УДК 34 **DOI: 10.34670/AR.2024.64.19.035**

Борьба с киберпреступностью как задача государства и гражданского общества

Багрецов Дмитрий Николаевич

Кандидат филологических наук,
доцент кафедры иностранных языков,
Уральский юридический институт МВД России,
620057, Российская Федерация, Екатеринбург, ул. Корепина, 66;
e-mail: Bagretsov@mail.ru

Аннотация

В статье рассматриваются киберпреступность и борьба с ней как с одним из ведущих вызовов современности. Оценивается важность данной задачи и инновационных подходов к ней. Киберпреступность включает в себя широкий спектр деяний, включая компьютерные атаки, кражу личных данных, финансовые мошенничества, распространение вредоносного программного обеспечения и многие другие формы противоправной деятельности в сети. Подобные преступления не только угрожают финансовой безопасности и личным данным индивидуумов, но также имеют потенциал нанести серьезный ущерб бизнес-сектору и даже государствам. По выводам автора, борьба с киберпреступностью требует постоянного развития и применения инновационных методов. Внедрение искусственного интеллекта, блокчейна и квантовых компьютеров открывает новые горизонты в области кибербезопасности, улучшая защиту информации и снижая уязвимость перед угрозами киберпреступников. Объединение этих методов позволяет создать эффективную систему, способную отвечать вызовам современного цифрового мира и обеспечивать защиту цифровых активов.

Для цитирования в научных исследованиях

Багрецов Д.Н. Борьба с киберпреступностью как задача государства и гражданского общества // Вопросы российского и международного права. 2024. Том 14. № 2А. С. 185-190. DOI: 10.34670/AR.2024.64.19.035

Ключевые слова

Киберпреступность, IT-преступления, защита информации, информационное общество.

Введение

Цифровизация – это внедрение современных цифровых технологий в различные сферы жизни и производства. В конце 90-х годов XX века в мире начали говорить о технологиях IoT и цифровой экономике, тогда как в России в это время только начали появляться первые мобильные телефоны. С тех пор прошло более двадцати лет, и Интернет вещей стал для нас привычным явлением: практически у каждого есть дома умные устройства, которых во всем мире насчитывается уже более 26 миллиардов единиц, а в России только за последний год было куплено почти 20 миллионов SIM-карт для IoT-оборудования. Производственная цифровизация занимается сокращением монотонного физического труда для человека, организовывает и контролирует трудовые и производственные процессы и обеспечивает безопасность сотрудников компании. Допустим, простой рабочий идет на свое место к станку, но почему-то включается сирена, а самому сотруднику сообщают о нарушении техники безопасности. Это «умная» система видеоаналитики заметила, что работник вошел в цех без каски, подала сигнал и спасла человеку жизнь. «Умные» системы при помощи машинного зрения выявляют бракованные детали, а система видеонаблюдения следит за соблюдением техники безопасности. Такие же системы применяются в непроизводственных компаниях и даже в маленьких офисах [Багрецов, 2023]. Цифровизация широко распространена и в быту: количество новых образцов домашней техники постоянно растет. Государство внедряет цифровизацию во все свои структуры. Для борьбы с коррупцией чрезвычайно эффективной исследователи считают систему электронной подачи обращений «одно окно». Система анализа данных давно уже эффективно используется в исполнительной власти. Яркий пример – розыск преступников с использованием онлайн-камер на улицах или возможность отправить обращение в нужные инстанции по Интернету. Одна из главных заслуг цифровизации государства – это снижение количества бумажной волокиты и бюрократии при оформлении документов. Справки и паспорта можно заказывать через приложение, там же хранить и обновлять все данные [Багрецов, 2023].

Параллельно с цифровизацией развивается и киберпреступность. В настоящее время киберпреступность стала одной из самых значительных проблем в области безопасности, представляя серьезную угрозу для международного сообщества. Развитие информационных технологий и всеобщее проникновение Интернета в повседневную жизнь людей создали идеальную почву для развития различных видов киберугроз.

Основная часть

Киберпреступность включает в себя широкий спектр деяний, в том числе компьютерные атаки, кражу личных данных, финансовые мошенничества, распространение вредоносного программного обеспечения и многие другие формы противоправной деятельности в сети. Подобные преступления не только угрожают финансовой безопасности и личным данным индивидуумов, но также имеют потенциал нанести серьезный ущерб бизнес-сектору и даже государствам [Что такое киберпреступность? Защита от киберпреступности, www].

Одной из главных причин роста киберпреступности является быстрый технологический прогресс и все большая зависимость общества от цифровой инфраструктуры. Такие явления, как интернет-банкинг, онлайн-покупки и социальные сети, стали неотъемлемой частью нашей жизни, предоставляя злоумышленникам бесчисленные возможности для совершения преступлений. Киберпреступники активно используют уязвимости в системах безопасности,

проявляя высокую квалификацию и часто оперируя на глобальном уровне [Рубанов, 2022].

Однако, помимо технологических аспектов киберпреступности, следует также уметь оценивать факторы, вызывающие мотивацию преступников. Часто кибератаки совершаются с целью получения финансовой выгоды, но также могут быть проведены из политических мотивов или с целью причинения ущерба репутации определенного лица, организации или государства.

Для борьбы с киберугрозами всем участниками общества требуется внимательность и подготовка. Государства должны разрабатывать и укреплять соответствующие правовые нормы, а также сотрудничать с другими государствами для координации действий и обмена информацией [Эксперты назвали низкую цифровую грамотность россиян причиной роста киберпреступности, www]. Бизнес-сектор должен внедрять современные меры безопасности, чтобы минимизировать уязвимости своих систем, а обычные пользователи должны обладать базовыми навыками и знаниями по защите своих данных онлайн.

Только взаимодействие и совместные усилия государств, бизнеса и граждан могут обеспечить эффективную защиту от киберпреступности и минимизировать ее воздействие на общество в целом.

Итак, киберпреступность является одной из наиболее острых проблем современного общества. Вместе с развитием информационных технологий и всемирной паутины киберугрозы становятся все более серьезными, труднопреодолимыми и разнообразными. Каждый год миллионы людей и организаций по всему миру сталкиваются с киберпреступлениями, причиняющими серьезный ущерб их безопасности, финансам и доверию.

Для борьбы с киберпреступностью существуют различные методы и подходы. Один из них – разработка эффективной правовой системы и улучшение законодательства. Государства продолжают принимать строгие законы и нормативные акты, которые квалифицируют киберпреступления, определяют и наказывают их. Кроме того, важно сотрудничество между странами для экстрадиции и судебного преследования отдельных лиц, которые выполняют киберпреступные действия в зарубежных юрисдикциях [Багрецов, 2023].

Однако исключительно юридические меры недостаточны для эффективности борьбы с киберугрозами. Необходимо укреплять сотрудничество между государствами, правоохранительными органами и частными компаниями. Совместные усилия по обмену информацией и опытом позволят лучше понимать и предотвращать новые виды киберпреступлений, которые появляются по мере развития технологий.

Наиболее распространенными методами борьбы с киберпреступностью являются использование современных технологий защиты и применение сертифицированных систем безопасности. Компании и организации вынуждены регулярно обновлять свое программное и аппаратное обеспечение, чтобы минимизировать уязвимости и предотвращать атаки. Также важно обучение пользователей основам кибербезопасности, чтобы они могли распознавать и избегать подозрительных действий и мошеннических попыток [Багрецов, Шунякова, Альтшулер-Феррейра, 2023; Эксперты назвали низкую цифровую грамотность россиян причиной роста киберпреступности, www].

В современной фантастике предложен радикальный выход из сложного положения с киберпреступностью: писатель Андрей Рубанов предполагает в обозримом будущем появление «разумных денег» [Рубанов, 2022], украсть которые будет невозможно. Более того, в конце года такие деньги будут автоматически списываться со счетов, что делает невозможным накопление средств. Вариант с ажиотажным спросом на любые товары к концу года писатель не рассматривает, как и появление квазиденег, разного рода взаимозачетов и в итоге возвращение

к натуральному товарообмену.

Между тем борьба с киберпреступностью продолжается. Она теперь требует активного содействия киберсообщества. «Белые хакеры» и специалисты по кибербезопасности играют все более важную роль в обнаружении и реагировании на угрозы. Они могут проникать в системы для тестирования их уязвимостей и разрабатывать меры по предотвращению атак.

Наконец, формирование глобальных партнерств, как государственных, так и частных, также является неотъемлемой частью борьбы с киберпреступностью. Международные организации, такие как Интерпол, осуществляют координацию действий по различным аспектам сотрудничества и обмену информацией. Компании должны также активно участвовать в разработке и реализации стандартов безопасности, чтобы минимизировать риски для своих клиентов и партнеров.

Заключение

В целом, борьба с киберпреступностью требует комплексного подхода, включающего правовые, технические и образовательные меры. Только в единстве и сотрудничестве мы сможем защитить себя и весь мир от киберугроз и обеспечить безопасность в Интернете.

В настоящем информационном веке, где зависимость общества от технологий с каждым днем усиливается, киберпреступность становится одной из наиболее серьезных угроз. Киберпреступники постоянно совершенствуют свои методы вторжения и махинирования, поэтому необходимы инновационные методы борьбы с ними.

Киберпреступность может нанести значительный ущерб как отдельным лицам, так и для организациям, государствам и даже всему международному сообществу. Возможность потерять ценные информационные активы и причинить значительный ущерб репутации становится все более реальной. Поэтому создание эффективных и инновационных систем защиты и предотвращения кибератак становится вопросом жизненной важности.

Одним из инновационных методов борьбы с киберпреступностью является использование искусственного интеллекта (ИИ) в качестве средства для обнаружения и предотвращения атак. Искусственный интеллект не может иметь корыстного умысла, следовательно, он не подвержен коррупции; при этом ИИ обладает всеми современными умениями, знаниями и компетенциями, в частности возможностью проанализировать большой объем данных и выявить аномальные шаблоны и поведение, которые могут указывать на нападение или вторжение. Системы на основе ИИ могут автоматически реагировать на такие угрозы и принимать соответствующие меры для защиты информации.

Другим инновационным методом является применение блокчейна для обеспечения безопасности и надежности цифровой информации. Блокчейн – это децентрализованная система хранения данных, которая гарантирует целостность и невозможность подмены или подделки информации. Путем использования блокчейна можно создать систему, в которой все транзакции и доступ к информации записываются и отслеживаются, обеспечивая прозрачность и безопасность данных.

Также одним из новейших инновационных методов борьбы с киберпреступностью является использование квантовых компьютеров. Квантовые компьютеры используют принципы квантовой механики, что их делает значительно более мощными и быстрыми по сравнению с традиционными компьютерами. Это открывает новые возможности для разработки алгоритмов и систем защиты, которые могут справиться с сложными шифровальными алгоритмами, используемыми киберпреступниками.

В конечном итоге, борьба с киберпреступностью требует постоянного развития и применения инновационных методов [Багрецов, Шунякова, 2023]. Внедрение искусственного интеллекта, блокчейна и квантовых компьютеров открывает новые горизонты в области кибербезопасности, улучшая защиту информации и снижая уязвимость перед угрозами киберпреступников. Объединение этих методов позволяет создать эффективную систему, способную отвечать вызовам современного цифрового мира и обеспечивать защиту цифровых активов.

Библиография

1. Багрецов Д.Н. Некоторые аспекты цифровизации в области народного образования // Молодежь и наука. 2023. № 7.
2. Багрецов Д.Н. Общественный порядок и коллективная безопасность как центральные идеологемы для консолидации общества и основа педагогической деятельности в гуманитарной сфере // Молодежь и наука. 2023. № 7.
3. Багрецов Д.Н., Шунякова О.В., Альтшулер-Феррейра О.Л. Коммуникативные стратегии киберпреступности // Материалы II Всероссийской научно-практической конференции «Уголовно-процессуальное и технико-криминалистическое обеспечение для борьбы с киберпреступлениями в современном обществе». Тамбов: Перо, 2023. С. 8-11.
4. Рубанов А. Аз Иванов. Выход в деньги // Время вышло. Современная русская антиутопия. М.: Альпина-нонфикшн, 2022. С. 23.
5. Что такое киберпреступность? Защита от киберпреступности \\ Kaspersky. URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime.
6. Эксперты назвали низкую цифровую грамотность россиян причиной роста киберпреступности // Форбс. URL: https://www.forbes.ru/tekhnologii/455881-eksperty-sprognozirovali-rost-userba-ot-kiberprestupnosti-v-rossii-do-165-mlrd-rublej.
7. Holt T., Bossler A. Cybercrime in progress: Theory and prevention of technology-enabled offenses. – Routledge, 2015.
8. Das S., Nayak T. Impact of cybercrime: Issues and challenges //International journal of engineering sciences & Emerging technologies. – 2013. – Т. 6. – №. 2. – С. 142-153.
9. Gordon S., Ford R. On the definition and classification of cybercrime //Journal in computer virology. – 2006. – Т. 2. – С. 13-20.
10. Anderson R. et al. Measuring the cost of cybercrime //The economics of information security and privacy. – 2013. – С. 265-300.

The fight against cybercrime is one of the most important modern tasks of the state and civil society

Dmitrii N. Bagretsov

PhD in Philology,
Associate Professor of the Department of Foreign Languages,
Ural Law Institute of the Ministry of Internal Affairs of Russia,
620057, 66 Korepina str., Ekaterinburg, Russian Federation;
e-mail: Bagretsov@mail.ru

Abstract

The article examines cybercrime and the fight against it as one of the leading challenges of our time. The importance of this task and innovative approaches to it are assessed. Cybercrime includes a wide range of activities, including computer attacks, identity theft, financial fraud, distribution of malware and many other forms of illegal activity online. Such crimes not only threaten the financial

security and personal data of individuals, but also have the potential to cause serious damage to the business sector and even states. According to the author's conclusions, the fight against cybercrime requires constant development and application of innovative methods. The introduction of artificial intelligence, blockchain and quantum computers opens up new horizons in the field of cybersecurity, improving information security and reducing vulnerability to cybercriminal threats. Combining these methods allows you to create an effective system that can meet the challenges of the modern digital world and ensure the protection of digital assets.

For citation

Bagretsov D.N. (2024) Bor'ba s kiberprestupnost'yu kak odna iz vazhneishikh sovremennykh zadach gosudarstva i grazhdanskogo obshchestva [The fight against cybercrime is one of the most important modern tasks of the state and civil society]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 14 (2A), pp. 185-190. DOI: 10.34670/AR.2024.64.19.035

Keywords

Cybercrime, it-crimes, information protection, information society.

References

1. Bagretsov D.N. (2023) Nekotorye aspekty tsifrovizatsii v oblasti narodnogo obrazovaniya [Some aspects of digitalization in the field of public education]. *Molodezh' i nauka* [Youth and Science], 7.
2. Bagretsov D.N. (2023) Obshchestvennyi poryadok i kollektivnaya bezopasnost' kak tsentral'nye ideologemy dlya konsolidatsii obshchestva i osnova pedagogicheskoi deyatel'nosti v gumanitarnoi sfere [Public order and collective security as central ideologies for the consolidation of society and the basis of pedagogical activity in the humanitarian sphere]. *Molodezh' i nauka* [Youth and Science], 7.
3. Bagretsov D.N., Shunyakova O.V., Al'tshuler-Ferreira O.L. (2023) Kommunikativnye strategii kiberprestupnosti [Cybercrime Communication Strategies]// *Materialy II Vserossiiskoi nauchno-prakticheskoi konferentsii «Ugolovno-protsessual'noe i tekhniko-kriminalisticheskoe obespechenie dlya bor'by s kiberprestupleniyami v sovremennom obshchestve»* [Proc. All-Russian Conf. "Criminal procedural and technical forensic support for combating cybercrime in modern society."]. Tambov: Pero Publ., pp. 8-11.
4. Chto takoe kiberprestupnost'? Zashchita ot kiberprestupnosti [Time's up. Modern Russian dystopia]. *Kaspersky*. Available at: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime [Accessed 12/03/2024].
5. Eksperty nazvali nizkuyu tsifrovuyu gramotnost' rossiyan prichinoi rosta kiberprestup nosti [Experts called the low digital literacy of Russians the reason for the increase in cybercrime]. *Forbs*. Available at: https://www.forbes.ru/tekhnologii/455881-eksperty-sprognozirovali-rost-userba-ot-kiberprestupnosti-v-rossii-do-165-mlrd-rublej [Accessed 12/03/2024].
6. Rubanov A. (2022) Az Ivanov. Vykhod v den'gi [Az Ivanov. Out of money]. *Vremya vyshlo. Sovremennaya russkaya antiutopiya* [Time's up. Modern Russian dystopia]. Moscow: Al'lpina-nonfikshn, Publ.
7. Holt, T., & Bossler, A. (2015). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.
8. Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. International journal of engineering sciences & Emerging technologies, 6(2), 142-153.
9. Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in computer virology, 2, 13-20.
10. Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. The economics of information security and privacy, 265-300.