УДК 004.056

БЕЗОПАСНОСТЬ ЦИФРОВОГО ГОСУДАРСТВА: ЗАЩИТА ИНФОРМАЦИИ И КИБЕРБЕЗОПАСНОСТЬ В КОНТЕКСТЕ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

В. С. Дерябин

Самарский университет им. С.П. Королёва,
Московское шоссе, 34, 443086, г. Самара, Россия, deryabinvs@ya.ru

В данной статье рассматривается вопрос безопасности цифрового государства с акцентом на защиту информации и кибербезопасность в контексте государственного управления. Анализируются современные вызовы, связанные с использованием информационных технологий в государственном управлении, и предлагает ряд мер, направленных на обеспечение безопасности цифрового пространства государства.

Ключевые слова: безопасность цифрового государства; информационные технологии; кибербезопасность; государственное управление; защита информации.

DIGITAL STATE SECURITY: INFORMATION PROTECTION AND CYBERSECURITY IN THE CONTEXT OF PUBLIC ADMINISTRATION

V. S. Deryabin

Samara University,
Moskovskoe shosse, 34, 44308, Samara, Russia, deryabinvs@ya.ru

This article examines the issue of digital state security with an emphasis on information protection and cybersecurity in the context of public administration. The modern challenges associated with the use of information technologies in public administration are analyzed and a number of measures aimed at ensuring the security of the digital space of the state are proposed.

***Keywords*:** digital state security; information technology; cybersecurity; public administration; information protection.

Цифровизация и применение информационных технологий в государственном управлении стали неотъемлемой частью современной общественной жизни. Однако, с ростом использования цифровых технологий возникает ряд угроз для безопасности цифрового государства, включая утечку и несанкционированный доступ к конфиденциальной информации, кибератаки и другие виды киберпреступности. В связи с этим,

вопросы защиты информации и кибербезопасности являются крайне актуальными и требуют серьезного подхода со стороны государственных органов [1, с. 20].

Важным шагом является разработка и внедрение политик и стандартов безопасности для государственных органов. Это должно включать установление правил для доступа к конфиденциальной информации, шифрование данных, регулярное обновление программного обеспечения и аппаратного обеспечения, а также мониторинг и анализ событий безопасности. Обучение персонала государственных органов основам кибербезопасности является критическим шагом. Сотрудники должны быть проинформированы о возможных угрозах, знать, как распознавать фишинговые письма, использовать сложные пароли и обращаться за помощью в случае возникновения подозрительных событий. Регулярные тренинги и обновление знаний являются неотъемлемой частью процесса обучения. Усиление мер по защите от несанкционированного доступа к информации также является важным аспектом безопасности. Это может включать двухфакторную аутентификацию, использование биометрических данных, контроль доступа на основе ролей и другие методы защиты.

Сотрудничество с международными организациями по обмену информацией о киберугрозах является необходимым шагом для обеспечения безопасности цифрового пространства. Это позволяет получать информацию о новых угрозах и обмениваться опытом с другими государствами в борьбе с киберпреступностью. Коллективные усилия, включая совместные учения и регулярные встречи, способствуют повышению эффективности борьбы с киберугрозами [2, с. 144].

Развитие систем раннего предупреждения и противодействия кибератакам играет важную роль в обеспечении кибербезопасности в сфере государственного управления. Это включает внедрение интеллектуальных систем мониторинга, анализа событий и реагирования на аномалии в сети. Быстрое обнаружение и реагирование на кибератаки позволяет минимизировать негативные последствия и восстановить работоспособность систем. Развитие криптографических методов защиты персональной информации граждан также является важным аспектом безопасности цифрового государства. Механизмы шифрования и аутентификации помогают защитить личные данные граждан от несанкционированного доступа и использования.

Защита интересов граждан в цифровом пространстве также является важной задачей. Государственные органы должны обеспечить безопасность информационных систем общественных служб, таких как здравоохранение, образование и социальное обслуживание. Это включает за-

щиту медицинских данных пациентов, личной информации студентов и других персональных данных граждан [3, с. 72].

Важным аспектом кибербезопасности цифрового государства является разработка сильных систем защиты данных. Это включает в себя использование современных технологий для обнаружения и предотвращения атак, таких как системы искусственного интеллекта и машинного обучения. Эти технологии позволяют автоматизировать процессы обнаружения и реагирования на угрозы, что повышает эффективность защиты. Развитие систем мониторинга и анализа данных также имеет важное значение для обеспечения безопасности. Системы, способные обрабатывать и анализировать большие объемы данных, позволяют выявить аномалии и потенциальные угрозы. Мониторинг событий и анализ активности пользователей позволяют своевременно распознавать и предотвращать кибератаки [4].

Сотрудничество с частным сектором также играет важную роль в обеспечении кибербезопасности государства. Частные компании могут предоставлять специализированные услуги по кибербезопасности, проводить аудиты и тестирования уязвимостей систем, а также предлагать инновационные решения для защиты данных. Партнерство с частным сектором позволяет использовать лучшие практики и опыт в области кибербезопасности. Внедрение стандартов и сертификации в области кибербезопасности также важно для обеспечения безопасности цифрового государства. Это может включать сертификацию информационных систем, сетей и оборудования, а также стандарты шифрования и аутентификации. Соблюдение этих стандартов помогает обеспечить соответствие систем и услуг требованиям безопасности.

Обеспечение кибербезопасности цифрового государства требует комплексного подхода и постоянного обновления мер безопасности. Разработка и внедрение сильных систем защиты данных, сотрудничество с частным сектором, обновление программного обеспечения, защита критической инфраструктуры и защита персональных данных граждан - все это является неотъемлемыми компонентами кибербезопасности цифрового государства. Развитие технологий, образование и повышение осведомленности граждан также играют важную роль в обеспечении безопасности в цифровом пространстве [5, с. 779].

Повышение осведомленности граждан о кибербезопасности и методах защиты своей личной информации имеет важное значение. Образовательные программы, кампании информирования и регулярные предупреждения о возможных киберугрозах помогают сделать граждан более осведомленными и более активно защищать свои данные.

Обеспечение безопасности цифрового государства требует комплексного подхода и усиленных усилий со стороны государственных органов. Разработка и внедрение политик и стандартов безопасности, обучение персонала, развитие кибербезопасности, сотрудничество с другими странами и общественностью, а также повышение осведомленности граждан о кибербезопасности - все это необходимо для эффективной защиты информации и обеспечения безопасности государственных органов и граждан.

Библиографические ссылки

1. Мухаметов, Д. Р. "Умное государство": перспективы внедрения цифровых технологий государственного управления в России / Д. Р. Мухаметов, К. В. Симонов // Мир новой экономики. 2021. Т. 15, № 3. С. 17-27.

2. Верхелст Э., Ваутерс Я. (2020) Глобальное управление в сфере кибербезопасности: взгляд с позиции международного права и права ЕС // Вестник международных организаций. Т. 15 № 2 С. 141–172 (на русском и английском языках).

3. Доклад Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека "Цифровая трансформация и защита прав граждан в цифровом пространстве" от 2021 // Портал Доклад Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека. 2021.

4. Искусственный интеллект и машинное обучение в кибербезопасности – прогноз на будущее // kaspersky.ru URL: https://www.kaspersky.ru/resource-center/definitions/ai-cybersecurity (дата обращения: 23.08.2023).

5. Артамонов В.А., Артамонова Е.В. Кибербезопасность в условиях цифровой трансформации социума // Большая Евразия: развитие, безопасность, сотрудничество. 2022. №5-1. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-v-usloviyah-tsifrovoy-transformatsii-sotsiuma (дата обращения: 23.08.2023).