

Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:

<https://studservis.ru/kontrolnaya-rabota/429967>

Тип работы: Контрольная работа

Предмет: Информационное право

Содержание

Введение 3

1. Правовые аспекты информационной безопасности 4

2. Виды компьютерных преступлений и их воздействие на экономическую безопасность 8

3. Методы борьбы с компьютерной преступностью 10

Заключение 13

Список использованных источников 15

В современном обществе понятие информационной безопасности выходит далеко за рамки простого защиты данных от несанкционированного доступа. В Российской Федерации информационная безопасность рассматривается как состояние защищенности национальных интересов в информационной сфере. Это означает предотвращение несанкционированного доступа, использования, искажения, исследования, раскрытия, изменения, записи или уничтожения информации, а также защиту целостности информационной инфраструктуры от различных видов воздействий.

В свете глобального развития информационно-телекоммуникационных технологий и цифровой революции, нормы действующего законодательства рассматривают информационную безопасность как приоритетное направление. Процесс законотворчества в России постоянно адаптируется к изменениям и новым вызовам, связанным с развитием и внедрением цифровых технологий в жизнь общества.

Сегодня проблематика информационной безопасности становится все более актуальной и важной. Рост и развитие новых видов мошенничества, правонарушений и преступлений в информационной среде создают необходимость в концепции кибербезопасности. Для решения этих проблем была разработана «Стратегия развития информационного общества в РФ» до 2030 года.

Эта стратегия подчеркивает, что информационная безопасность касается всех сфер жизнедеятельности общества: государственного управления, экономики, социальных сетей и личной информации, онлайн-банкинга, обороны страны, идеологии и других. Усугубляет эту проблему факт того, что все эти сферы общества становятся все более цифровизированными, что открывает новые уязвимости и угрозы для информационной безопасности.

В Российской Федерации существует разветвленная система правовых документов, регулирующих вопросы информационной безопасности. Эти документы охватывают как международные, так и внутренние аспекты защиты информации.

На международном уровне Россия придерживается соглашений и конвенций, направленных на обеспечение информационной безопасности. Эти документы представляют собой основу для взаимодействия с другими странами и международными организациями в сфере защиты информации.

На внутреннем уровне ключевую роль играют федеральные законы, включая законы, указы и распоряжения Президента РФ, а также кодексы, которые определяют основные принципы и правила в области информационной безопасности. Кроме того, существуют локальные акты, которые применяются конкретными организациями для обеспечения безопасности информации в их деятельности.

Правовая теория информационной безопасности охватывает широкий спектр вопросов, связанных с целями, задачами и направлениями развития политики в этой области. Эта теория является основой для формирования правительственной политики и разработки предложений по совершенствованию законодательства, методологии, научно-технических решений и других аспектов обеспечения информационной безопасности.

С точки зрения ресурсов, на государственном и международном уровнях, политика в области защиты информации включает использование инструментов авторского права, патентов и лицензий на защиту интеллектуальной собственности. Это способы обеспечения прав собственности на информацию и технологии, а также поощрения инноваций в этой области.

Правоприменительная практика в сфере информационной безопасности включает применение уголовного и гражданского законодательства, а также закона «Об информации, информационных технологиях и о защите информации». Эти нормативные акты определяют ответственность за нарушения в области информационной безопасности и меры по их предотвращению и устранению.

Таким образом, система правовых документов в Российской Федерации обеспечивает комплексный подход к обеспечению информационной безопасности на всех уровнях - от международного сотрудничества до регулирования внутренних процессов в организациях.

Нормативно-правовые акты, направленные на защиту информации, представляют собой сложную систему, охватывающую различные уровни законодательства. Условно можно выделить несколько уровней структуры таких актов.

Первый уровень составляет конституционное законодательство. В рамках конституции определяются основные принципы и положения, касающиеся защиты информации как важного элемента функционирования государства и общества.

Второй уровень включает в себя общие законы и кодексы, в которых содержатся нормы, регулирующие вопросы информационной безопасности. Эти законы устанавливают общие правила и требования к защите информации на уровне государства.

Список использованных источников

1. Головинов Олег Николаевич, Погорелов Александр Владимирович Киберпреступность в современной экономике: состояние и тенденции развития // Вопросы инновационной экономики. 2016. №1. URL: <https://cyberleninka.ru/article/n/kiberprestupnost-v-sovremennoy-ekonomike-sostoyanie-i-tendentsii-razvitiya> (дата обращения: 02.03.2024).
2. Номоконов В. А. Киберпреступность как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропинина // Криминология: вчера, сегодня, завтра. - 2012. - № 1 (24). -С. 45-55.
3. Тарасов А. Электронный банкинг и его безопасность // Экономическая политика. - 2010. - № 5. - С. 118-128.
4. Згадзай О. Э. Киберпреступность: факторы риска и проблемы борьбы / О. Э. Згадзай, С.Я. Казанцев // Вестник НЦ БЖД. - 2013. - № 4 (18). - С. 80-86.
5. Чекунов И.Г. Киберпреступность: понятие, классификация, современные вызовы и угрозы // Молодые ученые. - 2012. - № 3. - С. 178-186.
6. Пархоменко С.В. Предупреждение компьютерной преступности в Российской Федерации: интегративный и комплексный подходы / С.В. Пархоменко, К.Н. Евдокимов // Криминологический журнал Байкальского государственного университета экономики и права. - 2015. - Т. 9, № 2. - С. 265-276.
7. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
8. Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:

<https://stuservis.ru/kontrolnaya-rabota/429967>