

УДК 343

ГРНТИ 10.77

EDN: OTHUWF



Проблемы обеспечения кибербезопасности в современных цифровых системах

©Таков Асланбек Заурбиевич

Северо-Кавказский институт повышения квалификации (филиал)
Краснодарского университета МВД России, г.Нальчик, КБР, Россия
aslantak001@mail.ru

Аннотация: Целью данного исследования является изучение возможностей обеспечения кибербезопасности в современных цифровых системах. Примечательно, что использование современных технологий позволяет не только постоянно оставаться на связи, но и оптимизировать многие производственные отношения, ускорить процессы, рационализировать системы публичного управления, свести к минимуму издержки на транзакции, повысить качество социального обеспечения. Отсюда, можно заключить, что всемирная цифровизация — это не только удобно, но и опасно, так как многие преступники научились пользоваться глобальной сетью для достижения своих криминальных целей. Они могут посягать на публичные либо частные права, создавать непривычные для правоохранительной системы угрозы, бороться с которыми она умеет плохо.

Принимая во внимание, что цифровой рынок не стоит на месте, более того он активно развивается и меняется, следует отметить произошедший значительный рост применения ИТ-технологий во всех сферах жизни и экономической ситуации в стране, развитие киберпреступников, появление возможностей у них приобрести необходимое оборудование, получить узкоспециализированные знания. Преступники хорошо ориентированы на требования потенциальных покупателей, поэтому предложения на рынке меняются относительно спроса.

Сделан вывод о том, что кибербезопасность позволяет защищать частные и публичные данные, интересы преступных атак, совершаемых в отношении сетей, компьютерных систем, отдельных компьютеров, объектов критической информационной инфраструктуры государства. За последние 6 лет в РФ серьезно выросло количество хакерских атак. Это говорит о необходимости принятия эффективных и своевременных мер по борьбе с данным явлением. А для того, чтобы скрываться от правосудия, преступники не только стараются действовать максимально анонимно, но и применяют максимально сложные схемы, при которых достаточно сложно отыскать следы и шаги преступления.

Ключевые слова: киберпреступность, кибербезопасность, киберугроза, информационно-коммуникативные технологии, цифровизация, вредоносное программное обеспечение, даркнет, хакерские атаки, диверсия.

Для цитирования: Таков А.З. Проблемы обеспечения кибербезопасности в современных цифровых системах // Пробелы в российском законодательстве. 2023. Т. 16. №5. С. 232-236. EDN: OTHUWF

Cybersecurity Issues In Modern Digital Systems

©Takov Aslanbek Zaurbievich

North Caucasus Institute for Advanced Studies (branch)
of the Krasnodar University of the Ministry of Internal Affairs of Russia, Nalchik, Russia
aslantak001@mail.ru

Abstract: The purpose of this study is to study the possibilities of ensuring cybersecurity in modern digital systems. It is noteworthy that the use of modern technologies allows not only to stay in touch constantly, but also to optimize many industrial relations, speed up processes, rationalize public administration systems, minimize transaction costs, and improve the quality of social security. Hence, we can conclude that worldwide digitalization is not only convenient, but also dangerous, since many criminals have learned to use the global network to achieve their criminal goals. They can encroach on public or private rights, create threats unusual for the law enforcement system, which it knows how to deal with poorly.

Taking into account that the digital market does not stand still, moreover, it is actively developing and changing, it should be noted that there has been a significant increase in the use of IT technologies in all spheres of life and the economic situation in the country, the development of cybercriminals, the emergence of opportunities for them to purchase the necessary equipment, to obtain highly specialized knowledge. Criminals are well oriented to the requirements of potential

buyers, so the market offers change relative to demand.

It is concluded that cybersecurity makes it possible to protect private and public data, the interests of criminal attacks committed against networks, computer systems, individual computers, objects of critical information infrastructure of the state. Over the past 6 years, the number of hacker attacks in the Russian Federation has seriously increased. This indicates the need to take effective and timely measures to combat this phenomenon. And in order to hide from justice, criminals not only try to act as anonymously as possible, but also use the most complex schemes, in which it is quite difficult to find traces and steps of the crime.

Keywords: cybercrime, cybersecurity, cyber threat, information and communication technologies, digitalization, malicious software, darknet, hacker attacks, sabotage.

For citation: Takov A.Z. Cybersecurity Issues In Modern Digital Systems // Gaps in Russian Legislation. 2023. Vol. 16. №5. Pp. 232-236. (in Russ.). EDN: OTHUWF

ВВЕДЕНИЕ

Информационно-коммуникативные технологии приобретают широкое распространение. Это связано с их положительными качествами, например, удобством, возможностью передавать за доли секунды большой объем информации, при этом пользоваться разными файлами, как текстовыми, так фото и видео. Использование современных технологий позволяет не только постоянно оставаться на связи, но и оптимизировать многие производственные отношения, ускорить процессы, рационализировать системы публичного управления, свести к минимуму издержки на транзакции, повысить качество социального обеспечения. Всемирная цифровизация — это не только удобно, но и опасно, так как многие преступники научились пользоваться глобальной сетью для достижения своих криминальных целей. Они могут посягать на публичные либо частные права, создавать непривычные для правоохранительной системы угрозы, бороться с которыми она умеет плохо.

Киберугрозы — это совокупность условий и факторов, при которых нарушается частная и общественная безопасность, создается информационная опасность. Киберугрозы с объективной стороны — это действия, предпринимаемые преступниками в цифровом пространстве. Они могут проникать в информационную систему с целью совершения преступления, например, кражи, мошенничества, хищения личных данных, денежных средств, совершения иных общественно опасных деяний [1; 6].

ВОЗНИКНОВЕНИЕ УГРОЗ БЕЗОПАСНОСТИ КИБЕРСИСТЕМ

В современном мире цифровая индустрия проникла во все уровни существования общества. Для развития и выживания организациям нужно использовать новые стратегии, повышать, оптимизировать производства, поддерживать конкурентоспособность, сделать это удастся за счет внедрения цифровых технологий. Такие технологии могут участвовать в бизнес-процессах, однако стоит уделить повышенное внимание вопросам кибербезопасности. Особенно ярко эта проблема проявила себя в период карантина, когда многие предприятия перешли на удаленный режим работы. Было выявлено большое количество проблемных мест в безопасности киберсистем. Многие орга-

низации постепенно отказываются от бумажных носителей или по старинке применяют их, но дублируют с электронными носителями. На виртуальных носителях могут находиться личные данные клиентов компаний и сотрудников, вопрос безопасности в данном моменте важен не только для частных предпринимателей, но и для государственных структур, так как, пользуясь удаленным доступом, преступники могут неправомерно завладеть личными данными большого числа людей [11]. Эти данные могут быть использованы для хищения денежных средств со счетов и других противоправных действий.

Цифровая экономика подразумевает использование личных данных, например, при регистрации на сайте, продающем определенные виды продукции, предлагающем подписки. С одной стороны, это удобно для покупателей и продавцов, с другой — создает большую базу данных, к которой может появиться доступ у злоумышленников. Расширяется и объем незаконной торговли базами данных с личной информацией пользователей. Это могут быть не только электронные адреса и телефоны, но и номера счетов, данные паспорта. Согласно данным Group-IB, за 2022 год в России на 37% выросло число баз данных, не имеющих какую-либо защиту. Анализируя инвестиционную активность предприятий, можно сделать вывод о том, что наиболее востребованными сервисами являются облачные. Их применяет более 50% компаний по всему миру. В 2022 году предприятия стали уделять кибербезопасности больше внимания, вкладывать деньги в ее развитие. Однако стоит отметить, что теневой рынок по продаже баз данных постоянно увеличивается в объемах. Это связано с тем, что большинство компаний пользуется ИТ-технологиями и развивается в этом направлении [8; 9; 11].

Например, в 2020 году этот рост стал наиболее ощутимым, так как ему способствовал карантин. В даркнете (DarkNet) существуют специальные маркетплейсы и форумы, где можно приобрести незаконно распространяемый товар. Чаще всего это происходит через посредника. Российский незаконный рынок условно делится на следующие сегменты:

- Реализация баз данных.
- Продажа персональных данных отдельных людей.

Чаще всего получить такие данные злоумышленникам удастся посредством взлома базы данных определенной организации либо подкупа сотрудников выбранной компании. Получив доступ к интересующей

информации, преступники ее копируют и затем распространяют за вознаграждение. Чаще всего совершить взлом личных страниц или баз данных злоумышленникам удается за счет невнимательности жертвы и ее малой компьютерной грамотности. Кроме этого, не всегда разработчики и администраторы программного обеспечения организации уделяют кибербезопасности достаточное внимание. Например, серверы баз данных достаточно уязвимы, защита настроена по умолчанию, и никаких дополнительных мер не принимается. Для обеспечения высокого уровня безопасности потребуются финансовые вливания, так как необходимо обеспечить качественное программное обеспечение, подобрать надежный, квалифицированный персонал [3].

ПРЕСТУПНЫЕ ЦЕЛИ ЗЛОУМЫШЛЕННИКОВ В КИБЕРПРОСТРАНСТВЕ

Цифровой рынок не стоит на месте, он активно развивается и меняется. Это связано не только с распространением ИТ-технологий во всех сферах жизни, но и экономической ситуацией в стране, развитию киберпреступников, появление возможностей у них приобрести необходимое оборудование, получить узкоспециализированные знания. Преступники хорошо ориентированы на требования потенциальных покупателей, поэтому предложения на рынке меняются относительно спроса [5]. Например, в 2022 году наиболее популярными предложениями на рынке даркнета были:

- Доступ к учетным записям Active Directory. За счет этой информации у преступника появляется возможность нанести вред, в том числе и физический, компьютерам предприятия, быстро распространив на них вредоносное ПО.

- Первоначальный доступ к сети (Initial Network Access (RDP, VPN, SSH)). Помогает получить доступ к ресурсам компании-жертвы, взломать и отсканировать RDP-серверы.

Для управления чужим сервером или сайтом применяется скрипт веб-шелл (Web-shell). Он может дать доступ к системе файлов, узнать чужой пароль при помощи подбора, вскрыть базу данных. Получив удаленный доступ к записи администратора CMS, злоумышленник сможет управлять чужими ИТ-системами и скачивать, копировать, удалять, менять любой контент хостинга. Чаще всего злоумышленники получают доступ к системам, используя их слабые места, так называемые баги и недоработки разработчиков. Некоторые проблемы можно решить при помощи стандартных мер безопасности. Однако многие пользователи относятся к ним легкомысленно и пренебрегают. К таким мерам можно отнести:

- Надежный сложный пароль.
- Двухфакторная аутентификация (когда нужно ввести пароль и подтвердить действие по телефону).
- Регулярная проверка учетной записи.

Если провести мониторинг даркнета и его площадок, можно понять, какие предложения там есть, следовательно, на какие цели будут охотиться злоумышленники, и усилить их защиту. Обеспечение кибербезопасности играет важную роль для цифровой экономики и иных сфер в Российской Федерации, которые переходят на цифровой формат работы. Многие преступни-

ки совершают киберпреступления с целью наживы или преследуют иные цели. Они могут взламывать профили пользователей, похищать цифровую информацию, создавать различные ошибки и помехи для использования цифровых систем [2]. Все это снижает уровень доверия к ИТ-технологиям, замедляет переход экономики в цифровой формат.

Хакеры могут совершать различные атаки, целью которых не всегда является кража данных. Иногда они совершают диверсии с целью вывести систему из строя. Для этого злоумышленники разрабатывают и распространяют вредоносное программное обеспечение. Существуют специальные антивирусные программы и средства для обнаружения вирусов, однако преступники учитывают их возможности и стараются создать код, способный обойти антивирусы [4; 10]. Именно поэтому важно своевременно обновлять антивирусное ПО, иначе оно будет неэффективно против новых вирусов. Вредоносные программы могут иметь разный характер, они позволяют красть данные, мешать работе системы или выводить ее из строя, вымогать деньги или заниматься майнингом, используя для этого чужие компьютеры.

ЗАКЛЮЧЕНИЕ

Для того чтобы скрываться от правосудия, преступники не только стараются действовать максимально анонимно, но и применяют максимально сложные схемы, при которых достаточно сложно отыскать следы и шаги преступления. Атака может включать несколько этапов, например взлом и заражение вредоносной программой, которая уже будет выполнять свои цели незаметно для пользователя. Рост кибератак наблюдается в отношении физических и юридических лиц, органов власти. В связи с этим законодатель РФ принимает ряд мер, направленных на борьбу с киберугрозами. Например, в РФ существует государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак [7]. В отношении субъектов КИИ есть закрепленные в законодательстве нормы, согласно которым проводятся мероприятия по установке средств защиты КИИ.

В силу закона у субъектов появляется необходимость проявлять реакцию на киберпреступления, принимать меры по устранению последствий хакерских атак, взаимодействовать с ГосСОПКА. Это должно выполняться непрерывно. Закон направлен не только на борьбу с хакерскими атаками и их предупреждением, но и на устранение последствий, которые были вызваны, если они способны нанести вред государственному информационному пространству, создать угрозу экологической катастрофы, повредить информационную инфраструктуру, вызвать какую-либо финансовую или социальную катастрофу или выраженную проблему.

Кибербезопасность позволяет защищать частные и публичные данные, интересы преступных атак, совершаемых в отношении сетей, компьютерных систем, отдельных компьютеров, объектов критической информационной инфраструктуры государства. За последние 6 лет в РФ серьезно выросло количество хакерских атак. Это говорит о необходимости принятия эффективных и своевременных мер по борьбе с данным явлением.

ЛИТЕРАТУРА

1. Артамонов В.А., Артамонова Е.В. Кибербезопасность в условиях цифровой трансформации // Цифровая трансформация. 2021. № 4. С. 42-51.
2. Гребеников Д.Н., Марухленко А.Л., Лаврова Е.Д. Обеспечение кибербезопасности в современном мире // В сборнике: Современные информационные технологии и информационная безопасность. Сборник научных статей 2-й Всероссийской научно-технической конференции. Курск, 2023. С. 21-24.
3. Данкев Н.В. Обеспечение кибербезопасности // Студенческий. 2022. № 18-7 (188). С. 50-51.
4. Заикина С.Е., Кесова З.А. Проблемы кибербезопасности в условиях цифровизации экономики // В сборнике: Тенденции социально-экономического развития в период санкционного воздействия и цифровой трансформации. Материалы III Международной научно-практической конференции. Краснодар, 2023. С. 459-464.
5. Кафиятуллина Ю.Н., Харчилава Г.П. Обеспечение кибербезопасности в условиях цифровизации экономики // Самоуправление. 2020. № 3 (120). С. 87-90.
6. Кириленко В.П., Алексеев Г.В. Киберпреступность и цифровая трансформация // Теоретическая и прикладная юриспруденция. 2021. № 1. С. 39-53.
7. Малик Т.Н. Кибербезопасность: проблемы и перспективы // Молодой ученый. 2021. № 7 (349). С. 10-12.
8. Мирабова Л. Современная защита информации и кибербезопасность // Ceteris Paribus. 2023. № 4. С. 56-59.
9. Селиванов С.А., Огарок А.Л. Обеспечение кибербезопасности сложных информационных и управляющих систем // Информатизация и связь. 2020. № 1. С. 28-33.
10. Судомойкин К.Р., Федотов Б.В. Кибербезопасность в современном обществе // В сборнике: Интеллектуальный потенциал Сибири. Материалы 30-я Региональной научной студенческой конференции: в 4 частях. Новосибирск, 2022. С. 504-510.
11. Хашимходжаев Ш.И., Пилипенко Е.Ф. Информационная безопасность - важный фактор эффективного развития экономических объектов в условиях цифровой трансформации // Ученые записки юридического факультета. 2022. № 1. С. 38-41.

РЕЦЕНЗИЯ

на статью «Проблемы обеспечения кибербезопасности в современных цифровых системах», подготовленную преподавателем кафедры огневой подготовки СКИ(ф) КрУ МВД России, капитаном полиции Таковым Асланбеком Заурбиевичем

Использование современных технологий позволяет не только постоянно оставаться на связи, но и оптимизировать многие производственные отношения, ускорить процессы, рационализировать системы публичного управления, свести к минимуму издержки на транзакции, повысить качество социального обеспечения. Всемирная цифровизация – это не только удобно, но и опасно, так как многие преступники научились пользоваться глобальной сетью для достижения своих криминальных целей. Они могут посягать на публичные либо частные права, создавать непривычные для правоохранительной системы угрозы, бороться с которыми она умеет плохо.

Киберугрозы – это совокупность условий и факторов, при которых нарушается частная и общественная безопасность, создается информационная опасность. Они могут проникать в информационную систему с целью совершения преступления, например, кражи, мошенничества, хищения личных данных, денежных средств, совершения иных общественно опасных деяний.

Автор обращает внимание на то, что мире цифровая индустрия проникла во все уровни существования общества. Для развития и выживания организациям нужно использовать новые стратегии, повышать, оптимизировать

REFERENCES

1. Artamonov V.A., Artamonova E.V. Cybersecurity in conditions of digital transformation // Digital transformation. 2021. No. 4. pp. 42-51.
2. Grebenikov D.N., Marukhlenko A.L., Lavrova E.D. Ensuring cybersecurity in the modern world // In the collection: Modern information technologies and information security. Collection of scientific articles of the 2nd All-Russian Scientific and Technical Conference. Kursk, 2023. pp. 21-24.
3. Dankev N.V. Ensuring cybersecurity // Student. 2022. No. 18-7 (188). pp. 50-51.
4. Zaikina S.E., Kesova Z.A. Problems of cybersecurity in the conditions of digitalization of the economy // In the collection: Trends in socio-economic development during the period of sanctions and digital transformation. Materials of the III International Scientific and Practical Conference. Krasnodar, 2023. pp. 459-464.
5. Kafiyatullina Yu.N., Kharchilava G.P. Ensuring cybersecurity in the conditions of digitalization of the economy // Self-government. 2020. No. 3 (120). pp. 87-90.
6. Kirilenko V.P., Alekseev G.V. Cybercrime and digital transformation // Theoretical and applied jurisprudence. 2021. No. 1. pp. 39-53.
7. Malik T.N. Cybersecurity: problems and prospects // Young scientist. 2021. No. 7 (349). pp. 10-12.
8. Mirabova L. Modern information protection and cybersecurity // Ceteris Paribus. 2023.No. 4. pp. 56-59.
9. Selivanov S.A., Ogarok A.L. Ensuring cybersecurity of complex information and control systems // Informatization and communication. 2020. No. 1. Pp. 28-33.
10. Sudomoikin K.R., Fedotov B.V. Cybersecurity in modern society // In the collection: Intellectual potential of Siberia. Materials of the 30th Regional Scientific Student Conference: in 4 parts. Novosibirsk, 2022. pp. 504-510.
11. Hashimhodzhaev Sh.I., Pilipenko E.F. Information security is an important factor in the effective development of economic objects in the conditions of digital transformation // Scientific notes of the Faculty of Law. 2022. No. 1. pp. 38-41.

производства, поддерживать конкурентоспособность, сделать это удастся за счет внедрения цифровых технологий. Такие технологии могут участвовать в бизнес-процессах, однако стоит уделить повышенное внимание вопросам кибербезопасности. Особенно ярко эта проблема проявила себя в период карантина, когда многие предприятия перешли на удаленный режим работы. Было выявлено большое количество проблемных мест в безопасности киберсистем. Многие организации постепенно отказываются от бумажных носителей или по старинке применяют их, но дублируют с электронными носителями. На виртуальных носителях могут находиться личные данные клиентов компаний и сотрудников, вопрос безопасности в данном моменте важен не только для частных предпринимателей, но и для государственных структур, так как, пользуясь удаленным доступом, преступники могут неправомерно завладеть личными данными большого числа людей. Эти данные могут быть использованы для хищения денежных средств со счетов и других противоправных действий.

Отметим, что автор рецензируемого исследования с интересом относится к своей работе, по отдельным вопросам и положениям имеет своё мнение, которое может отстоять. В целом рецензируемая статья представляет научный и практический интерес и может быть рекомендована к публикации.

Рецензент: Старший преподаватель кафедры огневой подготовки Северо-Кавказского института повышения квалификации (филиал) Краснодарского университета России, к.ю.н. подполковник полиции А.А. Хараев

Статья прошла проверку системой «Антиплагиат»; оригинальность текста – 71,89%

Статья поступила в редакцию 07.07.2023, принята к публикации 29.07.2023

The article was received on 07.07.2023, accepted for publication 29.07.2023

СВЕДЕНИЯ ОБ АВТОРЕ

Таков Асланбек Заурбиевич, капитан полиции, преподаватель кафедры огневой подготовки, Северо-Кавказский институт повышения квалификации (филиал) Краснодарского университета МВД России, г. Нальчик, Россия. E-mail: aslantak001@mail.ru

ABOUT THE AUTHOR

Takov Aslanbek Zaurbievich, Police Captain, Lecturer at the Department of Fire Training, North Caucasus Institute for Advanced Studies (branch) of the Krasnodar University of the Ministry of Internal Affairs of Russia, Nalchik, Russia. E-mail: aslantak001@mail.ru