ПУБЛИЧНО-ПРАВОВЫЕ (ГОСУДАРСТВЕННО-ПРАВОВЫЕ) НАУКИ

УДК 614.8
DOI: 10.18384/2949-513X-2024-4-6-18

ПРОБЛЕМА БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ НАСЕЛЕНИЯ И КОМПЛЕКС ГОСУДАРСТВЕННЫХ МЕР ПО ЕЁ РЕШЕНИЮ

Власов Ю. Н., Дворянов В. А.
Государственный университет просвещения
105005, г. Москва, ул. Радио, д. 10А, Российская Федерация

Аннотация
Цель. Проанализировать актуальность мер, предпринимаемых государственными органами для обеспечения безопасности жизнедеятельности населения в современных условиях, и юридические основания этих мер.
Процедура и методы. Исследованы совершенные в последнее время кибератаки и иные мошеннические действия со стороны злоумышленников, а также вызовы, возникшие в 2022–2024 гг., в связи с ухудшением отношений России и стран западного мира. Использованы методы системного анализа и экспресс-анализа. В качестве источников привлекаются документы с официальных сайтов: Центрального банка, Министерства чрезвычайных ситуаций Российской Федерации, президента РФ, иные источники.
Результаты. Проведён анализ, касающийся кибератак, ориентированых на государственные структуры и ведомства, а также ключевые коммерческие структуры, оценён уровень несанкционированного оттока денежных средств граждан Российской Федерации. Систематизированы ключевые вызовы, перед которыми оказались российское государство и население страны. Выявлены государственные механизмы решения проблем, дан первичный анализ их эффективности. Рассмотрена актуальность нормативно-правовых документов с точки зрения современных вызовов, а также вызовов будущего, смысл которых пока ещё до конца не ясен.
Теоретическая и/или практическая значимость. В работе затрагиваются вопросы, касающиеся смены вектора приложения усилий со стороны государственных органов Российской Федерации, ориентированных на обеспечение безопасности жизнедеятельности населения в условиях проведения СВО на Украине. Материалы исследования могут быть полезны для уточнения государственной политики в сфере обеспечения безопасности жизнедеятельности населения в современных условиях.

Ключевые слова: государственная политика, обеспечение безопасности жизнедеятельности, кибернетические атаки, национальная безопасность

THE ISSUE OF THE POPULATION'S LIFE SAFETY AND A POLICY MIX TO ADDRESS IT

Y. Vlasov, V. Dvoryanov
Federal State University of Education
ul. Radio 10A, Moscow 105005, Russian Federation

Abstract

Aim. To analyze both the relevance of measures taken by state bodies to ensure the population's safety of life activity in modern conditions and the legal grounds of these measures.

Methodology. The study analyzes the recent cyberattacks and other fraudulent actions by malicious actors, as well as the challenges arising in 2022–2024 due to the deterioration of relations between Russia and the developed countries of the Western world. The authors apply the method of system analysis and the method of express analysis. Documents from the official websites of the Central Bank, the Ministry of Emergency Situations of the Russian Federation, the President of the Russian Federation, and other sources are used as sources.

Results. The analysis concerning cyberattacks, which were focused on government agencies and departments, as well as key commercial structures, the level of unauthorized outflow of funds of citizens of the Russian Federation is assessed. The article systematizes the key challenges faced by the Russian state and the country's population. The state mechanisms of problem solving are identified, the primary analysis of their effectiveness is given. The relevance of normative-legal documents is analyzed from the point of view of modern challenges, as well as the challenges of the future, the meaning of which is not yet completely clear.

Research implications. The article touches upon the issues concerning changing the vector of efforts application on the part of the Russian Federation's state bodies, focused on ensuring the safety of vital activities of the population under conditions of the Special military operation in Ukraine. The materials of the research can be useful for clarification of the state policy in the sphere of provision of life safety of the population in modern conditions.

Keywords: state policy, life safety, cyber-attacks, national security

Введение

Принято считать, что проблема безопасности жизнедеятельности заключается в обеспечении комфортных условий деятельности людей, в защите человека и окружающей его среды (производственной, природной, городской, жилой) от воздействия вредных факторов, превышающих нормативно-допустимые уровни. А основная цель безопасности жизнедеятельности как науки – защита человека от негативных воздействий антропогенного и естественного происхождения и достижение комфортных условий жизнедеятельности. Очевидно, что определяющая роль в этом принадлежит специально организованному государством комплексу мер.

В российском научном дискурсе присутствует большое количество статей и иных научных работ, анализирующих действия государства в сфере обеспечения безопасности жизнедеятельности населения в современных условиях. Например, возможность создания комплексной системы безопасности жизнедеятельности населения [5], перспективы её внедрения [9] и целесообразности [6], нормативно-правовые основы комплексной системы безопасности жизнедеятельности населения [8], обеспечение безопасности жизнедеятельности населения на уровне территориальных образований [11], перспективы создания единой технической платформы управления комплексной системой безопасности жизнедеятельности населения [10], экономические основы системы безопасности мегаполисов [7].

Характерной особенностью всех этих публикаций является анализ мер, предпринимаемых государством в исполнение существующих законопроектов, принятых для обеспечения безопасности жизнедеятельности населения в современных условиях. Известно, что законодательный процесс в Российской Федерации занимает долгое время: 172 дня – для правительства и около 217 дней – для депутатов Госдумы. Члены Совета Федерации показывают похожие 216 дней. В. Путин вносит законопроекты, принятие которых занимает в среднем 74 дня, что является абсолютным рекордом. Но важные зако-

нопроекты президента могут приниматься и дольше. Например, проект, связанный с присоединением Крыма занял 145 дней[1]. С учётом времени, необходимого на осознание конкретной проблемы и подготовку документов для внесения законопроекта, срок может увеличиться в 1,5-2 раза. Дополнительное время требуется для создания и принятия региональных и муниципальных нормативных документов, назначение федеральных и региональных чиновников, обеспечивающих выполнение новых норм.

Между тем скорость появления новых угроз безопасности людей постоянно увеличивается. Фактически любая новая технология почти сразу начинает использоваться в противоправных целях. Классическим примером последних лет стало использование преступниками ChatGPT. Он появился и стал массово использоваться в конце 2022 г. И сразу же начал использоваться для организации фишинговых атак. За 2023 г. их количество выросло на 4 151%[2]. Развитие информационной социальной активности людей ведёт к тому, что 50% атак на коммерческие компании происходит с использованием технологий социальной инженерии[3]. Искусственный интеллект оказался удобным средством для генерации дипфейков. С января по сентябрь 2024 г. в 30 раз выросло число использований дипфейков для совершения преступлений[4].

Особые риски создают военные конфликты, активизирующие специальный правовой режим, в рамках которого становится возможным то, что ранее было под запретом. Начиная со Второй мировой войны, создание массированных угроз для населения применяется воюющими сторонами для достижения военных целей. Массированные бомбардировки жилых кварталов (например, бомбардировки Дрездена, Любека, Гамбурга, Сталинграда и Ковентри) создавали угрозу жизнедеятельности населения, призванную устрашить людей и подорвать легитимность органов власти в их глазах.

Начало специальной военной операции России на территории Украины в феврале 2022 г. и реакция на неё стран Запада привели к возникновению новых угроз безопасности жизнедеятельности для населения России.

Достаточно вспомнить, что Конгресс США стал той политической площадкой, на которой открыто дискуссируются вопросы о ядерных ударах по Российской Федерации. Доказательством того, что это не просто дискуссии, выступает поставка Украине боеприпасов с элементами боевого урана [4].

Все эти и иные факторы, создающие угрозы безопасности жизнедеятельности населения, нашли своё отражение в поправках к Федеральному закону «О безопасности», внесённых в апреле 2023 г. Эти поправки отразили новые угрозы безопасности жизнедеятельности населения, возникшие в 2022 г. после начала СВО.

Чаще всего граждане РФ сталкиваются со следующими проблемами собственной безопасности:

– киберугрозы;

– мошеннические действия с финансовыми средствами;

– утечка персональных данных вследствие утечки данных банков, коммерческих и государственных структур.

Обращает на себя ряд публикаций по указанным темам. Проблемами, связанными с активизацией киберугроз, занимались, в частности, А. А. Бочкова [2], Л. А. Бураева

[1] Борзенкова Е. Со скоростью президента: путь законопроекта в России // Право.Ру: [сайт]. URL: https://pravo.ru/story/212484/ (дата обращения: 05.12.2024).

[2] Россия: утечки информации ограниченного доступа, 2022-2023 годы //https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-2023.pdf, 09.01.2024.

[3] The State of PHISHING 2024 Mid-Year Assessment [Электронный ресурс] URL: https://slashnext.com/wp-content/uploads/2024/05/SlashNext-The-State-of-Phishing-24-Midyear-Report.pdf (дата обращения: 05.12.2024).

[4] Чернов А. В Сбере заявили о росте в 30 раз числа преступлений с использованием дипфейков // Газета.Ру: [сайт]. URL: https://www.gazeta.ru/business/news/2024/09/15/23927527.shtml?updated (дата обращения: 05.12.2024).

[3], К. А. Кузнецова, А. С. Остапова[1], Л. Р. Талипова [13] и ряд других. Вопросов обеспечения безопасности населения касались в т. ч. В. М. Баранов, А. И. Николаев, В. И. Семиков [12]. Интересно исследование С. А. Шаронова и Я. А. Шаповалова о частноправовых средствах обеспечения национальной безопасности России [15] и работа А. А. Фатьянова о служебной тайне как элементе обеспечения национальной безопасности России [14].

Возрастание рисков, связанных с кибератаками и иными мошенническими схемами с денежными средствами граждан

Проанализируем проблемные вопросы, связанных с возрастанием кибератак, мошеннических схем с денежными средствами граждан и интеграции в единое целое ныне разрозненных систем РСЧС и ГО. Всё это может и влияет на безопасность жизни человека в целом, создавая своим проявлением негативный эмоциональный фон, который неблагоприятно влияет на здоровье.

После начала СВО на Украине ещё больше активизировались киберугрозы, заняв лидирующие позиции в спектре негативных факторов. В течение всего 2023 г. активно осуществлялись хакерские атаки на отечественный бизнес и фишинговые атаки на пользователей, а также кража данных[2].

В рейтинге угроз для отечественного бизнеса ведущие позиции в 2023 г. заняли программы-вымогатели – рост по сравнению с предыдущим годом составил 2,5 раза. Вымогатели смогли аккумулировать более 321 млн рублей. Среди потерпевших: строительные компании, предприятия ретейла и производства, страхования и туризма. Проявилась интересная тенденция, ранее не встречающаяся в этом пространстве злоумышленников, в частности, синдикат *Comet (Shadow),* который специализируется на хакерских атаках, зашифровывая и похищая корпоративные секреты, не выставлял требований по выкупу данного вида информации[3].

В 2023 г. в результате кражи информации зафиксированы 246 эпизодов публичного размещения баз данных отечественных компаний. Удивляет то, что подобного рода нападкам подвергаются не только крупный бизнес, но и представители малого бизнеса, которые совсем беззащитны против подобного рода действий[4].

Эта тенденция усилилась в 2024 г., в частности, в I квартале в сети было размещено в 5 раз больше украденных данных, чем годом ранее.

Крайне активизировались фишинговые атаки. Мошенниками созданы 29 200 доменов, которые удалось выявить, значительная часть из них – 17 300 – применялись для доставки фиктивных товаров[5].

В 2024 г. базовым инструментарием, помогающим злоумышленникам добиваться требуемых результатов в рамках проведения компьютерных атак, выступали механизмы социальной инженерии. Это своего рода психотехника, ключевой задачей которой выступает склонение людей к раскрытию конфиденциальных сведений или переводу денежных средств мошенникам, поддавшись их воздействию (рис. 1).

Статистика Банка России свидетельствует о 15% росте применения мошенниками механизмов социальной инженерии относительно средневзвешенного значения за 2023 г., одновременно с этим актив-

[1] Кузнецова К. А., Остапова А. С. 9 тенденций в области кибербезопасности на 2024 год: // SecurityLab: [сайт]. URL: https://www.securitylab.ru/analytics/544688.php (дата обращения: 05.12.2024).

[2] Хакеры активизировались: какие киберугрозы ждут российский бизнес в 2024-м // Деловой Петербург: [сайт]. URL: https://www.dp.ru/a/2024/01/07/hakeri-aktivizirovalis-kakie (дата обращения: 05.12.2024).

[3] Крупные кибератаки и утечки первой половины 2024 года в России [Электронный ресурс]. URL: https://blog.cortel.cloud/2024/05/23/krupnye-kiberataki-i-utechki-pervoj-poloviny-2024-goda-v-rossii (дата обращения: 05.12.2024).

[4] Хакеры активизировались: какие киберугрозы ждут российский бизнес в 2024-м // Деловой Петербург: [сайт]. URL: https://www.dp.ru/a/2024/01/07/hakeri-aktivizirovalis-kakie (дата обращения: 05.12.2024).

[5] Крупные кибератаки и утечки первой половины 2024 года в России [Электронный ресурс]. URL: https://blog.cortel.cloud/2024/05/23/krupnye-kiberataki-i-utechki-pervoj-poloviny-2024-goda-v-rossii (дата обращения: 05.12.2024).

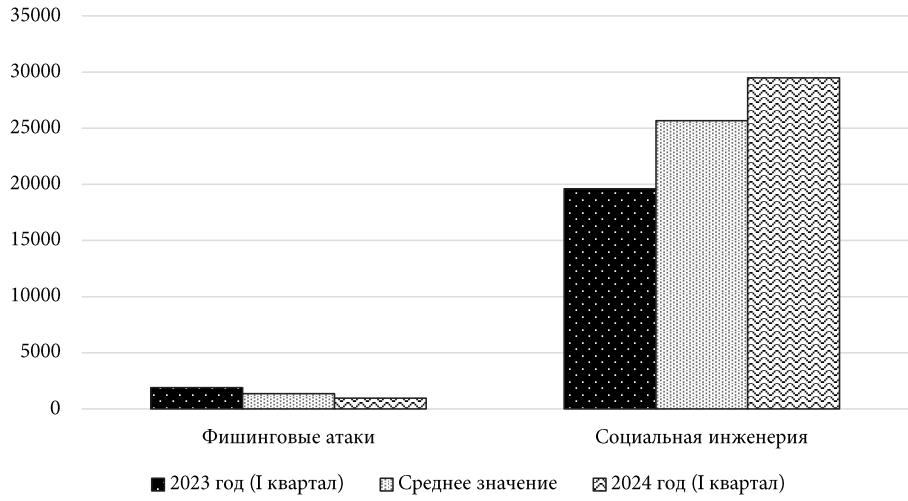

Рис. 1 / Fig. 1. Основные типы компьютерных атак / Main types of computer attacks
Источник: составлено авторами на базе статистики Банка России

ность фишинговых атак, напротив, сократилась на 30%.

Фишинговая атака представляет собой мошеннические действия в сети Интернет, ориентированные на незаконное овладение личной информацией, касающейся в т. ч. данных, открывающих доступ к банковской карте пользователя. Механизм, который применяют мошенники: создаётся фальшивый сайт, максимально похожий на реально существующий ресурс известной интернет-компании, которому доверяют клиенты, в надежде на то, что пользователь не сможет отличить официальный сайт компании от приманки в виде фальшивого сайта и оставит на нём личные данные.

7 октября 2024 г. IT-системы и сервисы телерадиовещательной компании ВГТРК подверглись хакерской атаке. Произошедший сбой затронул онлайн-вещание, внутренние IT-сервисы, интернет и телефонную связь внутри компании[1]. В результате пропали запросы на временный пропуск, и сотрудникам приходилось заполнять бумаги вручную, возникли проблемы с наполнением эфиров, т. к. хакерская атака вывела из строя программное обеспечение, в котором размещались отснятые сюжеты. В итоге компании пришлось выводить в эфир в архивное видео.

Крупнейшей кибератаке за всю историю своего существования подвергся Сбербанк. Атака длилась 13 ч; помимо IT-армии Украины в ней участвовали «несколько сторонних бот-сетей», состоящих из более 62 тыс. устройств[2]. В результате атаки стали недоступны мобильные приложения ВТБ, Росбанка, Альфа-банка и Газпромбанка.

Следует отметить, что во второй половины 2024 г. 49% кибератак приводили к утечкам конфиденциальной информации.

Утечки, связанные с медицинскими данными, вызывают особенное опасение. Ведь именно на базе этих сведений затем строятся эффективные фишинговые атаки. В открытый доступ поступили данные покупателей и заказов из базы интернет-аптеки apteka22.ru: 152 тыс. уникальных номеров телефонов, ФИО, адреса электронной почты, детали заказов и другие персональные данные.

В июле 2024 г. в открытом доступе оказался оттиск с 408 тыс. строк данных клиентов предположительно сети «ВинЛаб». В августе того же года была слита в сеть база данных всех лиц, пересекавших гра-

[1] Крупные кибератаки и утечки второй половины 2024 года в России [Электронный ресурс]. URL https://blog.cortel.cloud/2024/10/17/krupnye-kiberataki-i-utechki-dannyh-vtoroj-poloviny-2024-goda-v-rossii/?ysclid=m2fo17r0ci865759089 (дата обращения: 05.12.2024).

[2] Там же.

ницу России с 2014 по 2023 г. По словам участников IT-сообщества, это крупнейшая утечка из баз ФСБ за всё время существования ведомства. Утечку попытались опровергнуть, однако эксперты DLBI убедились в подлинности содержащихся в базе данных[1].

Риски для бизнеса растут не только из-за того, что растёт количество и сложность кибератак. Злоумышленники обратили внимание на объекты физического мира – они могут управлять станками, устройствами и промышленными объектами.

Только за 2023 г. в 2 раза выросло количество жертв кибератак, которым был нанесён ущерб на физическом уровне – с 18% до 37,5%[2]. Из недавних случаев –массовый взрыв пейджеров в Ливане.

В рамках обеспечения государственной политики, ориентированной в т. ч. на предотвращение кибератак, президентом России В. Путиным был подписан указ о дополнительных мерах по обеспечению информационной безопасности страны. Согласно этому указу, в госструктурах должны были появиться специалисты, отвечающие за предотвращение утечки данных и противодействие кибератакам[3]. Кроме того, на государственном уровне запрещено госорганам использовать средства защиты информации, которые разработаны в недружественных странах.

Указ Президента России № 250 определил, что:

1) устанавливается персональная ответственность за утечку данных;

2) в регионах создаются штабы по обеспечению кибербезопасности;

3) проводится регулярное стресс-тестирование систем;

4) к защите данных привлекаются специализированные организации[4].

Действия правительства в рамках борьбы с телефонным мошенничеством и спамом

ФАС и операторы связи разработали сервис для подачи жалоб на спам-рекламу. Блокировка нежелательной рекламы происходит в течение 72 ч. Одновременно с этим правительство планирует повысить стоимость лицензий для операторов связи с 7 тыс. до 1 млн руб. Этим пользуются недобросовестные операторы связи, которые в случае обнаружения нарушений просто переоформляют лицензию. Для усиления борьбы с подменными номерами Минцифры за 1,5 года заблокировало более 3,5 млн подозрительных сим-карт[5].

Разработаны меры, ужесточающие ответственность за утечку персональных данных, в частности, поправки в КоАП: за повторную утечку компанию будут штрафовать на сумму до 3% от её выручки, а согласно поправкам в Уголовный кодекс, за незаконный сбор и распространение персональных данных нарушителя будут лишать свободы сроком до 10 лет.

В рамках повышения безопасности в сети Интернет для безопасного использования сайтов было выдано более 10 тыс. национальных сертификатов и одновременно с этим заблокировано 27 тыс. фишинговых сайтов.

Автоматизированная система обеспечения безопасности российского интернета обрабатывает 80% трафика. Весь запрещённый контент блокируется.

---

1 Крупные кибератаки и утечки второй половины 2024 года в России [Электронный ресурс]. URL https://blog.cortel.cloud/2024/10/17/krupnye-kiberataki-i-utechki-dannyh-vtoroj-poloviny-2024-goda-v-rossii/?ysclid=m2fo17r0ci865759089 (дата обращения: 05.12.2024).

2 Хакеры активизировались: какие киберугрозы ждут российский бизнес в 2024-м // Деловой Петербург: [сайт]. URL: https://www.dp.ru/a/2024/01/07/hakeri-aktivizirovalis-kakie (дата обращения: 05.12.2024).

3 Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [Электронный ресурс]. http://www.kremlin.ru/acts/bank/47796 (дата обращения: 05.12.2024).

4 Там же.

5 ФАС и операторы связи разработали сервис для подачи жалобы на спам-рекламу // Федеральная антимонопольная служба: [сайт]. URL: https://fas.gov.ru/news/31967?ysclid=m2i0ufsjyz467129104 (дата обращения: 05.12.2024).

Реализация мошеннических действий, по уводу денег у клиентов банков

Рост мошеннических действий по отношению к российским граждан составил практически 17%, в 2024 г. по сравнению с 2023 г. (табл. 1–2).

Таблица 1 / Table 1

Количество операций без санкционирования клиентов / Number of transactions without client authorization

	I квартал 2023 г.	I квартал 2024 г.	Изменения, %
Количество операций без санкционирования клиентов (ед.)	252 101	294 414	106,78

Источник: Банк России: [сайт]. URL: https://cbr.ru (дата обращения: 05.12.2024)

Воровство с банковских карт возросло за рассматриваемый период более чем на 40% (табл. 2).

Таблица 2 / Table 2

Несанкционированное списание (воровство) денежных средств у россиян через банковские карты / Unauthorized debit (theft) of money from Russians via bank cards

	I квартал 2023 г.	I квартал 2024 г.	Изменения, %
Количество операций без согласия клиентов (ед.)	196 575	237 207	120,67
Объём операций без согласия клиентов (тыс. руб.)	1 363 735,83	1 918 855,52	140,71

Источник: Банк России: [сайт]. URL: https://cbr.ru (дата обращения: 05.12.2024)

Сегодня мошенники ориентируют свои усилия на удалённых банковских операциях [2]. Проблема здесь сводиться к тому, что, обеспечив за счёт средств и действия социальной инженерии возможность воспользоваться интернет-банкингом, мошенники способны в т. ч. оформить кредит на ничего не подозревающего клиента банка, похитив предварительно его средства. Именно удалённое банковское обслуживание принесло максимум потерь, в соответствии с аналитикой Банка России.

В целом следует отметить, что IT-технологии, с одной стороны, существенно упрощают процесс оплаты и перечисления денежных средств в удалённом режиме, но при этом являют собой систему рисков, которые смогут спровоцировать чрезвычайные ситуации, негативные явления и т. п. При этом IT-технологии актуализируют акты мошеннических проявлений в отношении прежде всего частных лиц, что негативно влияет на их психологическое здоровье и эффективность жизнедеятельности.

Рост напряжённости и противодействие этим процессам

Анализ приведённых фактов, которые свидетельствуют о нарастающем противостоянии РФ и тех стран, которые вводят против нашей страны санкции и снабжают Украину оружием. В сложившихся условиях должно поменяться отношение и к качеству и эффективности государственного управления национальной безопасностью, и к обеспечению безопасности жизнедеятельности населения. Именно поэтому государственная политика в этой сфере крайне важна и актуальна в настоящий момент как никогда ранее. Это осознаёт и В. Путин, и правительство РФ, что проявляется в адекватных современным условиям указах президента и разного рода законодательных актах.

Для разрешения комплекса проблем и обезопашивания граждан нашей страны от угроз, связанных с воровством денежных средств граждан, внедрён соответ-

ствующий механизм, который прописан в Федеральном законе № 161-ФЗ и касается контрмер по кражам средств клиентов банковской системы[1].

Нормы закона определяют, что оператор по переводу денежных средств при выявлении им операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия клиента (за исключением операции с использованием платёжных карт, перевода электронных денежных средств или перевода денежных средств с использованием сервиса быстрых платежей платежной системы Банка России), приостанавливает приём к исполнению распоряжения клиента на 2 дня[2].

В случае если оператор по переводу денежных средств, обслуживающий плательщика, получает от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, и после получения указанной информации исполняет распоряжение клиента – физического лица об осуществлении перевода денежных средств или совершает операцию с использованием платёжных карт, перевод электронных денежных средств или перевод денежных средств с использованием сервиса быстрых платежей платежной системы Банка России, соответствующие признакам осуществления перевода денежных средств без добровольного согласия клиента, оператор по переводу денежных средств обязан возместить клиенту сумму перевода или операции в течение 30 дней[3].

Можно также отметить, что предпринимаемые правительством меры, оказывают существенное воздействие на процесс обеспечения безопасности населения в плане хакерских атак, телефонного мошенничества и возврата несогласованного перечисления денежных средств клиентам банка. Всё это значимые шаги в проводимой государственной политике обеспечения безопасности наших граждан.

Юридические основания противодействия угрозам безопасности населения России: теория и реальность

Обеспечение безопасности жизнедеятельности неоднократно становилось темой принимаемых государством стратегий, законов и иных документов. Например, в принятой в 2016 г. Стратегии научно-технологического развития России[4] из 7 описанных в ней потенциальных угроз 6 связаны со сферой обеспечения безопасности жизнедеятельности, а одним из важнейших направлений научно-технического развития признаётся «…противодействие техногенным, биогенным, социокультурным угрозам, терроризму и идеологическому экстремизму…».

Долгое время панацеей признавалось развитие цифровых технологий. Не секрет, что история появления интернета связана с ядерным веком. Интернет был разработан как децентрализованная и распределённая технология коммуникаций, способная сохранить командные и контрольные функции во время ядерной войны. Но уже в 2010 г. в связи с заражением червём *Stuxnet* почти 1000 иранских центрифуг для обогащения уранового топлива, выяснилась уязвимость цифровых систем, обслуживающих ядерные программы [1].

Однако крен в сторону цифровизации в российских документах продолжается. В частности, в Стратегии в области развития гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций, обеспечения пожарной безопасности и безопасности людей на водных объектах на период до 2030 г. предполагается «…раз-

[1] Федеральный закон от 27.06.2010 № 161-ФЗ «О национальной платежной системе» [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/33484 (дата обращения: 05.12.2024)

[2] Федеральный закон от 27.06.2010 № 161-ФЗ «О национальной платежной системе» [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/33484 (дата обращения: 05.12.2024).

[3] Там же.

[4] Указ Президента Российской Федерации от 01.12.2016 № 642 «О Стратегии научно-технологического развития Российской Федерации» [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/41449 (дата обращения: 05.12.2024).

витие аппаратно-программных комплексов и технических средств мониторинга, прогнозирования и поддержки принятия решений…»[1].

В Указе президента Российской Федерации «О национальных целях развития Российской Федерации на период до 2030 года» средством обеспечения безопасности жизнедеятельности населения также должна стать цифровая трансформация систем управления мероприятиями по предупреждению и ликвидации негативных последствий кризисных и чрезвычайных ситуаций. Вводится понятие «цифровой зрелости» антикризисного управления[2].

В конце 2014 г. правительством РФ утверждается Концепция региональной информатизации[3], где предлагается «… реализовать автоматизированный информационный обмен между органами государственной власти субъектов Российской Федерации, территориальными органами федеральных органов исполнительной власти, органами местного самоуправления и администрациями объектов для организации комплексного мониторинга и управления уровнем угроз общественной безопасности, координации действий по предотвращению кризисных и чрезвычайных ситуаций и ликвидации их последствий».

Концепция требовала «…обеспечить внедрение в субъектах Российской Федерации информационных систем ”112” и “ЭРА-ГЛОНАСС”, Общероссийской комплексной системы информирования и оповещения населения в местах массового пребывания людей, комплексных систем видеонаблюдения, систем контроля доступа на опасные объекты; использование технических средств обеспечения безопасности, в т. ч. в области экологического, сейсмического и иного контроля, систем жизнеобеспечения, автоматизации мониторинга и предотвращения кризисных ситуаций, иных информационных систем в сферах безопасности жизнедеятельности…».

Пилотный проект по реализации мер, предусмотренных Концепцией, был реализован в 2015 г. в Курской области и распространён затем на всю страну. Но в ней не была предусмотрена возможность вторжения на территорию РФ чужой армии.

Среди прочих нормативных документов по анализируемой теме следует упомянуть Указ президента «О Стратегии национальной безопасности Российской Федерации»[4], и Федеральный закон № 172-ФЗ «О стратегическом планировании в Российской Федерации»[5], ст. 18 которого посвящена стратегии национальной безопасности Российской Федерации. Оба документа носят общий характер и, обозначая вызовы, связанные с возведением странами западного мира «железного занавеса» вокруг России, не ставят вопрос о необходимости создания технологии ответов на вызовы завтрашнего дня, ещё не проявивших себя в полной мере. Базовыми нормативными актами, связанными с обеспечением информационной безопасности, являются Федеральный закон «Об информации, информационных технологиях

[1] Указ Президента Российской Федерации от 16.10.2019 № 501 «О Стратегии в области развития гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций, обеспечения пожарной безопасности и безопасности людей на водных объектах на период до 2030 года» [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/44747 (дата обращения: 05.12.2024).

[2] Указ Президента Российской Федерации от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года» [Электронный ресурс]. http://www.kremlin.ru/acts/bank/45726 (дата обращения: 05.12.2024).

[3] Распоряжение Правительства РФ от 29.12.2014 N 2769-р (ред. от 18.10.2018) «Об утверждении Концепции региональной информатизации». - http://static.government.ru/media/files/Ea8O35fPr3I.pdf, 09.01.2024.

[4] Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 05.12.2024).

[5] Федеральный закон от 28.06.2014 № 72-ФЗ «О стратегическом планировании в Российской Федерации» [Электронный ресурс]. URL: http://www.kremlin.ru/acts/bank/38630 (дата обращения: 05.12.2024).

и о защите информации»[1] и Федеральный закон «О коммерческой тайне»[2].

Согласно ст. 16 закона № 149-ФЗ:

«1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации».

Пункт 4 ст. 16 предписывает, что:

«4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации;

7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации».

Пункт 5 ст. 16 закона определяет[3]:

«5. Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем, иных информационных систем государственных органов, государственных унитарных предприятий, государственных учреждений применяемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям».

Статья 10 «Охрана конфиденциальности информации» закона № 98-ФЗ предусматривает:

«*1. Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:*

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учёт лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

---

[1] Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 // СПС Консультант Плюс.

[2] Федеральный закон № 98-ФЗ «О коммерческой тайне» от 29.07.2004 // СПС Консультант Плюс.

[3] Там же.

5) нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна» с указанием обладателя такой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства)»[1].

Далее признается, что

«5. Меры по охране конфиденциальности информации признаются разумно достаточными, если:

1) исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;

2) обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

6. Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства»[2].

Резюмируя, необходимо отметить, что существующие нормативно-правовые документы, регулирующие действия государства в сфере обеспечения безопасности жизнедеятельности населения, фактически дают ответы на вызовы сегодняшнего дня. Но делают это в крайне общей форме, не дающей ответа на то, как действовать в каждой конкретной ситуации. Тем более они не предусматривают необходимости разработки методов противодействия вызовам будущего.

Заключение

Итак, сделан анализ тех негативных явлений, которые напрямую влияют на безопасность жизнедеятельности населения страны, в первую очередь кибернетические атаки на различного рода государственные и коммерческие организации, связанные с жизнеобеспечением населения. Рассмотрена связь между кибернетическими атаками и иными угрозами жизнедеятельности населения и государственной политикой по их нейтрализации, включая ее юридические основания. Показано, что проводимая государственная политика актуализируется, исходя из тех угроз, которые максимальным образом влияют на представление людей о легитимности государства. Важнейший фактор этой легитимности – способность государства защитить людей. Одно из самых чувствительных правонарушений в этом контексте – мошеннические схемы по изъятию денежных средств у населения. При этом уже после осознания общественной опасности указанной проблемы способствующий её решению закон был отложен на год, в течение которого банковская система смогла бы подготовиться к возвращению клиентам мошенническим образом снятых со счетов денежных средств.

В 2023–2024 гг. зафиксирован значительный рост мошенничеств, связанных с незаконным изъятием средств клиентов банков. Основная проблема – это запаздывающая реакция государства на новые возникающие угрозы, медлительность законодательного процесса. А также в том, что законодательство разрабатывается для решения уже существующих проблем, поэтому перед новыми проблемами люди часто оказываются беззащитными.

Статья поступила в редакцию 14.02.2024.

[1] Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // СПС Консультант Плюс.

[2] Там же.

ЛИТЕРАТУРА

1. Барроуз М. Глава 7. Будущее рассекречено: Каким будет мир в 2030 году / пер. с англ М. Гескиной. М.: Манн, Иванов и Фербер, 2015. 352 с.
2. Бочкова А. А. Киберугрозы на фондовых рынках: критерии анализа // Скиф. 2017. № 10. С. 39–43.
3. Бураева Л. А. О некоторых вопросах обеспечения кибербезопасности в современных условиях // Теория и практика общественного развития. 2015. № 13. С. 96–99.
4. Когут В. Г., Лукин В. Н., Мусиенко Т. В. Безопасность жизнедеятельности: проблемы нормативно-правового обеспечения // Культура и безопасность. 2023. № 4. С. 22–34.
5. Колиев Е. М. Комплексная система обеспечения безопасности жизнедеятельности населения // Проблемы обеспечения безопасности при ликвидации последствий чрезвычайных ситуаций. 2018. Т. 1. С. 285–290.
6. Новоселов Д. И. Целесообразность развития комплексной системы обеспечения безопасности жизнедеятельности населения в субъектах Российской Федерации // Международный журнал гуманитарных и естественных наук. 2024. № 1-2. С. 182–184. DOI: 10.24412/2500-1000-2024-1-2-182-184
7. Орловская Т. Н. Особенности обеспечения экономической безопасности российских мегаполисов с целью создания благоприятных и безопасных условий жизнедеятельности населения // Экономическая безопасность: опыт, проблемы, перспективы: мат-лы конф. / под ред. А.К. Моденова и др. СПб., 2022. С. 54–61.
8. Попов А. П., Грязнев Д. Ю. О нормативно-правовых основах дальнейшего развития комплексных систем обеспечения безопасности жизнедеятельности населения // Технологии гражданской безопасности. 2020. № 4. С. 41–44.
9. Попов А. П., Капральный Ю. В. О внедрении комплексных систем обеспечения безопасности жизнедеятельности населения // Пожарное дело. 2020. № 12. С. 40–41.
10. Предложения к концепции построения единой технической платформы управления комплексной системой обеспечения безопасности жизнедеятельности населения Российской Федерации В. Б. Крейнделин, С. С. Плясунов, А. В. Федулов, Н. В. Тамп // Научная мысль. 2020. Т. 14. № 4-1. С. 63–68.
11. Садыков Р. М. Обеспечение безопасности жизнедеятельности населения на уровне территориальных образований // Национальные интересы: приоритеты и безопасность. 2020. Т. 16. № 5. С. 980–994.
12. Семиков В. Л. Роль научно-технического творчества в исследованиях в области обеспечения безопасности // Культура и безопасность. 2022. № 4. С. 30–37.
13. Талипова Л. Р. Международно-правовая регламентация киберпреступности // Гуманитарные, и социально-экономические и общественные науки. 2016. № 4. С. 121–123.
14. Фатьянов А. А. Служебная тайна как элемент обеспечения национальной безопасности России // Сибирское юридическое обозрение. 2023. Т. 20. № 4. С. 397–405.
15. Шаронов С. А., Шаповалов Я. А. Частноправовые средства обеспечения национальной безопасности России // Цивилист. 2024. № 1. С. 37–42.

REFERENCES

1. Burrows M. *The Future, Declassified: Megatrends That Will Undo the World Unless We Take Action* (Rus. ed.: Geskina M., transl. *Glava 7. Budushcheye rassekrecheno: Kakim budet mir v 2030 godu*. Moscow, Mann, Ivanov and Ferber Publ., 2015. 352 p.)
2. Bochkova A. A. [Cyber threats in stock markets: analysis criteria]. In: *Skif* [Skif], 2017, no. 10, pp. 39–43.
3. Buraeva L. A. [On some issues of ensuring cybersecurity in modern conditions]. In: *Teoriya i praktika obshchestvennogo razvitiya* [Theory and Practice of Social Development], 2015, no. 13, pp. 96–99.
4. Kogut V. G., Lukin V. N., Musienko T. V. [Life safety: problems of regulatory and legal support]. In: *Kultura i bezopasnost* [Culture and Security], 2023, no. 4, pp. 22–34.
5. Koliev E. M. [Integrated system for ensuring the safety of life of the population]. In: *Problemy obespecheniya bezopasnosti pri likvidatsii posledstviy situatsiy* [Problems of Ensuring Safety in the Elimination of Consequences of Emergency Situations], 2018, vol. 1, pp. 285–290.
6. Novoselov D. I. [Feasibility of developing an integrated system for ensuring the safety of life of the population in the constituent entities of the Russian Federation]. In: *Mezhdunarodnyy zhurnal gumanitarnykh i promyshlennykh nauk* [International Journal of Humanities and Natural Sciences],

2024, no. 1–2, pp. 182–184. DOI: 10.24412/2500-1000-2024-1–2–182–184
7. Orlovskaya T. N. [Features of ensuring the economic security of Russian megacities in order to create favorable and safe living conditions for the population]. In: Modenova A. K. et al, eds. *Ekonomicheskaya bezopasnost': opyt, problemy, perspektivy* [Economic security: experience, problems, prospects]. St. Petersburg, 2022, pp. 54–61.
8. Popov A. P., Gryaznev D. Yu. [On the regulatory framework for further development of integrated life safety systems for the population]. In: *Tekhnologii grazhdanskoy bezopasnosti* [Civil Security Technologies], 2020, no. 4, pp. 41–44.
9. Popov A. P., Kapralny Yu. [On the implementation of integrated life safety systems for the population]. In: *Pozharnoye delo* [Firefighting]. 2020, no. 12, pp. 40–41.
10. Kreindelin V. B., Plyasunov S. S., Fedolov A. V., Tamp N. V. [Proposals for the concept of building a unified technical platform for managing an integrated life safety system for the population of the Russian Federation]. In*: Nauchnaya mysl* [Scientific Thought], 2020, vol. 14, no. 4-1, pp. 63–68.
11. Sadykov R. M. [Ensuring the safety of life of the population at the level of territorial entities]. In: *Natsionalnyye interesy: prioritety i bezopasnost* [National interests: priorities and security], 2020, vol. 16, no. 5, pp. 980–994.
12. Semikov V. L. [The role of scientific and technical creativity in research in the field of security]. In: *Kultura i bezopasnost* [Culture and Security], 2022, no. 4, pp. 30–37.
13. Talipova L. R. [International legal regulation of cybercrime]. In: *Gumanitarnyye, sotsialno-ekonomicheskiye i obshchestvennyye nauki* [Humanities, Social-Economic and Social Sciences], 2016, no. 4, pp. 121–123.
14. Fatyanov A. A. [Official secret as an element of ensuring national security of Russia]. In: *Sibirskoye yuridicheskoye obozreniye* [Siberian Legal Review], 2023, vol. 20, no. 4, pp. 397–405.
15. Sharonov S. A., Shapovalov Ya. A. [Private Law Means of Ensuring National Security of Russia]. In: *Tsivilist* [Civilist], 2024, no. 1, pp. 37–42.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Власов Юрий Николаевич – доктор технических наук, доцент кафедры безопасности жизнедеятельности и методики обучения Государственного университета просвещения;
e-mail: pobeda-872vlasov@yandex.ru

Дворянов Владимир Анатольевич – кандидат исторических наук, доцент кафедры истории России Государственного университета просвещения;
e-mail: dorochov2@yandex.ru

INFORMATION ABOUT THE AUTHORS

Yuri N. Vlasov – Dr. Sci. (Engineering), Associate Professor, Department of Life Safety and Teaching Methods, Federal State University of Education;
e-mail: pobeda-872vlasov@yandex.ru

Vladimir A. Dvoryanov – Cand. Sci. (History), Assoc. Prof., Department of Russian History, Federal State University of Education
e-mail: dorochov2@yandex.ru

ПРАВИЛЬНАЯ ССЫЛКА НА СТАТЬЮ

Власов Ю. Н., Дворянов В. А. Государственная политика обеспечения безопасности жизнедеятельности населения в современной России // Московский юридический журнал. 2024. № 4. С. 6–18.
DOI: 10.18384/2949-513X-2024-4-6-18

FOR CITATION

Vlasov Y. N., Dvoryanov V. A. The Issue of the Population's Life Safety and a Policy Mix to Address It. In: *Moscow Juridical Journal,* 2024, no. 4, pp. 6–18.
DOI: 10.18384/2949-513X-2024-4-6-18