

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«УФИМСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ  
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

## **ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ**

Альбом схем

Уфа 2026

УДК 004.056(075.8)  
ББК 16.8я73-1  
О-75

*Рекомендован к опубликованию  
редакционно-издательским советом Уфимского ЮИ МВД России*

**Рецензенты:**

кандидат экономических наук И. А. Черногор  
(Омская академия МВД России);  
кандидат технических наук С. В. Смирнов  
(Казанский юридический институт МВД России)

**Коллектив авторов:**

А. Р. Айдагулова – кандидат педагогических наук, б/з;  
Р. Р. Субхангулов – кандидат экономических наук, доцент;  
Г. А. Тугузбаев – б/с, б/з;  
А. Л. Арипов – кандидат юридических наук, б/з

О-75      **Основы кибербезопасности** : альбом схем / А. Р. Айдагулова,  
Р. Р. Субхангулов, Г. А. Тугузбаев, А. Л. Арипов. – Уфа : Уфим-  
ский ЮИ МВД России, 2026. – 48 с. – Текст : непосредственный.

В альбоме схем изложены и наглядно представлены в схемах и таблицах основные принципы и методы защиты компьютерной информации; вопросы правового обеспечения кибербезопасности; сведения о методах совершения киберпреступлений; основы технической и криптографической защиты компьютерной информации, в том числе в системе международной информационной безопасности.

Альбом схем предназначен для профессорско-преподавательского состава, обучающихся образовательных организаций МВД России.

УДК 004.056(075.8)  
ББК 16.8я73-1

© Коллектив авторов, 2026  
© Уфимский ЮИ МВД России, 2026

## ОГЛАВЛЕНИЕ

|                                                                                                                 |    |
|-----------------------------------------------------------------------------------------------------------------|----|
| ПОЯСНИТЕЛЬНАЯ ЗАПИСКА .....                                                                                     | 4  |
| РАЗДЕЛ 1. ОБЩИЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ<br>КИБЕРБЕЗОПАСНОСТИ .....                                                  | 6  |
| 1.1. Ключевые вопросы кибербезопасности.....                                                                    | 6  |
| 1.2. Принципы защиты информации.....                                                                            | 7  |
| 1.3. Основные угрозы безопасности информации.....                                                               | 8  |
| РАЗДЕЛ 2. НОРМАТИВНОЕ ПРАВОВОЕ ОБЕСПЕЧЕНИЕ<br>КИБЕРБЕЗОПАСНОСТИ .....                                           | 10 |
| 2.1. Основные законы Российской Федерации в области<br>кибербезопасности .....                                  | 10 |
| 2.2. Государственные органы Российской Федерации, контролирующие<br>деятельность в сфере защиты информации..... | 14 |
| 2.3. Ответственность за киберпреступления в Российской Федерации ..                                             | 18 |
| 2.4. Основные законы Республики Таджикистан<br>в области кибербезопасности.....                                 | 19 |
| РАЗДЕЛ 3. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНОЙ<br>БЕЗОПАСНОСТИ.....                                                | 21 |
| 3.1. Кибератака как способ реализации киберугрозы.....                                                          | 21 |
| 3.2. Вредоносное программное обеспечение.....                                                                   | 22 |
| 3.3. Способы защиты от кибератак.....                                                                           | 24 |
| РАЗДЕЛ 4. ИСТОЧНИКИ И КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ.<br>ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ .....                   | 28 |
| 4.1. Понятие и виды каналов утечки информации .....                                                             | 28 |
| 4.2. Технические каналы утечки информации.....                                                                  | 30 |
| 4.3. Защита информации от утечки по техническим каналам .....                                                   | 31 |
| РАЗДЕЛ 5. ОСНОВЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ<br>ИНФОРМАЦИИ .....                                                   | 32 |
| 5.1. Основные понятия криптографической защиты информации.....                                                  | 32 |
| 5.2. Методы криптографической защиты информации .....                                                           | 34 |
| 5.3. Электронная цифровая подпись.....                                                                          | 36 |
| РАЗДЕЛ 6. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ КИБЕРБЕЗОПАСНОСТИ<br>И ИХ ОБРАБОТКА .....                                   | 40 |
| 6.1. Этапы управления инцидентами кибербезопасности.....                                                        | 40 |
| 6.2. Оценка угроз безопасности информации.....                                                                  | 42 |
| 6.3. Средства управления событиями кибербезопасности SIEM .....                                                 | 44 |
| СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....                                                                           | 45 |

## ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Альбом схем является визуальным дидактическим материалом. Он предназначен для курсантов, слушателей, преподавателей и практических сотрудников подразделений органов внутренних дел (далее – ОВД), ответственных за защиту информации, техническую и криптографическую безопасность.

Альбом включает 6 разделов, структурированных в виде схем, диаграмм, алгоритмов и графических моделей.

Раздел 1 раскрывает основные положения защиты информации, виды киберугроз, методы совершения киберпреступлений, принципы построения системы защиты.

Раздел 2 представляет задачи нормативного регулирования, основные нормативные акты Российской Федерации и Республики Таджикистан, основы государственной политики в области международной информационной безопасности и международные стандарты (ISO 27001, NIST, ГОСТ Р).

Раздел 3 иллюстрирует способы совершения кибератак на средства хранения, обработки и передачи данных, методы защиты от вредоносного программного обеспечения (далее – ПО), принципы сетевой безопасности и особенности подсистем безопасности операционных систем (далее – ОС) Linux (SELinux, AppArmor, iptables/nftables).

Раздел 4 систематизирует состав и виды технических каналов утечки информации, классифицирует основные и вспомогательные технические средства, детализирует каналы утечки акустической, видовой и обрабатываемой информации.

Раздел 5 показывает роль криптографии, содержит исторические примеры (шифр Сципиона, Цезаря, Виженера, машина Enigma), раскрывает симметричные и асимметричные алгоритмы, цифровую подпись и сценарии ее использования.

Раздел 6 посвящен оценке угроз, реагированию на инциденты сетевой безопасности, работе с уязвимостями, уровневой структуре описания инцидентов VERIS и архитектуре SIEM-систем.

В условиях эскалации киберугроз и стремительного роста числа киберпреступлений наблюдается объективное противоречие:

- между потребностью ОВД в высококвалифицированных кадрах в области кибербезопасности и недостаточной систематизацией теоретико-методических знаний;
- между необходимостью унифицированного визуального обучения и дефицитом готовых наглядных материалов, адаптированных к специфике деятельности ОВД.

Альбом схем призван устранить этот разрыв, обеспечив целостное визуализированное представление о модели угроз, нормативной базе, тех-

нических каналах утечки информации, криптографических методах и процедурах реагирования на инциденты.

Цель работы – формирование у обучающихся целостного визуализированного представления о теоретических и методических основах обеспечения кибербезопасности ОВД, включая современные средства технической и криптографической защиты компьютерной информации.

Задачи:

1. Систематизировать базовые понятия, принципы и модели киберугроз в контексте деятельности ОВД.

2. Обобщить нормативную правовую базу Российской Федерации и Республики Таджикистан, а также международные стандарты в области защиты информации.

3. Выявить способы совершения кибератак и сформировать практические принципы сетевой безопасности, защиты от вредоносного ПО и безопасной настройки ОС на базе Linux.

4. Классифицировать источники и каналы утечки информации, включая технические каналы утечки акустической, видовой и обрабатываемой информации.

5. Изложить основы криптографической защиты (симметричные и асимметричные алгоритмы, цифровая подпись) с опорой на исторические примеры шифров.

6. Описать процедуры реагирования на инциденты кибербезопасности, оценки уязвимостей и использования систем управления событиями и данными безопасности (SIEM).

Альбом схем может использоваться в следующих форматах:

Лекция – преподаватель последовательно демонстрирует схемы (через проектор или раздаточный материал) с кратким комментарием.

Практическое занятие – обучающиеся по заданию преподавателя анализируют конкретную схему (например, схему технического канала утечки), выявляют уязвимости или строят модель угроз для типового объекта информатизации ОВД.

Самостоятельная работа – изучение схем в качестве опорного конспекта, подготовка ответов на контрольные вопросы (вопросы могут быть сформулированы преподавателем на основе каждой схемы).

Контроль знаний – использование схем как наглядной основы для устного опроса или для выполнения заданий на восстановление логической последовательности.

## РАЗДЕЛ 1. ОБЩИЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

### 1.1. Ключевые вопросы кибербезопасности

Информационная безопасность (см. схему 1.1.1):

1) состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность;

2) защита конфиденциальности, целостности и доступности информации.

Кибербезопасность (компьютерная безопасность) – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных (см. схему 1.1.2).



Схема 1.1.1. Ключевые вопросы кибербезопасности



Схема 1.1.2. Источники киберугроз

## 1.2. Принципы защиты информации

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право<sup>1</sup> (см. схему 1.2.1).

Доступность информации – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно<sup>2</sup>. Объекты защиты информации представлены на схеме 1.2.2.

Конфиденциальность информации – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.

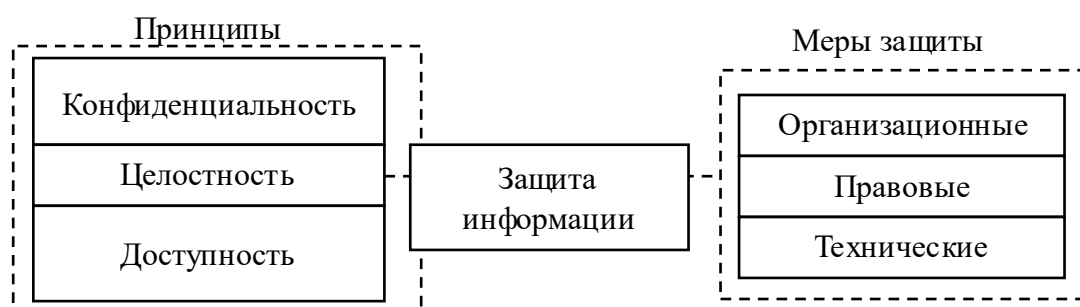


Схема 1.2.1. Принципы и меры защиты информации

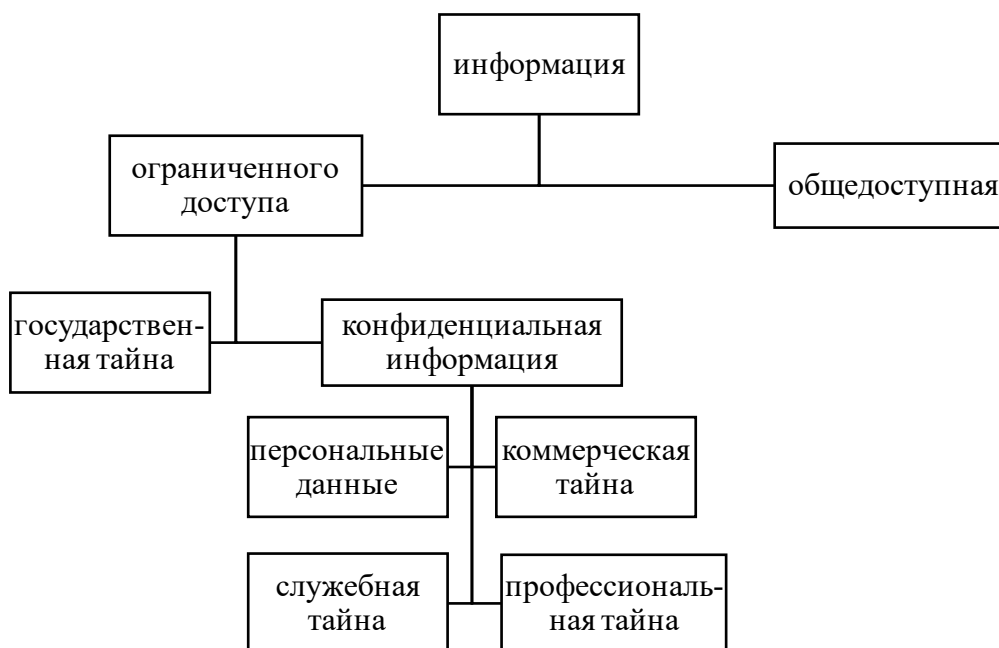


Схема 1.2.2. Объекты защиты информации

<sup>1</sup> Рекомендации по стандартизации Р 50.1.056-2005 Техническая защита информации. Основные термины и определения (утв. приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 479-ст.) // Справочно-правовая система «КонтурНорматив». URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=200721> (дата обращения: 04.04.2026).

<sup>2</sup> Там же.

### 1.3. Основные угрозы безопасности информации

Угроза безопасности информации (см. схему 1.3.1) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации<sup>1</sup>.

Уязвимость информационной системы – свойство информационной системы, предоставляющее возможность реализации угроз безопасности обрабатываемой в ней информации<sup>2</sup>.



Схема 1.3.1. Угрозы безопасности информации

<sup>1</sup> Национальный стандарт РФ ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения (утв. приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 532-ст) // Электронный фонд актуальных правовых и нормативно-технических документов. URL: <https://docs.cntd.ru/document/1200075565> (дата обращения: 04.04.2026).

<sup>2</sup> Рекомендации по стандартизации Р 50.1.056-2005 Техническая защита информации. Основные термины и определения (утв. приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 479-ст.) // Справочно-правовая система «КонтурНорматив». URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=200721> (дата обращения: 18.05.2026).

Угрозы конфиденциальности (угрозы утечки информации) – возможность противоправного получения либо передачи информации. Например, утечка персональных данных вследствие нарушения хранения или нарушения конфигурации.

Угрозы целостности (угроза несанкционированной модификации) – изменение содержания или формы представления обрабатываемой в информационной системе информации, нарушающее установленный в информационной системе порядок обработки информации. Например, искажение содержимого веб-сервера.

Угрозы доступности (угроза отказа в обслуживании) – недоступность информационной системы или ее компонентов и (или) приостановление оказания услуг или предоставления сервисов для авторизованных пользователей. Например, угроза отказа в доступе к интернет-сайту авторизованным пользователям.

## РАЗДЕЛ 2. НОРМАТИВНОЕ ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ

### 2.1. Основные законы Российской Федерации в области кибербезопасности

Информационная безопасность в Российской Федерации обеспечивается комплексом мер, закрепленных в ряде ключевых федеральных законов. Эти законы формируют правовую основу для защиты информации, персональных данных, критической информационной инфраструктуры и коммерческой тайны (см. схему 2.1.1).

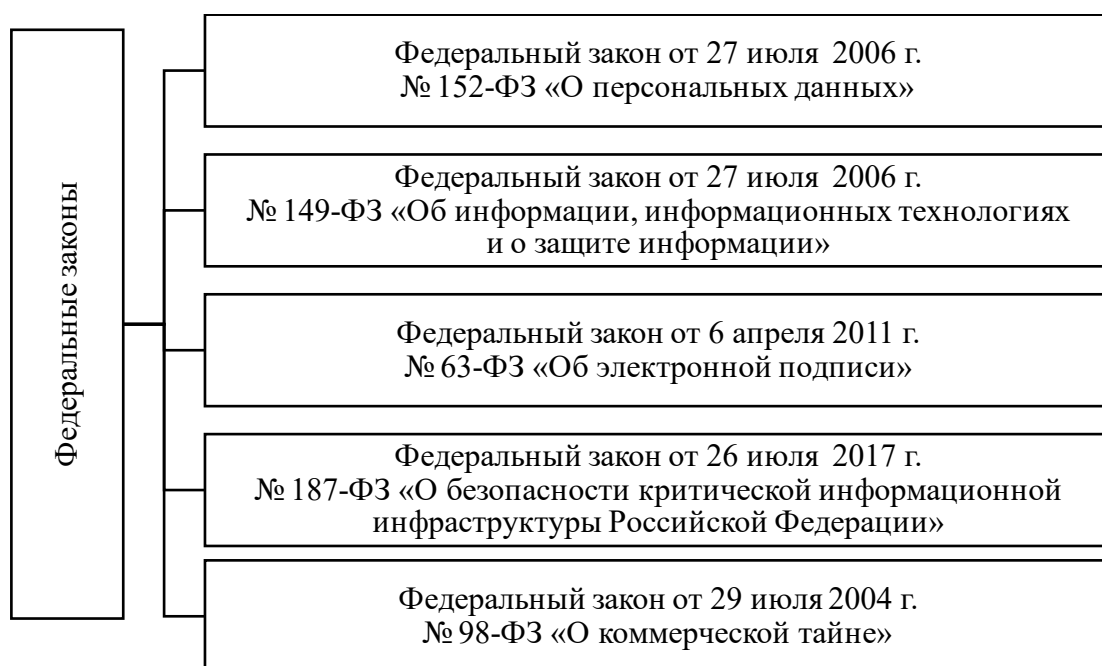


Схема 2.1.1. Основные законы Российской Федерации в сфере кибербезопасности

В совокупности эти федеральные законы формируют комплексную систему обеспечения информационной безопасности в Российской Федерации, направленную на защиту информации, прав и законных интересов граждан, общества и государства. Соблюдение этих законов является обязательным для всех субъектов, осуществляющих деятельность в информационной сфере.

В развитие законодательных положений указы Президента Российской Федерации конкретизируют стратегические направления государственной политики в области информационной безопасности, определяют приоритетные цели, задачи и механизмы их реализации, а также устанавливают правовой статус уполномоченных органов в сфере противодействия киберугрозам (см. схему 2.1.2). Тем самым акты главы государства обеспечивают оперативное и детализированное нормативное регулирова-

ние, восполняя пробелы, которые объективно возникают при разработке рамочных законодательных норм, и отражают системное стремление государства к поддержанию безопасного информационного пространства для граждан, организаций и государства в целом.

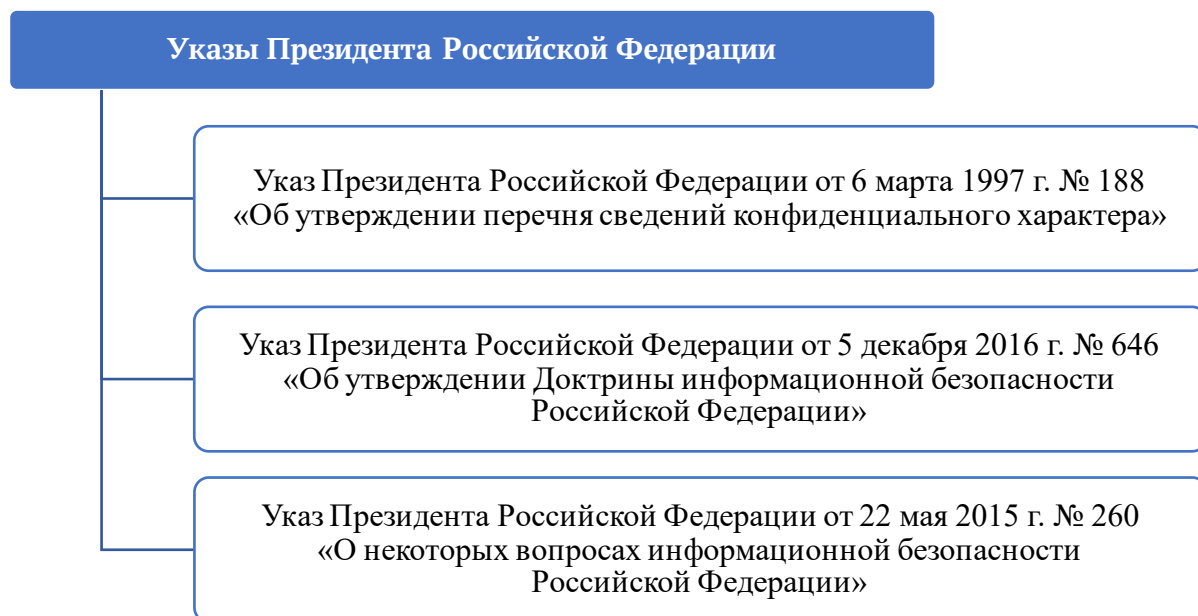


Схема 2.1.2. Ключевые указы Президента Российской Федерации в сфере информационной безопасности

Правительство Российской Федерации уделяет значительное внимание вопросам обеспечения информационной безопасности, особенно в части защиты персональных данных. Ряд постановлений Правительства Российской Федерации устанавливает требования и регламентирует процессы, направленные на предотвращение неправомерного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных и иных неправомерных действий (см. схему 2.1.3).

Ответственность за безопасность персональных данных несет оператор информационной системы (лицо, обрабатывающее персональные данные) или уполномоченное лицо (лицо, осуществляющее обработку данных по поручению оператора на основании договора).

Выбор средств защиты информации осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации (далее – ФСБ России) и Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК России) во исполнение части 4 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»<sup>1</sup>.

<sup>1</sup> О персональных данных : федеральный закон от 27 июля 2006 г. № 152-ФЗ. Доступ из справочно-правовой системы «КонсультантПлюс».

### Постановления Правительства Российской Федерации

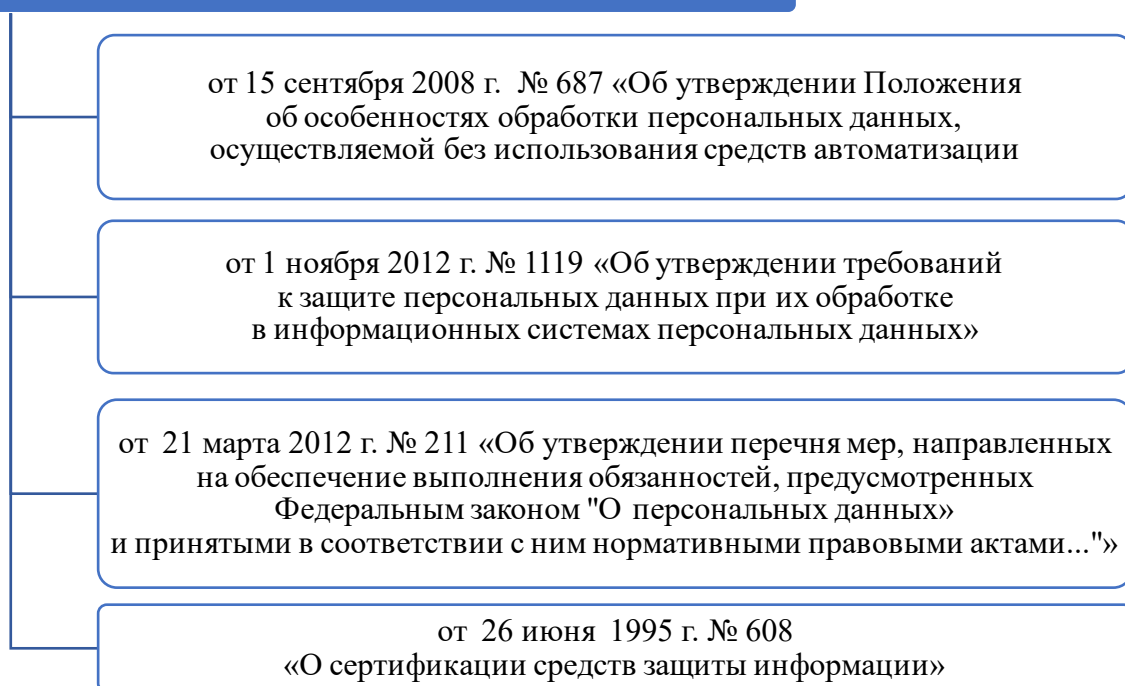


Схема 2.1.3. Постановления Правительства Российской Федерации в сфере защиты персональных данных и сертификации средств защиты информации

В области информационной безопасности в Российской Федерации действуют нормативные акты, изданные различными регуляторами, например, такими как ФСТЭК России и ФСБ России. Эти приказы регламентируют различные аспекты защиты информации в зависимости от ее категории и используемых информационных систем (см. схемы 2.1.4 и 2.1.5).

Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

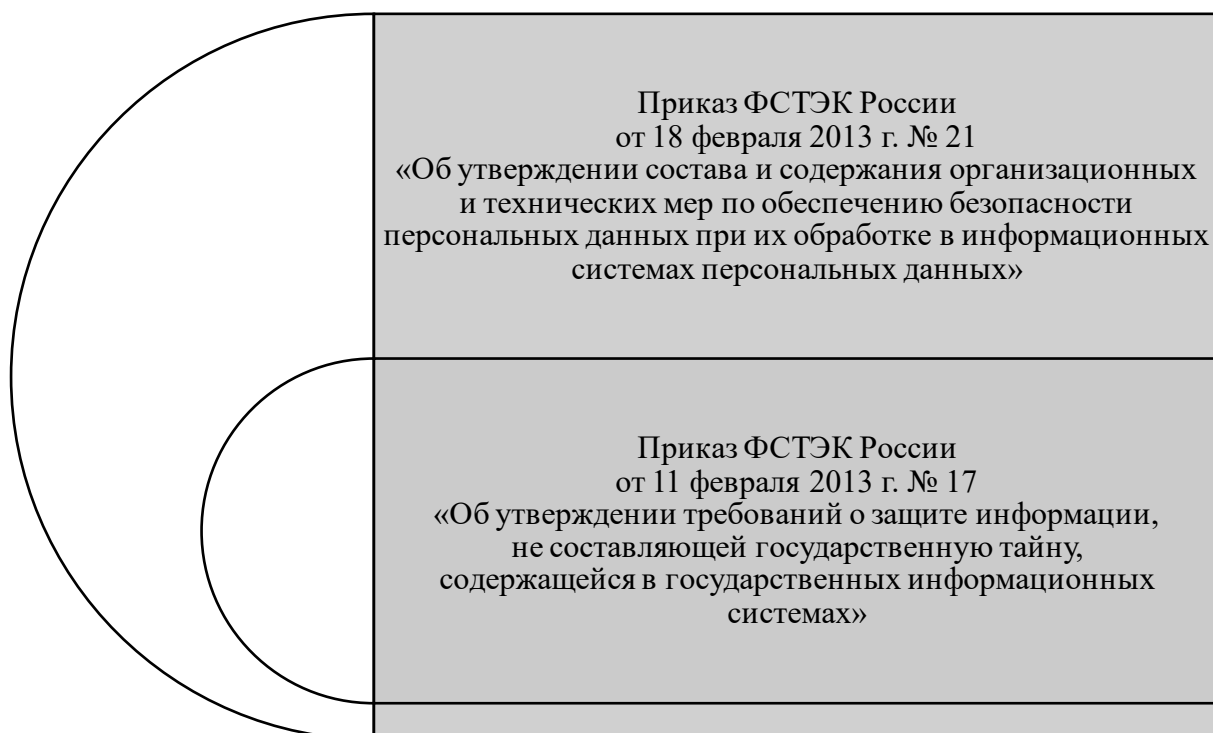


Схема 2.1.4. Приказы ФСТЭК России о мерах и требованиях к защите информации  
в информационных системах различного типа

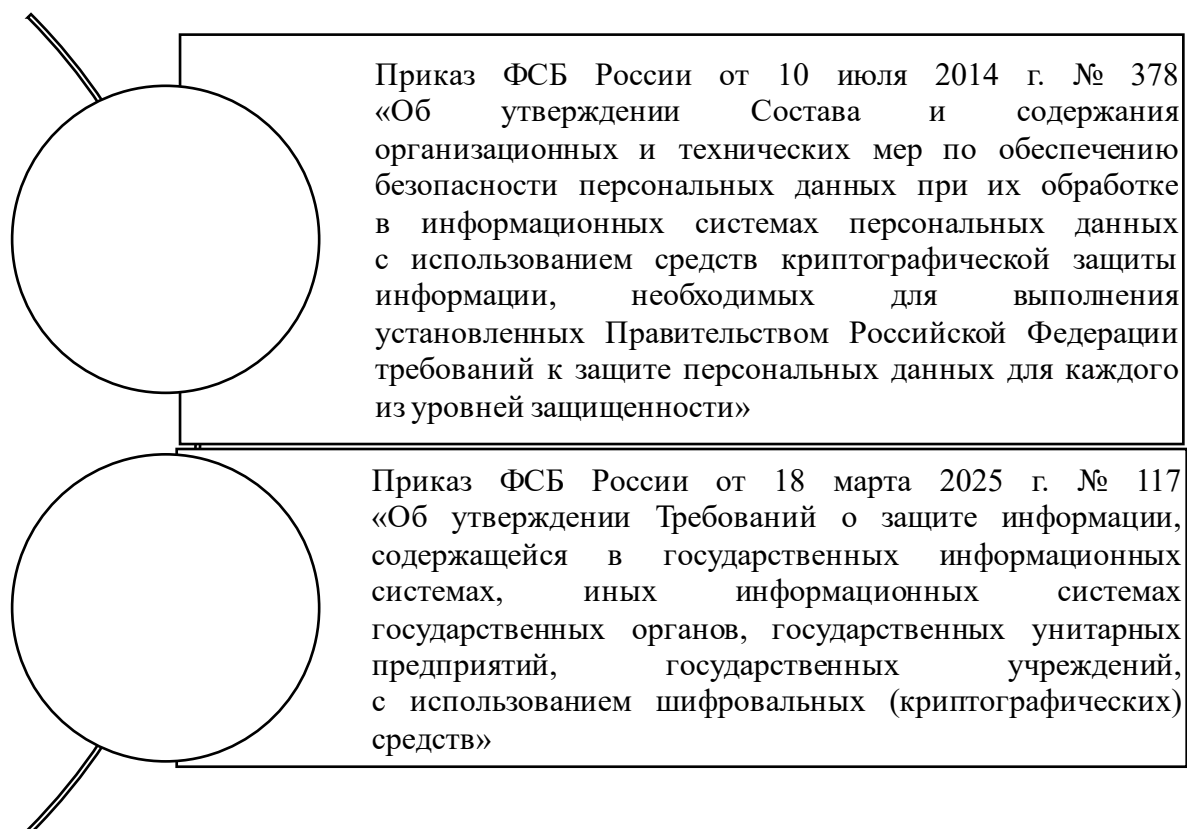


Схема 2.1.5. Ключевые приказы ФСБ России о криптографической защите информации  
в информационных системах персональных данных  
и государственных информационных системах

Приказы образуют нормативную базу для обеспечения информационной безопасности в различных аспектах, охватывая как конфиденциальную информацию, так и персональные данные, с учетом использования криптографических средств и специфики информационных систем (государственные и персональные). Соблюдение требований, установленных этими приказами, является обязательным для организаций, обрабатывающих соответствующую информацию.

## 2.2. Государственные органы Российской Федерации, контролирующие деятельность в сфере защиты информации

Государственные органы Российской Федерации в системе обеспечения информационной безопасности выполняют определенные функции и имеют конкретные предметы ведения (см. схему 2.2.1):

|                                                                                                               |                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Совет безопасности Российской Федерации                                                                       | <ul style="list-style-type: none"> <li>• Обеспечение международной информационной безопасности</li> <li>• Научные исследования в области обеспечения информационной безопасности</li> </ul>                                                                   |
| ФСБ России                                                                                                    | <ul style="list-style-type: none"> <li>• Расследование киберпреступлений</li> <li>• Управление системой ГосСОПКА</li> <li>• Выдача лицензий на использование криптографических средств</li> </ul>                                                             |
| ФСТЭК России                                                                                                  | <ul style="list-style-type: none"> <li>• Обеспечение защиты информации, содержащей сведения, составляющие государственную тайну</li> <li>• Обеспечение безопасности критической информационной инфраструктуры</li> </ul>                                      |
| Федеральная служба охраны Российской Федерации (ФСО России)                                                   | <ul style="list-style-type: none"> <li>• Участие в разработке средств защиты информации</li> <li>• Информационно-технологическое обеспечение госорганов</li> <li>• Разработка, создание, эксплуатация и развитие информационных систем</li> </ul>             |
| Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России)         | <ul style="list-style-type: none"> <li>• Сертификаты безопасности</li> <li>• Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы России</li> <li>• Защита персональных данных</li> </ul> |
| Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) | <ul style="list-style-type: none"> <li>• Пресечение распространения противоправной информации</li> <li>• Контроль соблюдения требований законодательства в области персональных данных</li> </ul>                                                             |

Схема 2.2.1. Органы государственной власти Российской Федерации в системе обеспечения информационной безопасности: функции и предметы ведения

Доктрина информационной безопасности Российской Федерации, принятая указом Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», является основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности. Государственная система защиты информации представлена на схеме 2.2.2.



Схема 2.2.2. Система защиты информации в Российской Федерации

**Информационная безопасность Российской Федерации** – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз (см. схему 2.2.3), при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территори-

альная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства<sup>1</sup>.



Схема 2.2.3. Типология информационных угроз в разрезе субъектов

**Угроза информационной безопасности Российской Федерации** – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере<sup>2</sup>.

Национальные интересы Российской Федерации в информационной сфере – объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы<sup>3</sup>. Национальные интересы Российской Федерации направлены на обеспечение и защиту конституционных прав и свобод, обеспечение функционирования информационной инфраструктуры Российской Федерации, развитие в Российской Федерации ИТ-отрасли и электронной промышленности, доведение до общественности достоверной

<sup>1</sup> Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента Российской Федерации от 5 декабря 2016 г. № 646. Доступ из справочно-правовой системы «КонсультантПлюс».

<sup>2</sup> Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента Российской Федерации от 5 декабря 2016 г. № 646. Доступ из справочно-правовой системы «КонсультантПлюс».

<sup>3</sup> Там же.

информации о государственной политике Российской Федерации, содействие формированию системы международной информационной безопасности (см. схему 2.2.4).

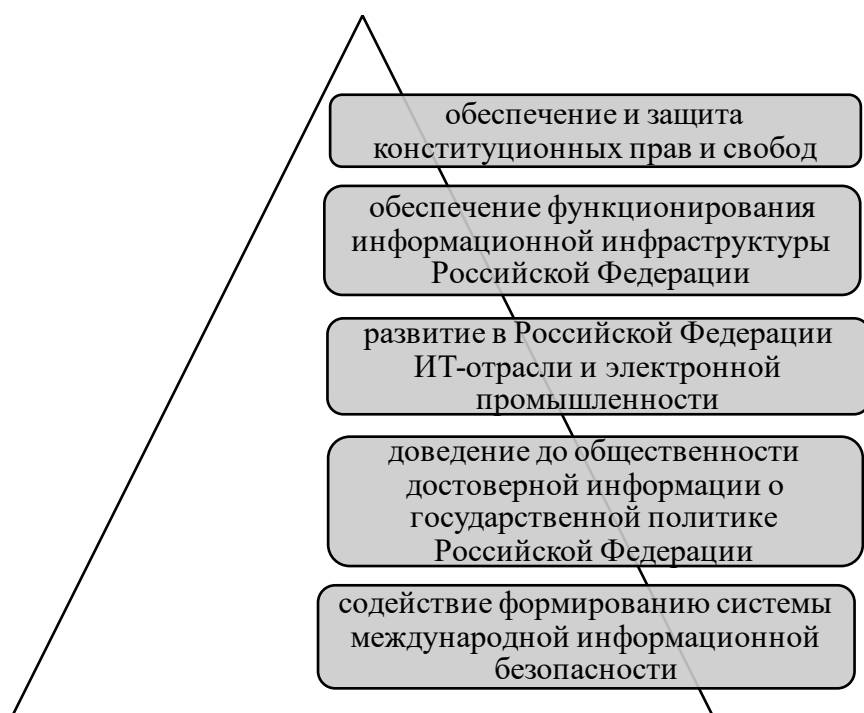


Схема 2.2.4. Национальные интересы Российской Федерации в информационной сфере

Принципы государственной политики обеспечения информационной безопасности представлены на схеме 2.2.5.



Схема 2.2.5. Принципы государственной политики обеспечения информационной безопасности

### 2.3. Ответственность за киберпреступления в Российской Федерации

Любые деяния, приводящие к повреждению или уничтожению информации, к ее намеренному искажению, а также стремление получить неправомерный доступ к чужой конфиденциальной информации являются преступлением (см. схему 2.3.1).



Схема 2.3.1. Виды киберпреступлений

В главе 28 «Преступления в сфере компьютерной информации» Уголовного кодекса Российской Федерации определена мера наказания за некоторые виды преступлений в области информационных технологий (см. схему 2.3.2):

- неправомерный доступ к охраняемой законом компьютерной информации, если это повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации;
- создание, распространение или использование вредоносных компьютерных программ;
- нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование информации.

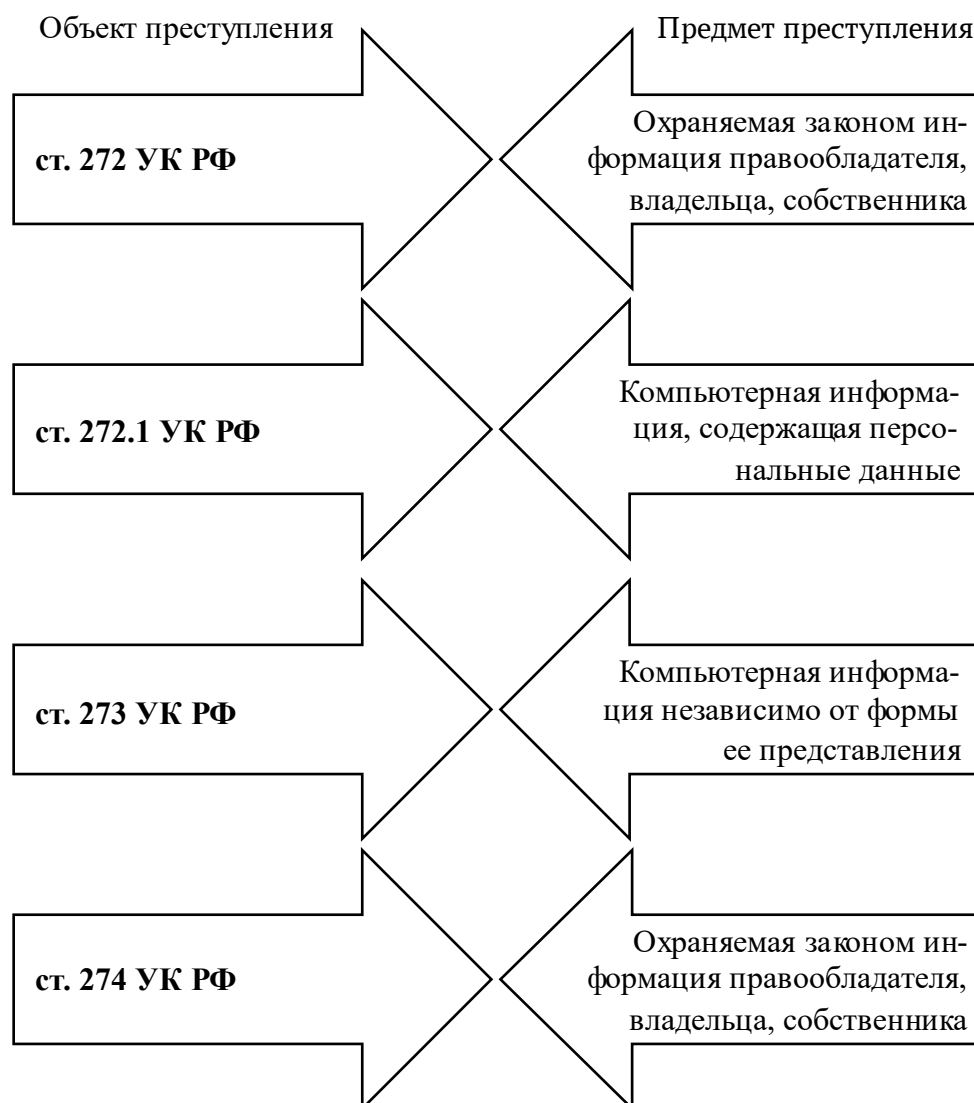


Схема 2.3.2. Преступления в сфере компьютерной информации  
(составы преступлений и виды информации)

## 2.4. Основные законы Республики Таджикистан в области кибербезопасности

Законодательство Республики Таджикистан о защите информации основывается на Конституции Республики Таджикистан и состоит из Закона от 2 декабря 2002 г. № 71 «О защите информации» (в редакции от 26 декабря 2005 г.), других нормативных правовых актов Республики Таджикистан, а также международных правовых актов, признанных Республикой Таджикистан (см. схему 2.4.1).



Схема 2.4.1. Законы Республики Таджикистан в области кибербезопасности

В соответствии с законом Республики Таджикистан от 2 декабря 2002 г. № 71 «О защите информации»<sup>1</sup> к целям защиты информации относятся:

предотвращение утечки, хищения, утраты, искажения, подделки информации;

предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

предупреждение санкционированных и несанкционированных действий, которые могут повлечь за собой преднамеренное или непреднамеренное уничтожение, блокирование, искажение (подделку), хищение, копирование, утечку, модифицирование и преобразование информации.

---

<sup>1</sup> О защите информации : закон Республики Таджикистан от 2 декабря 2002 г. № 71 (в редакции от 26 декабря 2005 г.) // Национальный центр законодательства при Президенте Республики Таджикистан. URL: <https://ncz.tj/content/закон-республика-таджикистан-о-защите-информации> (дата обращения: 12.01.2026).

## РАЗДЕЛ 3. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

### 3.1. Кибератака как способ реализации киберугрозы

**Кибератака (компьютерная атака)** – попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к активу или его несанкционированного использования (см. схему 3.1.1).



Схема 3.1.1. Примеры кибератак, нарушающих принципы защиты информации

**Актив** – все, что имеет ценность для организации (см. схему 3.1.2).

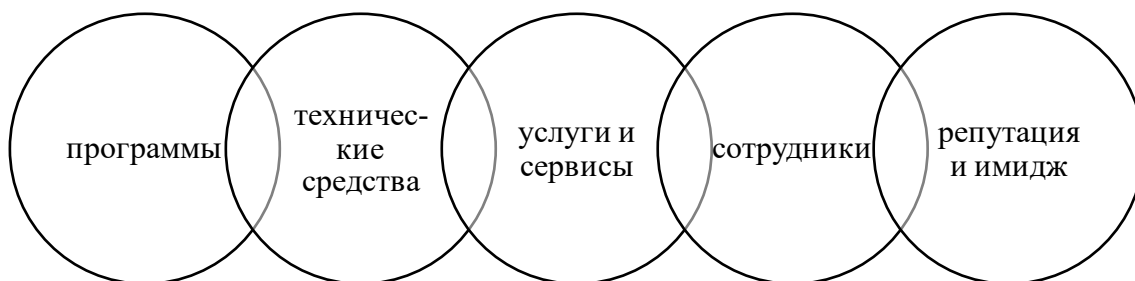


Схема 3.1.2. Виды активов

**DDoS-атака** – это распределенная атака, направленная на перегрузку сервера, сети или веб-приложения путем одновременной отправки огромного количества запросов со множества устройств (см. схему 3.1.3).



Схема 3.1.3. Схема DDoS-атаки



Схема 3.1.4. Способы реализации угроз и меры защиты

### 3.2. Вредоносное программное обеспечение

**Вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы<sup>1</sup>.

Среди вредоносных программ наиболее распространены такие виды, как червь, вирус, троян, руткит, буткит, ботнет (см. схему 3.2.1).

**Компьютерный вирус** – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения<sup>2</sup>. В отличие от вируса, обладающего точно также механизмом самовоспроизведения, компьютерный червь не внедряется в программное обеспечение, а создает свою копию как отдельный файл.

Существует несколько подходов к классификации вредоносного программного обеспечения. На схеме 3.2.2 представлен вариант классификации на основе композиций и комбинирования.

<sup>1</sup> Рекомендации по стандартизации Р 50.1.056-2005 Техническая защита информации. Основные термины и определения (утв. приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 479-ст.) // Справочно-правовая система «КонтурНорматив». URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=200721> (дата обращения: 18.05.2026).

<sup>2</sup> Там же.

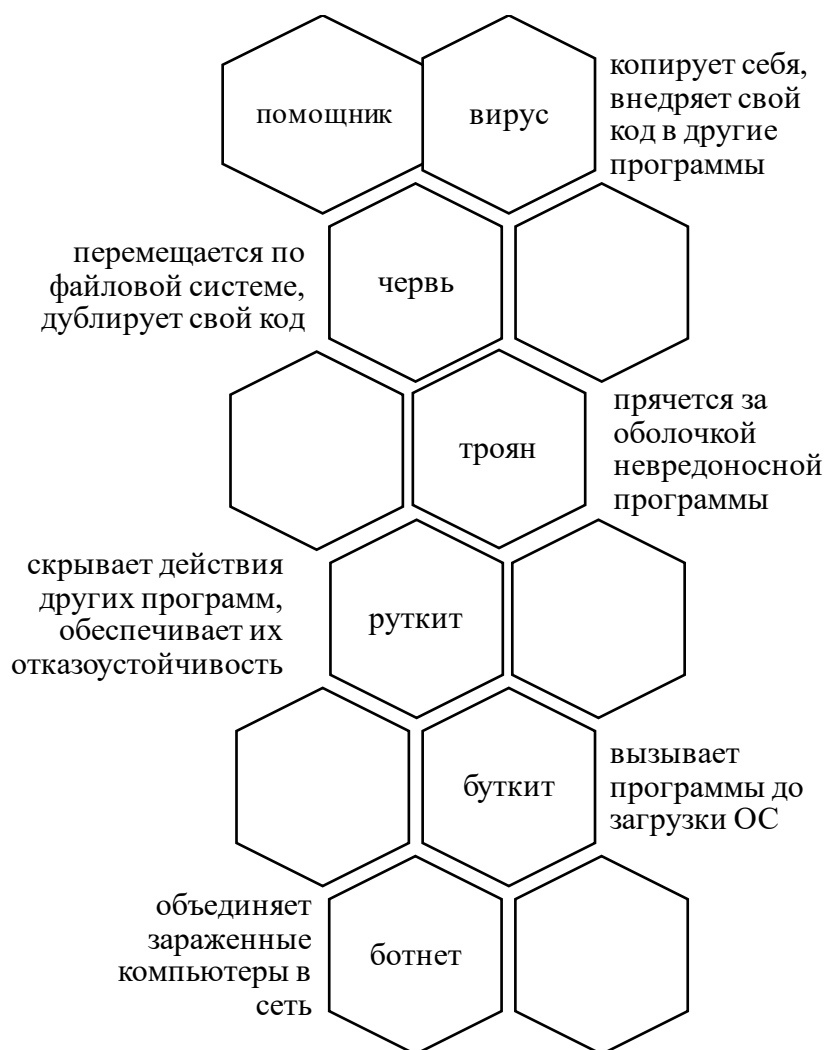


Схема 3.2.1. Виды вредоносных программ и их основное назначение

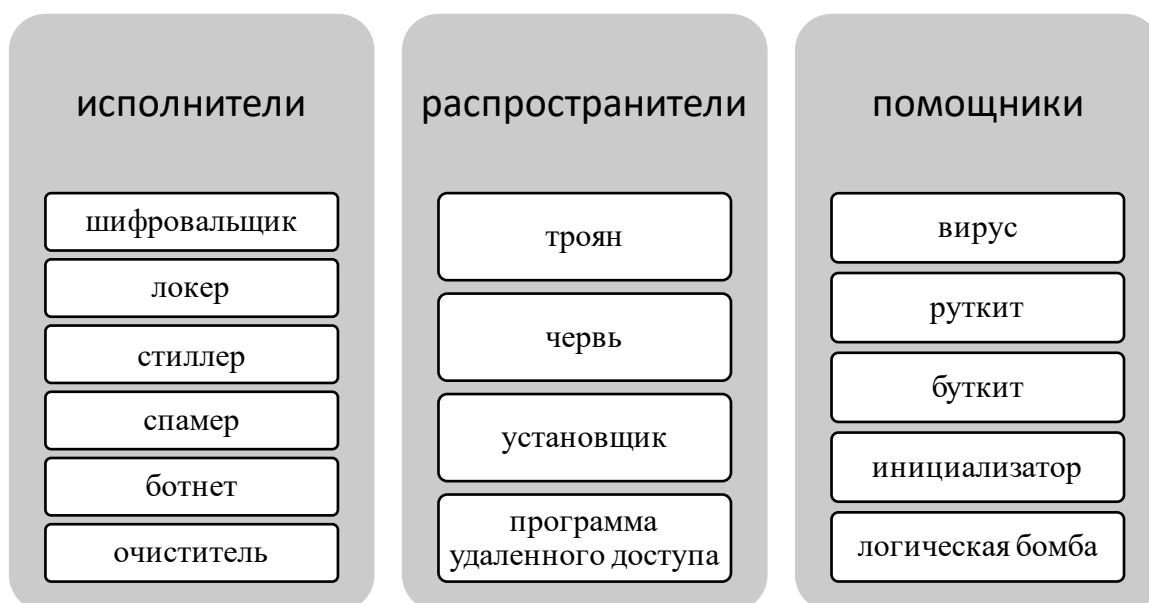


Схема 3.2.2. Классификация вредоносных программ

Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению<sup>1</sup>. Часто вредоносное программное обеспечение представляет собой композицию (см. схему 3.2.3).



Схема 3.2.3. Композиции классов вредоносного ПО

### 3.3. Способы защиты от кибератак

Основные способы защиты от вредоносного программного обеспечения представлены на схеме 3.3.1.

#### АНТИВИРУСНЫЕ СРЕДСТВА ЗАЩИТЫ

для защиты от вредоносных программ

#### СЕТЕВЫЕ ЭКРАНЫ

защита сегментов сети или хостов от несанкционированного доступа

#### ОБНОВЛЕНИЕ ПРОГРАММ

закрывание уязвимостей программного обеспечения, устранение ошибок, защита от вредоносных программ

#### ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ

подтверждение права на доступ

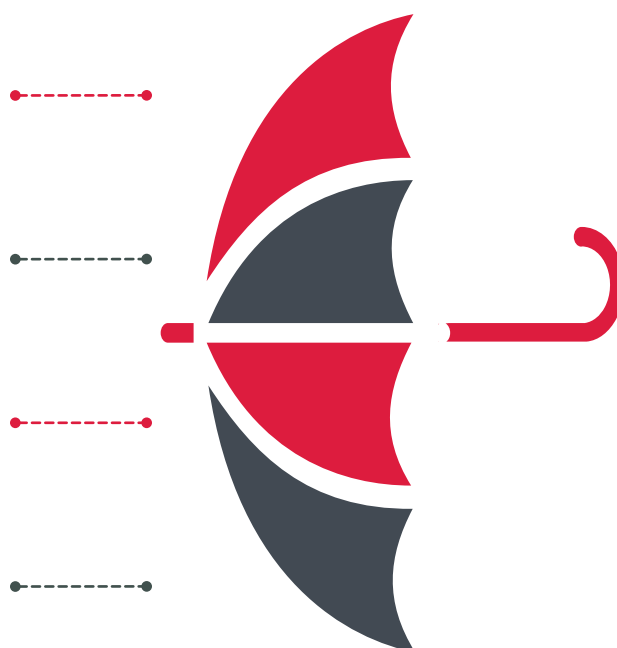


Схема 3.3.1. Способы защиты от вредоносного программного обеспечения

<sup>1</sup> Рекомендации по стандартизации Р 50.1.056-2005 Техническая защита информации. Основные термины и определения (утв. приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 479-ст.) // Справочно-правовая система «КонтурНорматив». URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=200721> (дата обращения: 18.05.2026).

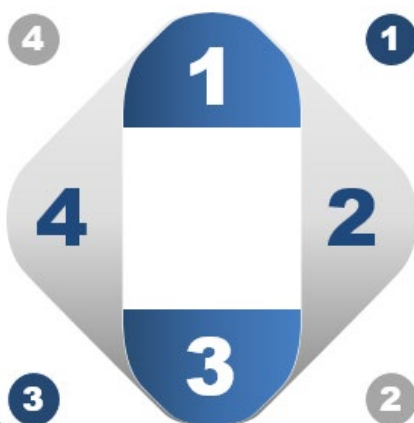
Процессу аутентификации предшествует идентификация (процесс установления личности пользователя). Идентификация, аутентификация и авторизация – это три последовательных этапа взаимодействия пользователя с информационной системой, которые обеспечивают управление доступом и защиту информации (см. схему 3.3.2). Авторизация – это процесс определения прав пользователя внутри системы после идентификации и аутентификации.



Схема 3.3.2. Составляющие процесса авторизации пользователя

Существуют правовые, организационные, аппаратные и программные меры защиты информации (см. схему 3.3.3).

**АППАРАТНЫЕ**  
средства защиты  
информации и инфор-  
мационных систем,  
реализованных  
на аппаратном уровне



**ОРГАНИЗАЦИОННЫЕ**  
меры организационного (ад-  
министративного) характера

**ПРАВОВЫЕ**  
совокупность норматив-  
ных и правовых актов,  
регулирующих вопросы  
защиты информации

**ПРОГРАММНЫЕ**  
программы, предназна-  
ченные для обеспече-  
ния информационной  
безопасности

Схема 3.3.3. Меры защиты информации

Организационные меры предусматривают установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации<sup>1</sup>. Организационные мероприятия – это мероприятия по защите информации, проведение которых не требует применения специально разработанных технических средств.

Организационные и технические меры защиты информации детализированы в методическом документе ФСТЭК России «Меры защиты информации в государственных информационных системах» (далее – методический документ). Методический документ разработан и утвержден в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

Программные и аппаратные меры защиты информации дополняют друг друга. Программные меры защиты информации в операционной системе не ограничиваются установкой антивирусного программного обеспечения. Защита информации в операционной системе предполагает выполнение следующих мер: управление учетными записями, регистрация событий информационной безопасности, анализ защищенности информации, устранение уязвимостей системы и др. (см. схему 3.3.4).

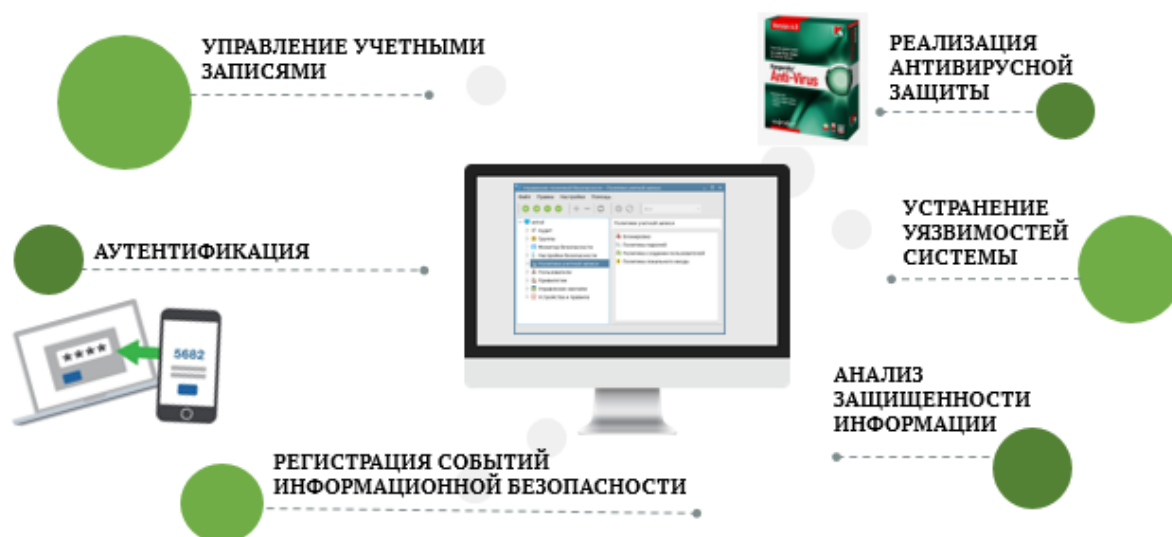


Схема 3.3.4. Меры защиты информации в операционной системе

<sup>1</sup> Рекомендации по стандартизации Р 50.1.056-2005 Техническая защита информации. Основные термины и определения (утв. приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 № 479-ст.) // Справочно-правовая система «КонтурНорматив». URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=200721> (дата обращения: 18.05.2026).

Меры защиты информации в телекоммуникационных сетях представлены на схеме 3.3.5.

**Технологии идентификации и аутентификации**

- позволяют подтвердить личность пользователя и источник сетевого пакета

**Технология межсетевого и персонального экранирования**

- обеспечивает фильтрацию любого вида трафика на основе заданных правил

**Технологии инкапсуляции и туннелирования**

- позволяют упаковать IP-пакет вместе со служебными полями в IP-пакет стандартного вида для сокрытия информации при ее передаче по открытым каналам связи

**Технология создания виртуальных защищенных сетей (VPN)**

- позволяет соединить защищенными каналами связи компьютеры независимо от их месторасположения

**Технология криптографического преобразования данных**

- обеспечивает конфиденциальность информации при ее передаче и хранении

Схема 3.3.5. Технологии защиты информации

VPN (Virtual Protected Network) – это обобщенное название технологий, которые позволяют объединить в виртуальную защищенную сеть произвольное количество локальных сетей и отдельных компьютеров. VPN-сеть строится поверх других сетей передачи данных (в том числе и сети Интернет). С помощью криптографических методов VPN-сеть позволяет обеспечить конфиденциальность, аутентичность и целостность передаваемой информации.

Технология ViPNet – технология, предназначенная для развертывания защищенных виртуальных частных сетей (VPN) поверх глобальных и локальных сетей.

Криптографическая защита информации предполагает использование средств шифрования данных и сложных алгоритмов кодирования. Осуществляется с помощью программных и аппаратных средств. Наиболее известный элемент средств криптографической защиты информации – ключ с электронной подписью.

## РАЗДЕЛ 4. ИСТОЧНИКИ И КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ. ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

### 4.1. Понятие и виды каналов утечки информации

**Утечка информации по техническому каналу** – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации<sup>1</sup>. Источники утечки информации представлены на схеме 4.1.1.

**Перехват информации** – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информационных сигналов<sup>2</sup>. Структура канала утечки информации представлена на схеме 4.1.2.



Схема 4.1.1. Источники утечки информации



Схема 4.1.2. Структура канала утечки информации

<sup>1</sup> Рекомендации по стандартизации Р 50.1.056-2005 Техническая защита информации. Основные термины и определения (утв. приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 № 479-ст.) // Справочно-правовая система «КонтурНорматив». URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=200721> (дата обращения: 18.05.2026).

<sup>2</sup> Там же.

Формы и каналы утечки могут быть разнообразными и зависят от причин, методов и способов передачи информации (см. схему 4.1.3).



Схема 4.1.3. Формы утечки информации

Каналы утечки информации разделяют на агентурные, легальные и технические (см. схему 4.1.4).

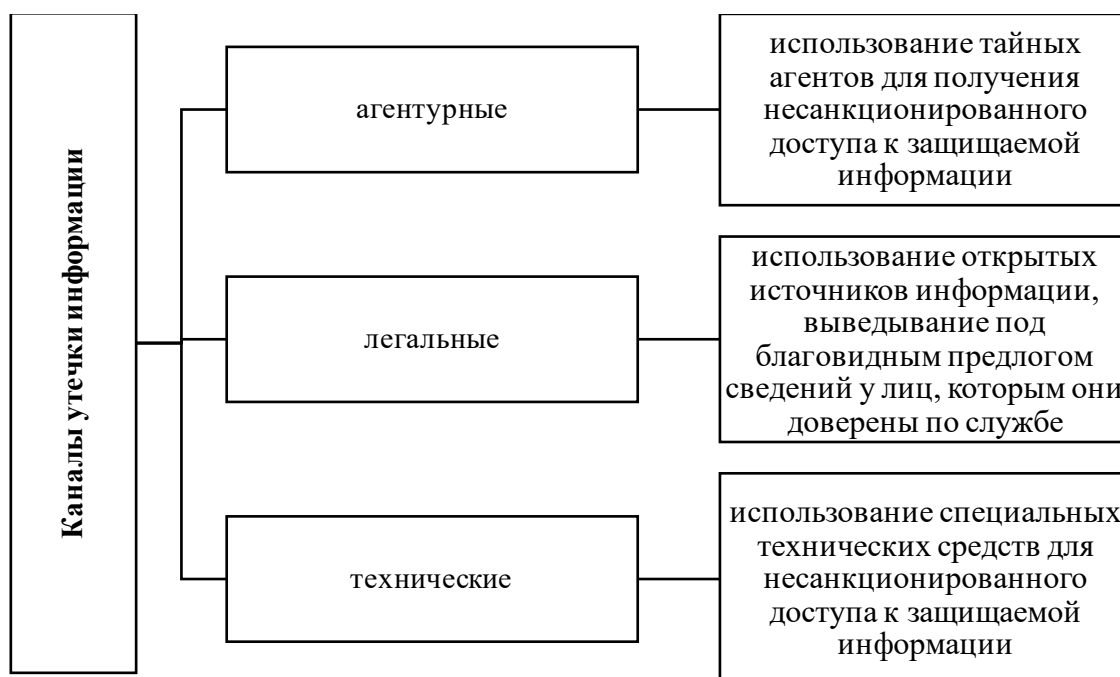


Схема 4.1.4. Каналы утечки информации

## 4.2. Технические каналы утечки информации

**Технический канал утечки информации** – совокупность объекта разведки, технического средства разведки, с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал (см. схему 4.2.1).

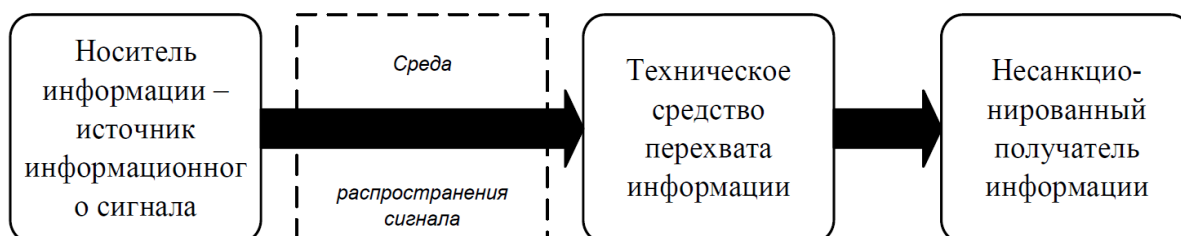


Схема 4.2.1. Структура технического канала утечки информации

В зависимости от физической природы возникновения информационных сигналов технические каналы утечки информации разделяют на акустические, материально-вещественные, визуально-оптические, электромагнитные (см. схему 4.2.2).

Каждый тип технического канала утечки информации требует специфического подхода к выбору мер защиты информации.

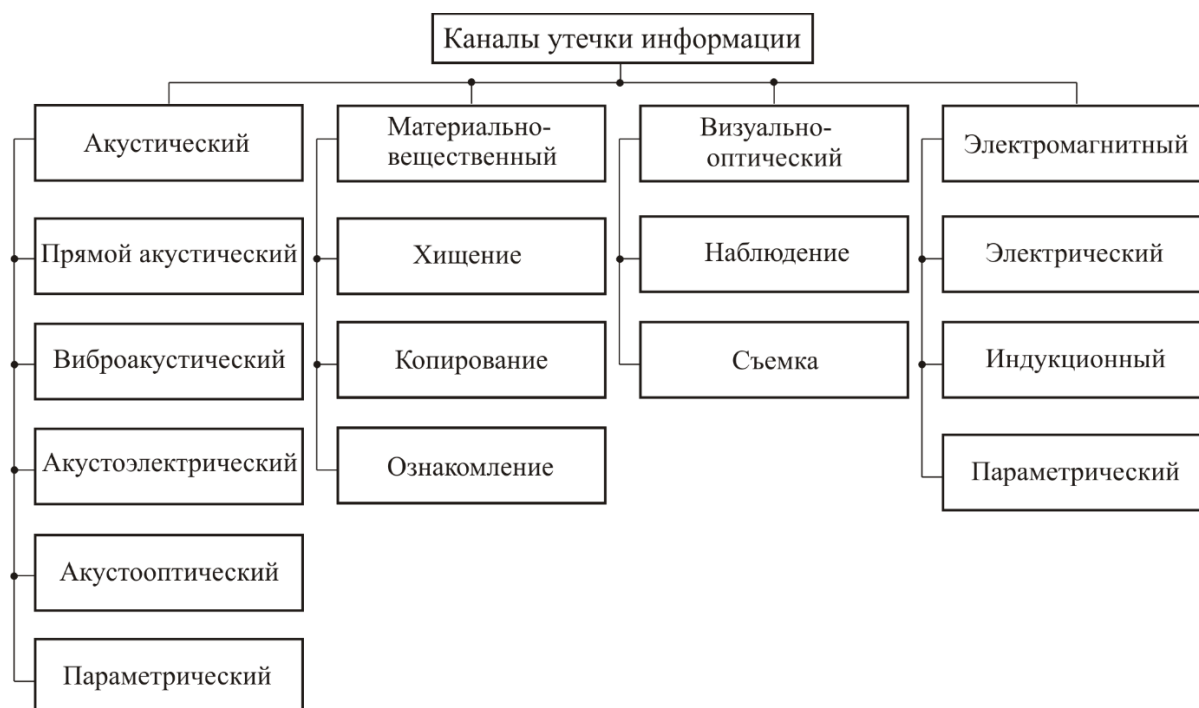


Схема 4.2.2. Технические каналы утечки информации по физической природе носителя

### 4.3. Защита информации от утечки по техническим каналам

**Средство защиты информации от утечки по техническим каналам** – техническое средство, вещество или материал, предназначенные и (или) используемые для защиты информации от утечки по техническим каналам (см. схему 4.3.1).

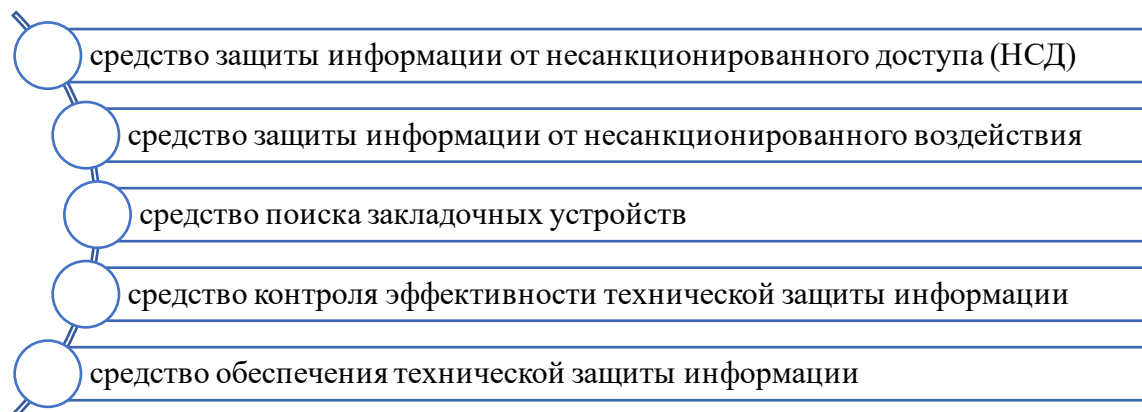


Схема 4.3.1. Средства технической защиты информации

Технические мероприятия – это мероприятия по защите информации, предусматривающие применение специальных технических средств, а также реализацию технических решений. Например, пространственное зашумление, линейное зашумление, уничтожение закладных устройств.

## РАЗДЕЛ 5. ОСНОВЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

### 5.1. Основные понятия криптографической защиты информации

**Криптография** – наука о методах обеспечения конфиденциальности и аутентичности (целостности и подлинности авторства) информации. Криптография являются одним из способов защиты информации (см. схему 5.1.1).

Аутентификация сторон и аутентификация данных – это два взаимосвязанных процесса проверки подлинности в информационных системах (см. схему 5.1.2).

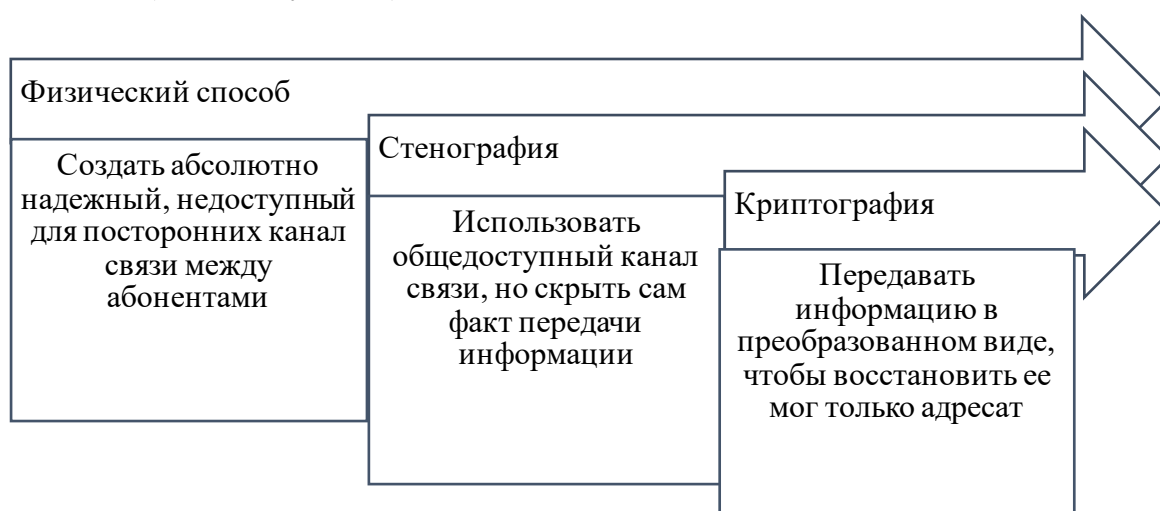


Схема 5.1.1. Способы защиты информации



Схема 5.1.2. Составляющие процесса аутентификации

Меры криптографической защиты информации – это комплекс правовых, организационных и технических действий, направленных на обеспечение конфиденциальности, проверку целостности и подлинности информации (см. схему 5.1.3).



Схема 5.1.3. Задачи криптографической защиты информации

Правовое регулирование криптографической защиты информации в России осуществляется несколькими ключевыми органами и нормативными актами (см. схему 5.1.4).

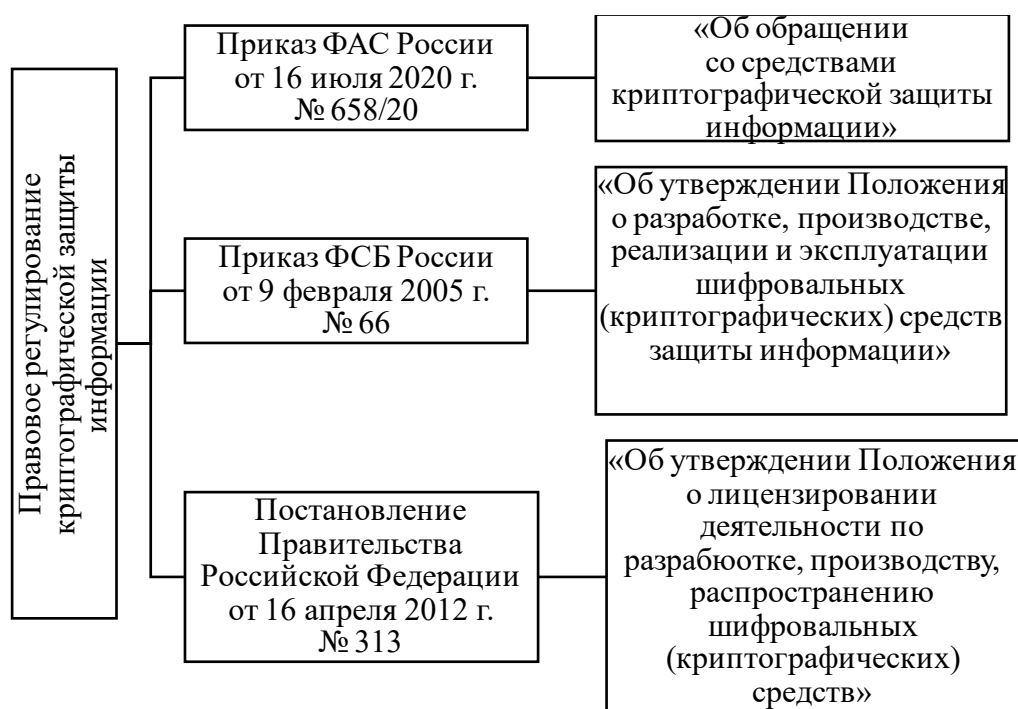


Схема 5.1.4. Правовое регулирование криптографической защиты информации

Некоторые исторические примеры шифрования представлены на схеме 5.1.5.

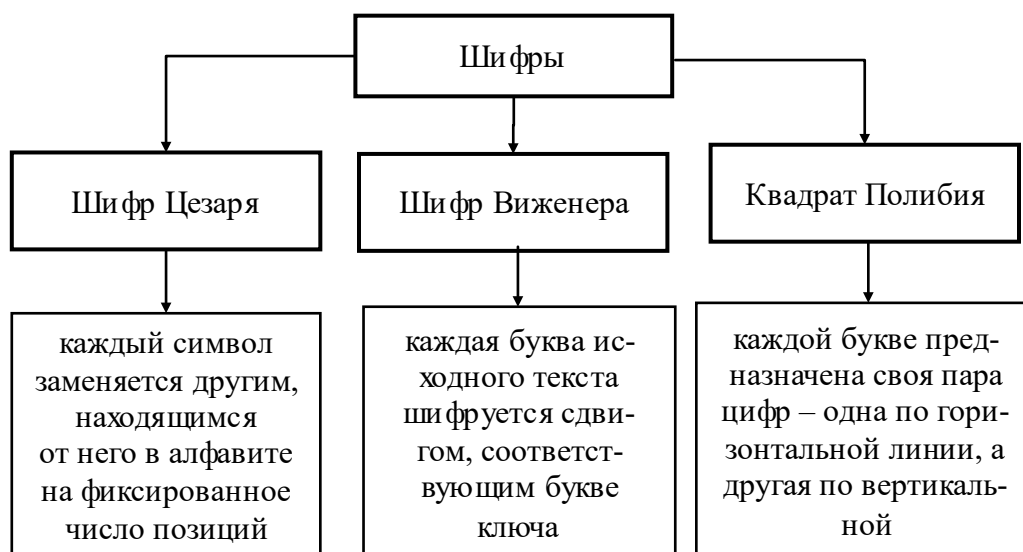


Схема 5.1.5. Исторические примеры шифрования

## 5.2. Методы криптографической защиты информации

Для обеспечения конфиденциальности, целостности и подлинности данных применяются различные криптографические методы. Ключевые из них систематизированы на схеме 5.2.1.

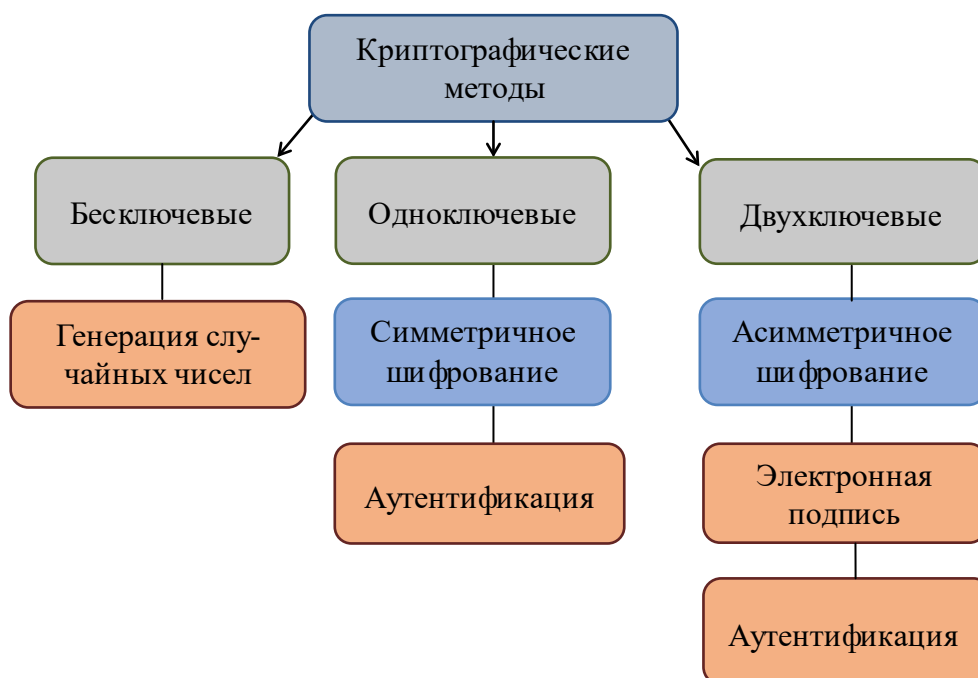


Схема 5.2.1. Методы криптографической защиты информации

**Симметричная система шифрования** – система шифрования, являющаяся симметричной криптографической системой, в которой для зашифрования и расшифрования применяются одинаковые секретные ключи<sup>1</sup> (см. схему 5.2.2).

**Асимметричная система шифрования** – система шифрования, являющаяся асимметричной криптографической системой, в которой зашифрование осуществляется с использованием открытого ключа получателя, а расшифрование – с помощью личного (закрытого) ключа получателя<sup>2</sup> (см. схему 5.2.3).



Схема 5.2.2. Симметричный метод шифрования

**Открытый текст** (исходный текст или сообщение) – подлежащие защите данные.

**Шифротекст** – защищенные данные, полученные посредством зашифрования.

**Зашифрование** – зависящий от криптографического ключа процесс обратимого преобразования открытого текста в шифрованный текст<sup>3</sup>.

**Расшифрование** – зависящий от криптографического ключа процесс преобразования шифрованного текста в соответствующий ему открытый текст<sup>4</sup>.

**Ключ** – секретная информация, используемая **криптографическим** алгоритмом при зашифровании/расшифровании сообщений, постановке и проверке цифровой подписи.

<sup>1</sup> Информационная технология. Криптографическая защита информации. Термины и определения. ПНСТ 799-2022 // Электронный фонд правовых и нормативно-технических документов. URL: <https://docs.cntd.ru/document/1200194122> (дата обращения: 18.04.2026).

<sup>2</sup> Там же.

<sup>3</sup> Там же.

<sup>4</sup> Там же.

Принцип действия асимметричного шифрования: субъект А генерирует два ключа – открытый и закрытый (публичный и приватный), передает открытый ключ субъекту Б. Передача может осуществляться по незащищенным каналам. Субъект Б шифрует пакет данных при помощи полученного открытого ключа и передает его А. Передача может осуществляться по незащищенным каналам. Субъект А расшифровывает полученную от Б информацию при помощи секретного, закрытого ключа.

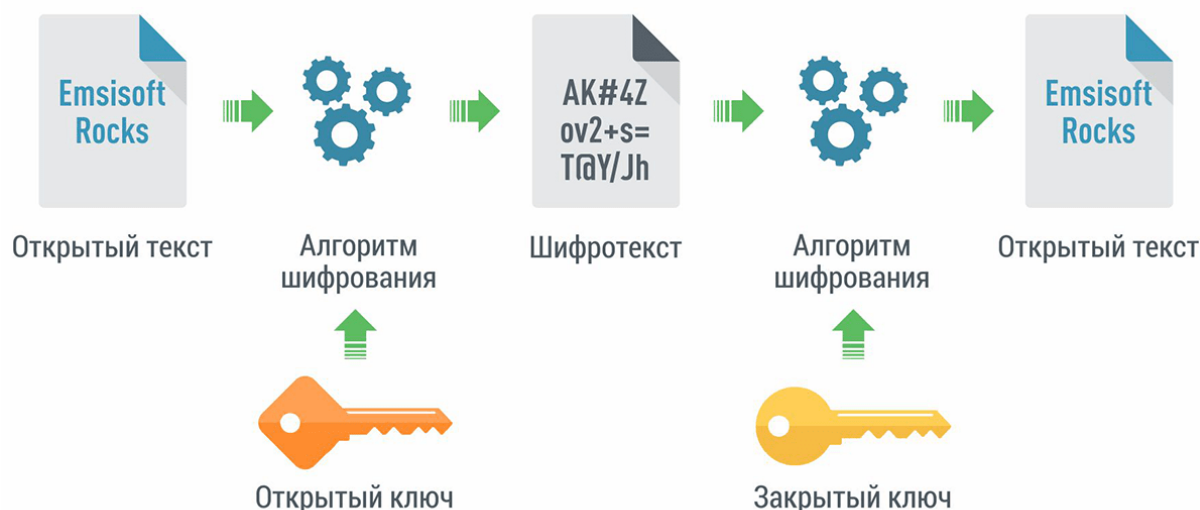


Схема 5.2.3. Асимметричный метод шифрования

**Средства криптографической защиты информации (СКЗИ)** – средства, системы и комплексы, реализующие криптографическую систему.

К средствам криптографической защиты информации относятся:

- средства шифрования;
- средства имитозащиты;
- средства электронной подписи;
- средства кодирования;
- средства изготовления ключевых документов;
- ключевые документы.

### 5.3. Электронная цифровая подпись

**Цифровая подпись** – результат зависящего от ключа подписи и параметров схемы цифровой подписи криптографического преобразования набора данных (сообщения), обеспечивающий возможность аутентифика-

пии источника и проверки целостности набора данных (сообщения) и невозможность отрицания факта создания подписи<sup>1</sup>.

**Средство электронной подписи (далее – ЭП)** – средство криптографической защиты информации, реализующее хотя бы одну из следующих функций: создание электронной подписи с использованием ключа электронной подписи, проверка электронной подписи с использованием ключа проверки электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи<sup>2</sup>.

Принцип формирования ЭП представлен на схеме 5.3.1.

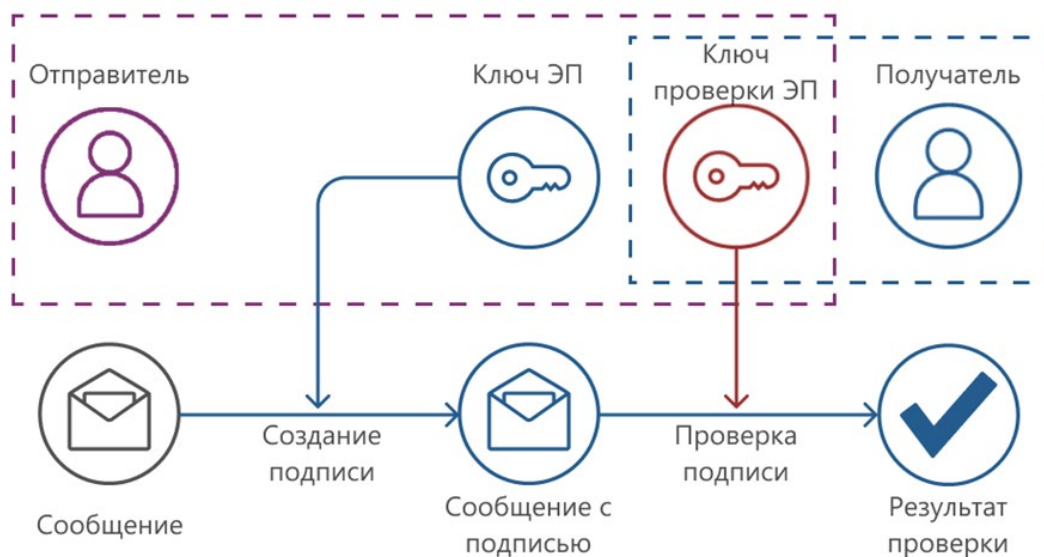


Схема 5.3.1. Принцип формирования ЭП

**Квалифицированный сертификат ключа проверки электронной подписи** – сертификат ключа проверки ЭП, соответствующий требованиям, установленным Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи и являющийся в связи с этим официальным документом<sup>3</sup>.

Жизненный цикл проверки сертификата включает несколько взаимосвязанных этапов от момента его выпуска до окончания срока действия или отзыва (см. схему 5.3.2).

<sup>1</sup> Информационная технология. Криптографическая защита информации. Термины и определения. ПНСТ 799-2022 // Электронный фонд правовых и нормативно-технических документов. URL: <https://docs.cntd.ru/document/1200194122> (дата обращения: 18.04.2026).

<sup>2</sup> Там же.

<sup>3</sup> Об электронной подписи : федеральный закон от 6 апреля 2011 г. № 63-ФЗ. Доступ из справочно-правовой системы «КонсультантПлюс».



Схема 5.3.2. Жизненный цикл проверки сертификата

Для защиты ЭП применяются программно-аппаратные средства защиты (см. схему 5.3.3).

**Сетевая атака** – это вторжение в операционную систему удаленного компьютера. Злоумышленники предпринимают сетевые атаки, чтобы захватить управление над операционной системой, привести ее к отказу в обслуживании или получить доступ к защищенной информации.

Сетевые атаки можно разделить на пассивные и активные (см. схему 5.3.4).

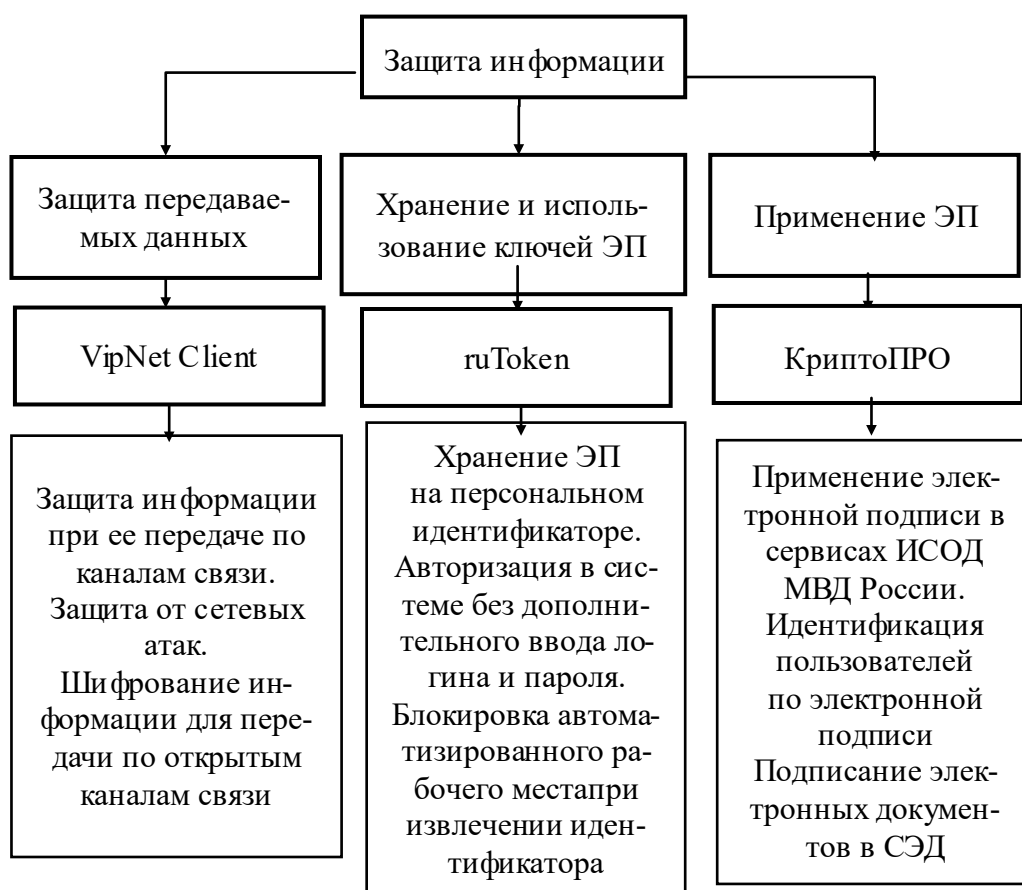


Схема 5.3.3. Программно-аппаратные средства защиты информации

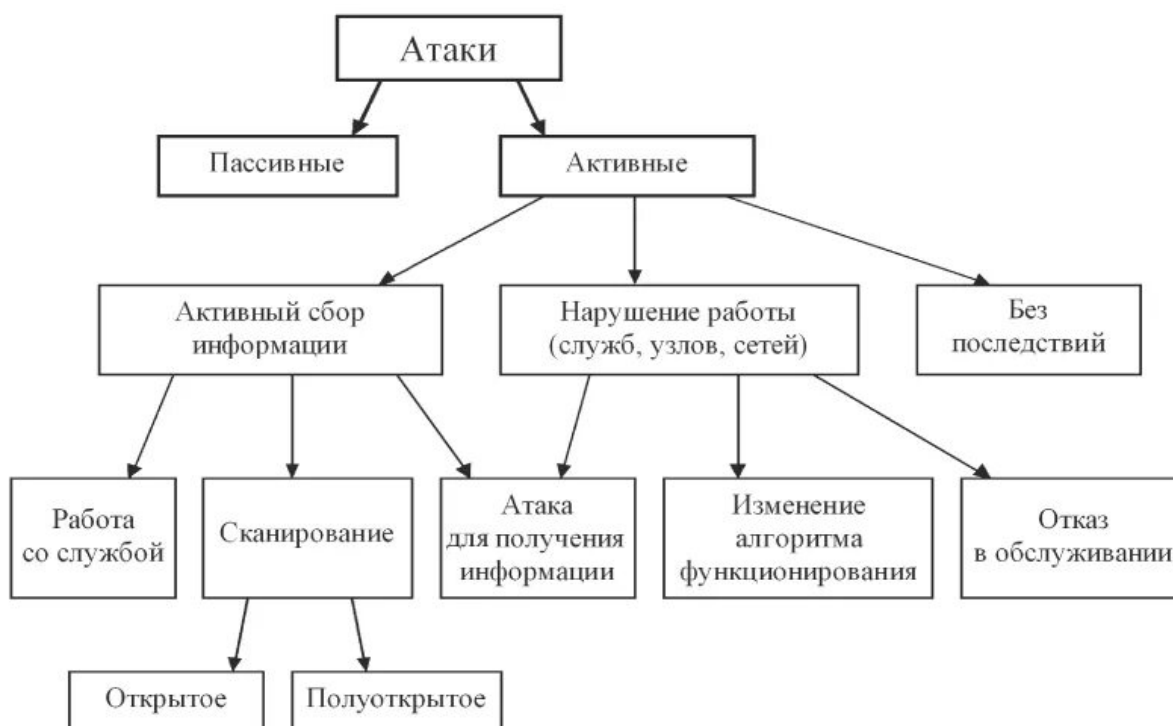


Схема 5.3.4. Виды сетевых атак

## РАЗДЕЛ 6. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ КИБЕРБЕЗОПАСНОСТИ И ИХ ОБРАБОТКА

### 6.1. Этапы управления инцидентами кибербезопасности

**Инцидент информационной безопасности** – одно или несколько нежелательных или неожиданных событий информационной безопасности, которые со значительной вероятностью приводят к компрометации бизнес-операций и создают угрозы для информационной безопасности<sup>1</sup>.

**Управление инцидентами информационной безопасности** – выявление недопустимых событий, ликвидация их последствий и минимизация повторного возникновения<sup>2</sup>. Этапы управления инцидентами кибербезопасности представлены на схеме 6.1.1.

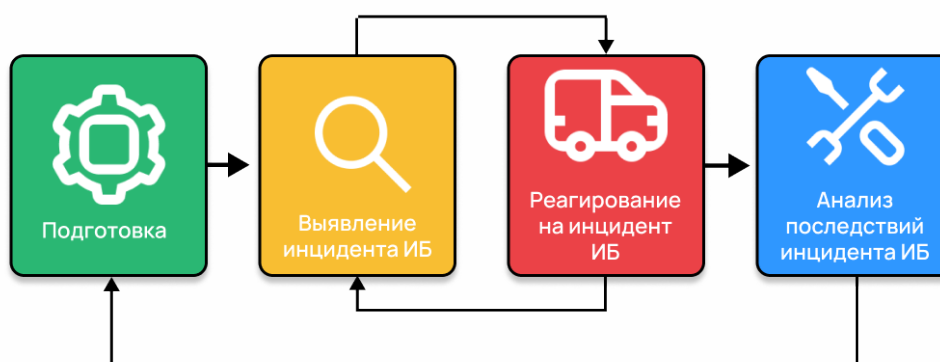


Схема 6.1.1. Этапы управления инцидентами кибербезопасности

Основными целями реагирования на инциденты кибербезопасности являются минимизация ущерба, скорейшее восстановление исходного состояния ИС и разработка плана по недопущению подобных инцидентов в будущем. Эти цели достигаются на двух основных этапах: расследование инцидента и восстановление системы (см. схему 6.1.2).



Схема 6.1.2. Этапы реагирования на инциденты кибербезопасности

Объекты воздействия информационных угроз представлены на схеме 6.1.3.

<sup>1</sup> Словарь терминов ФСТЭК России // Официальный сайт Федеральной службы по техническому и экспертному контролю (ФСТЭК России). URL: <https://bdu.fstec.ru/terms> (дата обращения: 19.04.2026).

<sup>2</sup> Там же.



Схема 6.1.3. Объекты воздействия угроз безопасности информации

Условием реализации угрозы безопасности обрабатываемой в системе информации может быть недостаток (уязвимость) информационной системы. Если уязвимость соответствует угрозе, то существует риск<sup>1</sup>. Взаимосвязь данных понятий отражена на схеме 6.1.2.

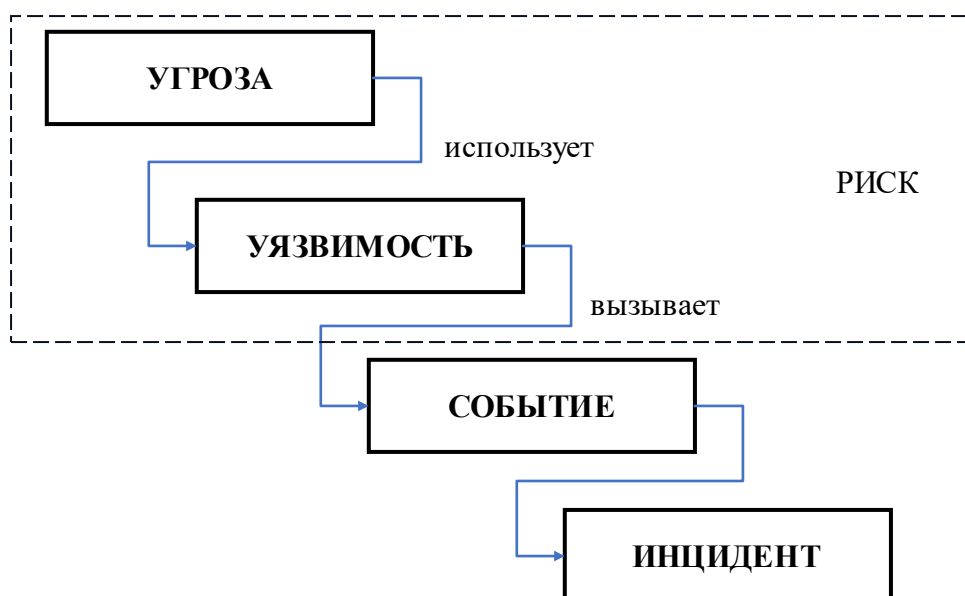


Схема 6.1.4. Взаимосвязь понятий «угроза безопасности», «уязвимость информационной системы», «событие информационной безопасности», «инцидент информационной безопасности»

<sup>1</sup> Рекомендации по стандартизации Р 50.1.056-2005 Техническая защита информации. Основные термины и определения (утв. приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 479-ст.) // Справочно-правовая система «КонтурНорматив». URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=200721> (дата обращения: 18.05.2026).

**Уязвимость** (информационной системы) – свойство информационной системы, предоставляющее возможность реализации угроз безопасности обрабатываемой в ней информации<sup>1</sup>.

## 6.2. Оценка угроз безопасности информации

**Угрозы безопасности информации** (далее – УБИ) определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности)<sup>2</sup> (см. схему 6.2.1).



Схема 6.2.1. Составляющие УБИ

При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, применяемые информационные технологии и особенности (условия) функционирования информационной системы.

Эффективность принимаемых мер защиты информации в информационной системе зависит от качества определения угроз безопасности информации для конкретной информационной системы в конкретных условиях ее функционирования.

**Модель угроз безопасности информации** представляет собой формализованное описание угроз безопасности информации для конкретной информационной системы или группы информационных систем в определенных условиях их функционирования.

---

<sup>1</sup> Рекомендации по стандартизации Р 50.1.056-2005 Техническая защита информации. Основные термины и определения (утв. приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 479-ст.) // Справочно-правовая система «КонсультантПлюс». URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=200721> (дата обращения: 18.05.2026).

<sup>2</sup> Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г. Доступ из справочно-правовой системы «КонсультантПлюс».

Модель угроз безопасности информации разрабатывается обладателем информации (оператором, разработчиком (проектировщиком)) и должна по содержанию соответствовать Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы, разрабатываемые и утверждаемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о ФСТЭК России, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

Управление инцидентами кибербезопасности включает три этапа: определение негативных последствий, определение объектов воздействия, оценка возможности реализации угроз и их актуальности (см. схему 6.2.2).

|                                                                                  |                                                                        |
|----------------------------------------------------------------------------------|------------------------------------------------------------------------|
| <b>Этап 1.<br/>Определение<br/>негативных<br/>последствий</b>                    | Анализ документации систем и сетей и иных исходных данных              |
|                                                                                  | Определение негативных последствий от реализации угроз                 |
| <b>Этап 2.<br/>Определение<br/>объектов<br/>воздействия</b>                      | Анализ документации систем и сетей и иных исходных данных              |
|                                                                                  | Инвентаризация систем и сетей                                          |
|                                                                                  | Определение групп информационных ресурсов и компонентов систем и сетей |
| <b>Этап 3. Оценка<br/>возможности<br/>реализации угроз и их<br/>актуальности</b> | Определение источников угроз                                           |
|                                                                                  | Оценка способов реализации угроз                                       |
|                                                                                  | Оценка актуальности угроз                                              |

Схема 6.2.2. Этапы управления инцидентами кибербезопасности

### 6.3. Средства управления событиями кибербезопасности SIEM

SIEM (Security information and event management, «управление событиями и информацией о безопасности») – класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности. Компоненты SIEM представлены на схеме 6.2.3.

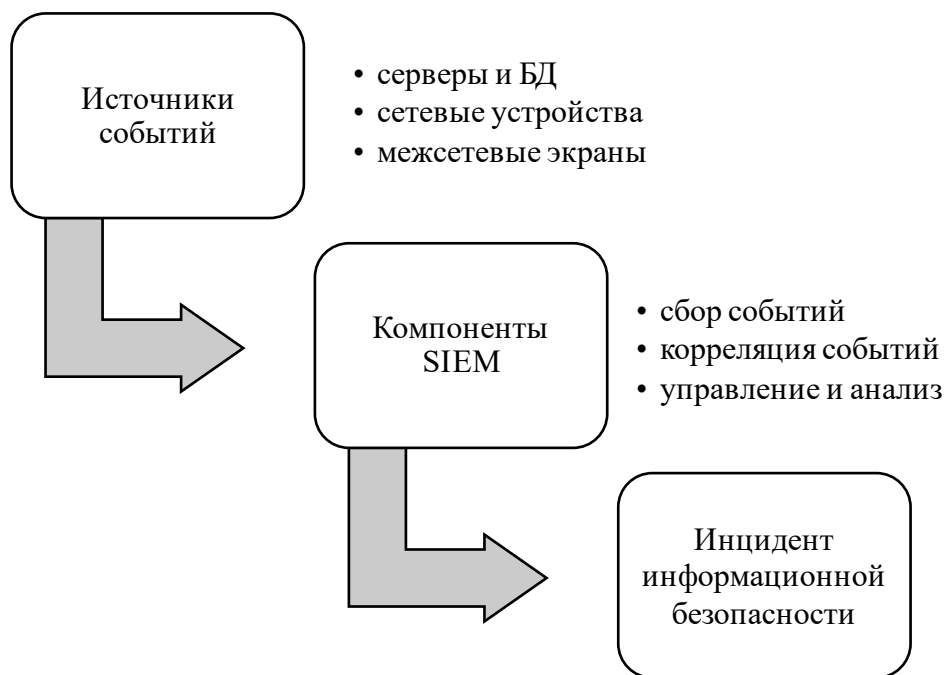


Схема 6.2.3. Компоненты SIEM

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

### I. Нормативные правовые акты и иные официальные документы

1. **Российская Федерация. Законы.** О безопасности : Федеральный закон от 28 декабря 2010 г. № 390 // Доступ из справочно-правовой системы «КонсультантПлюс». – URL: <http://www.consultant.ru> (дата обращения: 25.05.2026). – Текст : электронный.

2. **Российская Федерация. Законы.** Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ // Доступ из справочно-правовой системы «КонсультантПлюс». – URL: <http://www.consultant.ru> (дата обращения: 25.05.2026). – Текст: электронный.

3. **Российская Федерация. Законы.** Об электронной подписи : Федеральный закон от 6 апреля 2011 г. № 63-ФЗ // Доступ из справочно-правовой системы «КонсультантПлюс». – URL: <http://www.consultant.ru> (дата обращения: 25.05.2026). – Текст : электронный.

4. Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 // Доступ из справочно-правовой системы «КонсультантПлюс». – URL: <http://www.consultant.ru> (дата обращения: 25.05.2026). – Текст : электронный.

5. О защите информации : Закон Республики Таджикистан от 2 декабря 2002 г. № 71 // Национальный центр законодательства при Президенте Республики Таджикистан. – URL: <https://ncz.tj/content/закон-республика-таджикистан-о-защите-информации> (дата обращения: 25.05.2026). – Текст : электронный.

6. О защите персональных данных : Закон Республики Таджикистан от 3 августа 2018 г. № 1537 // Национальный центр законодательства при Президенте Республики Таджикистан. – URL: <https://ncz.tj/content/о-защите-персональных-данных> (дата обращения: 25.05.2026). – Текст : электронный.

7. О праве на доступ к информации : Закон Республики Таджикистан от 18 июня 2008 г. № 411 // Национальный центр законодательства при Президенте Республики Таджикистан. – URL: <https://ncz.tj/content/закон-республики-таджикистан-о-праве-на-доступ-к-информации> (дата обращения: 25.05.2026). – Текст : электронный.

8. Об информатизации : Закон Республики Таджикистан от 6 августа 2001 г. № 40 // Национальный центр законодательства при Президенте Республики Таджикистан. – URL: <https://ncz.tj/content/%C2%A0закон-республики-таджикистан-%C2%A0об-информатизации> (дата обращения: 25.05.2026). – Текст : электронный.

9. Об информации : Закон Республики Таджикистан от 10 мая 2002 г. № 55 // Национальный центр законодательства при Президенте Республики

Таджикистан. – URL: <https://ncz.tj/content/закон-республики-таджикистан-об-информации> (дата обращения: 25.05.2026). – Текст : электронный.

10. Уголовный кодекс Республики Таджикистан от 21 мая 1998 г. № 574 // Национальный центр законодательства при Президенте Республики Таджикистан. – URL: <https://ncz.tj/content/уголовный-кодекс-республики-таджикистан> (дата обращения: 25.05.2026). – Текст : электронный.

11. Об утверждении Концепции государственной информационной политики Республики Таджикистан : Указ Президента Республики Таджикистан от 30 апреля 2008 г. № 451 // База данных «Законодательство стран СНГ». – URL: <https://base.spinform.ru> (дата обращения: 25.05.2026). – Текст : электронный.

12. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г. // Официальный сайт ФСТЭК России. – URL: <https://fstec.ru/dokumenty-filter> (дата обращения: 25.05.2026). – Текст : электронный.

13. Национальный стандарт РФ ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения (утв. приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 532-ст) // Федеральное агентство по техническому регулированию и метрологии. – URL: <https://www.rst.gov.ru/> (дата обращения: 25.05.2026). – Текст : электронный.

14. Рекомендации по стандартизации Р 50.1.056-2005 Техническая защита информации. Основные термины и определения : утверждены Приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 479-ст // Федеральное агентство по техническому регулированию и метрологии. – URL: <https://www.rst.gov.ru/> (дата обращения: 25.05.2026). – Текст : электронный.

15. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 19 августа 2015 г. № 1181-ст // Электронный фонд правовых и нормативно-технических документов. – URL: <https://docs.cntd.ru/document/1200123702> (дата обращения: 25.05.2026). – Текст : электронный.

## **II. Учебная, научная литература и иные материалы**

1. **Щеглов, А. Ю.** Защита информации : основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. – Москва : Юрайт, 2026. – 349 с. – (Высшее образование). – ISBN 978-5-534-19762-4 // Образовательная платформа «Юрайт». – URL: <https://urait.ru/bcode/561077/p.1> (дата обращения: 25.05.2026). – Текст : электронный.

2. **Внуков, А. А.** Защита информации : учебник для вузов / А. А. Внуков. – 3-е изд., перераб. и доп. – Москва : Юрайт, 2026. – 161 с. – (Высшее образование). – ISBN 978-5-534-07248-8 // Образовательная платформа «Юрайт». – URL: <https://urait.ru/bcode/561313> (дата обращения: 25.05.2026). – Текст : электронный.

3. **Запечников, С. В.** Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. – Москва : Юрайт, 2026. – 309 с. – (Высшее образование). – ISBN 978-5-534-02574-3 // Образовательная платформа «Юрайт». – URL: <https://urait.ru/bcode/536453/p.9> (дата обращения: 25.05.2026). – Текст : электронный.

4. **Корабельников, С. М.** Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. – Москва : Юрайт, 2026. – 111 с. – (Высшее образование). – ISBN 978-5-534-12769-0 // Образовательная платформа «Юрайт». – URL: <https://urait.ru/bcode/543351> (дата обращения: 25.05.2026). – Текст : электронный.

5. **Зенков, А. В.** Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. – 2-е изд., перераб. и доп. – Москва : Юрайт, 2026. – 107 с. – (Высшее образование). – ISBN 978-5-534-16388-9 // Образовательная платформа «Юрайт». – URL: <https://urait.ru/bcode/567915> (дата обращения: 25.05.2026). – Текст : электронный.

### **III. Интернет-ресурсы**

1. Основы государственной политики Российской Федерации в области международной информационной безопасности // Совет безопасности Российской Федерации. – URL: <http://www.scrf.gov.ru> (дата обращения: 25.05.2026). – Текст : электронный.

2. Банк данных угроз безопасности информации // Федеральная служба по техническому и экспортному контролю (ФСТЭК России). – URL: <https://fstec.ru> (дата обращения: 25.05.2026). – Текст : электронный.

3. Направления деятельности Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. – URL: <https://digital.gov.ru/> (дата обращения: 25.05.2026). – Текст : электронный.

4. Публичная декларация целей и задач Роскомнадзора // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. – URL: <https://rkn.gov.ru> (дата обращения: 25.05.2026). – Текст : электронный.

*Учебное издание*

**Айдагулова** Алиса Расиховна  
(кандидат педагогических наук, б/з)

**Субхангулов** Рустем Раисович  
(кандидат экономических наук, доцент)

**Тугузбаев** Гаяз Ахтямович  
(б/с, б/з)

**Арипов** Анвар Лутфиллоевич  
(кандидат юридических наук, б/з)

## **ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ**

Альбом схем

*Редактор Р. Р. Гафарова*

---

Подписано в печать 18.06.2026

Гарнитура Times

Уч.-изд. л. 2,8

Тираж 220 экз.

Выход в свет 30.06.2026

Формат 60x84<sup>1</sup>/<sub>16</sub>

Усл. печ. л. 3

Заказ № 48

---

*Редакционно-издательский отдел  
Уфимского юридического института МВД России  
450103, г. Уфа, ул. Муксинова, 2*

*Отпечатано в группе полиграфической и оперативной печати  
Уфимского юридического института МВД России  
450103, г. Уфа, ул. Муксинова, 2*