Занятие 21. Лекция

Конспект лекции присылать на почту tankae@inbox.ru до 21:00

Тема: Защита информации. Информационная безопасность.

План лекции:

- В чем заключается проблема информационной безопасности?
- Дайте определение понятию "информационная безопасность"
- Какие перспективы у развития законодательства?
- Выписать сравнительную таблицу.

Определение информационной безопасности

Информационная безопасность – это область знаний и практик, которая занимается защитой информации от несанкционированного доступа, использования, раскрытия, изменения или уничтожения. Она включает в себя меры, методы и технологии, направленные на обеспечение конфиденциальности, целостности и доступности информации.

Цель информационной безопасности – обеспечить защиту информации от угроз, которые могут возникнуть как извне, так и изнутри организации. Угрозы могут быть различными, включая хакерские атаки, вирусы, фишинг, утечки данных и другие.

Информационная безопасность включает в себя не только технические аспекты, но и организационные, процессные и человеческие. Она требует комплексного подхода, включающего в себя разработку политик и процедур, обучение персонала, использование специальных технологий и инструментов.

Основные принципы информационной безопасности включают:

- Конфиденциальность – обеспечение доступа к информации только уполномоченным лицам;
- Целостность – сохранение целостности информации и защита от несанкционированных изменений;
- Доступность – обеспечение доступа к информации в нужное время и место;
- Аутентификация – проверка подлинности пользователей и устройств;
- Авторизация – установление прав доступа к информации;
- Аудит – контроль и регистрация действий пользователей и системы;
- Физическая безопасность – защита физического доступа к информации и оборудованию.

Информационная безопасность является важной составляющей в современном мире, где информация стала одним из самых ценных активов. Правильное обеспечение безопасности информации позволяет предотвратить утечки данных, финансовые потери, нарушение репутации и другие негативные последствия.

Законодательная база информационной безопасности в России

В России информационная безопасность регулируется рядом законов и нормативных актов, которые устанавливают правила и требования к защите информации. Эти законы и акты создают основу для обеспечения безопасности информации в различных сферах деятельности.

Основные законы и нормативные акты:

- Федеральный закон “Об информации, информационных технологиях и о защите информации” от 27 июля 2006 года № 149-ФЗ;
- Федеральный закон “О персональных данных” от 27 июля 2006 года № 152-ФЗ;
- Федеральный закон “О защите детей от информации, причиняющей вред их здоровью и развитию” от 29 декабря 2010 года № 436-ФЗ;
- Федеральный закон “О государственной тайне” от 21 июля 1993 года № 5485-1;
- Постановление Правительства РФ “Об утверждении Правил обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных” от 1 ноября 2012 года № 1119;
- Постановление Правительства РФ “Об утверждении требований к защите информации, содержащейся в государственных информационных системах” от 1 ноября 2012 года № 1118;
- Постановление Правительства РФ “Об утверждении требований к защите информации, содержащейся в информационных системах персональных данных” от 1 ноября 2012 года № 1118.

Эти законы и нормативные акты определяют правила обработки, хранения и передачи информации, а также требования к системам защиты информации. Они также устанавливают ответственность за нарушение правил информационной безопасности и предусматривают меры по защите информации от несанкционированного доступа, утечек и других угроз.

Основные законы и нормативные акты

В России существует ряд законов и нормативных актов, которые регулируют область информационной безопасности. Некоторые из них включают:

Федеральный закон “О защите персональных данных”

Этот закон определяет правила обработки персональных данных и устанавливает требования к организациям, которые собирают, хранят и обрабатывают такие данные. Он также устанавливает права и обязанности субъектов персональных данных и определяет ответственность за нарушение закона.

Федеральный закон “Об информации, информационных технологиях и о защите информации”

Этот закон определяет основные принципы защиты информации и устанавливает требования к организациям, которые обрабатывают информацию. Он также устанавливает правила использования криптографических средств защиты информации и определяет ответственность за нарушение закона.

Постановление Правительства РФ “Об утверждении требований к защите информации, содержащейся в информационных системах персональных данных”

Этот нормативный акт устанавливает требования к защите информации, содержащейся в информационных системах персональных данных. Он определяет меры по защите информации от несанкционированного доступа, утечек и других угроз. Также он устанавливает требования к системам защиты информации и определяет ответственность за нарушение требований.

Эти законы и нормативные акты являются основой для обеспечения информационной безопасности в России. Они определяют правила обработки, хранения и передачи информации, а также требования к системам защиты информации. Они также устанавливают ответственность за нарушение правил информационной безопасности и предусматривают меры по защите информации от несанкционированного доступа, утечек и других угроз.

Текущее состояние законодательства в области информационной безопасности

На сегодняшний день законодательство в области информационной безопасности в России находится в постоянном развитии и совершенствовании. Существует ряд законов и нормативных актов, которые регулируют вопросы защиты информации и обеспечения информационной безопасности.

Федеральный закон “Об информации, информационных технологиях и о защите информации”

Один из основных законов, регулирующих информационную безопасность в России, – Федеральный закон “Об информации, информационных технологиях и о защите информации”. Он устанавливает основные принципы и правила обработки, хранения и передачи информации, а также требования к системам защиты информации.

Федеральный закон “О защите персональных данных”

Другой важный закон, касающийся информационной безопасности, – Федеральный закон “О защите персональных данных”. Он определяет правила обработки персональных данных, включая сбор, хранение, использование и передачу таких данных. Закон также устанавливает требования к защите персональных данных от несанкционированного доступа и утечек.

Нормативные акты ФСТЭК и ФСБ

Федеральная служба технической и экспортной контроля (ФСТЭК) и Федеральная служба безопасности (ФСБ) также разрабатывают и принимают нормативные акты, которые регулируют вопросы информационной безопасности. Эти акты устанавливают требования к системам защиты информации, методам шифрования, процедурам аттестации и другим аспектам информационной безопасности.

Таким образом, текущее законодательство в области информационной безопасности в России предоставляет основу для обеспечения защиты информации и предотвращения угроз. Однако, с учетом быстрого развития информационных технологий и появления новых угроз, законодательство постоянно совершенствуется и дополняется новыми нормативными актами.

Проблемы и вызовы

В области информационной безопасности существуют ряд проблем и вызовов, которые требуют внимания и решения. Рассмотрим некоторые из них:

Рост угроз информационной безопасности

С каждым годом растет количество и сложность угроз информационной безопасности. Киберпреступники постоянно разрабатывают новые методы атак и вирусы, которые могут нанести серьезный ущерб информационным системам. Это создает необходимость в постоянном обновлении и усовершенствовании систем защиты информации.

Недостаточная осведомленность пользователей

Одной из основных проблем в области информационной безопасности является недостаточная осведомленность пользователей о правилах безопасного использования информационных технологий. Многие люди не знают о рисках, связанных с небезопасным поведением в сети, и не принимают необходимые меры для защиты своей информации. Это делает их уязвимыми для атак и вирусов.

Недостаточное финансирование информационной безопасности

Организации и государственные учреждения часто сталкиваются с проблемой недостаточного финансирования информационной безопасности. Разработка и поддержка

систем защиты информации требуют значительных затрат, но не всегда получают достаточное финансирование. Это может привести к недостаточной защите информации и увеличению рисков.

Сложность соблюдения законодательства

Соблюдение законодательства в области информационной безопасности может быть сложной задачей. Законы и нормативные акты в этой области постоянно меняются и дополняются, что требует от организаций и государственных учреждений постоянного обновления своих систем и процедур. Невыполнение требований законодательства может привести к штрафам и другим негативным последствиям.

Глобальный характер угроз

Угрозы информационной безопасности имеют глобальный характер и могут затронуть не только одну организацию или страну, но и весь мир. Киберпреступники могут атаковать системы и сети в любой точке планеты, что требует сотрудничества и координации усилий между различными странами и организациями для борьбы с угрозами.

Все эти проблемы и вызовы требуют постоянного внимания и усилий для обеспечения надежной защиты информации и минимизации рисков. Это важная задача, которая требует сотрудничества и взаимодействия между различными сторонами, включая организации, государственные учреждения, специалистов по информационной безопасности и пользователей.

Перспективы развития законодательства

Развитие законодательства в области информационной безопасности является важным аспектом обеспечения защиты информации и борьбы с угрозами. В настоящее время существует несколько перспективных направлений развития законодательства:

Усиление международного сотрудничества

В связи с глобализацией информационных технологий и угрозами, которые они несут, все большее внимание уделяется международному сотрудничеству в области информационной безопасности. Разработка и принятие международных норм и стандартов, а также соглашений о сотрудничестве между странами становится все более актуальной задачей. Это позволит эффективнее бороться с киберпреступностью и другими угрозами информационной безопасности.

Развитие технических средств защиты

С развитием информационных технологий и появлением новых угроз, необходимо постоянно совершенствовать технические средства защиты информации. Законодательство должно учитывать эти изменения и обеспечивать правовую базу для использования новых технологий и методов защиты. Важно также разработать механизмы контроля и

сертификации технических средств, чтобы обеспечить их надежность и соответствие требованиям безопасности.

Расширение прав пользователей

С развитием информационных технологий и распространением интернета все больше людей становятся активными пользователями информации. Важно разработать законодательство, которое будет защищать права пользователей и обеспечивать их безопасность в сети. Это включает в себя защиту персональных данных, свободу выражения мнения, доступ к информации и другие аспекты, которые влияют на безопасность и конфиденциальность пользователей.

Обучение и повышение осведомленности

Одним из важных аспектов обеспечения информационной безопасности является обучение и повышение осведомленности пользователей. Законодательство должно предусматривать меры по обучению пользователей основам безопасности информации, а также по повышению их осведомленности о существующих угрозах и методах защиты. Это поможет снизить риски и повысить общий уровень безопасности в целом.

В целом, развитие законодательства в области информационной безопасности должно быть направлено на обеспечение надежной защиты информации, сотрудничество между странами, защиту прав пользователей и повышение осведомленности о безопасности. Это позволит эффективно бороться с угрозами и обеспечить безопасное использование информационных технологий во всех сферах жизни.

Сравнительная таблица законодательства по информационной безопасности

Закон/Нормативный акт	**Основные положения**	**Преимущества**	**Недостатки**
Федеральный закон “Об информации, информационных технологиях и о защите информации”	Устанавливает основные принципы и правила обработки информации, определяет требования к защите информации, устанавливает ответственность за нарушение правил	– Широкий охват различных аспектов информационной безопасности – Установление ответственности за нарушение правил обработки и	– Некоторые положения могут быть неоднозначными и требовать дополнительной интерпретации – Не всегда эффективное

Закон/Нормативный акт	Основные положения	Преимущества	Недостатки
	обработки и защиты информации.	защиты информации	применение мер по защите информации
Федеральный закон “О персональных данных”	Устанавливает правила обработки персональных данных, определяет права и обязанности субъектов персональных данных и операторов, устанавливает требования к защите персональных данных.	– Четкое определение прав и обязанностей субъектов персональных данных и операторов – Установление требований к защите персональных данных	– Не всегда эффективное применение мер по защите персональных данных – Некоторые положения могут быть неоднозначными и требовать дополнительной интерпретации
Федеральный закон “О защите детей от информации, причиняющей вред их здоровью и развитию”	Устанавливает требования к информации, предназначенной для детей, определяет запреты на распространение определенной информации, устанавливает ответственность за нарушение правил защиты детей от вредной информации.	– Защита детей от вредной информации – Установление ответственности за нарушение правил защиты детей от вредной информации	– Некоторые положения могут быть неоднозначными и требовать дополнительной интерпретации – Не всегда эффективное применение мер по защите детей от вредной информации