УДК 37

Информационная безопасность личности, общества, государства

Затравина Светлана Владимировна
НИУ Кыргызский экономический университет имени Мусы Рыскулбекова
Преподаватель
Приамурский государственный университет имени Шолом-Алейхема
Магистрант

Научный руководитель: Баженов Руслан Иванович
Заведующий кафедрой «Информационных систем, математики и правовой информатики», кандидат педагогических наук, доцент

Аннотация
В статье рассматриваются проблемы информационной безопасности на уровне личности, общества и государства в контексте современного цифрового мира, освещаются основные аспекты, связанные с угрозами, рисками и защитой данных в условиях расширяющейся цифровой среды. Авторами изложены меры, необходимые для защиты конфиденциальной информации, личных данных и критической инфраструктуры как на уровне индивида, так и на уровне социума и государства.
Ключевые слова: Информационная безопасность, защита данных, социальная безопасность, государственная безопасность, угрозы кибербезопасности, утечки данных, терроризм, информационная война.

Information security of individuals, society, state

Zatravina Svetlana Vladimirovna
Kyrgyz Economic University named after Musa Ryskulbekov
Lector
Sholom-Aleichem Priamursky State University
Graduate student

Academic Supervisor: Ruslan Ivanovich Bazhenov, Head of the Department of Information Systems, Mathematics, and Legal Informatics, Candidate of Pedagogical Sciences, Associate Professor

Abstract
The article examines the problems of information security at the level of the individual, society and state in the context of the modern digital world, highlighting the main aspects related to threats, risks and data protection in an expanding digital environment. The authors outline the measures necessary to protect confidential information, personal data and critical infrastructure both at the individual level and at the level of society and the state.

Keywords: Information security, data protection, social security, state security, cybersecurity threats, data leaks, terrorism, information warfare.

1. Введение

1.1 Актуальность

Исследования в области информационной безопасности личности, общества и государства представляют важный аспект современного информационного общества. С ростом цифровизации и расширением использования информационных технологий возрастает уровень угроз для конфиденциальности данных как на уровне индивидов, так и на уровне социума и государства. Защита персональных данных, обеспечение безопасности информационных систем и государственных структур становятся важными аспектами обеспечения стабильности и надежности в сфере информационной безопасности.

Исследования в этой области помогают выявить уязвимость, проанализировать киберугрозы и разработать методы и инструменты для эффективной защиты данных.

Таким образом, изучение вопросов информационной безопасности на всех уровнях не только обеспечивает разработку адекватных стратегий по борьбе с угрозами безопасности, но и способствуют формированию новых подходов и методологий в области информационной безопасности, что имеет важное значение для создания устойчивого и безопасного информационного пространства.

1.2 Обзор исследований

Значительный вклад в исследования, связанные с процессами обеспечения информационной безопасности на различных уровнях, внесли российские и зарубежные ученые. Их работа охватывает широкий спектр вопросов, включая защиту личных данных, кибербезопасность, защиту информационных систем государства и организаций, а также разработку новых методов и технологий в области защиты данных и предотвращения киберугроз. Коллективные усилия специалистов, направленные на обеспечение безопасности информации и поддержание стабильности в цифровом мире, имеют важное значение для создания эффективных стратегий и решений в области информационной безопасности.

Так, М.А. Ермаков в своих исследованиях рассматривает вопрос об актуальной для формирующегося информационного общества характеристики - информационная безопасность, анализируя её специфику в зависимости от различных субъектов – носителей, подчёркивая ключевые особенности и выделяя проблемы и противоречия [2].

В.А. Хроколов акцентирует внимание на процессах трансформации информации и информационных потоков в современном мире, а также их роли в осуществлении манипулирования сознанием личности и общества. В своих исследованиях он предполагает акцентуацию внимания на организационно-правовых аспектах информационной составляющей безопасной экзистенции

личности в современном обществе, актуализируя информационное противоборство, раскрывая особенности целенаправленного использования латентными силами информации в киберпространстве для проведения деструктивной пропаганды, а также использования информационных ресурсов в качестве средства организации массовых мероприятий, в том числе и противоправных [9].

А.А. Соколова утверждает, что в современном информационном мире, с все более возрастающим потоком информации, стремительно изменяющихся формах и методах влияния на личность весьма актуальными становятся вопросы повышения уровня информационной безопасности личности, общества и государства [8].

А.В. Никишкин рассматривает информационную безопасность государства и считает, что она является важнейшим и неотъемлемым элементом не только государственной политики, но и всего общества в целом [5].

Р. Г. Побегайлов считает, что в настоящее время информационная безопасность государства, ее уровень неадекватны действительности и отмечает ту существенную информационную угрозу для России, что массовая компьютеризация и информатизация в ней осуществляются на основе импортной техники и программного обеспечения [7].

С. М. Плеханов рассматривает вопрос об информационной безопасности как приоритетном направлении национальной безопасности в условиях современной реальности, актуальных вызовов и угроз [6].

Ю.А. Кузнецова затрагивает проблемные ситуации, которые сопряжены с обеспечением информационной безопасности государства в современном мире, определяет задачи государства в информационной сфере [4].

М.И. Грачев и Н.Г. Грачева рассматривают вопросы информационной безопасности личности, общества и государства в целом в разрезе противодействия цифровым web-угрозам в цифровом обществе посредством применения современного антивирусного обеспечения [1].

Что касается зарубежных авторов, то Jordan Shropshire, Merrill Warkentin и Shwadhin Sharma утверждают, что поведение пользователей компьютеров становится особенно важными и внедрение защитного программного обеспечения влияет на безопасность информационных ресурсов [12].

Hanna Paananen, Michael Lapke и Mikko Siponen показали, что фокус должен смещаться на потребности конкретной организации в информационной безопасности, поскольку в имеющихся исследованиях недостаточно материалов, которые бы показали, как контекстуальные факторы могут быть успешно интегрированы в развитие Интернет-провайдера [11].

Mike Potts показывает, что постоянно ведутся промышленные атаки, инсайдерские угрозы и стало сложно разграничивать различные векторы угроз и определять, какие из них являются наиболее опасными. По его мнению, наибольшую озабоченность вызывают правительственные и корпоративные сети, а новые тенденции, в том числе облачные технологии, мобильность

пользователей и использование собственного устройства (BYOD), ещё больше усложняют ситуацию, увеличивая поверхность атаки и одновременно снижая эффективность традиционной защиты периметра [13].

Álvaro Arenas, Gautam Ray, Antonio Hidalgo и Alberto Urueña исследуют инструменты безопасности и мероприятия по обеспечению безопасности. Используя многомерную, логит- и пробит-регрессию , они показали, что наличие инструментов безопасности связано с действиями с более высоким риском и большим количеством заражений, в то время как выполнение мер по обеспечению безопасности снижает количество заражений вредоносным ПО [10].

Xing Gao, Siyu Gong, Ying Wang, Xifan Wang и Manting Qiu рассмотрели стратегическое взаимодействие в среде совместного использования ресурсов между двумя фирмами, которые инвестируют в информационную безопасность в соответствии с обязательным стандартом, и одним хакером, который предпринимает усилия по атаке на фирмы, чем показали, что строгий обязательный стандарт не всегда приносит пользу каждой фирме, хотя ее информационные системы могут быть лучше защищены [14].

1.3 Цель исследования

Цель исследования состоит в анализе и понимании сложных механизмов и методов защиты информационной безопасности на различных уровнях – от индивидуальной безопасности до защиты государственных и корпоративных информационных систем. Необходимость выявления уязвимости и угроз способствуют разработке эффективных стратегий и решений для предотвращения кибератак, обеспечения защиты данных и укрепления безопасности информационного пространства.

2 Материалы и методы исследования

Теоретическая база научного исследования включает в себя широкий спектр работ и концепций, разработанных как отечественными, так и зарубежными учёными. В ходе работы были проанализированы не только классические теории, но и современные тенденции и разработки в области кибербезопасности, такие как искусственный интеллект, блокчейн-технологии, квантовые методы шифрования, а также актуальные нормативные и правовые документы в сфере информационной безопасности.

3 Результаты и обсуждения

В современном мире информационные технологии являются неотъемлемой частью повседневной жизни, обеспечивая обмен информацией на различных уровнях – от личных переписок до корпоративных данных и информационных систем государства. Вместе с ростом объёмов и ценности передаваемой информации, растёт и угроза нарушения информационной безопасности.

Кибератаки, утечки данных и другие угрозы становятся все более сложными и разрушительными, требуя эффективных и инновационных методов защиты информации на всех уровнях.

На сегодняшний день угрозы для личной информационной безопасности весьма разнообразны. Среди них можно выделить:

- кибермошенничество - воровство личных данных, фишинговые атаки, финансовое мошенничество, поддельные веб-сайты и мошеннические практики;
- кража личных данных для создания фальшивых профилей, взлома учётных записей, получения доступа к личной конфиденциальной информации;
- кибербуллинг - онлайн-беллинг, угрозы, негативные комментарии, оскорбления и шантаж через интернет и социальные сети;
- недостатки в защите данных - незащищённые учётные записи, слабые пароли, отсутствие обновлений программного обеспечения, что делает личные данные уязвимыми для кибератак;
- нарушение конфиденциальности - несанкционированный доступ к личным сообщениям, файлам и информации, что может привести к их утечке;
- отслеживание онлайн-активности - компании и социальные сети могут собирать данные о поведении пользователя для персонализированной рекламы, что вызывает вопросы о приватности;
- идентификационные угрозы - незаконное использование личных данных для идентификации личности в целях мошенничества или несанкционированного доступа.

Совершенствование цифровой экономики влечёт за собой угрозу того, что отдельная личность становится полностью уязвимой перед глобальными платформами, в результате получения доступа к частной информации [3].

Что касается жизни социума и угрозы для общества в целом, то они также весьма разнообразны. Среди них можно выделить:

- кибератаки и киберугрозы - взломы информационных систем, атаки на критическую инфраструктуру, кибершпионаж, распространение вредоносного программного обеспечения, что может привести к серьёзным последствиям для экономики, безопасности и функционирования общества;
- терроризм и экстремизм - угрозы террористических атак, радикализации и экстремизма, включая кибертерроризм и использование онлайн-ресурсов для распространения идеологии;
- политическая нестабильность - манипуляции информацией, дезинформация, кибератаки на политические институты и процессы выборов, что может повлиять на доверие к правительству и политическим структурам;
- экономические угрозы - включают в себя кражу данных, финансовые мошенничества, угрозы бизнесу и финансовой инфраструктуре;
- киберразведка - попытки получения конфиденциальной информации, в том числе важных коммерческих секретов, через кибершпионаж;

- кибербезопасность детей и подростков - угрозы онлайн-беллинга, киберзависимости, доступ к нежелательному контенту и другие проблемы, связанные с интернетом для молодежи.

- информационная война и дезинформация - использование интернета и социальных сетей для распространения ложной информации, манипуляций с общественным мнением, что может создавать общественные разногласия и нестабильность.

Угрозы для государства могут оказать катастрофическое воздействие на его функционирование и стабильность. Кибератаки на государственные системы могут привести к параличу важных инфраструктурных объектов, таких как энергетика, транспорт, финансовые институты или здравоохранение. Это влечёт за собой хаос, нарушение общественного порядка и безопасности граждан, а также может привести к значительным экономическим потерям и угрозе жизни людей. К ним относятся:

- кибератаки и кибервойны - атаки на критическую информационную инфраструктуру государства, такие как правительственные системы, военные объекты, критически важные объекты, а также попытки кибершпионажа и киберразведки;

- террористические атаки - использование киберпространства для планирования и координации террористических актов, а также угрозы кибертерроризма;

- информационная война - манипуляция информацией, дезинформация, кибератаки на государственные системы, дестабилизация политических и социальных процессов, цель которых - дестабилизация государства;

- экономические угрозы - киберпреступность и кибершпионаж, нацеленные на важные экономические объекты и конфиденциальные данные;

- кибербезопасность национальной обороны - защита военных технологий, объектов оборонной промышленности и военной информационной инфраструктуры от киберугроз;

- киберразведка и кибершпионаж - попытки получения конфиденциальной информации, включая секреты государственной безопасности, политики и стратегии.

Как показывает анализ, чёткого разграничения экономической безопасности личности, общества и государства в целом практически не существует. Все виды угроз тесно переплетаются между собой и вытекают один из другого.

Изучив и проанализировав существующие системы защиты данных, нами предложены следующие меры для защиты конфиденциальной информации, личных данных и критической инфраструктуры как на уровне индивида, так и на уровне социума и государства:

На уровне отдельно взятой личности необходимо устанавливать более сложные пароли и использовать многофакторную систему аутентификации, таких как отпечатки пальцев или одноразовые коды. На регулярной основе осуществлять обновление операционных систем и приложений для закрытия уязвимостей. Немаловажно уделить внимание и правилам кибергигиены,

осведомлённости о фишинговых атаках, а также избегать перехода по сомнительным ссылкам и открытия неизвестных вложений.

На уровне социума необходимо уделить пристальное внимание разработке образовательных программ и проведению обучающих тренингов по вопросам кибербезопасности, включая детей, взрослых и предпринимателей. Необходима разработка и реализация жёсткого законодательства о защите данных и кибербезопасности для защиты конфиденциальной информации и наказания за нарушения. При этом важно не забывать и о международном сотрудничестве для обмена информацией о киберугрозах и совместного реагирования на них.

На уровне государства необходимы разработка и внедрение национальных стратегий по кибербезопасности для защиты критической инфраструктуры и данных государства. Регулярное финансирование и развитие технологий, которые защищают от киберугроз, способствуют обеспечению безопасности и поддержке существующей инфраструктуры, а создание программ обучения для специалистов в области кибербезопасности и расширение кадрового резерва способствуют усилению защиты и противодействия кибератакам.

Комбинация вышеперечисленных мер на разных уровнях поможет укрепить защиту информации, личных данных и критической инфраструктуры от киберугроз на различных уровнях общества.

2. Выводы

Таким образом, исследования в области кибербезопасности являются важной в современном мире, где цифровые технологии проникают во все сферы жизни. Они позволяют понять множество аспектов существующей проблемы, начиная от угроз, с которыми сталкиваются индивиды, до сложностей, с которыми сталкиваются общество и государство.

Исследования показали, что необходим комплексный подход к защите информации. При этом важной составляющей выступают образование, международное сотрудничество и разработка эффективного законодательства, так как угрозы информационной безопасности эволюционируют, обуславливая необходимость постоянного совершенствования защитных механизмов.

Библиографический список

1. Грачев М.И., Грачева Н.Г. Информационная безопасность личности, общества и государства в целом // В книге: Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. Санкт-Петербург, 2022. С. 150-152.
2. Ермаков М.А. Информационная безопасность государства, личности и общества // Вестник ПНИПУ. Социально-экономические науки. 2013. №18. URL: https://cyberleninka.ru/article/n/informationnaya-bezopasnost-

gosudarstva-lichnosti-i-obschestva
3. Затравина С.В., Усупбаева А. Экономическая безопасность как один из факторов риска цифровизации экономики // Наука и инновационные технологии. 2022. № 2 (23). С. 104-109.
4. Кузнецова Ю.А. Информационная безопасность государства // Вестник молодых ученых Самарского государственного экономического университета. 2022. № 2 (46). С. 42-43.
5. Никишкин А.В., Степанов И.В., Аюпов М.С. Информационная безопасность личности, общества, государства: сборник трудов конференции // Актуальные вопросы права, экономики и управления / редкол.: С.В. Лукашевич [и др.] Чебоксары: ИД «Среда», 2019. С. 176-178.
6. Плеханов, С. М. Информационная безопасность как приоритет национальной безопасности // Молодой ученый. 2022. № 24 (419). С. 261-263.
7. Побегайлов Р. Г. Информационная безопасность личности, государства и общества в России. Электронный ресурс: URL: https:// www.gramota.net/materials/1/2007/2/89.html
8. Соколова А.А. Безопасность личности, общества и государства: информационно-психологический аспект // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. 2018. №1. URL: https://cyberleninka.ru/article/n/bezopasnost-lichnosti-obschestva-i-gosudarstva-informatsionno-psihologicheskiy-aspekt
9. Хроколов В.А. Информационная безопасность личности, общества и государства: организационно-правовой аспект // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. 2019. №1. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-lichnosti-obschestva-i-gosudarstva-organizatsionno-pravovoy-aspekt
10. Arenas Á. et al. How to keep your information secure? Toward a better understanding of users security behavior //Technological Forecasting and Social Change. 2024. Т. 198. С. 123028.
11. Paananen H., Lapke M., Siponen M. State of the art in information security policy development //Computers & Security. 2020. Т. 88. С. 101608.
12. Shropshire J., Warkentin M., Sharma S. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior //Computers & security. 2015. Т. 49. С. 177-191.
13. Potts M. The state of information security //Network Security. 2012. Т. 2012. №. 7. С. 9-11.
14. Gao X. et al. An economic analysis of information security decisions with mandatory security standards in resource sharing environments //Expert Systems with Applications. 2022. Т. 206. С. 117894.