

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/kurovaya-rabota/425118>

Тип работы: Курсовая работа

Предмет: Право (другое)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 3

1 Теоретические основы формирования и обеспечения правового регулирования обеспечения цифровой безопасности общества 6

1.1 Понятие цифровой безопасности, ее роль, основные компоненты 6

1.2 Специфика правового регулирования обеспечения цифровой безопасности общества 11

2 Проблемы развития правового регулирования цифровой безопасности общества 16

2.1 Основные требования к цифровой безопасности и защите государственной тайны при решении задач профессиональной деятельности 16

2.2 Основные методы, способы и средства получения, хранения и переработки цифровой информации для решения профессиональных задач 19

2.3 Использование технологий поиска в сети Интернет для решения профессиональных задач 24

ЗАКЛЮЧЕНИЕ 33

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 36

1 Теоретические основы формирования и обеспечения правового регулирования обеспечения цифровой безопасности общества

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.

Информационная безопасность - понятие более широкое и распространяется на контент.

Судя по недавно принятым документам, на уровне государственных источников этот вопрос решен в пользу использования термина "цифровая безопасность".

Так, Указом Президента РФ от 05.12.2016 № 646 утверждена доктрина информационной безопасности Российской Федерации. Концепция программы "Цифровая экономика" предусматривает, что ее (цифровой экономики) развитие в период до 2024 года будет обеспечиваться за счет достижения определенных целей, одной из которых является информационная безопасность.

Принятые нормативные акты затрагивают ряд вопросов, касающихся создания современных технических средств, их практической реализации, согласования схожих по содержанию проектов в области национальных технических инициатив, выбора исполнителей и т.д.

В то же время юридический анализ этих и других документов приводит к выводу, что понятие "информационная безопасность" трактуется очень широко.

Это создает широкие возможности для масштабного вмешательства государства в регулирование общественных отношений в цифровой среде, что, собственно, и происходит. В частности, отмечается, что общий вектор законодательства продолжает оставаться запретительным, и предложения по регулированию социальных сетей, поисковых сервисов и контента появляются с завидной регулярностью, определяя новые категории информации, распространение которой в Российской Федерации запрещено. При этом интерес представителей информационного сообщества и многих пользователей заключается в сохранении саморегулирования на основе этического кодекса, а интерес государственных структур - в установлении правового регулирования для предотвращения угроз личной, государственной и общественной безопасности.

Таким образом, в целях сохранения регулирующей роли закона и обеспечения баланса интересов, только когда передовые информационные технологии, саморегулируемые организации и этические нормы оказываются не в состоянии разрешить ситуации, когда негативные последствия носят многократный и массовый характер и затрагивают интересы значительного числа людей, цифровая среда Государственное вмешательство в регулирование общественных отношений должно быть допустимым.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

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. Информация Банка России от 4 сентября 2017 г. "Об использовании частных "виртуальных валют" (криптовалют)" // Вестник Банка России. 2017. 14 сентября.
7. Бачило, И. Л. Информационное право : учебник для вузов / И. Л. Бачило. - 5-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2023. - 419 с.
8. 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.
9. Гамзабеков, Р. Р. Перспективы развития системы межведомственного электронного взаимодействия (СМЭВ) / Р. Р. Гамзабеков, В. Г. Почуев // Экономика и предпринимательство. - 2017. - № 12-3(89). - С. 935-938.
10. Емельянов, А.С. Информационная безопасность Российской Федерации и перспективы правовой регламентации информационно-коммуникационной сети Интернет // Журнал российского права. 2022. № 5. С.70.
11. Информационное право : учебник для вузов / Н.Н. Ковалева [и др.] ; под редакцией Н.Н. Ковалевой. - Москва : Издательство Юрайт, 2020. - 353 с.
12. Информационное право : учебник для вузов / М.А. Федотов [и др.] ; под редакцией М.А. Федотова. - Москва : Издательство Юрайт, 2022. - 497 с.
13. 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.
14. Мамонтова, С. В. Особенности трансформации цифровой экономики России / С. В. Мамонтова, О. А. Максимова // Регион: системы, экономика, управление. - 2019. - № 1(44). - С. 26-31.
15. Маскайкин, Н. А. Использование автоматизированных информационных систем в органах местного самоуправления / Н. А. Маскайкин // Инновационная наука. - 2023. - № 6-1. - С. 159-161.
16. 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.
17. 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.
18. Палехова, Е.А. Понятие информации и цифровой экономики: правовые аспекты // Предпринимательское право. Приложение "Право и Бизнес". 2019. № 2. С. 46.
19. 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.
20. Пономарева, М. В. Основные особенности организации взаимодействия между поставщиками и потребителями информации в системе электронного межведомственного взаимодействия (СМЭВ) / М. В. Пономарева // Science Time. - 2017. - № 3(39). - С. 355-360.
21. Примаков, Т. К. Цифровая безопасность: правовое регулирование, соотношение с кибербезопасностью / Т. К. Примаков, О. А. Серова // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. - 2019. - № 2(56). - С. 57-60.
22. Романенко, Г. С. Проблемы организации межведомственного информационного взаимодействия федеральных и региональных органов исполнительной власти / Г. С. Романенко, И. Г. Савченко, Ю. Ф. Юшутин // Информатизация и связь. - 2017. - № 1. - С. 96-101.
23. 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.

24. Хиабахян, А. Р. Применение СМЭВ для повышения эффективности размещения заказов для государственных нужд / А. Р. Хиабахян // Государственное и муниципальное управление в XXI веке: теория, методология, практика. – 2016. – № 26. – С. 207-211.
25. Христинич, И.В. Информационная безопасность в сети Интернет // Законность. 2022. № 4. С. 20.
26. Элькин, В. Д. Информационные технологии в юридической деятельности [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: 22.02.2024).

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/kursovaya-rabota/425118>