители, не имеющие прав доступа в контролируруемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации;
- ❑ внутренние нарушители – нарушители, имеющие права доступа в контролируруемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей.



### Этап 3. Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности

Нарушители признаются актуальными для систем и сетей, когда **возможные** цели реализации ими угроз безопасности информации могут привести к определенным для систем и сетей негативным последствиям и соответствующим рискам (видам ущерба)





## Этап 3. Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности

В ходе оценки угроз безопасности информации должны быть определены возможные способы реализации (возникновения) угроз безопасности информации, за счет использования которых актуальными нарушителями могут быть реализованы угрозы безопасности информации в системах и сетях, – актуальные способы реализации (возникновения) угроз безопасности информации

### Основные способы реализации угроз:

- ☐ использование уязвимостей;
- ☐ внедрение вредоносного программного обеспечения;
- ☐ использование недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств;
- ☐ установка программных и (или) программно-аппаратных закладок в программное обеспечение и (или) программно-аппаратные средства;
- ☐ формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных;
- ☐ перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей) для доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;
- ☐ инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;
- ☐ нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию);
- ☐ ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств.

### Этап 3. Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности

В ходе оценки угроз безопасности информации должны быть определены возможные угрозы безопасности информации и оценена их актуальность для систем и сетей – актуальные угрозы безопасности информации.

Угроза безопасности информации возможна, если имеются нарушитель или иной источник угрозы, объект, на который осуществляются воздействия, способы реализации угрозы безопасности информации, а реализация угрозы может привести к негативным последствиям

**УБИ<sub>і</sub> = [нарушитель (источник угрозы); объекты воздействия; способы реализации угроз; негативные последствия]**

Возможная угроза ≠ актуальная угроза

### Этап 3. Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности

- ☐ Актуальность возможных угроз безопасности информации определяется наличием сценариев их реализации
- ☐ При наличии хотя бы одного сценария угрозы безопасности информации такая угроза признается актуальной для системы и сети и включается в модель угроз безопасности систем и сетей

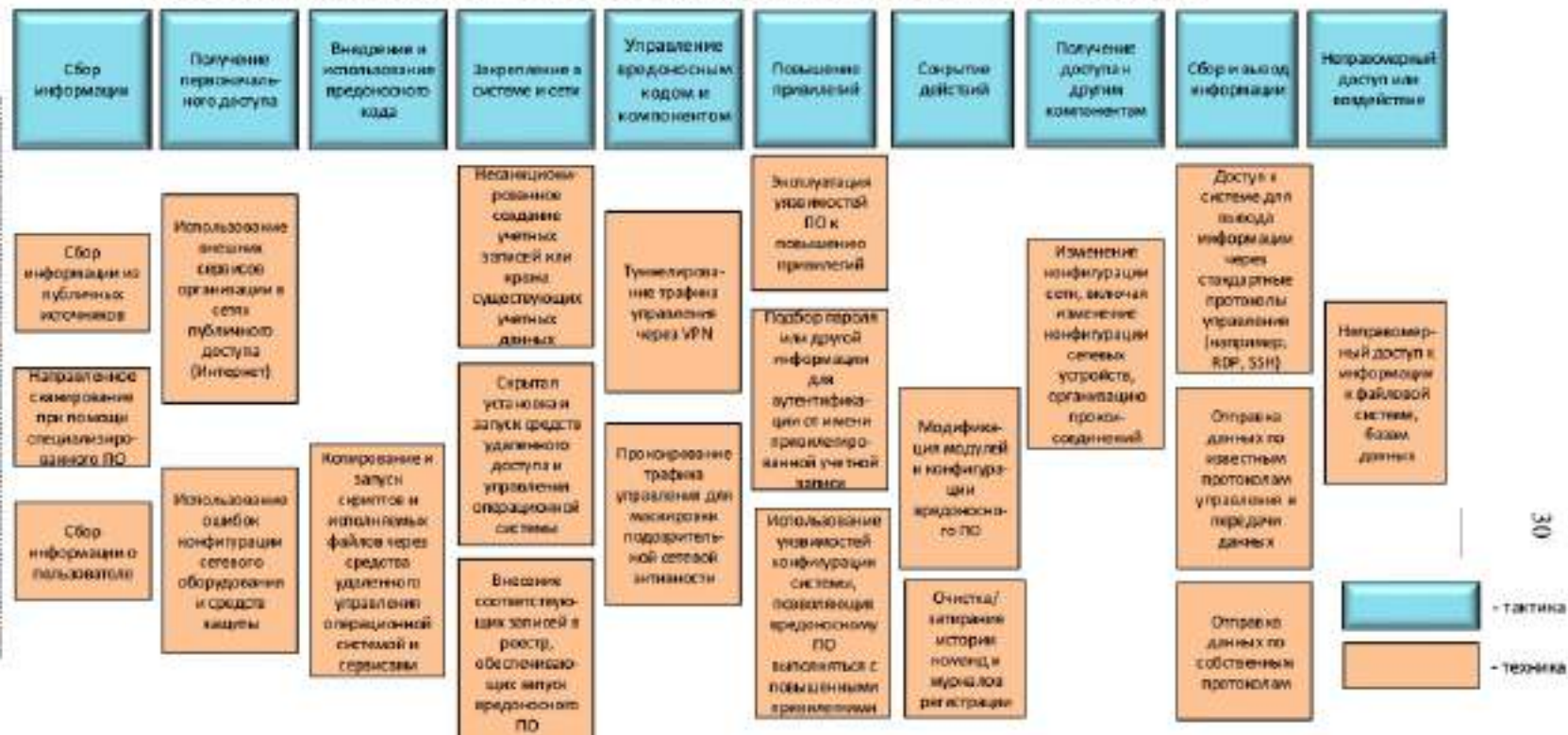
Определение сценариев предусматривает установление последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей, а также доступности интерфейсов для использования соответствующих способов реализации угроз безопасности информации

Перечни возможных тактик и техник приведены в приложении 11 к Методике оценки угроз

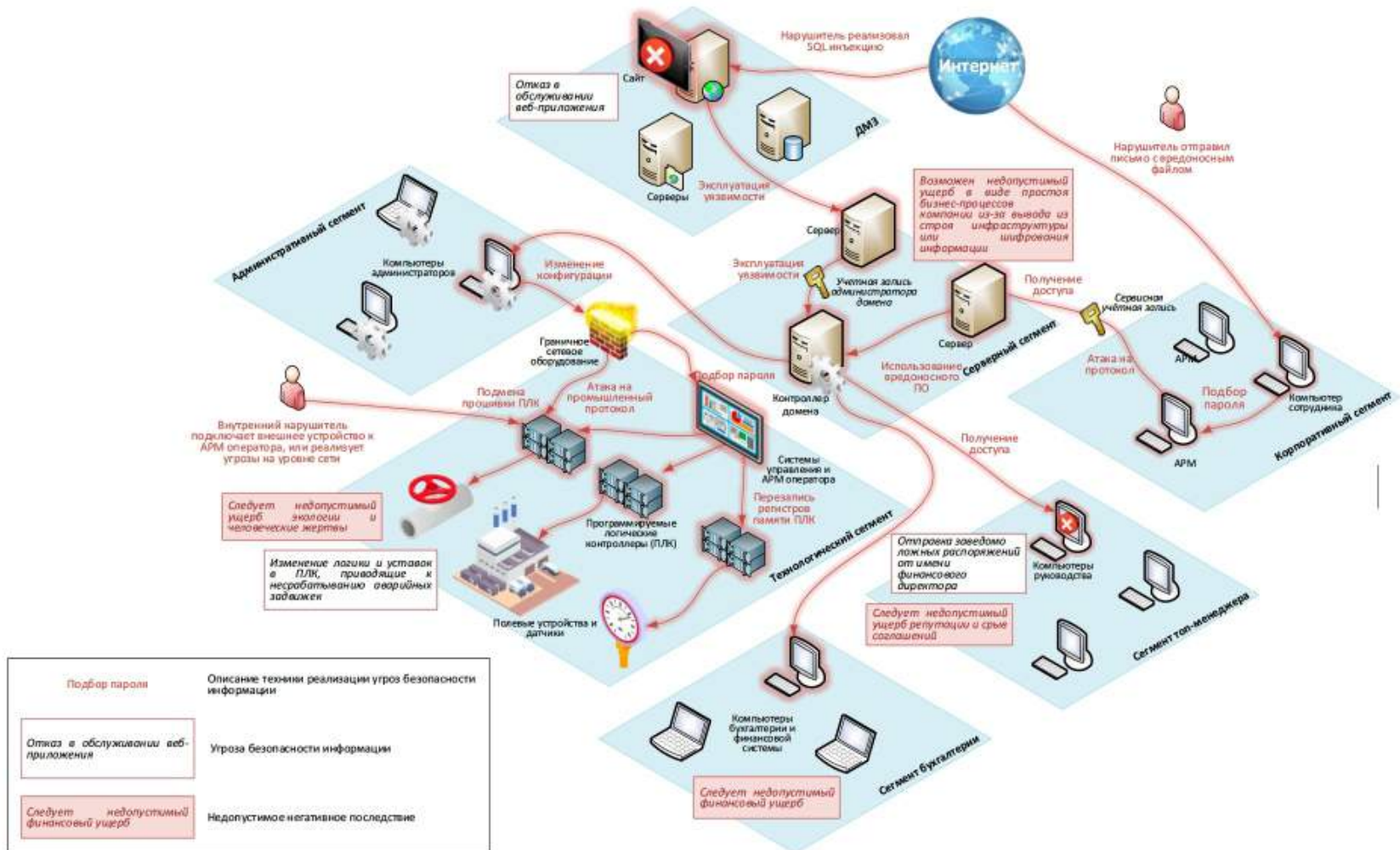
# Этап 3. Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности

## Пример описания сценариев угроз

Угроза несанкционированного доступа к базе данных, содержащей защищаемую информацию



## Пример визуализации сценариев угроз



# Рекомендуемая структура модели угроз

1. Общие положения
2. Описание систем и сетей и их характеристика как объектов защиты
3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации
4. Возможные объекты воздействия угроз безопасности информации
5. Источники угроз безопасности информации
6. Способы реализации (возникновения) угроз безопасности информации
7. Актуальные угрозы безопасности информации



# Актуализация модели угроз

Изменение модели угроз безопасности информации осуществляется в случаях:

- а) изменения требований нормативных правовых актов Российской Федерации, методических документов ФСТЭК России, регламентирующих вопросы оценки угроз безопасности информации;
- б) изменений архитектуры и условий функционирования систем и сетей, режима обработки информации, правового режима информации, влияющих на угрозы безопасности информации;
- в) выявления, в том числе по результатам контроля уровня защищенности систем и сетей и содержащейся в них информации (анализа уязвимостей, тестирований на проникновение, аудита), новых угроз безопасности информации или новых сценариев реализации существующих угроз;
- г) включения в банк данных угроз безопасности информации ФСТЭК России ([bdu.fstec.ru](http://bdu.fstec.ru)) сведений о новых угрозах безопасности информации, сценариях (тактиках, техниках) их реализации.