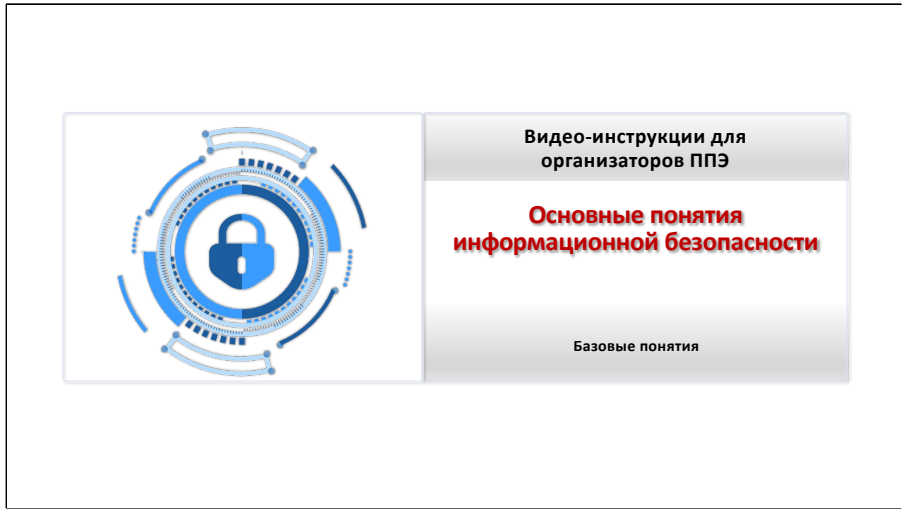


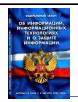
Видео-инструкции для организаторов государственной итоговой аттестации.
Базовые понятия информационной безопасности.

ФЗ «Об информации, информационных технологиях и о защите информации»

Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г. - **определяет основные понятия в области информационной безопасности и устанавливает требования к организации и защите информации**.

В России существуют несколько законов и нормативных актов, которые регулируют вопросы информационной безопасности. Основополагающим является федеральный закон "Об информации, информационных технологиях и о защите информации" №149-ФЗ. Он определяет основные понятия и требования в области информационной безопасности. Содержит требования к защите информации, правила обработки информации, установление правил доступа к информации, а также права и обязанности операторов информационных систем в области защиты информации.

ФЗ «Об информации, информационных технологиях и о защите информации»

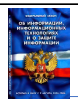


Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

Информация – любая информация в электронном или ином виде, передаваемая посредством информационных систем или иных технических средств.

Информация - любая информация в электронном или ином виде, передаваемая посредством информационных систем или иных технических средств.

ФЗ «Об информации, информационных технологиях и о защите информации»

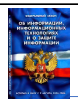


Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

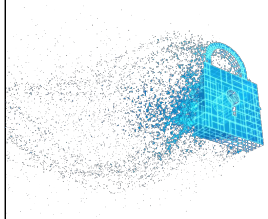
Информационная система – совокупность взаимосвязанных компьютерных устройств и программного обеспечения, предназначенных для обработки, хранения и передачи информации.

Информационная система это - совокупность взаимосвязанных компьютерных устройств и программного обеспечения, предназначенных для обработки, хранения и передачи информации.

ФЗ «Об информации, информационных технологиях и о защите информации»



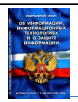
Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.



Информационная безопасность – состояние защищенности информации от неправомерного доступа, уничтожения, изменения, блокирования и распространения.

Информационная безопасность - это состояние защищенности информации от неправомерного доступа, уничтожения, изменения, блокирования и распространения.

ФЗ «Об информации, информационных технологиях и о защите информации»

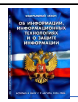


Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

Оператор информационной системы – юридическое или физическое лицо, осуществляющее деятельность по созданию, использованию и обслуживанию информационной системы.

Оператор информационной системы – это юридическое или физическое лицо, осуществляющее деятельность по созданию, использованию и обслуживанию информационной системы.

ФЗ «Об информации, информационных технологиях и о защите информации»



Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

Оператор информационной системы обязан:

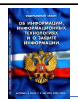
- установить режим работы информационной системы
- обеспечить её защиту от неправомерного доступа
- обеспечить контроль за обработкой информации
- установить правила доступа к информации

и т.д.

В обязанности оператора информационной системы входит установление режима работы информационной системы. Обеспечение ее защиты от неправомерного доступа. Контроль за обработкой информации и установление правил доступа к информации. Под режимом работы информационной системы понимается установление ограничений на доступ к информации. Установление порядка доступа к информации, установление требований к аутентификации пользователей.

Напомним, что аутентификация отличается от идентификацией не только установлением личности, но и подтверждением личности.

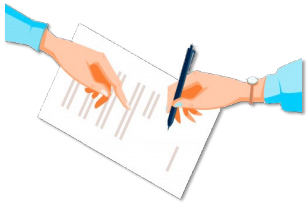
ФЗ «Об информации, информационных технологиях и о защите информации»



Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

Средства защиты информации - технические и организационные меры, применяемые для защиты информации.

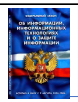
технические



организационные

Средства защиты информации - технические и организационные меры, применяемые для защиты информации.

ФЗ «Об информации, информационных технологиях и о защите информации»

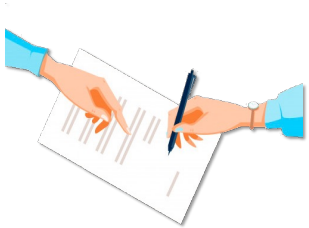


Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

Технические средства защиты информации:
- файрволлы (брэндмауэры)

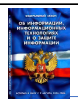
программное или аппаратное обеспечение, которое контролирует доступ к сети или компьютеру и блокирует нежелательный трафик

К техническим средствам защиты информации, относят:



технические **организационные**

ФЗ «Об информации, информационных технологиях и о защите информации»

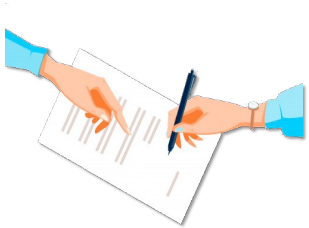


Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

Технические средства защиты информации:
- файрволлы (брэндмауэры)

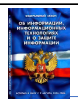
программное или аппаратное обеспечение, которое контролирует доступ к сети или компьютеру и блокирует нежелательный трафик

Фаерволлы: программное или аппаратное обеспечение, которое контролирует доступ к сети или компьютеру и блокирует нежелательный трафик.



технические **организационные**

ФЗ «Об информации, информационных технологиях и о защите информации»

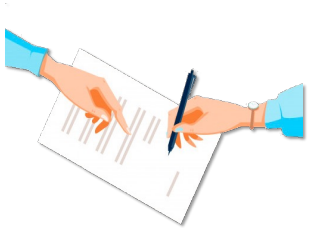


Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

Технические средства защиты информации:
- файрволлы (брэндмауэры)
- антивирусы

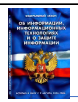
приложение, предназначенное для обнаружения и удаления вирусов и других вредоносных программ.

Антивирусное ПО: приложение, предназначенное для обнаружения и удаления вирусов и других вредоносных программ.



технические **организационные**

ФЗ «Об информации, информационных технологиях и о защите информации»

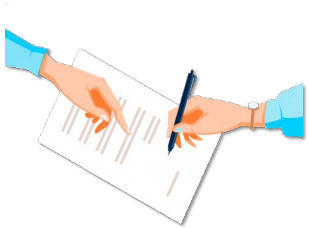


Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

Технические средства защиты информации:
- файрволлы (брэндмауэры)
- антивирусы
- шифрование

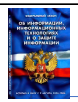
процесс преобразования данных в непонятный для посторонних вид, который может быть прочитан только с использованием соответствующего ключа.

Шифрование: процесс преобразования данных в непонятный для посторонних вид, который может быть прочитан только с использованием соответствующего ключа.



технические **организационные**

ФЗ «Об информации, информационных технологиях и о защите информации»

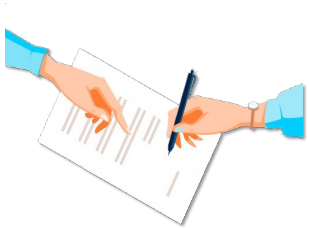


Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

Технические средства защиты информации:
- файрволлы (брэндмауэры)
- антивирусы
- шифрование
- vpn (виртуальные частные сети)

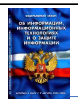
виртуальная частная сеть обеспечивает защищённое с помощью шифрования соединение между компьютерами или сетями через общедоступную сеть, такую как Интернет.

VPN: виртуальная частная сеть, которая обеспечивает защищенное соединение между компьютерами или сетями через общедоступную сеть, такую как Интернет.



технические **организационные**

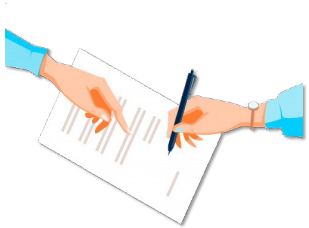
ФЗ «Об информации, информационных технологиях и о защите информации»



Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

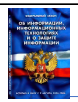
Технические средства защиты информации:
- файрволлы (брэндмауэры)
- антивирусы
- шифрование
- vpn (виртуальные частные сети)
- безопасные протоколы передачи данных

Безопасные протоколы передачи данных: такие, как HTTPS, который обеспечивает защищенную передачу данных между веб-браузером и веб-сервером.



технические **организационные**

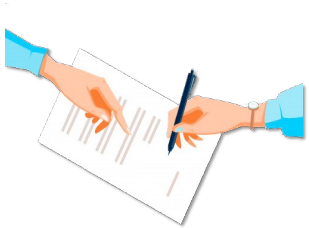
ФЗ «Об информации, информационных технологиях и о защите информации»



Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

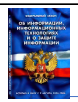
Технические средства защиты информации:
- файрволлы (брэндмауэры)
- антивирусы
- шифрование
- vpn (виртуальные частные сети)
- безопасные протоколы передачи данных
- бэкапы (резервные копии)

Бэкапы: копии данных, созданные для восстановления данных в случае их потери или повреждения.



технические **организационные**

ФЗ «Об информации, информационных технологиях и о защите информации»

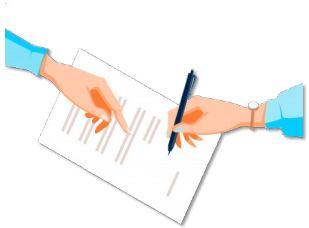


Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

Технические средства защиты информации:
- файрволлы (брэндмауэры)
- антивирусы
- шифрование
- vpn (виртуальные частные сети)
- безопасные протоколы передачи данных
- бэкапы (резервные копии)
- системы аутентификации

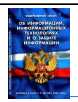
процесс проверки подлинности пользователей, использующих систему, например, пароль или биометрические данные

Системы аутентификации: процесс проверки подлинности пользователей, использующих систему, например, пароль или биометрические данные.



технические **организационные**

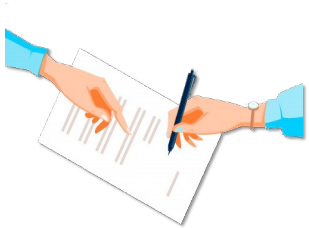
ФЗ «Об информации, информационных технологиях и о защите информации»



Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

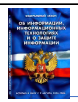
Технические средства защиты информации:
- файрволлы (брэндмауэры)
- антивирусы
- шифрование
- vpn (виртуальные частные сети)
- безопасные протоколы передачи данных
- бэкапы (резервные копии)
- системы аутентификации
- системы мониторинга безопасности

Системы мониторинга безопасности: приложения, которые мониторят события в системе и обнаруживают попытки несанкционированного доступа или другие аномалии в работе системы.



технические **организационные**

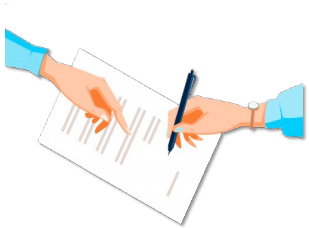
ФЗ «Об информации, информационных технологиях и о защите информации»



Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

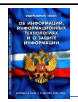
Технические средства защиты информации:
- файрволлы (брэндмауэры)
- антивирусы
- шифрование
- vpn (виртуальные частные сети)
- безопасные протоколы передачи данных
- бэкапы (резервные копии)
- системы аутентификации
- системы мониторинга безопасности
- контент-фильтры

Фильтры контента: программное обеспечение, которое блокирует доступ к определенным категориям сайтов или материалов.



технические **организационные**

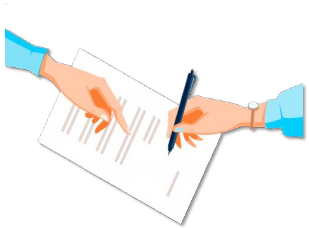
ФЗ «Об информации, информационных технологиях и о защите информации»



Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

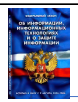
Технические средства защиты информации:
- файрволлы (брэндмауэры)
- антивирусы
- шифрование
- vpn (виртуальные частные сети)
- безопасные протоколы передачи данных
- бэкапы (резервные копии)
- системы аутентификации
- системы мониторинга безопасности
- контент-фильтры
- системы защиты от DDoS-атак

Системы защиты от DDoS-атак: меры, которые принимаются для предотвращения или минимизации эффектов DDoS-атак, например, блокировка IP-адресов или распределение нагрузки.



технические **организационные**

ФЗ «Об информации, информационных технологиях и о защите информации»



Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

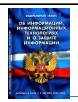
Технические средства защиты информации:
- файрволлы (брэндмауэры)
- антивирусы
- шифрование
- vpn (виртуальные частные сети)
- безопасные протоколы передачи данных
- бэкапы (резервные копии)
- системы аутентификации
- системы мониторинга безопасности
- контент-фильтры
- системы защиты от DDoS-атак
- система защиты от несанкционированного доступа

ющих

Система защиты от несанкционированного доступа - это комплекс мер, направленных на предотвращение или обнаружение попыток несанкционированного доступа к защищаемой системе или данным. Включают в себя различные технические и программные решения, такие как авторизация пользователей, пароли и биометрические данные.

технические **организационные**

ФЗ «Об информации, информационных технологиях и о защите информации»



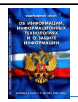
Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

Организационные меры защиты информации –

это комплекс мероприятий, осуществляемых организацией для обеспечения безопасности информации.

Организационные меры защиты информации - это комплекс мероприятий, осуществляемых организацией для обеспечения безопасности информации. Эти меры включают в себя политики, процедуры и правила, которые разрабатываются и внедряются в организации для защиты информации от угроз.

технические **организационные**



Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

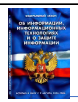
Организационные меры защиты информации:

- разработка политики безопасности информации – это документ, который описывает политику безопасности и правила, которые необходимо соблюдать в организации.

Организационные меры защиты информации могут быть разными и зависят от размера организации, ее бизнес-процессов, правовых требований и других факторов. Они включают в себя

- разработку политики безопасности информации – это документ, который описывает политику безопасности и правила, которые необходимо соблюдать в организации. Он может включать в себя правила использования электронной почты, доступа к информации, управления паролями и т.д.

технические **организационные**



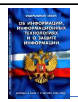
Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

Организационные меры защиты информации:

- разработка политики безопасности информации
- обучение сотрудников правилам и процедурам защиты информации, принятым в организации

Обучение сотрудников - это процесс обучения сотрудников организации правилам и процедурам защиты информации, включая защиту от вредоносных программ, вредоносных сайтов и фишинга.

технические **организационные**



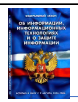
Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

Организационные меры защиты информации:

- разработка политики безопасности информации
- обучение сотрудников
- управление доступом сотрудников к информации и ресурсам организации

Управление доступом - это процесс управления правами доступа сотрудников к информации и ресурсам организации. Это может включать в себя установку различных уровней доступа, использование паролей, аутентификацию

технические **организационные**



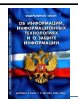
Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

Организационные меры защиты информации:

- разработка политики безопасности информации
- обучение сотрудников
- управление доступом
- контроль и мониторинг – периодический и непрерывный процесс проверки состояния защищённости информации

Контроль и мониторинг - это процесс контроля и мониторинга системы защиты информации для выявления несанкционированных доступов, нарушений безопасности или других инцидентов, которые могут привести к утечке информации или нарушению ее целостности.

технические **организационные**



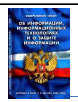
Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

Организационные меры защиты информации:

- разработка политики безопасности информации
- обучение сотрудников
- управление доступом
- контроль и мониторинг
- резервное копирование и восстановление

Резервное копирование и восстановление - это процесс создания резервных копий данных и разработки планов восстановления для минимизации ущерба в случае нарушения безопасности информации.

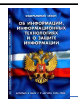
технические **организационные**



Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

Организационные меры защиты информации снижают риски нарушения безопасности, связанные с ошибками и действиями людей и в особенности – собственных сотрудников организации.

Многие нарушения безопасности информации происходят из-за ошибок или злонамеренных действий. Например, работники могут случайно отправить конфиденциальную информацию на неправильный адрес электронной почты или утерять устройство, содержащее важную информацию. Злоумышленники могут использовать социальную инженерию, чтобы получить доступ к информации, получая доступ к паролям или перехватывая сообщения. Организационные меры защиты информации позволяют организациям снизить риски нарушения безопасности информации, связанные с такими ошибками и действиями.

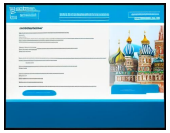


Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 г.

информация

государственная тайна

конфиденциальная



общедоступная

В соответствии с законом вся информация делится на три типа:

- общедоступная информация – свободно распространяемая;
- конфиденциальная информация – требующая защиты информация, передача её третьим лицам преследуется по закону и карается штрафом в соответствии с Административным кодексом, а также компенсацией нанесённого ущерба и морального вреда;
- государственная тайна.

Отнесение информации к конфиденциальной информации или государственной тайне возможно только на основании федеральных законов.

Какая информация является конфиденциальной?

Закон №152-ФЗ «О персональных данных» относит к конфиденциальной информации **персональные данные участников** государственной итоговой аттестации, а также **сотрудников**, привлекаемых к организации и проведению ГИА.

Закон №273-ФЗ «Об образовании в Российской федерации» относит к конфиденциальной информации **содержание контрольных измерительных материалов** государственной итоговой аттестации.

Сотрудникам, привлекаемым к ГИА следует знать и помнить, что в соответствии с законом №152-ФЗ "О персональных данных", персональные данные участников государственной итоговой аттестации и сотрудников, привлекаемых к её проведению, относятся к конфиденциальной информации. А законом №273-ФЗ "Об образовании в Российской Федерации» к таковой категории информации отнесено содержание контрольных измерительных материалов государственной итоговой аттестации.

Какая информация является конфиденциальной?

Ответственность:
- административная
- гражданская
- уголовная

Простой способ не нарушить - соблюдать правила, описанные в методических материалах.

В соответствии с этим законом, за разглашение конфиденциальной информации может быть наложен административный штраф. Кроме того, должностные лица могут быть лишены права занимать определенные должности или заниматься определенной деятельностью. В случае если разглашение конфиденциальной информации приводит к причинению материального ущерба, то лицо, допустившее разглашение, может быть привлечено к гражданской ответственности и возмещению ущерба.
Кроме того, разглашение конфиденциальной информации может быть квалифицировано как уголовное преступление и вести к уголовной ответственности.
Таким образом, ответственность за разглашение конфиденциальной информации в России может быть достаточно серьезной, включая административную, гражданскую и уголовную ответственность.

Правила работы с конфиденциальной информацией

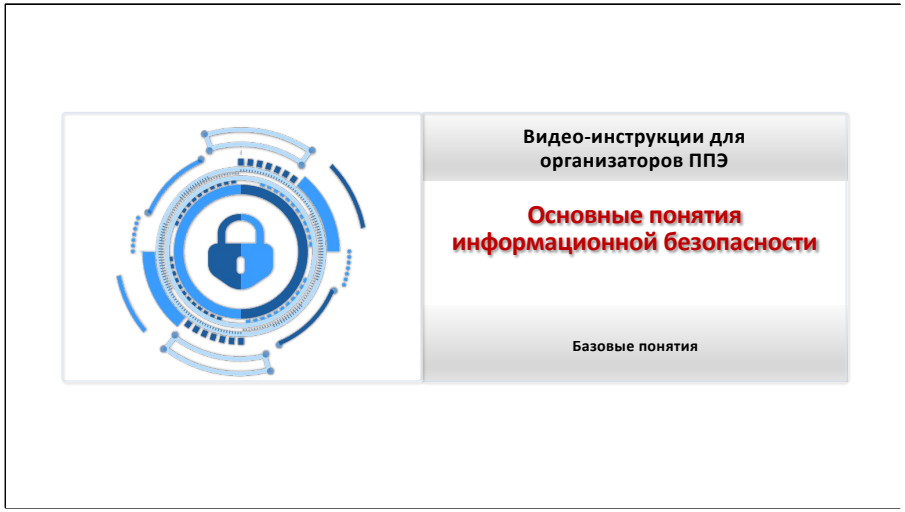
Правило №1: не делать копий информации

Правило №2: не выносить носители за пределы защищаемых помещений

Правило №2: не передавать информацию третьим лицам

Правило №3: не принимать самостоятельных решений, при любых сомнениях – свериться с инструкцией или спросить правила работы у руководителя пункта проведения экзаменов

Достаточно помнить всего четыре правила: нельзя делать копий носителей информации, выносить их за пределы защищаемых помещений, передавать информацию третьим лицам. И главное правило, соответствующее служебной этике – никогда не принимать самостоятельных решений, все действия сверять с инструкциями или указаниями руководителя ППЭ.



Видео-инструкции для организаторов государственной итоговой аттестации.
Базовые понятия информационной безопасности.