УДК 33 **DOI: 10.34670/AR.2022.76.86.031**

Глобализация киберугрозы в современном мире

Ахмедов Равиль Тофиг оглы

Студент,
Финансовый университет при Правительстве Российской Федерации,
125993, Российская Федерация, Москва, Ленинградский просп., 49;
e-mail: ravil.ahmedov.00@mail.ru

Сайдаев Адам Мумадиевич

Студент,
Финансовый университет при Правительстве Российской Федерации,
125993, Российская Федерация, Москва, Ленинградский просп., 49;
e-mail: Adam.saedaev@mail.ru

Аннотация

Исследование посвящено вопросу проблем и перспектив киберугрозы. Цель работы – рассмотрение киберпреступлений и способы их противодействия, так как в мире данный вид преступления набирает обороты по мере того, как подключение к Интернету и другие аспекты информационных технологий распространяются по всему земному шару. Методология исследования сводится к статистическим данным, взятых из официальных источников, рассматривающих киберугрозу и на основе которых были сделаны выводы, что главная проблема кибербезопасности – это спекулятивный характер угроз, так как диапазон возможных угроз довольно широк как для правительств, так и для предприятий во всем мире. Были выделены положительные и отрицательные стороны по борьбе с киберугрозой, проанализирован ряд недостатков данных преступлений. Также в качестве объекта исследования в работе была затронута сфера здравоохранения, которая набирает все более высокую популярность среди целей современных хакеров, по причине глобальной пандемии «COVID-19», тем самым подвергают к угрозам и рискам жизни пациентов. В статье также рассмотрен глобальный рынок кибербезопасности и приводилась сравнительная статистика, которая указывает, что стоимость рынка вырастет до 270 млрд. долларов к 2026 году, в связи с тем, что растет привлекательность цифровизации, а хакерские атаки по причине сложившейся ситуации будут продолжать расти. Сделан вывод, что в перспективе мир будет сталкиваться с незначительными угрозами и потребуется эффективная разработка передовых технологий, чтобы предотвратить дальнейшие атаки хакеров.

Для цитирования в научных исследованиях

Ахмедов Р.Т., Сайдаев А.М. Глобализация киберугрозы в современном мире // Экономика: вчера, сегодня, завтра. 2022. Том 12. № 3А. С. 257-265. DOI: 10.34670/AR.2022.76.86.031

Ключевые слова

Киберугроза, информационные технологии, ИТ-преступления, мошенничество, хакеры, COVID-19, здравоохранение, электронная почта.

Введение

Технологии произвели революцию во взаимосвязанности земного шара. Флагманом этой глобализации является Интернет. Однако, как все предшествующие технологии взаимосвязи, Интернет может превратиться в некое оружие в интересах государств, преступников и террористов. Терминологии вроде «кибервойна» или «киберконфликт» сбили с толку различных специалистов и экспертов в области информационных технологий так как вызвали все более отчаянные споры о том, как нужно исправить и реагировать на такие ситуации, данная проблематика развития уже многократно становилась предметом научных исследований [Идрисов, 2022].

Вопросы и проблемы, связанные с изучением киберугрозы нашли свое отражение в научных работах авторов: Агаркова А.А., Синицына В.А. [Агаркова, Синицына, 2021], Гладыча Н.В. [Гладыч, 2021], Прончева Г.Б. [Прончев, 2022] и др.

Поскольку государства-члены ООН изо всех сил пытаются защитить свои сети и связанную инфраструктуру от сбоев и атак из-за рубежа, технологии будущего стали жизненно важным средством в нашу эпоху. Анонимность атак - основная часть проблемы, так как злоумышленники могут оперативно вывести из строя индивидуальных пользователей, государственные учреждения и частные фирмы, не раскрывая, кто осуществил атаку в первую очередь.

Целью представленного исследования является анализ киберпреступлений в современном мире и выявление уязвимостей рисков хакерских атак.

Методология исследования основывается на достоверных источниках, которые приводят официальные статистики.

Основная часть

В условиях непрерывно интегрирующейся глобальной экономики перспектива киберугроз нависает над всеми. ООН остается наиболее значимым форумом для решения глобальных проблем. Для противодействия этим угрозам были предприняты важные шаги, в том числе в рамках Генеральной Ассамблеи, Совета Безопасности и нескольких технических организаций ООН [Наркулов, 2022]. В них установлены важные принципы, которыми будут руководствоваться международные действия. Если страны-участницы хотят выработать действительно универсальный подход к решению проблем киберпространства, необходимо проделать дополнительную работу.

Многие государства хотят, чтобы все сообщество ООН играло активную роль в реагировании на угрозы, исходящие от кибератак. По их мнению, необходимо приложить больше усилий для решения этого вопроса на Генеральной Ассамблее, тем более что именно здесь согласовываются глобальные моральные принципы. Текущая неоднозначность кибератак оставляет под сомнение давние вопросы об определении и значении атаки, и ее последствиях. Двусмысленность, несомненно, помогает злоумышленникам, которые будет использовать Интернет в злонамеренных целях.

Основная часть. Основная часть кибератак была в значительной степени приписана различным хакерам и отдельным террористическим организациям, но были заметные нападения со стороны государств на другие субъекты за последние несколько лет. Ниже приведены несколько ярких примеров атак, направленных на нарушение информационных сетей, доступ к важным материалам, уничтожение данных или введение в заблуждение общественности разных штатов.

1) В 2009–2010 годах Соединенные Штаты и Израиль запустили вирус, известный как «Stuxnet», Flame или Olympic Games, против иранских центрифуг по обогащению урана на своей территории [Корнилов, Лобанова, Жерновая, 2022]. Атака Stuxnet остановила 10% иранских мощностей по обогащению урана на полный год и задержала Ядерные планы Ирана. Широко распространено мнение, что они действовали путем нацеливания на ядерные центрифуги с помощью флэш-накопителей, а не через Интернет. Даже спустя 10 лет «Stuxnet» остается одним из самых успешных и наглядных примеров того, чего может достичь кибератака. Он вызвал широкую похвалу и осуждение в международном сообществе, причем некоторые рассматривают его как прецедент того, как киберпространство будет использоваться в будущем;

2) В Австралии с июня 2020 года резко возросло количество атак тех, кого сам премьер-министр страны Скотт Моррисон назвал «злонамеренным» и «изощренным» государственным субъектом. Атаки были широко распространены, затронув правительство, промышленность, образование, здравоохранение и критически важную инфраструктуру, но без серьезного ущерба [Казарян, 2022]. Австралийские эксперты считают, что виновником является Китай, главным образом потому, что атаки произошли после того, как Австралия открыто поставила под сомнение происхождение коронавируса. Эти и многие другие случаи демонстрируют, что кибератаки являются далеко идущим средством проецирования государственной власти с целью негативного воздействия на другое государство или сообщество.

В 2021 году число кибер-инцидентов, связанных с COVID-19, выросло в пять раз за первые две недели марта как в Европе, так и в Российской Федерации. Это показывает, как киберпреступники с самого начала нашли значительный источник использования для этой проблемы. Что касается месяцев с мая по июнь 2020 года, то около 60% электронных писем, полученных пользователями, имели мошеннические цели, включая фишинговые или вредоносные программы.

Кроме того, примерно 40% отправленных электронных писем, связанных с COVID-19, являются спамом или направлены на получение конфиденциальной информации от пользователей (см. Рисунок 1)

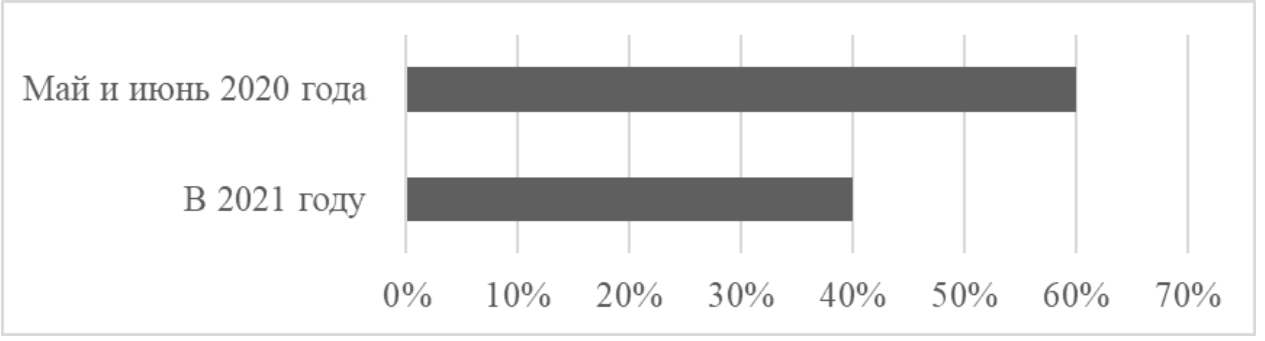

Рисунок 1 - Мошеннические схемы с помощью электронных писем (фишинги) 2020-2021 гг. [Число киберпреступлений в России, www]

Увеличение числа кибератак в летний период вызывает серьезную озабоченность экспертов, поскольку все больше и больше организаций всех размеров становятся полностью неработоспособными в результате атаки вымогателей. В то же время потребители становятся все более равнодушными к кибератакам. Наблюдалось значительное снижение уровня терпимости потребителей к тем компаниям, с которыми они работают и которые, возможно, подверглись кибератаке.

Глобальный рынок кибербезопасности в настоящее время оценивается в 173 миллиарда долларов и, по прогнозам, достигнет 270 миллиардов долларов к 2026 году (см. Рисунок 2).

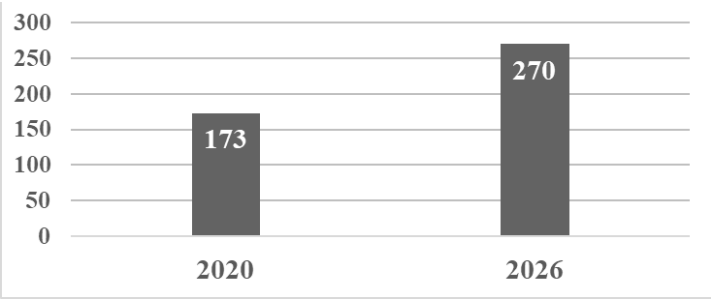

Рисунок 2 - Стоимость глобального рынка кибербезопасности (в млрд. $) [там же]

Крупные компании относятся к кибербезопасности более серьезно, чем когда-либо прежде. Кибератаки и мошенничество с данными были третьими по величине коммерческими проблемами, связанными с COVID. Это вызов для многих организаций, но также и возможность для стартапов, поскольку инвестиции в эти типы киберкомпаний продолжают увеличиваться с каждым годом. Поскольку тенденции в области кибербезопасности развиваются с экспоненциальной скоростью из года в год, корпоративные и деловые партнеры должны объединить усилия, чтобы не отставать [Султыгова, Кунцман, 2021].

Многие компании продвигают свои цифровые бизнес-инициативы, принимая решения о кибербезопасности практически каждый день. Рост кибер-рисков реален, но также реальны и решения для обеспечения безопасности данных. Например, существуют инструменты, которые точно оценивают, почему сотрудники переходят по определенным фишинговым электронным письмам. Эти инструменты используют данные в режиме реального времени для оценки сложности и качества фишинговых атак, чтобы помочь организациям понять, в чем заключаются их уязвимости [Гладыч, 2021].

В связи с этим многие компании регулярно проводят тренинги по фишингу, чтобы узнать, могут ли их сотрудники отличать реальные письма от фишинговых [Ермакова, Чаплыгина, 2022]. Эти тренинги направлены на повышение бдительности сотрудников и обучение их обнаружению признаков атак. Организации, которые хорошо информированы о новых технологиях и соответствующих угрозах, будут в лучшем положении для принятия выигрышных решений.

В 3 квартале 2020 года наблюдалось замедление взрывного роста активности злоумышленников, сопровождавшего начало пандемии COVID-19 в начале года, но число нападений остается стабильно высоким, и рост числа инцидентов по сравнению с предыдущим кварталом продолжает расти. В 3 квартале 2020 года количество атак выросло по сравнению со 2 кварталом (на 2,7%) и 3 кварталом 2019 года (на 54%), как это продемонстрировано на статистике, описанной ниже (см. Рисунок 3.)

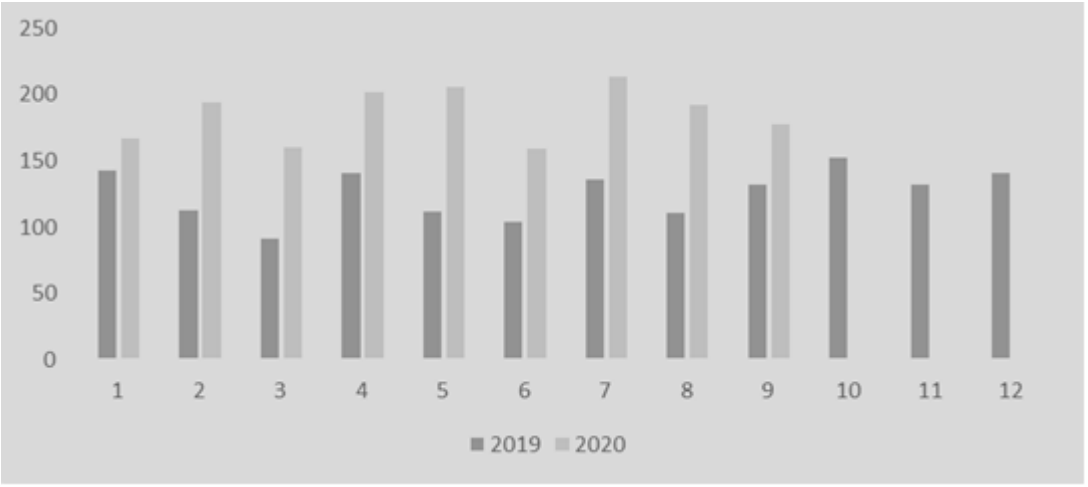

Рисунок 3 - Количество инцидентов в месяцах с 2019 по 2020 год (1=январь, 12=декабрь) [Количество инцидентов в сфере киберпреступлений, www]

Как и прежде, электронная почта является основным вектором, используемым для взлома внутренних корпоративных сетей и доставки вредоносных программ, также наблюдался последовательный ежеквартальный рост использования уязвимостей по периметру корпоративной сети для распространения вредоносных программ. Например, как отмечают исследователи Хеймдаля, операторы «Netwalker» доставляли вымогателей жертвам через фишинговые электронные письма до апреля 2020 года [Зиновьева, Пахомов, 2021]. Именно тогда они изменили подходы и начали использовать уязвимости в непроверенных VPN-решениях, пароли RDP (Remote Desktop Protocol) для удаленного доступа brute force (метод угадывания пароля) и поиск уязвимостей в веб-приложениях.

Эта тенденция была усилена пандемией, поскольку компании срочно сделали доступными услуги по периметру, которые ранее были ограничены только локальной сетью [Агаркова, Синицына, 2021]. Периметр быстро изменился, и многие организации не смогли в достаточной степени обеспечить безопасность этих услуг или просто не имели для этого достаточно времени. Большинство компаний частично или полностью были переведены на удаленный доступ, что делает инвентаризацию доступных извне ресурсов и эффективный процесс управления уязвимостями более важными, чем когда-либо [Прончев, 2022].

С февраля 2020 года COVID-19 вызывает серьезную озабоченность почти во всех странах мира. Это особенно актуально для учреждений здравоохранения, которые продолжают работать в условиях колоссального бремени. Тем самым киберпреступники пользуются эпидемией. В третьем квартале наблюдалось больше атак, направленных именно на подобные учреждения, как это демонстрирует статистика, приведенная ниже (см. Рисунок 4).

Половина атак на здравоохранение была совершена вымогателями с болезненными последствиями. В начале февраля российские больницы подверглись кибератакам из Европы. Врачи не могли получить доступ к результатам анализов или рецептам пациентов, а также получать данные с диагностических устройств или оказывать помощь пациентам [Клебанов, Полубинская, 2021]. Компьютеры были отключены, и все необходимые данные, хранящиеся в электронном виде, были зашифрованы злоумышленниками.

Пострадали далеко не только клиники и больницы. Злоумышленники даже нацеливаются на исследовательские центры, работающие над вакциной против COVID-19. В сентябре 2020 года

исследовательские центры в Испании подверглись нападению. Основной целью злоумышленников было получение информации о разработке и тестировании [Иджитканлар, Кугурульо, 2022].

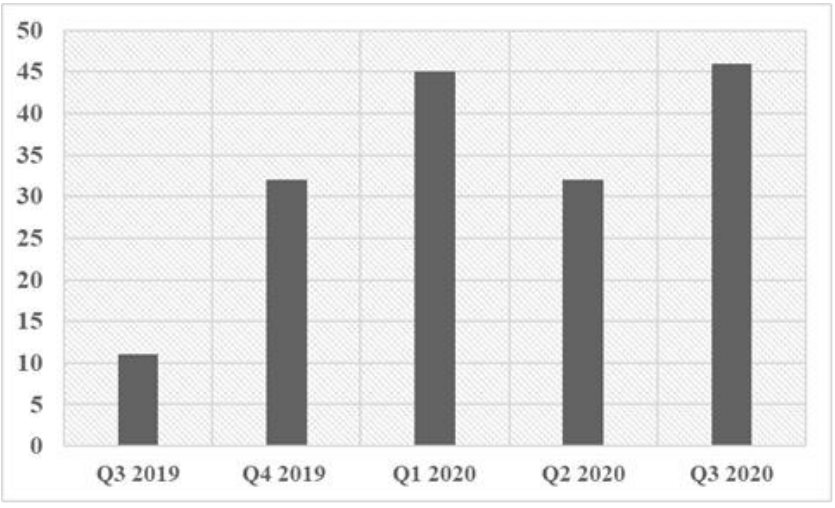

Рисунок 4 - Количество нападений на здравоохранение («Q – квартал») [Шифровальщики…, www]

В предыдущем квартале фишинговые сообщения, как правило, предлагали средства индивидуальной защиты или дополнительную информацию о вирусе, но теперь, чаще всего, вместо этого они используют интерес к вакцине [Черепашкин, 2021]. В одном письме, адресованном жителям Соединенного Королевства, утверждалось, что местные усилия по вакцинации продвигаются медленно, и предлагалась предполагаемая вакцина для продажи на сайте канадской аптечной сети. Говоря вкратце, подвох заключался в том, что ссылка вела на мошеннический сайт, предлагающий подделки.

Заключение

Нет никаких сомнений в том, что кибератаки участились в течение многих лет и что кризис COVID-19 только усугубил эту проблему. Из данных, которые были упомянуты в исследовании следует сделать важный вывод о том, что основным фактором, с которым необходимо бороться, чтобы предотвратить атаки, которые в настоящее время растут, является человеческий фактор. Очевидно, что также необходимы передовые технологии и протоколы безопасности, но обучение, как для сотрудников, так и для потребителей, вероятно, является наиболее важным фактором в настоящее время в предотвращении мошенничества.

Поэтому крайне важно сосредоточиться на продвижении передовых методов, чтобы пользователи могли идентифицировать и отклонять подозрительные электронные письма, проверять отправителей и URL-адреса, прежде чем переходить на них, и не предоставлять конфиденциальные данные, даже будучи на 100% уверенными в получателе и т.д.

В настоящее время киберпространство рассматривается как расширение международного права, а это означает, что кибератаки рассматриваются как юридически то же самое, что и физические атаки, а не как отдельная проблема. Генеральная ассамблея и Совет Безопасности проявляют некоторый интерес к противодействию киберугрозам путем создания новых норм

реагирования, но разрыв между международными опасностями и национальными возможностями в киберпространстве снижает потенциал для решительных действий ООН, даже когда они наиболее необходимы.

Библиография

1. Агаркова А.А., Синицына В.А. Киберпреступность в современной России // Международный журнал гуманитарных и естественных наук. 2021. № 10. С. 13-16.
2. Гладыч Н.В. Особенности квалификации финансовых преступлений в киберпространстве // Российское право: образование, практика, наука. 2021. № 3. С. 10-15.
3. Ермакова А.Л., Чаплыгина В.Н. Фишинг как распространенное киберпреступление современности // Закон и право. 2022. № 2. С. 149-151.
4. Зиновьева Н.С., Пахомов С.В. К вопросу об обнаружении, изъятии и использовании компьютерной информации, преобразованной методами криптографии, в ходе раскрытия и расследования преступлений: постановка проблемы // Философия права. 2021. № 2 (97). С. 117-121.
5. Иджитканлар Т., Кугурульо Ф. Устойчивость искусственного интеллекта: взгляд урбаниста сквозь призму концепции умного и устойчивого города // Городские исследования и практики. 2022. № 1. С. 35-64.
6. Идрисов И.К., Вердиев М.А. Основные направления противодействия киберпреступности // StudNet. 2022. № 3. С. 1331-1340.
7. Казарян К.К., Белан В.В. Кибервойна // StudNet. 2022. № 1. С. 575-584.
8. Клебанов Л.Р., Полубинская С.В. Цифровое здравоохранение, пандемия COVID-19 и проблемы кибербезопасности // Вестник Томского государственного университета. 2021. № 468. С. 243-252.
9. Количество инцидентов в сфере киберпреступлений. URL: https://www.ptsecurity.com/ru-ru/
10. Корнилов А.А., Лобанова Н.С., Жерновая О.Р. Обсуждение палестино-израильского конфликта в комитете британского парламента по иностранным делам (2014 год) // Научный диалог. 2022. № 2. С. 437-462.
11. Наркулов А. Нормативно-правовая база зарубежных стран и международных организаций в области противодействия кибертерроризму // Academic research in educational sciences. 2022. № 3. С. 217-224.
12. Прончев Г.Б. Киберпандемия в контексте пандемии коронавируса // Социально-гуманитарные знания. 2022. № 1. С. 143-150.
13. Султыгова А.А. Кунцман М.В. Киберпреступность как следствие цифровизации экономики // Экономика и бизнес: теория и практика. 2021. № 9-2. С. 88-91.
14. Черепашкин А.С., Тансыкова А.Ш. Противодействие киберпреступности в России: уголовно-правовые и криминологические аспекты // Вестник Уральского института экономики, управления и права. 2021. № 3 (56). С. 63-66.
15. Число киберпреступлений в России. URL: https://www.tadviser.ru/index.php
16. Шифровальщики: атаки на здравоохранение. URL: https://www.kaspersky.ru/blog/ransomware-vs-healthcare/30604/
17. Asgarov B.M., Mustafayev M.H. Justification of the cognition subject problem in the methodology of contemporary human // Opcion / Venezuela: Universidad del Zulia, Vol. 34, Núm. 86-2 (2018), pp. 376-384
18. Аскеров Б.М. О некоторых проблемах использования оперативно-розыскной информации в уголовном судопроизводстве // Пробелы в российском законодательстве. М., 2017, № 4, с.68-76;
19. Васяев А. А. Исследование доказательств в ходе судебного следствия в суде первой инстанции в российском уголовном процесса: автореф. дис … канд. юрид. наук. Саранск, 2008. 24 с.

Globalization of cyberthreats in the modern world

Ravil' T. Akhmedov

Graduate Student,
Financial University under the Government of the Russian Federation,
125993, 49, Leningradskii ave., Moscow, Russian Federation;
e-mail: ravil.ahmedov.00@mail.ru

Adam M. Saidaev

Graduate Student,
Financial University under the Government of the Russian Federation,
125993, 49, Leningradskii ave., Moscow, Russian Federation;
e-mail: Adam.saedaev@mail.ru

Abstract

This study is devoted to the issue of problems and prospects of cyber threats. The purpose of this work is to consider cybercrime and how to counter it, as in the world this type of crime is gaining momentum as the connection to the Internet and other aspects of information technology spread around the globe. The research methodology boils down to statistical data that were taken from official sources considering the cyber threat and on the basis of which it was concluded that the main problem of cyber security is the speculative nature of threats, since the range of possible threats is quite wide for both governments and enterprises in around the world. The positive and negative aspects of combating the cyber threat were also highlighted a number of shortcomings of these crimes were analyzed. Also, as an object of study in this work, the healthcare sector was affected, which is gaining more and more popularity among the targets of modern hackers, due to the global COVID-19 pandemic, thereby exposing patients to threats and risks. The article also examined the global cybersecurity market and provided comparative statistics that indicate that the market value will grow to $270 billion by 2026, due to the growing attractiveness of digitalization, and hacker attacks due to the current situation will continue to grow. It was concluded that in the long run, the world would face minor threats and the effective development of advanced technologies would be required to prevent further attacks by hackers.

For citation

Akhmedov R.T., Saidaev A.M. (2022) Globalizatsiya kiberugrozy v sovremennom mire [Globalization of cyberthreats in the modern world]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 12 (3A), pp. 257-265. DOI: 10.34670/AR.2022.76.86.031

Keywords

Cyber threat, information technology, IT crime, fraud, hackers, COVID-19, healthcare, e-mail.

References

1. Agarkova A.A., Sinitsyna V.A. (2021) Kiberprestupnost' v sovremennoi Rossii [Cybercrime in modern Russia]. *Mezhdunarodnyi zhurnal gumanitarnykh i estestvennykh nauk* [International Journal of the Humanities and Natural Sciences], 10, pp. 13-16.
2. Cherepashkin A.S., Tansykova A.Sh. (2021) Protivodeistvie kiberprestupnosti v Rossii: ugolovno-pravovye i kriminologicheskie aspekty [Counteracting cybercrime in Russia: criminal law and criminological aspects]. *Vestnik Ural'skogo instituta ekonomiki, upravleniya i prava* [Bulletin of the Ural Institute of Economics, Management and Law], 3 (56), pp. 63-66.
3. *Chislo kiberprestuplenii v Rossii* [Number of cybercrimes in Russia]. Available at: https://www.tadviser.ru/index.php [Accessed 03/03/2022]
4. Ermakova A.L., Chaplygina V.N. (2022) Fishing kak rasprostranennoe kiberprestuplenie sovremennosti [Fishing as a common modern cybercrime]. *Zakon i pravo* [Law and Right], 2, pp. 149-151.
5. Gladych N.V. (2021) Osobennosti kvalifikatsii finansovykh prestuplenii v kiberprostranstve [Features of qualifying financial crimes in cyberspace]. *Rossiiskoe pravo: obrazovanie, praktika, nauka* [Russian law: education, practice,

science], 3, pp. 10-15.
6. Idrisov I.K., Verdiev M.A. (2022) Osnovnye napravleniya protivodeistviya kiberprestupnosti [The main directions of combating cybercrime]. *StudNet*, 3, pp. 1331-1340.
7. Ijitkanlar T., Kugurulyo F. (2022) Ustoichivost' iskusstvennogo intellekta: vzglyad urbanista skvoz' prizmu kontseptsii umnogo i ustoichivogo goroda [Sustainability of artificial intelligence: an urbanist's view through the prism of the concept of a smart and sustainable city]. *Gorodskie issledovaniya i praktiki* [Urban Research and Practice], 1, pp. 35-64.
8. Kazaryan K.K., Belan V.V. (2022) Kibervoina [Cyberwar]. *StudNet*, 1, pp. 575-584.
9. Klebanov L.R., Polubinskaya S.V. (2021) Tsifrovoe zdravookhranenie, pandemiya COVID-19 i problemy kiberbezopasnosti [Digital Health, COVID-19 Pandemic and Cybersecurity Issues]. *Vestnik Tomskogo gosudarstvennogo universiteta* [Tomsk State University Bulletin], 468, pp. 243-252.
10. *Kolichestvo intsidentov v sfere kiberprestuplenii* [Number of cybercrime incidents]. Available at: https://www.ptsecurity.com/ru-ru/ [Accessed 03/03/2022]
11. Kornilov A.A., Lobanova N.S., Zhernovaya O.R. (2022) Obsuzhdenie palestino-izrail'skogo konflikta v komitete britanskogo parlamenta po inostrannym delam (2014 god) [Discussion of the Palestinian-Israeli conflict in the British Parliament Foreign Affairs Committee (2014)]. *Nauchnyi dialog* [Scientific Dialogue], 2, pp. 437-462.
12. Narkulov A. (2022) Normativno-pravovaya baza zarubezhnykh stran i mezhdunarodnykh organizatsii v oblasti protivodeistviya kiberterrorizmu [Regulatory framework of foreign countries and international organizations in the field of countering cyberterrorism]. *Academic research in educational sciences*, 3, pp. 217-224.
13. Pronchev G.B. (2022) Kiberpandemiya v kontekste pandemii koronavirusa [Cyberpandemic in the context of the coronavirus pandemic]. *Sotsial'no-gumanitarnye znaniya* [Social and Humanitarian Knowledge], 1, pp. 143-150.
14. *Shifroval'shchiki: ataki na zdravookhranenie* [Cryptographers: attacks on healthcare]. Available at: https://www.kaspersky.ru/blog/ransomware-vs-healthcare/30604/ [Accessed 03/03/2022]
15. Sultygova A.A. Kuntsman M.V. (2021) Kiberprestupnost' kak sledstvie tsifrovizatsii ekonomiki [Cybercrime as a consequence of the digitalization of the economy]. *Ekonomika i biznes: teoriya i praktika* [Economics and business: theory and practice], 9-2, pp. 88-91.
16. Zinov'eva N.S., Pakhomov S.V. (2021) K voprosu ob obnaruzhenii, iz''yatii i ispol'zovanii komp'yuternoi informatsii, preobrazovannoi metodami kriptografii, v khode raskrytiya i rassledovaniya prestuplenii: postanovka problemy [On the issue of detection, seizure and use of computer information converted by cryptography methods in the course of crime detection and investigation: problem statement]. *Filosofiya prava* [Philosophy of Law], 2 (97), pp. 117-121.
17. Asgarov B.M., Mustafayev M.H. Justification of the cognition subject problem in the methodology of contemporary human // Opcion / Venezuela: Universidad del Zulia, Vol. 34, Núm. 86-2 (2018), pp. 376-384
18. Askerov B.M. On some problems of using operational-investigative information in criminal proceedings // Gaps in Russian legislation. M., 2017, No. 4, pp.68-76;
19. Vasyaev A. A. Investigation of evidence during the judicial investigation in the court of first instance in the Russian criminal process: autoref. dis... cand. jurid. sciences'. Saransk, 2008. 24 p.