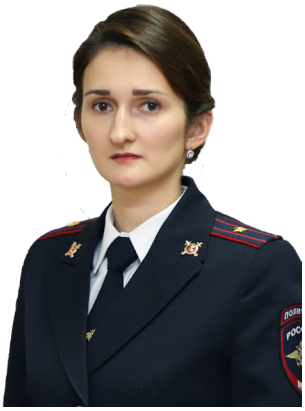
Научная статья
УДК 343.8+338.2
DOI: 10.37973/KUI.2022.21.24.007

СОВРЕМЕННЫЕ ПРОБЛЕМЫ БЕЗОПАСНОСТИ НАЦИОНАЛЬНОЙ ЭКОНОМИКИ В УСЛОВИЯХ ЕЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ



Лейсан Рафиковна Назмеева,
Казанский юридический институт МВД России, Казань, Россия,
nazmeevalr@mail.ru

Аннотация

Введение: статья посвящена исследованию проблем обеспечения экономической безопасности в условиях цифровизации экономики и определению подходов, способствующих ее укреплению.

Материалы и методы: методологическую основу исследования составили общенаучные и частнонаучные методы познания, в частности, сравнительно-правовой, хронологический, статистический и другие методы. Материалами исследования послужили статистические данные Главного информационно-аналитического центра МВД России, Судебного департамента при Верховном Суде Российской Федерации, Экспертно-аналитического центра InfoWatch, а также опубликованные материалы Банка России и научные труды по проблематике исследования.

Результаты исследования: в статье проанализированы современные вызовы и угрозы экономической безопасности в условиях цифровизации экономики. Особое внимание уделено исследованию преступлений экономической направленности, совершаемых с использованием информационных технологий.

Обсуждение и заключения: автором сформулированы основные направления минимизации наиболее значимых вызовов и угроз безопасности национальной экономики.

Ключевые слова: экономическая безопасность; киберпреступность; вызовы и угрозы безопасности; цифровизация; информационные технологии; цифровая трансформация

Для цитирования: Назмеева Л.Р. Современные проблемы безопасности национальной экономики в условиях ее цифровой трансформации // Вестник Казанского юридического института МВД России. 2022. Т. 13. № 3 (49). С. 69 – 78. DOI: 10.37973/KUI.2022.21.24.007

Scientific article
UDC 343.8
DOI: 10.37973/KUI.2022.21.24.007

MODERN SECURITY PROBLEMS OF NATIONAL ECONOMY DURING ITS DIGITAL TRANSFORMATION

Leysan Rafikovna Nazmeeva,
the Kazan Law Institute of MIA of Russia, Kazan, Russia,
nazmeevalr@mail.ru

Abstract

Introduction: the author studies the issues of economic security in the context of digitalization of the economy and the definition of approaches that contribute to its strengthening.

Materials and Methods: the methodological basis of the study consisted of general scientific and private scientific methods of knowledge, in particular, comparative legal, chronological, statistical and other methods. The materials of the study are statistical data of the Main Information and Analytical Center of

the Ministry of Internal Affairs of Russia, the Judicial Department under the Supreme Court of the Russian Federation, the Expert Analytical Center InfoWatch, as well as published materials of the Bank of Russia and scientific works on the subject of research.

Results: the article analyzes modern challenges and threats to economic security in the context of digitalization of the economy. Particular attention is paid to the study of economic crimes committed with the use of information technology.

Discussion and Conclusions: the author formulated the main directions of minimization of the most significant challenges and threats to national economic security.

Keywords: economic security; cybercrime; security challenges and threats; digitalization; information technology

For citation: Nazmeeva L.R. Modern Security Problems of National Economy During its Digital Transformation // Bulletin of the Kazan Law Institute of MIA of Russia. 2022. Vol. 13, No. 3 (49). P. 69 – 78. DOI: 10.37973/KUI.2022.21.24.007

Введение

В современных условиях стратегическое значение для обеспечения суверенитета, обороноспособности, безопасности государства и опережающего развития экономики приобретает внедрение в разные сферы жизни новых информационных технологий, информационных систем, средств телекоммуникации и связи.

На этапе цифровой трансформации экономики российское государство преодолевает воздействие внешних политизированных санкционных давлений, нарастающих новых форм противоправной деятельности с использованием информационных технологий, подрывающих социально-экономическую стабильность в обществе.

Обзор литературы

Цифровизация, выступая сравнительно новым процессом по внедрению инноваций в целях роста фактора конкурентоспособности страны, обусловливает увеличение угроз безопасности отечественной экономики. Актуальные аспекты обеспечения безопасности национальной экономики рассматривались в научных трудах О.С. Гурьянова, С.В. Лим, И.В. Филатовой и других авторов. Исследованию вызовов и угроз экономической безопасности посвящены работы Т.О. Графовой, А.Ф. Шаповалова [1], М.С. Кобышевой, А.А. Володина, М.В. Иванова, Т.Ю. Феофиловой, Т.М. Манасерян [2] и др.

Результаты исследования

Стратегией экономической безопасности Российской Федерации к числу главных угроз в области экономики отнесены высокий уровень криминализации в экономической сфере, уязвимость информационной инфраструктуры финансово-банковской системы, подверженность финансовой системы глобальным рискам[1].

Под влиянием общемировой рекапитализации экономического рынка (*реорганизации структуры капитала рыночной экономики для целей недопущения процедуры банкротства)*, роста числа киберпреступлений, формирования новых видов мошенничества с использованием информационных технологий [3], оттока из страны капитала (*не регулируемого государством стихийного вывоза капитала за рубеж юридическими и физическими лицами*)[2], масштабных кибератак на энергетический сектор, банковскую сферу, серверы компаний и др., а также последствий введения ограничительных мер из-за пандемии коронавирусной инфекции COVID-19 усилилось деструктивное воздействие на все социально-экономические процессы в российском обществе.

Негативное влияние волатильности (*изменчивости цен*) мировых товарных рынков модифицирует организованную преступность в большой теневой сектор экономики, обладающий транснациональным характером, с использованием информационно-телекоммуникационных технологий. Организованные криминальные сообщества, овладевая современными технологиями, проявляя повышенный интерес к передовым разработкам в области искусственного интеллекта, робототехники, Интернета вещей (*технологической концепции подключения физических объектов /компьютеров, планшетов, смартфонов, телевизоров и др./ к Интернету для удаленного управления ими*), технологии блокчейн (*быстрой, прозрачной передачи цифровой информации, включая деньги, интеллектуальную собствен-*

[1] О Стратегии экономической безопасности Российской Федерации на период до 2030 года: указ Президента Российской Федерации от 13.05.2017 № 208 // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения: 02.03.2021).

[2] Чистый отток капитала из России в январе – июне 2020 года вырос на 24%. URL: https://tass.ru/ekonomika/8937285 (дата обращения: 03.09.2020).

ность), активно инвестируют немалые средства в их развитие и адаптацию к решению своих криминальных задач.

Проведенный в ходе исследования анализ статистических данных Министерства внутренних дел Российской Федерации свидетельствует, что в период с января по апрель 2022 г. количество преступлений экономической направленности, совершенных с использованием информационно-телекоммуникационных технологий (*показатели сформированы в соответствии с Перечнем № 25, введенным в действие указанием Генеральной прокуратуры Российской Федерации и Министерства внутренних дел Российской Федерации*[1], составило 2957 ед., что на 8,9% больше аналогичного периода 2021 года, в 2021 г. – 18256 ед., что на 7,3% больше 2020 года (2020 г. – 17052 ед., что 71,3% больше 2019 года)[2].

Анализ отечественной судебной практики по материалам уголовных дел[3] за период с 2017 по 2021 год и статистических данных о состоянии преступности за период с 2020 по январь 2022 год[4] свидетельствует о тенденции роста количества преступлений, приобретающих профессионально-усложненный характер и предполагающих наличие высокого уровня знаний и навыков в сфере интернет-технологий.

Необходимо отметить, что рассматриваемая категория преступлений с использованием фактора удаленности совершается в сфере дистанционного банковского обслуживания с применением изощренных средств, методов и способов посягательства на информацию, а также трансформируемых механизмов совершения мошеннических схем с нацеленностью на определённые группы людей (хищение денежных средств с банковской карты, синхронизированной с мобильным банком, путем установки вредоносной программы на сотовый телефон[5]. Характерными примерами данной категории преступлений являются совершенные мошеннические действия по внесению в единые государственные реестры фиктивных сведений о юридических лицах и индивидуальных предпринимателях, завладению имуществом, активами физических и юридических лиц, в том числе с государственной долей в уставном капитале; дистанционные мошенничества, совершаемые лицами, отбывающими наказание в местах лишения свободы; тайные хищения в отношении электронных денежных средств [4**,** с. 22].

Проявляется высокий уровень криминализации преступлений и в финансово-кредитной (банковской) сфере, поскольку их характер напрямую коррелирует с состоянием информационной безопасности участников экономических отношений. Так, за период с январь по декабрь 2021 года выявлено 31435 преступлений, что на 0,4% больше аналогичного периода 2020 года (2020 г. – 31309 ед., что на 5,1% больше 2019 года)[6].

По статистическим данным Центра мониторинга и реагирования на компьютерные атаки в финансово-кредитной сфере Банка России, в первом квартале 2022 г. количество операций без согласия клиентов составила 258097 единиц[7], в 2021 году количество несанкционированных операций с использованием платежных карт составило 83900 единиц, в том числе 22,5% из этого количества совершено путем обмана или злоупотребления доверием методами социальной инженерии (*побуждения граждан к самостоятельному осуществлению операций*)[8], в 2020 году зафиксировано 48700 случаев использования платежных карт без согласия их владельцев в банкоматах или терминалах, из которых 15,8% операций произошло в результате использования приемов и методов социальной инженерии[9]. Об-

[1] О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности: указание Генеральной прокуратуры Российской Федерации и Министерства внутренних дел Российской Федерации № 790/11/1 от 29.12.2021// Состояние преступности в России за январь 2022 г. Министерство внутренних дел Российской Федерации: официальный сайт. URL: https://xn--b1aew.xn--p1ai/reports/item/28726056/ (дата обращения: 10.03.2022).

[2] Состояние преступности в России // Министерство внутренних дел Российской Федерации: официальный сайт. URL: https://xn--b1aew.xn--p1ai/folder/101762/ (дата обращения: 02.03.2022).

[3] Судебные и нормативные акты Российской Федерации. URL: https://sudact.ru/ (дата обращения: 04. 06.2022).

[4] Состояние преступности в России // Министерство внутренних дел Российской Федерации: официальный сайт. URL: https://xn--b1aew.xn--p1ai/folder/101762/ (дата обращения: 02.03.2022).

[5] Приговор № 1-3/2019 1-50/2018 1-580/2017 от 02.12.2019 по делу 1-3/2019. URL: http://sudact.ru/regular/doc/xbU4lTLIinWd/ (дата обращения: 28.12.2020); приговор № 1-25/2019 1-377/2018 от 09.12.019 по делу № 1-275/2018. URL: http://sudact.ru/regular/doc/hktokOrwZgbO/ (дата обращения: 28.12.2020).

[6] Состояние преступности в России // Министерство внутренних дел Российской Федерации: официальный сайт. URL: https://xn--b1aew.xn--p1ai/folder/101762/ (дата обращения: 02.03.2022).

[7] Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств 1 квартал 2022 г. //Банк России: официальный сайт. URL: https://www.cbr.ru/analytics/ib/review_4q_2022/(дата обращения: 06.06.2022).

[8] Обзор операций, совершенных без согласия клиентов финансовых организаций за 2021 год // Банк России: официальный сайт. URL: https://cbr.ru/analytics/ib/operations_survey_2021/ (дата обращения: 06.06.2022).

[9] Обзор операций, совершенных без согласия клиентов финансовых организаций за 2020 год // Банк России: официальный сайт. URL: https://www.cbr.ru/analytics/ib/fincert/ (дата обращения: 02.03.2022).

щая сумма ущерба по хищениям через банкоматы и терминалы в 2021 году выросла на 62,4% по сравнению с аналогичным показателем 2020 года (740,6 млн руб.) и составила свыше 1971,2 млн рублей[1].

Необходимо акцентировать внимание на том, что, несмотря на определенную закрытость банковской системы и предпринимаемые защитные меры, возникают новые возможности для осуществления неправомерного доступа к базе данных клиентов банков, а также неправомерного завладения денежными средствами с использованием средств сотовой связи, банковских карт, способствующие появлению явления фишинга *(вид интернет-мошенничества для получения доступа к паролям и логинам пользователей)*.

Отдельным видом преступлений, создающих дополнительную угрозу экономической безопасности в банковской сфере, выступает легализация (отмывание) денежных средств, полученных преступным путем. В этот процесс перехода криминальных денежных средств из теневого сектора экономики в легальные финансовые потоки вовлекаются различные секторы экономики (финансовый сектор, розничная торговля, сфера платных услуг и др.), нарушающие стабильность всех сфер общественной жизни [5, с. 75].

Высокий уровень киберугроз в финансовой сфере, снижение надежности современной мировой валютной системы способствуют появлению новых способов легализации криминальных денежных средств с привлечением профессионалов из финансовой, валютной и нормативной областей, использующих высокотехнологичные способы совершения безналичных расчетов и платежей (в системе электронных денег и в криптовалютной системе, в том числе с возможностью заключения смарт-контрактов), которые в последующем влекут сложности в выявлении и подавлении данных киберугроз [6, с. 85-86].

В современных условиях процесс повышения эффективности применения информации в обществе с помощью информационных технологий способствует возрастанию угроз неправомерного их распространения.

По экспертным данным российского экспертно-аналитического центра InfoWatch *(контролирующего около 50% российского рынка систем защиты конфиденциальных данных),* в 2021 г. в мире зарегистрировано 8420 млн утечек записей персональных данных и платежной информации[2], за период с января по сентябрь 2020 года в мире зарегистрировано 9,93 млрд утечек записей персональных данных и платежной информации, из них в России – 96,5 млн, что на 5,6% больше аналогичного года[3].

В период распространения пандемии коронавирусной инфекции COVID-19 введение временных ограничительных мер обязало субъектов малого и среднего бизнеса, ввиду недостаточной финансовой прочности в случае непредвиденных обстоятельств, осуществлять экономические отношения в киберсреде (в режиме удаленного доступа). При этом зачастую нарушаются требования информационной безопасности, что способствует совершению преступлений с использованием IT-технологий.

В результате проведенного исследования экспертами международной компании Positive Technologies (*создающей инновационные решения в сфере информационной безопасности*) установлено, что 80% опрошенных пользователей, работавших в режиме удалённого доступа, использовали домашние персональные компьютеры, а 57% респондентов не планировали менять способы организации удаленного доступа, не настроенные по стандартам информационной безопасности[4].

Осуществление деятельности в режиме удаленного доступа обусловило появление иных механизмов завладения обманным путем конфиденциальной информацией и денежными средствами, к числу которых следует отнести распространение писем, содержащих ссылку на вредоносный интернет-сайт, от имени Всемирной организации здравоохранения и Роспотребнадзора с ложными рекомендациями, рассылку сообщений в мессенджерах от Министерства финансов Российской Федерации о получении денежной компенсации из-за введенного режима самоизоляции [7, с. 39 – 43], продаже средств индивидуальной защиты, фармацевтической продукции.

Из неблагоприятных факторов угроз безопасности национальной экономики необходимо вы-

[1] Обзор операций, совершенных без согласия клиентов финансовых организаций за 2021 год // Банк России: официальный сайт. URL: https://cbr.ru/analytics/ib/operations_survey_2021/ (дата обращения: 06.06.2022).

[2] Отчёт об исследовании утечек информации ограниченного доступа в 2021 году// INFOWATCH.RU: официальный сайт. URL: https://www.infowatch.ru/ (дата обращения: 06.06.2022).

[3] Утечки информации ограниченного доступа: отчет за 9 месяцев 2020 // INFOWATCH.RU: официальный сайт. URL: https://www.infowatch.ru/analytics/analitika/utechki-informatsii-ogranichennogo-dostupa-otchet-za-9-mesyatsev-2020 (дата обращения: 10.03.2022).

[4] PositiveTechnologies: 80% опрошенных сотрудников российских компаний используют домашние компьютеры для удаленной работы // SECURITYLAB.RU: информационный портал по безопасности. URL: https://www.securitylab.ru/news/508002.php (дата обращения: 21.08.2020).

делить не контролируемый государством отток капитала из страны.

Согласно данным Центрального банка Российской Федерации, чистый отток капитала из страны в январе-марте 2022 г. вырос в 3,6 раза по сравнению с январем-мартом 2021 г. и составил 64,2 млрд[1], по итогам 2021 г. – 72 млрд (на 1,4 раза больше аналогичного периода 2020 г. (50,4 млрд)[2]. Причинами этого, по мнению авторов научных исследований [8, 9], в современных условиях цифровой экономики являются усиление внешних экономических санкционных давлений, тенденция снижения курса национальной валюты и уровня доверия населения к отечественным кредитным организациям, общие неблагоприятные условия формирования инвестиционного климата в стране.

Ключевыми элементами в этих условиях выступает минимизация данного процесса посредством скоординированных правовых, социально-экономических и других мероприятий на всех уровнях государственного управления. С этой целью в Российской Федерации предпринят комплекс мер по контролю за финансово-кредитными организациями, проводящими операции по переводу капитала и валютному регулированию.

Одной из мер, направленной на защиту национальных интересов России и ограничивающей возможность оттока валюты из страны, является подписание указа о применении специальных экономических мер в связи с недружественными действиями США и примкнувших к ним стран и международных организаций[3].

В условиях нарастающих новых форм противоправной деятельности с использованием информационных технологий особую актуальность приобретают программно-технические меры, средства защиты информации, и чрезвычайно важным становится выбор максимально эффективных технологий с минимальным количеством ложных срабатываний.

По результатам обобщения материалов исследований научно-исследовательского института Высшей школы экономики и данных российского экспертно-аналитического центра InfoWatch, одним из ключевых инструментов защиты информации, используемых в современном экономическом пространстве в условиях применения удаленного доступа к финансовым услугам, выступает антивирусное программное обеспечение [10, с. 135-136] информационной безопасности, киберустойчивости и повсеместного использования защищенных технологий.

В ходе совместного исследования независимой коммерческой организации «Роскачество» и Международной ассамблеи организаций потребительских испытаний (*International Consumer Research and Testing – ICRT*) установлено, что наиболее эффективными программно-техническими средствами обеспечения защиты от хакерских угроз выступают антивирусные программы иностранного производства для операционной системы Windows – Bitdefender Internet Security, ESET Internet Security, и только на втором месте выступает отечественная антивирусная программа – Kaspersky Internet Security – для операционной системы Macos[4].

В этих условиях представляется целесообразным непрерывное совершенствование отечественных линеек продуктов и решений информационных технологий для обеспечения высококачественной, надежной и безопасной передачи и хранения конфиденциальной (секретной, служебной, личной и другой) информации.

Одной из попыток улучшения продукции является предложенное в 2020 году «Лабораторией Касперского» интегрированное решение для защиты рабочих мест, выступающее мощной защитой и объединяющее целый ряд передовых технологий в едином решении, позволяющее адаптивно отвечать на актуальные вызовы в области кибербезопасности[5].

Отечественным производителям информационных и высоких технологий приходится сталкиваться с жесткой конкуренцией со стороны глобальных корпораций, лидирующих в данной индустрии и принуждающих инвестировать экономики своих стран за счет финансирования из российского бюджета [11, с. 383-384].

[1] Чистый отток капитала из России за квартал составил $64,2 млрд. URL: https://www.bfm.ru/news/497438 (дата обращения: 09.06.2022).

[2] Чистый отток капитала из России в 2021 году вырос в 1,4 раза. URL: https://rg.ru/2022/01/18/chistyj-ottok-kapitala-izrossii-v-2021-godu-vyros-v-14-raza.html (дата обращения: 10.03.2022).

[3] О применении специальных экономических мер в связи с недружественными действиями Соединенных Штатов Америки и примкнувших к ним иностранных государств и международных организаций: указ Президента РФ от 28.02.2022 № 79// rg.ru: Российская газета. Официальный сайт. URL: https://rg.ru/2022/02/28/prezident-ukaz79-site-dok.html (дата обращения: 10.03.2022).

[4] Антивирусы // RSKRF.RU: портал для умного покупателя. URL: https://rskrf.ru/ratings/tekhnologii/programmnoe-obespechenie/antivirusy/ (дата обращения: 28.12.2020).

[5] Интегрированное решение для защиты рабочих мест // KASPERSKY.RU: АО «Лаборатория Касперского»: официальный сайт. URL: https://www.kaspersky.ru/small-to-medium-business-security/endpoint-security-solution (дата обращения: 28.12.2020).

В условиях возрастающего санкционного давления, угрозы ограничения российского доступа к иностранному программному обеспечению (*например, официальный отказ в 2020 году дистрибутора продуктов Microsoft – компании «Софтлайн» предоставлять МГТУ им. Н.Э. Баумана программное обеспечение в связи с новыми экспортными ограничениями, введенными правительством США*[1]*; в 2022 году ограничение действия на территории России приложений: UAV Forecast, предназначенного для отслеживания погодных условий и безопасных полетных зон операторами летательных беспилотников*[2] *и Insydium, выпускающей плагины для графических программ*[3]) для целей эффективного противодействия новым схемам изощренных хакерских целевых атак могут оказаться полезными современные программно-технические средства защиты информации, сертифицированные ФСТЭК России.

Во исполнение требований российского законодательства в области защиты секретной информации, персональных данных, государственных систем на отечественном рынке появились средства защиты информации от несанкционированного доступа, сертифицированные Федеральной службой по техническому и экспортному контролю Российской Федерации, среди которых выделяется продукция компаний «Код Безопасности», «Конфидент» «ОКБ САПР», «Газинформсервис», НПП «Безопасные информационные технологии», «ТСС», «Рубинтех», «СПИИРАН», «РНТ»[4].

Возрастающая роль высоких технологий в национальной и мировой экономике обусловила изменение способов взаимодействия экономических субъектов, выраженной в активном развитии электронной коммерции (*форма коммерческой деятельности, где взаимодействие между участниками в целом или в некоторых его этапах происходит электронным способом [12, с. 32]),* определяемой не географическими или национальными границами, а распространением информационно-телекоммуникационных сетей.

Доступ к электронному информационному обмену способствует эффективности деятельности экономических субъектов за счет снижения транзакционных издержек, минимизации времени, затраченного для организации сделки, а также обеспечивает быстрое и точное получение информации, высокую скорость финансовых расчетов, предоставляет одинаковый доступ к рынку, как для крупных корпораций, так и для небольших организаций [13, с. 159].

Основные аспекты регулирования коммерческой деятельности, осуществляемой в Интернете, отражены в отдельных нормативных правовых актах: законе «О защите прав потребителей», Гражданском кодексе Российской Федерации, Федеральном законе «Об электронной подписи», Федеральном законе «О связи», Федеральном законе «Об информации, информационных технологиях и о защите информации» и т.д. Однако не сложилось единого, четко оформленного законодательного решения, обеспечивающего особую систему регулирования деятельности участников электронных операций в ходе осуществления продажи товаров и услуг в сети Интернет.

В качестве примера регулирования в Интернете коммерческой деятельности можно привести действующий в Китайской Народной Республике закон «Об электронной коммерции»[5], устанавливающий принципы и требования осуществления коммерческой деятельности посредством сети связи, предусматривающий правила поведения субъектов экономических отношений на электронных площадках.

Электронная среда, затрудняя идентификацию преступника, способствует появлению многоэпизодности преступлений, изощрённости схем их совершения, дестабилизации основных структур обеспечения жизнедеятельности.

Возрастающая нагрузка на органы внутренних дел по раскрытию преступлений с использованием информационных технологий обусловила в УМВД России по Мурманской области [14, с. 48] проведение процесса автоматизации контроля, сбора, учета сведений и анализа работы по уголовным делам путем разработки и в последующем осуществления опытной эксплуатации в составе программно-технического комплекса интегрированного банка данных коллективного пользования федерального уровня *(решение*

[1] Ведущий технический вуз попадает под санкции США за подготовку специалистов по вооружениям. URL: https://www.vedomosti.ru/technology/articles/2020/12/08/850139-microsoft-otkazalsya (дата обращения: 28.12.2020).

[2] Американское приложение для дронов закрыло бесплатную версию в России. URL: https://www.rbc.ru/technology_and_media/24/02/2022/6217a3d19a794736d6ac71a8 (дата обращения: 04.03.2022).

[3] Обойтись без иностранного софта: грозит ли России технологическая блокада // Газета.Ru (gazeta.ru). URL: https://www.gazeta.ru/tech/2022/02/25/14577109.shtml?updated (дата обращения: 04.03.2022).

[4] Обзор сертифицированных средств защиты информации от несанкционированного доступа (СЗИ от НСД). URL: https://www.anti-malware.ru/analytics/Market_Analysis/certified-unauthorized-access-security (дата обращения: 28.12.2020).

[5] 1 января 2019 года вступил в силу закон КНР «Об электронной коммерции». URL: https://zakon.ru/blog/2020/3/24/1_yanvarya_2019_goda_vstupil_v_silu_zakon_knr_ob_elektronnoj_kommercii (дата обращения: 28.12.2020).

о введении в эксплуатацию до 01.04.2020[1], введена в эксплуатацию с 30.04.2020 [15, с. 72]) информационно-поисковой системы «Дистанционное мошенничество». Эта система позволяет систематизировать уголовные дела по заданным реквизитам: номерам телефонов, с которых поступали звонки потерпевшим и на которые перечислялись денежные средства; уникальным номерам телефонных аппаратов (IMEI); адресам базовых станций; номерам счетов и банковских карт; фамилиям физических лиц; адресам банкоматов и иным устройствам снятия денежных средств. Так, за период с апреля 2020 г. по май 2021 г. в ходе анализа сведений на предмет выявления совпадений идентификационных данных, используемых при совершении преступлений, содержащихся в материалах уголовных дел, находящихся в производстве, обнаружено более 324 тыс. признаков серийных преступлений[2]

Важнейшим условием своевременного реагирования на преступления с использованием информационно-телекоммуникационных технологий является усиление практико-ориентированного подхода по обеспечению кибербезопасности.

Ключевая проблема в условиях цифровизации общества, находящая отражение во многих научных исследованиях, заключается в недостаточной компетентности лиц, занимающихся выявлением и раскрытием киберпреступлений. В связи с этим формирование цифровой компетентности сотрудников органов внутренних дел приобретает особое значение.

Полагаем, что деятельность по укреплению квалифицированного кадрового состава включает усиление теоретической подготовки в области раскрытия и расследования преступлений, а также обмен знаниями и опытом экспертов в области обеспечения информационной безопасности «Лаборатория Касперского», InfoWatch, Positive Technologies, «Ростелеком-Солар», ИнфоТеКС, «Group-IB», а также Сбербанк и Центробанк[3].

Одним из положительных примеров такой работы выступает программа повышения квалификации следователей, разработанная Московским университетом МВД России им. В.Я. Кикотя совместно со Следственным департаментом МВД России и направленная на проведение учебных занятий с участием сотрудников Следственного департамента МВД России, Экспертно-криминалистического центра МВД России, Банка России, ПАО «Сбербанк» и АО «Лаборатория Касперского» [16, с. 90-91].

Ключевым инструментом действенного раскрытия преступлений с использованием информационно-телекоммуникационных технологий в условиях стремительного увеличения объема информации выступает внедрение в деятельность органов внутренних дел эффективной интеллектуальной технологии для принятия решения (экспертной системы), не являющейся способом замещения деятельности следственных и оперативных подразделений, а ориентированной на оказание помощи следователю, оперативному работнику при выполнении возложенных на них функциональных задач. Например, ранее активное применение получили в деятельности органов внутренних дел экспертные системы «Блок» (устанавливает способы совершения хищений в ходе строительных работ), «Автоэкс» (определяет числовые параметры различных элементов дорожно -транспортного происшествия), «Маньяк» (сопоставляет вводимую исходную информацию с имеющейся в программе о наиболее значимых криминалистических признаков, с помощью которых устанавливается связь между преступлением и убийцей) [17, с. 205-206], «СПРУТ» (выявляет связи субъектов преступного формирования на основании знаний о них и фактов, представляющих оперативный интерес), «Розыск» (ориентирована на предоставление помощи следователю, оперативному работнику при выдвижении типовых версий о сексуальном насилии) [18, с. 271].

Экспертная система (основными элементами которой являются интерфейс, ядро, база знаний, рабочая память, машина ввода (решатель), а также подсистема объяснения и приобретения знаний [18, с. 270]), являясь программным средством с применением искусственного интеллекта [19, с. 77 – 83], использует знания экспертов (опыт сотрудников следственных, экспертных и оперативных подразделений) для решения узкопрофильных задач, способствует приобретению знаний и обогащению своевременных разрешений проблемных ситуаций и принятию превентивных мер по установлению способов совершения экономических преступлений с использованием информационных технологий и типов

[1] Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 01.11.2019 № 3км: приказ МВД России от 25.11.2019 № 878. СПС «КонсультантПлюс» (дата обращения: 11.03.2022).

[2] МВД стало выявлять серийные киберпреступления с помощью специальной программы. URL: https://tass.ru/obschestvo/11298615?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (дата обращения 04.03.2022).

[3] ЦБ запускает для них учебный курс при участии МВД. URL: https://www.kommersant.ru/doc/4537640 (дата обращения: 28.12.2020).

преступников, распознать которых другими методами затруднительно.

С помощью экспертной системы реализуется возможность определения хода расследования (формирование версии о событиях с учетом различных источников получения информации), уменьшения нагрузки субъектов расследования, сокращения следственных ошибок; предоставления пользователю рекомендаций относительно дальнейших действий (назначения экспертиз, проведение оперативно-поисковых мероприятий, проверочных и следственных действий и т.д.) [18, с. 270].

Обсуждение и заключения

Таким образом, на основании проведенного исследования обозначим основные аспекты нивелирования современных вызовов и угроз безопасности цифровизации экономики:

в условиях возрастающего санкционного давления, угрозы ограничения российского доступа к иностранному программному обеспечению для целей эффективного противодействия новым схемам изощренных хакерских целевых атак представляется целесообразным уделять особое внимание современным программно-техническим средствам зашиты информации, сертифицированным ФСТЭК России.

Для организации эффективной следственной и оперативно-розыскной работы по раскрытию преступлений, совершенных с использованием информационно-телекоммуникационных сетей, предлагается рассмотреть вопрос о разработке экспертной системы, направленной на аккумулирование опыта и знаний высококвалифицированных сотрудников в области информационных технологий. Данная экспертная система будет способствовать выбору наилучшего варианта механизма раскрытия преступлений по аналогии с действующими в органах внутренних дел по иным направлениям экспертными системами («Блок», «Автоэкс», «Маньяк», «СПРУТ», «Розыск»).

В связи с отсутствием специального закона, содержащего систематизированный свод правил, охватывающий все аспекты функционирования электронной торговли, необходимо рассмотреть вопрос о разработке проекта закона «Об электронной коммерции», который будет способствовать регулированию субъектов экономических отношений, возникающих в связи с реализацией сделок по продаже товаров и оказанием услуг и иных действий юридического характера, совершенных посредством информационно-телекоммуникационных технологий.

В целях действенного противодействия преступлениям с использованием информационно-телекоммуникационных технологий особую значимость приобретает последовательная реализация мероприятий, направленных на повышение уровня специальных знаний сотрудников правоохранительных органов в сфере информационных технологий.

СПИСОК ИСТОЧНИКОВ

1. Графова Т.О., Шаповалов А.Ф. Риски и угрозы экономической безопасности в цифровой экономике // Азимут научных исследований: экономика и управление. 2020. № 1 (30). Т. 9. С. 382 – 386.
2. Риски и угрозы экономической безопасности России в условиях цифровой трансформации / М.С. Кобышева, А.А. Володин, М.В. Иванов [и др.] // Вестник Алтайской академии экономики и права. 2021. № 2. С. 53 – 60. DOI: 10.17513/vaael.1597. EDN SKVGEW.
3. Де А.Е. Мошенничество в условиях пандемии COVID-19 и самоизоляции // Столица Науки. 2020. № 6 (23). URL: https://www.scientific-capital.ru (дата обращения: 25.08.2020).
4. Химичева О.В., Андреев А.В. Цифровизация как тренд развития современного уголовного процесса // Вестник Московского университета МВД России. 2020. № 3. С. 21–23.
5. Гурьянов О.С., Лим С.В. Преступления в области денежно-кредитных и банковских отношений как угроза экономической безопасности страны // Внедрение передового опыта и практическое применение результатов инновационных исследований: сборник статей Международной научно-практической конференции, Волгоград, 20 мая 2020 года. Волгоград: «Аэтерна», 2020. С. 72 – 80.
6. Филатова И.В. Легализация денежных средств, приобретенных преступным путем в условиях цифровизации экономики // Уголовное судопроизводство: проблемы теории и практики. 2020. № 3. С. 85 – 88.
7. Бутин А.А., Василевская А.Н. Обзор основных рекомендаций по предупреждению инцидентов информационной безопасности в условиях удаленной работы и режима самоизоляции // Информационные технологии и математическое моделирование в управлении сложными системами. 2020. № 2 (7). С. 39 – 45.
8. Буров В.Ю. Опыт Российской Федерации по противодействию оттоку капитала за рубеж и легализации доходов, полученных преступным путем // Теневая экономика. 2019. Т. 3. № 3. С. 153 – 164.

9. Баранова И.С. Значение оттока капитала за рубеж в экономике Российской Федерации // Open innovation: сборник статей X Международной научно-практической конференции, Пенза, 17 сентября 2019 года. Пенза: «Наука и Просвещение» (ИП Гуляев Г.Ю.), 2019. С. 68 – 70.
10. Акмаров П.Б., Газетдинов М.Х., Третьякова Е.С. Проблемы защиты коммерческой информации в условиях цифровизации экономики // Вестник Казанского государственного аграрного университета. 2020. Т. 15. № 2 (58). С. 133 – 138.
11. Графова Т.О., Шаповалов А.Ф. Риски и угрозы экономической безопасности в цифровой экономике // Азимут научных исследований: экономика и управление. 2020. № 1 (30). Т. 9. С. 382 – 386.
12. Абдулхаликова А.И. Развитие системы электронной коммерции // Современная экономика: актуальные вопросы, достижения и инновации: сборник статей XXXV Международной научно-практической конференции. Пенза. 2020. С. 31 – 33.
13. Кубкина Ю.С. Основные тенденции развития электронной коммерции в мировой экономике и экономики Российской Федерации // Terra Economicus. 2014. Т. 12. № 2-2. С. 157 – 161.
14. Опальский А.П., Смирнов А.И. О деятельности информационно-поисковой системы по противодействию дистанционному мошенничеству // Алтайский юридический вестник. 2017. № 3 (19). С. 47 – 55.
15. Гаврилин Ю. В., Нуянзина С.В. Обеспечение законности при приеме, регистрации и разрешении сообщений о преступлениях, совершаемых с использованием информационно-телекоммуникационных технологий // Академическая мысль. 2020. № 4 (13). С. 70 – 73.
16. Давыдов В.О., Тишутина И.В. Об актуальных проблемах криминалистического обеспечения раскрытия и расследования мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий // Криминалистика: вчера, сегодня, завтра. 2020. № 2 (14). С. 81 – 91.
17. Плитенка А.В., Сопильняк Ю.Н. Использование экспертных систем в современной деятельности органов внутренних дел // Актуальные вопросы эксплуатации систем охраны защищенных телекоммуникационных систем: сборник материалов Всероссийской научно-практической конференции. Воронежский институт МВД России. Воронеж. 2016. С. 205 – 207.
18. Ткаченко А.П. Место и значение экспертных систем в деятельности по выявлению и расследованию преступлений // Юриспруденция в теории и на практике: актуальные вопросы и современные аспекты: сборник статей IV Международной научно-практической конференции, Пенза, 25 апреля 2020 года. Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2020. С. 269 – 272.
19. Сухарева М.А., Виниченко М.В. Построение экспертных систем с применением технологий искусственного интеллекта как системы поддержки принятия управленческих решений // Новое поколение. 2019. № 20. С. 77 – 83.

REFERENCES

1. Grafova T.O., SHapovalov A.F. Riski i ugrozy ekonomicheskoj bezopasnosti v cifrovoj ekonomike // Azimut nauchnyh issledovanij: ekonomika i upravlenie. 2020. № 1 (30). T. 9. S. 382 – 386.
2. Riski i ugrozy ekonomicheskoj bezopasnosti Rossii v usloviyah cifrovoj transformacii / M.S. Kobysheva, A.A. Volodin, M. V. Ivanov [i dr.] // Vestnik Altajskoj akademii ekonomiki i prava. 2021. № 2. S. 53 – 60. DOI 10.17513/vaael.1597. EDN SKVGEW.
3. De A.E. Moshennichestvo v usloviyah pandemii covid-19 i samoizolyacii // Elektronnyj zhurnal «Stolica Nauki». 2020. № 6 (23). URL: https://www.scientific-capital.ru (data obrashcheniya: 25.08.2020).
4. Himicheva O.V., Andreev A.V. Cifrovizaciya kak trend razvitiya sovremennogo ugolovnogo processa // Vestnik Moskovskogo universiteta MVD Rossii. 2020. № 3. S. 21–23.
5. Gur'yanov O.S., Lim S.V. Prestupleniya v oblasti denezhno-kreditnyh i bankovskih otnoshenij kak ugroza ekonomicheskoj bezopasnosti strany // Vnedrenie peredovogo opyta i prakticheskoe primenenie rezul'tatov innovacionnyh issledovanij: Sbornik statej Mezhdunarodnoj nauchno-prakticheskoj konferencii, Volgograd, 20 maya 2020 goda. Volgograd: «Aeterna», 2020. S. 72 – 80.
6. Filatova I.V. Legalizaciya denezhnyh sredstv, priobretennyh prestupnym putem v usloviyah cifrovizacii ekonomiki // Ugolovnoe sudoproizvodstvo: problemy teorii i praktiki. 2020. № 3. S. 85 – 88.
7. Butin A.A., Vasilevskaya A.N. Obzor osnovnyh rekomendacij po preduprezhdeniyu incidentov informacionnoj bezopasnosti v usloviyah udalennoj raboty i rezhima samoizolyacii // Informacionnye tekhnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami. 2020. № 2 (7). S. 39 – 45.
8. Burov V.YU. Opyt Rossijskoj Federacii po protivodejstviyu ottoku kapitala za rubezh i legalizacii dohodov, poluchennyh prestupnym putem // Tenevaya ekonomika. 2019. T. 3. № 3. S. 153 – 164.

9. Baranova I.S. Znachenie ottoka kapitala za rubezh v ekonomike Rossijskoj Federacii // Open innovation: sbornik statej X Mezhdunarodnoj nauchno-prakticheskoj konferencii, Penza, 17 sentyabrya 2019 goda. Penza: «Nauka i Prosveshchenie» (IP Gulyaev G.YU.), 2019. S. 68 – 70.
10. Akmarov P.B., Gazetdinov M.H., Tret'yakova E.S. Problemy zashchity kommercheskoj informacii v usloviyah cifrovizacii ekonomiki // Vestnik Kazanskogo gosudarstvennogo agrarnogo universiteta. 2020. T. 15. № 2 (58). S. 133 – 138.
11. Grafova T.O., SHapovalov A.F. Riski i ugrozy ekonomicheskoj bezopasnosti v cifrovoj ekonomike // Azimut nauchnyh issledovanij: ekonomika i upravlenie. 2020. № 1 (30). T. 9. S. 382 – 386.
12. Abdulhalikova A.I. Razvitie sistemy elektronnoj kommercii // Sovremennaya ekonomika: aktual'nye voprosy, dostizheniya i innovacii: sbornik statej XXXV Mezhdunarodnoj nauchno-prakticheskoj konferencii. Penza. 2020. S. 31-33.
13. Kubkina YU.S. Osnovnye tendencii razvitiya elektronnoj kommercii v mirovoj ekonomike i ekonomiki Rossijskoj Federacii // Terra Economicus. 2014. T. 12. № 2- 2. S. 157 – 161.
14. Opal'skij A.P., Smirnov A.I. O deyatel'nosti informacionno-poiskovoj sistemy po protivodejstviyu distancionnomu moshennichestvu // Altajskij yuridicheskij vestnik. 2017. № 3 (19). S. 47 – 55.
15. Gavrilin YU.V., Nuyanzina S.V. Obespechenie zakonnosti pri prieme, registracii i razreshenii soobshchenij o prestupleniyah, sovershaemyh s ispol'zovaniem informacionno-telekommunikacionnyh tekhnologij / YU. V. Gavrilin // Akademicheskaya mysl'. 2020. № 4 (13). S. 70 – 73.
16. Davydov V.O., Tishutina I.V. Ob aktual'nyh problemah kriminalisticheskogo obespecheniya raskrytiya i rassledovaniya moshennichestv, sovershennyh s ispol'zovaniem informacionno-telekommunikacionnyh tekhnologij // Kriminalistika: vchera, segodnya, zavtra. 2020. № 2 (14). S. 81 – 91.
17. Plitenka A.V., Sopil'nyak YU.N. Ispol'zovanie ekspertnyh sistem v sovremennoj deyatel'nosti organov vnutrennih del // Aktual'nye voprosy ekspluatacii sistem ohrany zashchishchennyh telekommunikacionnyh sistem: sbornik materialov Vserossijskoj nauchno-prakticheskoj konferencii. Voronezhskij institut MVD Rossii. Voronezh. 2016. S. 205 – 207.
18. Tkachenko A.P. Mesto i znachenie ekspertnyh sistem v deyatel'nosti po vyyavleniyu i rassledovaniyu prestuplenij // YUrisprudenciya v teorii i na praktike: aktual'nye voprosy i sovremennye aspekty: sbornik statej IV Mezhdunarodnoj nauchno-prakticheskoj konferencii, Penza, 25 aprelya 2020 goda. Penza: Nauka i Prosveshchenie (IP Gulyaev G.YU.), 2020. S. 269 – 272.
19. Suhareva M.A., Vinichenko M.V. Postroenie ekspertnyh sistem s primeneniem tekhnologij iskusstvennogo intellekta kak sistemy podderzhki prinyatiya upravlencheskih reshenij // Novoe pokolenie. 2019. № 20. S. 77 – 83.

Информация об авторе:
Назмеева Лейсан Рафиковна, кандидат экономических наук, старший преподаватель кафедры экономики, финансового права и информационных технологий в деятельности органов внутренних дел Казанского юридического института МВД России, nazmeevalr@mail.ru

Автор прочитал и одобрил окончательный вариант рукописи.

Information about the author:
Nazmeeva Leysan R., Candidate of Economic Sciences (Research doctorate), Senior Lecturer of the Department of Economics, Financial Law and Information Technologies in the Activities of Internal Affairs Bodies of the Kazan Law Institute of MIA of Russia, nazmeevalr@mail.ru

The author has read and approved the final version of the manuscript.

Статья получена: 14.06.2022.
Статья принята к публикации: 16.09.2022.
Статья опубликована онлайн: 29.09.2022.

Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаю.