Тип работы: Курсовая работа

Предмет: Право

Актуальность темы исследования. Безопасность - это государственная защита прав и свобод личности, материальных и духовных ценностей общества, конституционного строя государства, суверенитета и жизненно важных интересов территориальной целостности. Развитие информационных технологий в экономической сфере стало неотъемлемой частью жизни современного общества, а поскольку информация является одним из наиболее ценных и важных ресурсов в любом бизнес-процессе, то информационная безопасность стала важнейшим аспектом грамотного ведения бизнеса. Цифровая безопасность включает в себя комплекс мер, направленных на предотвращение или исключение несанкционированного доступа к данным, их обработки, искажения, форматирования, анализа, последовательного обновления, модификации или уничтожения. Проще говоря, это комплекс мер, стандартов и технологий, необходимых для защиты конфиденциальных данных. Проблема защиты информации от несанкционированного доступа и нежелательных воздействий существует давно и становится все более актуальной с развитием человеческого общества, появлением частной собственности, государственных режимов и дальнейшим расширением сферы деятельности человека. Информация приобрела ценность, и обладание ею приносит определенные выгоды ее нынешним и потенциальным владельцам.
В настоящее время в Российской Федерации цель информационного общества определяется как повышение качества жизни человека, а одним из направлений его развития является обеспечение конституционных прав человека и гражданина в информационной сфере. Этими положениями руководствуется юриспруденция, поскольку они гарантируют формирование новой объективной реальности, в которой информация приобретает беспрецедентное значение, обостряются традиционные и возникают новые формы конфликтов, в том числе цифровая преступность. Действующее законодательство, направленное на преодоление цифровой преступности, неадекватно отражает новые тенденции в развитии информационного общества. В последние годы динамика развития цифровой преступности стала угрозой национальной и международной безопасности. Системообразующая роль информации и влияние современных компьютерных технологий на все сферы жизнедеятельности в части ее обработки не только положительно сказываются на устойчивом развитии всех социальных институтов, но и способствуют формированию условий для совершения правонарушений в сфере цифровой безопасности. Это определяет актуальность выбранной темы.
Объект исследования составляют общественные отношения, складывающиеся при исследовании правового регулирования правонарушений в сфере цифровой безопасности.
Предметом исследования настоящей работы являются нормы права, регулирующие вопросы правового регулирования правонарушений в сфере цифровой безопасности.
Целью исследования является анализ понятия, видов и общая характеристика правонарушений в сфере цифровой безопасности.
Для достижения поставленной цели были сформулированы следующие задачи:
1.раскрыть понятие цифровой безопасности, ее роль, основные компоненты;

2.рассмотреть специфику правового регулирования обеспечения цифровой безопасности общества;
3.исследовать природу и сущность правонарушений в сфере цифровой безопасности;
4.раскрыть правовую характеристику административной и уголовной ответственности за правонарушения в сфере цифровой безопасности;
5.дать правовую характеристику гражданской и дисциплинарной за правонарушения в сфере цифровой безопасности.
Методологическая основа исследования. Методологическую основу исследования составили общенаучный диалектический метод познания, а также следующие общие, специальные и частные методы исследования: формально-юридический, системный, комплексный, нормативный.
Нормативную и эмпирическую базу исследования составили: Конституция РФ; законодательство РФ, иные материалы юридической практики.
Теоретическая основа исследования. Теоретической основой исследования являются труды российских ученых по праву, такие как: Афанасьев К.К., Бачило И.Л., Волков Ю.В., Дубень А.К., Емельянов А.С., Магадиев М.Ф., Овчинников А.И., Парфенов Д.А., Перина А.С., Христинич И.В. и другие авторы.
Теоретическая значимость исследования заключается в том, что сформулированные в ней теоретические положения могут быть использованы в целях дальнейшего изучения и решения актуальных проблем правового регулирования правонарушений в сфере цифровой безопасности.
Практическая значимость исследования состоит в том, что содержащиеся в ней положения, практические рекомендации могут быть в дальнейшем использованы при разработке целенаправленных и конкретных мер, направленных на исследование правового регулирования правонарушений в сфере цифровой безопасности.
Структура работы. Курсовая работа состоит из введения, двух глав основного текста, заключения, списка литературы.
1 Теоретические основы сущности правонарушений в сфере цифровой безопасности
1.1 Понятие цифровой безопасности, ее роль, основные компоненты
Ни одна система не может существовать без информационных потоков, а нарушение или отсутствие информационных потоков может привести к краху, потере эффективности и прибыльности, снижению стимула к развитию. Информация является важнейшим элементом любой экономической системы. Информационная сфера является системообразующим фактором общественной жизни и оказывает позитивное влияние на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность России во многом зависит от информационной безопасности, и эта зависимость будет возрастать по мере технического прогресса. В доктрине информационной безопасности под информационной сферой понимается "информация, информационные объекты, информационные системы, сайты информационно-коммуникационной сети "Интернет", сети связи, информационные технологии, формирование и обработка информации, разработка и использование этих технологий, субъекты, осуществляющие деятельность по обеспечению информационной безопасности, и связанные с ними" .
Информация должна быть надежно защищена, так как наличие различных угроз может привести к потере целостности, доступности и конфиденциальности информации. Каждый человек ежедневно сталкивается с событиями, которые могут представлять угрозу для информационной сферы, такими как:
-неправомерное присвоение чужой собственности;
-хищение имущества (информационного оборудования, компонентов);
-подделка или несанкционированное изменение данных;
-нарушение прав частной собственности и конфиденциальности информации;
-несанкционированный или несанкционированный доступ к частной информации владельца;
-компьютерное вымогательство или шантаж;
-искажение или уничтожение данных;
-нарушение авторских прав или прав интеллектуальной собственности.
Основным нормативным правовым актом, регулирующим вопросы безопасности, является Федеральный закон от 28.12.2010 № 390-ФЗ "О безопасности ". Данный Федеральный закон определяет основные принципы и содержание деятельности по обеспечению национальной безопасности, общественной безопасности, экологической безопасности, безопасности личности и других видов безопасности, полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и региональных органов власти в области безопасности.
Статья 2 ФЗ от 28.12.2010 № 390-ФЗ устанавливает основные принципы, на основе которых органы,

наделенные властными полномочиями, обеспечивают безопасность личности, общества и государства от внутренних и внешних угроз.
Первый принцип - принцип соблюдения и защиты прав и свобод человека и гражданина, второй - принцип законности, третий - системность и комплексность применения политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности.
Таким образом, безопасность должна основываться как на эффективной и развитой правовой системе, так и на социально-экономических, политических, организационных, административных, идеологических и иных институтах и мерах. Однако сегодня именно правовые нормы служат базовой основой деятельности всех без исключения субъектов права, включая органы власти и управления на разных уровнях. Таким образом, в практическом плане можно говорить о правовой основе обеспечения безопасности, что четко закреплено в ФЗ от 28.12.2010 № 390-ФЗ.
Другое дело, что понятие и содержание безопасности, в частности, объекты и субъекты, подлежащие защите, могут меняться с течением времени.
Следует отметить, что непосредственное изучение вопроса цифровой безопасности показывает, что в большинстве западных стран используется термин "кибербезопасность", в то время как в Российской Федерации предпочтение отдается термину "информационная безопасность".
Решение этого вопроса имеет больше практическое, чем доктринальное значение, включая установление нормативно-правовых границ.
Кибербезопасность - более узкое понятие, и в первую очередь это защита каналов связи (в частности, интернета) и оборудования.

1. Федеральный закон от 28.12.2010 № 390-ФЗ (ред. от 10.07.2023) "О безопасности" // Собрание законодательства РФ, 03.01.2011, № 1, ст. 2
2. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" // Собрание законодательства РФ. - 2006. - № 31 (ч. 1). - Ст. 3448.
3. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // Собрание законодательства РФ. – 1994. - № 32. - Ст.3301
4. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" // Собрание законодательства РФ. – 2006. - № 31 (1 ч.). - Ст.3451.
5. Указ Президента РФ от 02.07.2021 № 400 "О Стратегии национальной безопасности Российской Федерации" // Собрание законодательства РФ. – 2021. - № 27 (часть II). - Ст. 5351
6. Указ Президента РФ от 25.01.2023 № 35 "О внесении изменений в Основы государственной культурной политики, утвержденные Указом Президента Российской Федерации от 24 декабря 2014 г. № 808" // Собрание законодательства РФ", 30.01.2023, № 5, ст. 777
7. Информация Банка России от 4 сентября 2017 г. "Об использовании частных "виртуальных валют" (криптовалют)" // Вестник Банка России. 2017. 14 сентября.
8. Постановление Пленума Верховного Суда РФ от 28.06.2011 № 11 (ред. от 28.10.2021) "О судебной практике по уголовным делам о преступлениях экстремистской направленности" // Бюллетень Верховного Суда РФ, № 8, август, 2011
9. Афанасьев, К. К. Административно-правовое противодействие распространению недостоверной информации: отдельные аспекты / К. К. Афанасьев // Проблемы права: теория и практика. – 2022. – № 59. – С. 69-82.
10. Бачило, И. Л. Информационное право : учебник для вузов / И. Л. Бачило. - 5-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2023. - 419 с.
11. Волков, Ю. В. Информационное право. Информация как правовая категория : учебное пособие для вузов / Ю. В. Волков. - 3-е изд., стер. - Москва : Издательство Юрайт, 2023. - 109 с.
12. Григорян, Г. Р. "Цифровые" имущественные преступления: вопросы криминализации и законодательной регламентации / Г. Р. Григорян // Юридический аналитический журнал. – 2020. – Т. 15, № 2. – С. 73-90.
13. Дубень, А. К. Актуальные проблемы административной ответственности в сфере обеспечения информационной безопасности / А. К. Дубень // №В: Административное право и практика администрирования. – 2022. – № 4. – С. 28-39.
14. Емельянов, А.С. Информационная безопасность Российской Федерации и перспективы правовой регламентации информационно-коммуникационной сети Интернет // Журнал российского права. 2022. № 5. С.70.
15. Информационное право : учебник для вузов / Н.Н. Ковалева [и др.] ; под редакцией Н.Н. Ковалевой. -

Москва : Издательство Юрайт, 2020. - 353 с.
16. Информационное право : учебник для вузов / М.А. Федотов [и др.] ; под редакцией М.А. Федотова. - Москва : Издательство Юрайт, 2022. - 497 с.
17. Магадиев, М. Ф. Система межведомственного электронного взаимодействия (СМЭВ) в структуре электронного правительства Российской Федерации / М. Ф. Магадиев // Вопросы политологии. – 2022. – Т. 12, № 11(87). – С. 3699-3712.
18. Маскайкин, Н. А. Использование автоматизированных информационных ситем в органах местного самоуправления / Н. А. Маскайкин // Инновационная наука. – 2023. – № 6-1. – С. 159-161.
19. Мосечкин И. Н. Понятие преступлений против безопасности цифровой информации // Lex russica. — 2023. — Т. 76. — № 5. — С. 49-59.
20. Мочалов, Н. А. Административная ответственность за информационные правонарушения / Н. А. Мочалов // Вестник науки. – 2023. – Т. 4, № 11(68). – С. 201-210.
21. Назаретян, А. Р. Цифровая безопасность, защищенность и анонимность в интернет пространстве как новые ценности современного общества / А. Р. Назаретян // Социальная интеграция и развитие этнокультур в евразийском пространстве. – 2020. – Т. 2, № 9. – С. 209-214.
22. Овчинников, А. И. Права человека в условиях цифровой трансформации общества и государства / А. И. Овчинников // Вестник юридического факультета Южного федерального университета. – 2021. – Т. 8, № 4. – С. 93-98.
23. Парфенов, Д. А. Развитие механизма обеспечения экономической безопасности в РФ в условиях цифровизации / Д. А. Парфенов // Вестник Московского университета. Серия 21: Управление (государство и общество). – 2020. – № 4. – С. 106-122.
24. Перина, А. С. «Цифровые преступления»: понятие, типология, признаки / А. С. Перина // Юридический вестник Самарского университета. – 2023. – Т. 9, № 3. – С. 106-115.
25. Перина, А. С. Квалификация цифровых преступлений против личности: проблемные вопросы / А. С. Перина // Вестник Югорского государственного университета. – 2023. – № 2(69). – С. 89-104.
26. Тенденции формирования потенциала общества в условиях цифровой экономики / Е. А. Юрина, Е. С. Алексашина, О. Н. Горбунова, Я. А. Куликова // Вестник Тверского государственного университета. Серия: Экономика и управление. – 2020. – № 2(50). – С. 123-131.
27. Христинич, И.В. Информационная безопасность в сети Интернет // Законность. 2022. № 4. С. 20.
28. Элькин, В. Д. Информационные технологии в юридической дея-тельности [Электронный ресурс] : учебник и практикум для вузов / В. Д. Элькин и др. - М. : Юрайт, 2021. - 472 с. - Режим доступа: https://urait.ru/book/informacionnye-tehnologii-v-yuridicheskoy-deyatelnosti- 431764 (дата обращения: 10.03.2024).