Научная статья / Original research article
УДК 352.071
DOI: 10.31660/1993-1824-2024-4-77-93

Угрозы информационной безопасности в государственном секторе России

А. А. Попкова✉, К. В. Парфенов, А. Р. Алборов

Тюменский индустриальный университет, Тюмень, Россия
✉ *popkovaaa@tyuiu.ru*

Аннотация. В условиях развития информационного общества информация становится объектом преступных посягательств, совершаемых, чтобы дестабилизировать происходящие в государстве социальные процессы. Инфраструктура государственного сектора наиболее привлекательна для кибератак, осуществляемых с целью получения конфиденциальной информации о гражданах, широко использующих государственные информационные сервисы. Несмотря на активную политику обеспечения информационной безопасности, до сих пор Российской Федерации не удается снизить значение и последствия информационных угроз в деятельности органов государственной власти и учреждений. При анализе факторов, обеспечивающих возникновение этих кибератак, было выявлено, что ключевая роль принадлежит социальному фактору, являющемуся следствием безответственного поведения граждан при работе с персональными данными, открытию фишинговых писем, а также реакции граждан на информационно-психологическое воздействие со стороны киберпреступников. Проведенный в статье анализ информационных угроз подтвердил тезис о том, что государственный сектор в последние годы выступает объектом постоянных кибератак, а работники государственных учреждений часто становятся субъектом нейтрализации существующей в данном секторе системы информационной безопасности. Цель исследования — анализ специфики информационных угроз и факторов, способствующих их распространению в государственном секторе современной России. В статье проведен анализ исследований в сфере информационной безопасности органов государственной власти и бюджетных учреждений, позволяющий определить систему информационных угроз и их специфику. В выводах представлена систематизация информационных угроз для государственного сектора Российской Федерации.

Ключевые слова: информационная безопасность, информационные угрозы, кибератака, государственный сектор, цифровизация органов государственной власти, политика обеспечения информационной безопасности, государство

Для цитирования: Попкова, А. А. Угрозы информационной безопасности в государственном секторе России / А. А. Попкова, К. В. Парфенов, А. Р. Алборов. – DOI 10.31660/1993-1824-2024-4-77-93 // Известия высших учебных заведений. Социология. Экономика. Политика. – 2024. – № 4. – С. 77–93.

Threats to information security in the Russian public sector

Alena A. Popkova✉, Konstantin V. Parfenov, Arsen R. Alborov

Industrial University of Tyumen, Tyumen, Russia
✉ *popkovaaa@tyuiu.ru*

Abstract. In the context of the development of the information society, data has become an object of criminal encroachments aimed at destabilizing social processes within the state. The public sector infrastructure especially appeals to cyber criminals seeking to obtain confidential information about citizens who utilize government services. Despite active information security policy, the Russian Federation faces challenges in mitigating the impact and consequences of information threats affecting government institutions. An analysis of various factors contributing to these threats reveals that a significant element is social behaviour, which includes irresponsible actions by citizens regarding their data, such as opening phishing emails and responding to psychological manipulation by cybercriminals. An analysis of the information threats confirmed the thesis that the public sector has been the target of persistent cyberattacks in recent years. As a result of this employees of government agencies often become the subject of neutralization of the existing information security system in the sector. The aim of this research is to examine the specific information threats and the factors that facilitate their proliferation in the public sector of modern Russia. The article reviews existing studies on information security within government agencies and public institutions, which helps to clarify the system of information threats and their characteristics. The findings presented offer a comprehensive overview of information threats facing the public sector in the Russian Federation.

Keywords: information security, information threats, cyberattack, public sector, digitalization of government authorities, information security policy, state

For citation: Popkova, A. A., Parfenov, K. V., & Alborov, A. R. (2024). Threats to information security in the Russian public sector. Proceedings of Higher Educational Institutions. Sociology. Economics. Politics, (4), pp. 77-93. (In Russian). DOI: 10.31660/1993-1824-2024-4-77-93

Введение

Трансформационные изменения социальных отношений, вызванные повышением роли информации, привели к необходимости рассмотрения информационного пространства как объекта политического воздействия, формирования системы государственных мер, способствующих снижению уязвимости государственной информационной инфраструктуры, предотвращению деструктивного воздействия информационных угроз на российское общество.

Президент Российской Федерации в марте 2024 года, выступая на расширенной коллегии Федеральной службы безопасности Российской Федерации (ФСБ), акцентировал внимание на том, что количество атак на информационную инфраструктуру нашего государства растет и это требует расширения системы превентивной реакции на данные угрозы, усиления мер информационной защиты [1].

Значимость государственного сектора в системе общественных отношений делает его наиболее привлекательным для реализации информационного воздействия и кибератак. По сведениям аналитического центра Positive Technologies, среди успешных информационных атак на российские организации 15 % пришлось на государственный сектор, и данная тенденция усиливается — в первом полугодии 2024 года доля подобных преступлений в отношении государственных организаций составила 14 % [2].

Российская Федерация в 2022 году вошла в десятку стран-лидеров по цифровизации государственного управления, что свидетельствует о расширении значимости информационных угроз в критически важных направлениях жизнедеятельности российского общества [3]. Развитие государственных систем и облачных хранилищ, доступность государственных услуг в электронном виде, реализация политики, направ-

ленной на внедрение инновационных ИТ-решений в систему государственного управления, создание институциональной среды для развития информационной инфраструктуры, возможность получения обратной связи для граждан являются ключевыми параметрами цифровизации государственного сектора и ключевыми направлениями обеспечения информационной безопасности.

Наличие уязвимостей для информационных атак в инфраструктуре государственного сектора, количество которых возрастает с каждым годом, является существенным фактором для общества, провоцируя политическую напряженность, снижение доверия, утечку персональных данных граждан, сбои в электронных сервисах работы с населением. Следовательно, необходимость системного подхода к анализу угроз информационной безопасности для выработки эффективной государственной политики является базовым условием для функционирования госсектора, обеспечения национальной безопасности и стратегического развития страны.

Материалы и методы

Исследование методологических основ информационной безопасности определяет комплексность характеристик данной категории. В связи с развитием информационного общества формируется двойственность содержания информационной безопасности. С одной стороны, информационная безопасность предполагает развитие технологического аспекта, позволяющего создать систему, обеспечивающую недопустимость несанкционированного доступа к информации, ее утечке и использованию против государства, органов управления и организаций. А с другой стороны, информационная безопасность определяется социально-психологическим аспектом, формирующимся под воздействием киберугроз, распространения фейковой информации, технологий социальной инженерии.

Анализ исследований в сфере информационной безопасности в государственном секторе позволил выделить несколько методологических аспектов данной категории. Информационная безопасность как элемент национальной безопасности России исследуется в трудах Е. В. Алексеевой [4], А. А. Галушкина [5], В. П. Шерстюка [6], М. А. Чаписа [7] и др. Общесистемные аспекты исследований информационной безопасности в государственном секторе исследованы С. А. Дятловым, О. С. Лобановым, Д. В. Гильмановым, И. А. Корх, Е. В. Юмашевой [8]. Утечка данных как проблема обеспечения информационной безопасности в государственных организациях представлена в работах Р. А. Фазылова [9], М. И. Назиева, Л. Р. Магомаевой [10]. Вопросам технологического развития системы информационной безопасности в государственном секторе посвящены исследования М. В. Андроповой [11]. Систематизация основных направлений государственной политики в сфере обеспечения информационной безопасности Российской Федерации представлены в работе И. Л. Морозова [12].

Ключевые тенденции обеспечения информационной безопасности в государственном секторе Российской Федерации по сравнению с другими секторами определены на основе вторичного анализа данных исследования, проведенного компанией «SearchInform», в котором приняли участие 1 200 респондентов, представителей служб

информационной безопасности, топ-менеджмента и экспертов организаций государственного, коммерческого и некоммерческого секторов [13].

Специфика реализации киберугроз в государственном секторе определена на основе вторичного анализа результатов исследования аналитического агентства «Positive Technologies», которые основаны на данных 213 источников (телеграмм-каналы, форумы в дарквебе) за период 2023–2024 годов, а также отчетных данных об исследовании серии кибератак на органы государственной власти РФ, представленных Solar JSOC компании «Солар» совместно с Национальным координационным центром по компьютерным инцидентам (НКЦКИ) [14] .

Проведенный анализ нормативных правовых актов в сфере информационной безопасности основан на исследовании Доктрины информационной безопасности РФ [15], Основных направлений государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации [16], Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации [17].

Результаты и обсуждение

В качестве стратегического приоритета Российской Федерации до 2030 года было определено развитие информационного общества, на законодательном уровне в очередной раз было подчеркнуто, что для российского общества «информация и уровень ее применения кардинальным образом влияют на экономические и социокультурные условия жизни граждан» [18]. Активизация политики развития использования информационных ресурсов в функционировании системы государственного и муниципального управления потребовала не только проработки законодательства об использовании информационных технологий, но и обеспечения информационной безопасности.

В Указе Президента РФ № 474 от 21.07.2021 года «О национальных целях развития Российской Федерации» в качестве приоритета развития государственного сектора была определена необходимость «увеличения доли массовых социально значимых услуг, доступных в электронном виде, до 95 %» в рамках цифровой трансформации данного сектора [19].

Расширение использования информационно-коммуникационных технологий в системе государственного управления, поступательность достижения заявленных приоритетов стали возможным в рамках принятия и реализации федерального проекта «Цифровое государственное управление», который сконцентрирован в своих целях на повышении качества жизни граждан и развитии бизнеса за счет предоставления услуг в электронном виде, повышении качества процесса их предоставления, обеспечения информационного взаимодействия государства, граждан и организаций в цифровом пространстве [20]. Активная цифровизация государственного управления определена необходимостью обработки больших массивов данных, включающих в себя персональную и стратегически важную информацию о гражданах и объектах государственной инфраструктуры. Следовательно, сформировалась необходимость не только защиты

данной информации от несанкционированного доступа, но и ее использования в интересах других государств, юридических и физических лиц.

На фоне современных геополитических конфликтов вопросы обеспечения информационной безопасности стали объектом регулирования документов международного значения. В мае 2023 года Россия совместно со странами-партнерами внесла Концепцию конвенции Организации объединенных наций (ООН) по международной информационной безопасности, целями которой является предотвращение и урегулирование межгосударственных конфликтов в глобальном информационном пространстве, развитие сотрудничества в сфере информационной безопасности и содействие наращиванию потенциала государств в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий [21]. Россия с 2011 года выступает с инициативой совместных международных действий по обеспечению безопасности в мировом информационном пространстве, но единства целей и системы мер по данному вопросу среди всех стран-участников ОНН не достигнуто.

Регламентация ключевых вопросов в обеспечении информационной безопасности России закреплена в Доктрине информационной безопасности РФ, которая определяет содержание политики информационной безопасности и информационных угроз. В качестве угроз информационной безопасности определяется «совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере».

Выделенные в данном документе угрозы информационной безопасности связаны с трансграничным оборотом информации, которая используется для достижения геополитических, военных, террористических и иных целей, направленных на подрыв стабильности и безопасности в отдельных государствах, формирование угроз их суверенитету: применение информационных технологий и средств для нанесения ущерба информационной инфраструктуре, используемой в военной сфере; деструктивное информационное воздействие спецслужб отдельных государств на население в целом и отдельные группы граждан с целью психологического воздействия и дестабилизацию социальных процессов в обществе; пропаганда экстремисткой идеологии, склонение к реализации террористических актов на территории государства с целью разрушения объектов значимой информационной инфраструктуры; рост преступлений с использованием информационно-коммуникационных технологий, связанных с утечкой персональных данных, взломом содержащих их систем; рост кибератак на государственные ресурсы, системы, инфраструктуру; неразвитость отечественного программного обеспечения и технологий, используемых в информационной сфере, технологическая зависимость от других государств.

Наиболее уязвимым с позиции оказываемого социального воздействия является государственный сектор, так как именно госсектор, представляющий собой многоуровневую систему организаций, учреждений и предприятий, полным или частичным собственником которых выступает государство, обеспечивает реализацию государственных функций и приоритетов социально-экономического развития [22].

В отношении государственного сектора основной целью информационных атак является либо полная компрометация информационно-телекоммуникационной инфра-

структуры органов государственной власти и государственных учреждений, либо кража конфиденциальной информации, содержащейся в почтовой переписке, файлов общего и ограниченного доступа, инфраструктурно-производственных схем и т. п. Наиболее распространенными видами информационных атак являются фишинговая рассылка, веб-приложения, распространяющиеся в сети Интернет, взлом организаций, взаимодействующих с органами государственной власти в качестве подрядчика.

В силу функциональной специфики организации государственного сектора взаимодействуют с огромным числом граждан и массивом информационных данных, используемых в их работе и имеющих существенное значение для обеспечения деятельности государства, его национальной безопасности. Именно эти особенности государственного сектора, его социальная значимость делают его приоритетным объектом для кибератак.

В исследованиях компании «Солар» выделяется два типа киберпреступников, атакующих госсектор. К первому типу относятся киберхулиганы, которые находят уязвимости в инфраструктуре государственных организаций с целью перепродажи полученной информации. Второй тип — кибернаемники и кибервойска, проникающие в инфраструктуру государственного сектора незаметно для осуществления длительного контроля и доступа к конфиденциальным данным, осуществляющие кибершпионаж.

Как показывает практика последних лет, объектами информационных атак являются как информационные системы и сервисы, так и работники организаций государственного сектора. Результаты вторичного анализа данных исследования, проведенного аналитическим центром Positive Technologies, показывают, что в первом квартале 2024 года по сравнению с 2023 годом количество атак на компьютеры, серверы и сетевое оборудование госсектора сократилось на 12 % (с 88 до 76 %), а на сотрудников организаций, напротив, выросла на 11 % (с 46 до 57 %). Для успешного достижения целей атак чаще всего используется вредоносное программное обеспечение. Активизация технологий социальной инженерии для усиления влияния социальных факторов при реализации кибератак вызвана высокой степенью уязвимости работников, восприимчивости к информационному воздействию.

Причинами использования вредоносного программного обеспечения являются:

- простота и эффективность использования вредоносного программного обеспечения за счет автоматизированных инструментов применения и низких ресурсозатрат;
- развитый рынок доступного вредоносного программного обеспечения.

Исследование показывает, что если в 2022 году преобладал шифровальный тип вредоносного программного обеспечения, то в 2024 году существенно выросла доля вредоносного программного обеспечения для удаленного управления (с 29 % в 2022 году до 37 % в 2024) [2]. Государственный сектор наиболее привлекателен для внедрения вредоносного программного обеспечения по причине возможности сбора и анализа большого объема данных и их использования для манипулятивного воздействия в информационном противоборстве, внедрения шпионского программного обеспечения, которое можно распространять через устройства госучреждений для дальнейших атак.

Ключевым способом распространения вредоносного программного обеспечения является рассылка писем по электронной почте с использованием почтовых доменов организаций госсектора (70 % случаев успешных кибератак в 2023 году). При использовании электронной почты в отношении объекта атаки в 93 % случаев подключаются технологии социальной инженерии, способствующие реакции получателя письма на его содержимое. Все это способствует утечке данных и неэффективности работы системы информационной безопасности.

При анализе последствий успешных информационных атак в 2022–2024 годах на государственный сектор можно выделить следующие тенденции:

- снижение влияния атак на основную деятельность учреждений (51 % в 2022 году к 43 % в первом квартале 2024 года);
- существенное увеличение фактов утечки конфиденциальной информации (на 11 % в первом квартале 2024 года по сравнению с 2022);
- значительное снижение ущерба интересам государства (на 30 % по сравнению с 2022 годом).

Данные тенденции свидетельствуют о том, что российские государственные органы и учреждения совершенствуют систему информационной безопасности в отношении значимых ранее угроз, но в целом это до сих пор носит ситуационный характер — преодоление последствий, а не профилактика и предотвращение противоправных действий в информационной среде.

Исследуя специфику обеспечения информационной безопасности в государственном секторе, необходимо отметить, что данный сектор как объект информационных угроз не является абсолютным лидером. Итоги 2023 года показывают, что утечка данных как последствие информационных атак наблюдается во всех социально значимых сферах. Наиболее уязвимой с позиции потери данных является банковская сфера и страхование, строительство, нефтегазовая отрасль, транспорт и логистика, здравоохранение (рис. 1).

Анализ вторичных данных результатов исследования уровня информационной безопасности в организациях России показывает, что 66 % фактов утечки данных вследствие роста киберугроз является результатом деятельности сотрудников организаций. Неблагонадежность работника — ключевой социальный фактор, снижающий эффективность системы информационной безопасности. По значению данного фактора в потери персональных данных лидерами являются сфера финансов, государственного управления и здравоохранения. В структуре организации виновниками потери данных выступают чаще всего линейные сотрудники (71 %) и линейные руководители (27 %). Данные тенденции приводят к необходимости активизации развития компетенций граждан в сфере цифровой гигиены, что заявлено в качестве базового условия обеспечения информационной безопасности и определено как стратегический вектор государственной политики, реализуемой Министерством цифрового развития, связи и массовых коммуникаций (Минцифры) РФ [23].

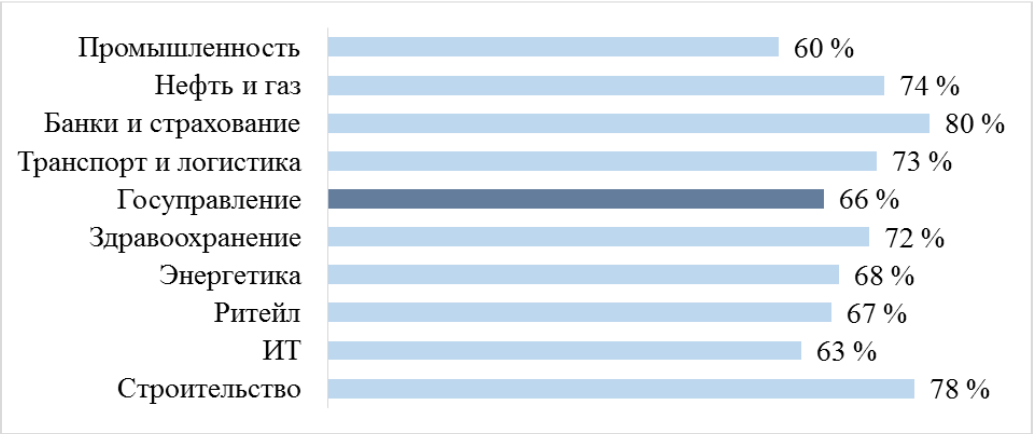

Рис. 1. ***Отрасли, в которых происходили утечки данных в 2023 году (% от общего объема ущерба в результате киберугроз) [13]***

Несмотря на возрастающее год от года количество информационных атак на организации, коммерческий сектор, в отличие от государственного, активнее развивает финансирование обеспечения информационной безопасности — 41 % компаний отмечают увеличение бюджетов. Государственный сектор не стремится к финансированию глобальных изменений в системах противодействия информационным угрозам год от года, оставляя бюджет большинства организаций данного сектора без изменений (рис. 2).

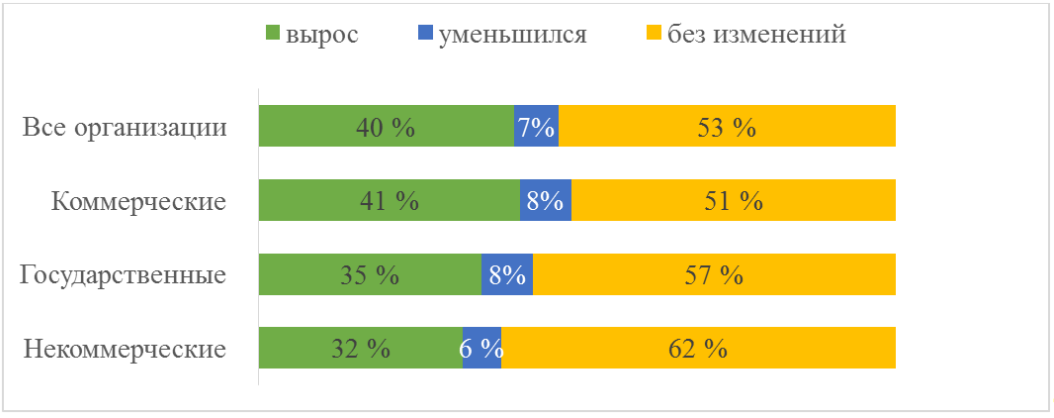

Рис. 2. ***Динамика изменения бюджета на информационную безопасность в организациях различных секторов***

Организации отраслей, столкнувшиеся с существенными потерями, в результате кибератак, активизировали свою политику повышения эффективности противодействия информационным угрозам и финансирования систем обеспечения безопасности, в частности, наиболее подвергающиеся атакам банки и страховые организации почти в половину увеличили свой бюджет на информационную безопасность (рис. 3).

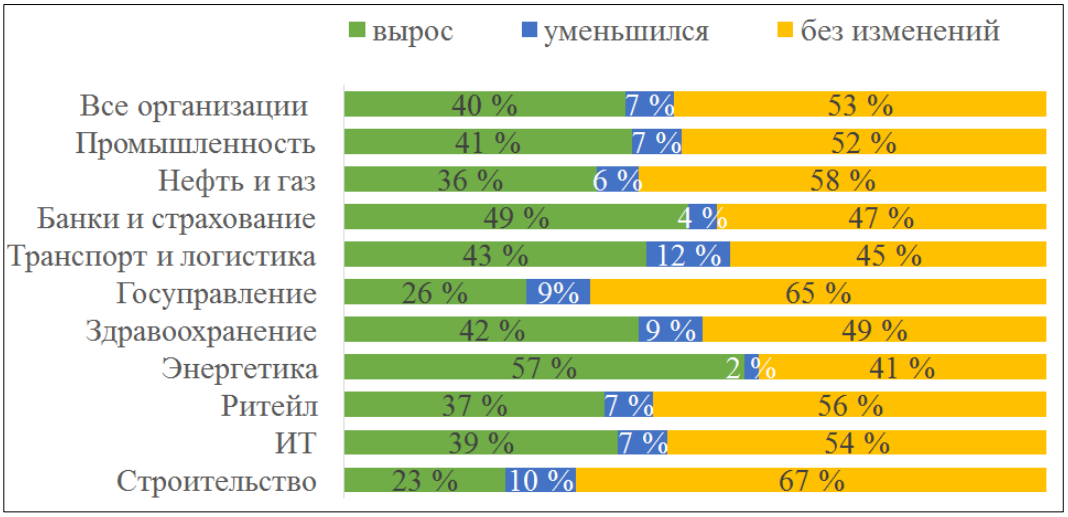

Рис. 3. ***Изменение финансирования информационной безопасности в организациях различных отраслей***

Госсектор в отраслевом разрезе занял еще меньшую позицию в системе повышения объемов финансирования информационной безопасности. По результатам исследования, именно в отрасли государственного управления меньше всего отмечаются изменения в направлении увеличения бюджета на обеспечение информационной безопасности.

Преодоление уязвимости информационных ресурсов и систем в государственном секторе осуществляется за счет активизации внедрения отечественных операционных систем и баз данных (рис. 4).

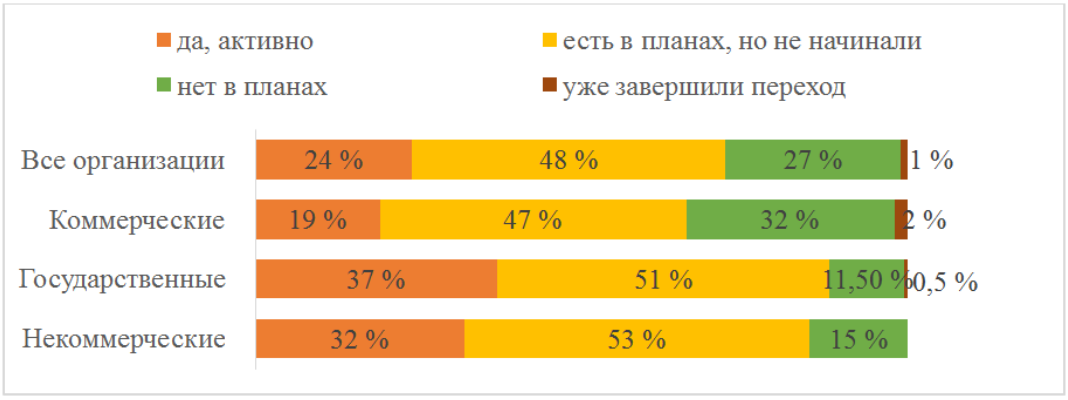

Рис. 4. ***Осуществление перехода организаций на использование отечественного программного обеспечения и баз данных***

Доля государственных организаций, осознающих необходимость импортозамещения в информационно-коммуникационной сфере для преодоления угроз, составляет 88,5 %, из них очень маленькая доля (0,5 %) учреждений, которые завершили переход

на отечественные программные продукты, и достаточно большое количество организаций (51 %), планирующих активную политику перехода на российское программное обеспечение (рис. 5).

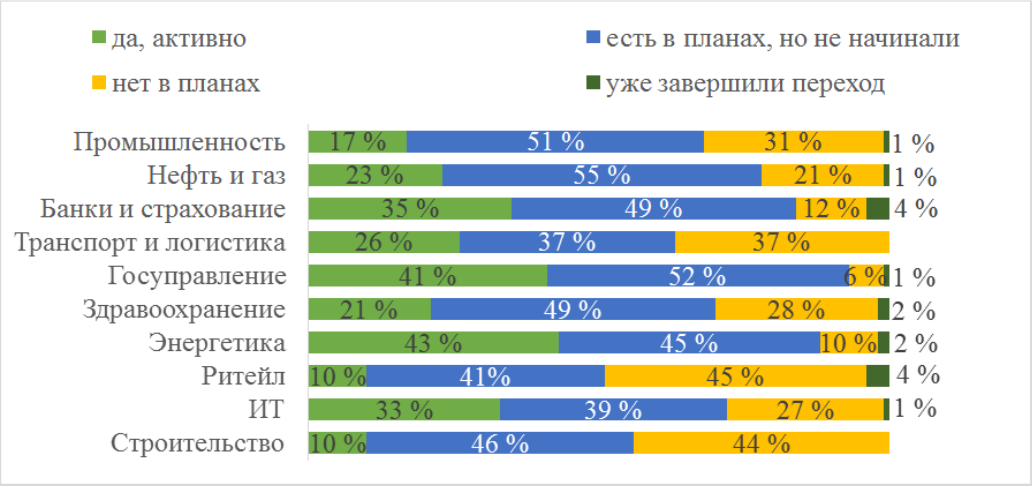

Рис. 5. ***Степень импортозамещения технологий для обеспечения информационной безопасности в отраслевом разрезе***

Результаты исследования показывают, что прослеживается зависимость выявления интенсивности информационных угроз и перехода на использование отечественного программного обеспечения. Те отрасли, которые в период 2021–2023 гг. активно подвергались кибератакам, имеют опыт завершенного перехода к российским технологиям (банки и страхование, ритэйл, госуправление, здравоохранение). В государственном секторе этому процессу еще и поспособствовало принятие Указа президента РФ № 166 от 30 марта 2022 года «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации», который запрещает с 1 января 2025 года использовать иностранное программное обеспечение на значимых объектах критической информационной инфраструктуры органами государственной власти. В соответствии с законодательством к объектам критической информационной инфраструктуры относятся информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, используемые органами государственной власти и учреждениями, то есть фактически все, что обеспечивает технологические условия обработки и хранения информации, информационной безопасности государственного сектора [24].

Анализируя сложившиеся тенденции в системе информационной безопасности государственного сектора, нельзя не согласиться с позицией И. Л. Морозова, который выделяет в качестве основополагающих факторов, определяющих уязвимость России перед информационными угрозами, следующие:

- нескоординированность системы реализации государственной политики обеспечения информационной безопасности между различными органами государственного и муниципального управления, отраслевыми ведомствами и службами, осу-

ществляющими деятельность по противодействию информационным угрозам различного характера (Совет безопасности РФ, Минцифры РФ, Министерство иностранных дел РФ и др.);

- недостаточно эффективно выстроенная система подготовки кадров в сфере обеспечения информационной безопасности, отсутствие системной работы с населением по повышению цифровой гигиены и информационной грамотности, неразвитость консультационно-методической, воспитательной работы, обучения применению технологий противодействия информационным угрозам и социально-психологическому воздействию;
- низкая степень информированности населения о деятельности органов государственной власти, организаций государственного сектора, принятых и реализуемых ими решениях, действующих информационных ресурсах, способствующих доступу населения к данной информации, что порождает возможности для злоумышленников использовать недостоверную информацию о государственных структурах для воздействия на граждан, провоцируя их деятельность, направленную на распространение и повышение значения информационных угроз.

Выводы

В последние годы на фоне геополитических событий информационная безопасность стала стратегически важным свойством системы управления государством. Цифровизация государственных услуг, развитие автоматизированных сервисов обработки данных и регулирования процессов, хранения информации, с одной стороны, направлены на повышение качества услуг для граждан со стороны государственного сектора, а с другой — социальная значимость данного сектора является существенной причиной активизации в отношении его кибератак, целью которых является дискредитация государственных институтов в обществе, развитие социальной напряженности, снижение доверия к государству.

Данные обстоятельства формируют вызовы для политики обеспечения информационной безопасности, требуя регламентации новых процессов, возникающих в информационной среде, вызванных постоянным технологическим совершенствованием используемых систем и инструментов реализации кибератак.

Проведенный анализ показал, что несмотря на постоянное совершенствование правового поля в отношении снижения значимости воздействия информационных угроз на государственный сектор России, он остается одной их самых уязвимых секторов, последствия атак на который имеют существенное значение для граждан, формируя риски для их нормальной жизнедеятельности, повышая их восприимчивость и незащищенность в условиях информационного воздействия.

Информационные угрозы сегодня определены двумя видовыми группами: информационно-техническими и информационно-психологическими. В отношении первой группы постепенно формируется система защиты через отказ от использования зарубежного оборудования и программного обеспечения, импортозамещение средств информационной безопасности, оснащение деятельности органов государственной власти

и объектов критической инфраструктуры российским программным обеспечением, работа ИТ-разработчиков над снижением уязвимостей информационных систем. Вторая же группа угроз, напротив, на сегодняшний день не только остается значимой, но и активно развивается, создавая препятствия для эффективной работы технологических разработок по обеспечению информационной безопасности. Именно человек является ключевой причиной неэффективности мер информационной безопасности. Использование технологий социальной инженерии делают его первостепенным субъектом распространения информационных угроз, уязвимостью самой проработанной технологически системы информационной безопасности.

Современная российская политика обеспечения информационной безопасности должна быть направлена на формирование цифровой гигиены, прежде всего у работников органов государственной власти и бюджетных учреждений, повышение их информационной грамотности, создание и применение технологий противостояния информационным угрозам в киберпространстве.

Список источников

1. Путин призвал повысить требования в сфере информационной безопасности. – Текст : электронный // РИА Новости : сайт. – 2024. – 19 мар. – URL: https://ria.ru/20240319/bezopasnost-1934233370.html?ysclid=m2im9d2az8955279655 (дата обращения: 13.09.2024).

2. Вяткина, А. Киберугрозы в государственном секторе. – Текст : электронный // Positive Technologies : сайт. – 2024. – 03 сен. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/kiberugrozy-v-gosudarstvennom-sektore/ (дата обращения: 10.09.2024).

3. Россия вошла в топ-10 стран по цифровизации госуправления. – Текст : электронный // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : сайт. – 2022. – 17 нояб. – URL: https://digital.gov.ru/ru/events/42223/#:~:text (дата обращения: 10.09.2024).

4. Алексеева, Е. В. Доктрина информационной безопасности Российской Федерации как ключевой аспект правового обеспечения национальной безопасности в информационной сфере / Е. В. Алексеева. – Текст : непосредственный // Ленинградский юридический журнал. – 2016. – № 4 (46). – С. 97–103.

5. Галушкин, А. А. К вопросу о значении понятий «национальная безопасность», «информационная безопасность», «национальная информационная безопасность» / А. А. Галушкин. – Текст : электронный // Правозащитник. – 2015. – № 2. – С. 8. – URL: https://www.elibrary.ru/item.asp?id=23414774.

6. Шерстюк, В. П. Информационная безопасность в системе обеспечения национальной безопасности России, федеральные и региональные аспекты обеспечения информационной безопасности / В. П. Шерстюк – Текст : электронный // Информационное общество. – 1999. – № 5. – С. 3–5. – URL: https://www.elibrary.ru/item.asp?id=9117964.

7. Чапис, М. А. Информационная безопасность государства как правовой порядок обеспечения национальной безопасности в информационной сфере / М. А. Чапис. – Текст : электронный // Наукосфера. – 2024. – № 6 (1). – С. 551–557. – URL: https://doi.org/10.5281/zenodo.11638587.

8. Дятлов, С. А. Цифровая нейро-сетевая экономика : институты и технологии развития : монография / С. А. Дятлов, О. С. Лобанов, Д. В. Гильманов. – Текст : непосредственный. – Санкт-Петербург : СПбГЭУ, 2018. – 325 с.

9. Фазылов, Р. А. Интересы и угрозы Российской Федерации в информационной сфере / Р. А. Фазылов. – Текст : электронный // Инновации. Наука. Образование. – 2021. – № 34. – С. 1617–1623. – URL: https://drive.google.com/file/d/19SYLwY000XRsG0QeMeJTb8W1 KwWGf3Y7/view.

10. Назиев, М. И. Проблема утечки конфиденциальных данных и обеспечение информационной безопасности в государственном секторе / М. И. Назиев, Л. Р. Магомаева. – Текст : непосредственный // Наука и творчество : вклад молодежи : материалы IV всероссийской молодежной научно-практической конференции студентов, аспирантов и молодых ученых, Махачкала, 8–9 ноября 2023 г. – Махачкала : Формат, 2023. – С. 36–40.

11. Андропова, М. В. Совершенствование системы информационной безопасности в государственных учреждениях в РФ / М. В. Андропова. – Текст : непосредственный // Фундаментальные и прикладные исследования : от теории к практике : материалы II международной научно-практической конференции, приуроченной ко Дню Российской науки, Воронеж, 05–09 февраля 2018 г. Том 3. – Воронеж : ООО «АМиСта», 2018. – С. 172–175.

12. Морозов, И. Л. Государственное управление в сфере информационной безопасности современной России : учебно-методическое пособие / И. Л. Морозов ; ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», Волгоградский институт управления. – Волгоград : Волгоградский институт управления — филиал РАНХиГС, 2021. – 88 с.

13. Исследование уровня информационной безопасности в организациях России. Итоги 2023. – URL: https://searchinform.ru/uploads/sites/1/2024/03/godovoe-issledovanie-2023.pdf?ysclid=m2ry1khvcq167845928 (дата обращения: 15.09.2024). – Текст : электронный.

14. Отчет о проблемах информационной безопасности в ИТ-инфаструктурах государственных организаций. Первое полугодие 2020 года. Открытая часть исследования. – URL: https://rt-solar.ru/upload/iblock/e98/Otchet-o-problemakh-informatsionnoy-bezopasnosti-v-IT_infrastrukturakh-gosudarstvennykh-organizatsiy-_pervoe-polugodie-2020-goda_.pdf (дата обращения: 15.09.2024). – Текст : электронный.

15. Указ Президента Российской Федерации «О Стратегии национальной безопасности Российской Федерации» : введ. в действие с 02.07.2021. – Москва, 2021. – URL: https://base.garant.ru/401425792/?ysclid=lt450uou35234098396 (дата обращения: 16.09.2024). – Текст : электронный.

16. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. – URL: http://www.scrf.gov.ru/security/information/document113/ (дата обращения: 16.09.2024). – Текст : электронный.

17. Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. – URL: http://www.scrf.gov.ru/security/information/document131/ (дата обращения: 16.09.2024). – Текст : электронный.

18. Указ Президента Российской Федерации «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» : введ. в действие с 09.05.2017. – URL: https://www.garant.ru/products/ipo/prime/doc/71570570/?ysclid=m2ryfkmc9z631221878 (дата обращения: 16.09.2024). – Текст : электронный.

19. Указ Президента Российской Федерации «О национальных целях развития Российской Федерации на период до 2030 года». – URL: https://www.garant.ru/products/ipo/prime/doc/74304210/?ysclid=m2j203893d649138882 (дата обращения: 16.09.2024). – Текст : электронный.

20. «Цифровое государственное управление». – Текст : электронный // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации : официальный сайт. – 2023. – 05 окт. – URL: https://digital.gov.ru/ru/activity/directions/882/ (дата обращения: 20.09.2024).

21. Обновленная Концепция конвенции ООН по международной информационной безопасности. – URL: http://www.scrf.gov.ru/media/files/file/P7ehXmaBUDOAAcATW2Rwa3yNK1bNAWl9.pdf (дата обращения: 20.09.2024). – Текст : электронный.

22. Герсонская, И. В. Государственный сектор в современной России / И. В. Герсонская. – Текст : непосредственный // Актуальные проблемы развития социально-экономических систем : теория и практика : сборник научных статей 10-й Международной научно-практической конференции, Курск, 29 мая 2020 года. – Курск : ЮЗГУ, 2020. – С. 75–77.

23. Программа кибергигиены и повышения грамотности широких слоев населения по вопросам информационной безопасности. – Текст : электронный // TAdviser : [сайт]. – 2024. – 07 окт. – URL: https://www.tadviser.ru/index.php/Статья:Программа_кибергигиены_и_повышения_грамотности_широких_слоев_населения_по_вопросам_информационной_безопасности (дата обращения: 20.09.2024).

24. Российская Федерация. Законы. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон № 187-ФЗ : [принят Государственной думой 12 июля 2017 года : одобрен Советом Федерации 19 июля 2017 года]. – Москва, 2017. – URL: https://base.garant.ru/71730198/?ysclid=m2ryy5sy2g666124582. – Текст : электронный.

References

1. Putin prizval povysit' trebovaniya v sfere informatsionnoy bezopasnosti. (2024). (In Russian). Available at: https://ria.ru/20240319/bezopasnost-1934233370.html?ysclid=m2im9d2az8955279655

2. Vyatkina, A. (2024). Kiberugrozy v gosudarstvennom sektore. (In Russian). Available at: https://www.ptsecurity.com/ru-ru/research/analytics/kiberugrozy-v-gosudarstvennom-sektore

3. Rossiya voshla v top-10 stran po tsifrovizatsii gosupravleniya. (2022). (In Russian). Available at: https://digital.gov.ru/ru/events/42223/#:~:text

4. Alekseeva, E. V. (2016). Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii kak klyuchevoy aspekt pravovogo obespecheniya natsional'noy bezopasnosti v informatsionnoy sfere. Leningrad legal journal, (4(46)), pp. 97-103. (In Russian).

5. Galushkin, A. A. (2015). K voprosu o znachenii ponyatiy "natsional'naya bezopasnost'", "informatsionnaya bezopasnost'", "natsional'naya informatsionnaya bezopasnost'". Pravozashchitnik, (2), p. 8. (In Russian). Available at: https://www.elibrary.ru/item.asp?id=23414774

6. Sherstyuk, V. P. (1999). Informatsionnaya bezopasnost' v sisteme obespecheniya natsional'noy bezopasnosti Rossii, federal'nye i regional'nye aspekty obespecheniya informatsionnoy bezopasnosti. Information society, (5), pp. 3-5. (In Russian). Available at: https://www.elibrary.ru/item.asp?id=9117964

7. Chapis, M. A. (2024). Information security of the state as a legal procedure for ensuring national security in the information sphere. Naukosphere, (6(1)), pp. 551-557. (In Russian). Available at: https://doi.org/10.5281/zenodo.11638587

8. Dyatlov, S. A., Lobanov, O. S., & Gil'manov, D. V. (2018). Tsifrovaya neyrosetevaya ekonomika: instituty i tekhnologii razvitiya: monografiya. Saint Petersburg, Saint Petersburg Stat University of Economics Publ., 325 p. (In Russian).

9. Fazylov, R. A. (2021). Interesy i ugrozy Rossiyskoy Federatsii v informatsionnoy sfere. Innovatsii. Nauka. Obrazovanie, (34), pp. 1617-1623. (In Russian). Available at: https://drive.google.com/file/d/19SYLwY000XRsG0QeMeJTb8W1KwWGf3Y7/view

10. Naziev, M. I., & Magomaeva, L. R. (2023). Problema utechki konfidentsial'nykh dannykh i obespechenie informatsionnoy bezopasnosti v gosudarstvennom sektore. Nauka i tvorchestvo: vklad molodezhi: materialy IV vserossiyskoy molodezhnoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uchenykh. Makhachkala, Format Publ., pp. 36-40. (In Russian).

11. Andropova, M. V. (2018). Sovershenstvovanie sistemy informatsionnoy bezopasnosti v gosudarstvennykh uchrezhdeniyakh v RF. Fundamental'nye i prikladnye issledovaniya: ot teorii k praktike: materialy II mezhdunarodnoy nauchno-prakticheskoy konferentsii, priurochennoy ko Dnyu Rossiyskoy nauki, T. 3. – Voronezh, OOO "AMiSta", pp. 172-175. (In Russian).

12. Morozov, I. L. (2021). Gosudarstvennoe upravlenie v sfere informatsionnoy bezopasnosti sovremennoy Rossii: uchebno-metodicheskoe posobie. Volgograd, Volgogradskiy institut upravleniya - filial Rossiyskoy akademii narodnogo khozyaystva i gosudarstvennoy sluzhby pri Prezidente Rossiyskoy Federatsii Publ., 88 p. (In Russian).

13. Issledovanie urovnya informatsionnoy bezopasnosti v organizatsiyakh Rossii. Itogi 2023. (2023). (In Russian). Available at: https://searchinform.ru/uploads/sites/1/2024/03/godovoe-issledovanie-2023.pdf?ysclid=m2ry1khvcq167845928

14. Otchet o problemakh informatsionnoy bezopasnosti v IT-infastrukturakh gosudarstvennykh organizatsiy. Pervoe polugodie 2020 goda. Otkrytaya chast' issledovaniya. (In Russian). Available at: https://rt-solar.ru/upload/iblock/e98/Otchet-o-problemakh-informatsionnoy-bezopasnosti-v-IT_infrastrukturakh-gosudarstvennykh-organizatsiy-_pervoe-polugodie-2020-goda_.pdf

15. Ukaz Prezidenta Rossiyskoy Federatsii "O Strategii natsional'noy bezopasnosti Rossiyskoy Federatsii". (In Russian). Available at: https://base.garant.ru/401425792/?ysclid=lt450uou35234098396

16. Osnovnye napravleniya gosudarstvennoy politiki v oblasti obespecheniya bezopasnosti avtomatizirovannykh sistem upravleniya proizvodstvennymi i tekhnologicheskimi protsessami kriticheski vazhnykh ob"ektov infrastruktury Rossiyskoy Federatsii. (In Russian). Available at: http://www.scrf.gov.ru/security/information/document113

17. Vypiska iz Kontseptsii gosudarstvennoy sistemy obnaruzheniya, preduprezhdeniya i likvidatsii posledstviy komp'yuternykh atak na informatsionnye resursy Rossiyskoy Federatsii. (In Russian). Available at: http://www.scrf.gov.ru/security/information/document131/

18. Ukaz Prezidenta Rossiyskoy Federatsii "O Strategii razvitiya informatsionnogo obshchestva v Rossiyskoy Federatsii na 2017-2030 gody". (In Russian). Available at: https://www.garant.ru/products/ipo/prime/doc/71570570/?ysclid=m2ryfkmc9z631221878

19. Ukaz Prezidenta Rossiyskoy Federatsii "O natsional'nykh tselyakh razvitiya Rossiyskoy Federatsii na period do 2030 goda". (In Russian). Available at: https://www.garant.ru/products/ipo/prime/doc/74304210/?ysclid=m2j203893d649138882

20. "Tsifrovoe gosudarstvennoe upravlenie". (2023). (In Russian). Available at: https://digital.gov.ru/ru/activity/directions/882/

21. Obnovlennaya Kontseptsiya konventsii OON po mezhdunarodnoy informatsionnoy bezopasnosti. (In Russian). Available at: http://www.scrf.gov.ru/media/files/file/P7ehXmaBUDOAAcATW2Rwa3yNK1bNAWl9.pdf

22. Gersonskaya, I. V. (2020). Gosudarstvennyy sektor v sovremennoy Rossii. Aktual'nye problemy razvitiya sotsial'no-ekonomicheskikh sistem: teoriya i praktika: sbornik nauchnykh statey 10-y Mezhdunarodnoy nauchno-prakticheskoy konferentsii. Kursk, SWSU Publ., pp. 75-77. (In Russian).

23. Programma kibergigieny i povysheniya gramotnosti shirokikh sloev naseleniya po voprosam informatsionnoy bezopasnosti. (2024). (In Russian). Available at: https://www.tadviser.ru/index.php/Статья:Программа_кибергигиены_и_повышения_грамотности_широких_слоев_населения_по_вопросам_информационной_безопасности

24. Rossiyskaya Federatsiya. Zakony. O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii: Federal'nyy zakon No 187-FZ. (In Russian). Available at: https://base.garant.ru/71730198/?ysclid=m2ryy5sy2g666124582

Информация об авторах / Information about the authors

Попкова Алена Анатольевна, кандидат социологических наук, доцент кафедры маркетинга и муниципального управления, Тюменский индустриальный университет, г. Тюмень, popkovaaa@tyuiu.ru, ORCID: https://orcid.org/0000-0002-8507-8151

Парфенов Константин Владимирович, аспирант, кафедра маркетинга и муниципального управления, Тюменский индустриальный университет, г. Тюмень

Алборов Арсен Робинзонович, соискатель, кафедра маркетинга и муниципального управления, Тюменский индустриальный университет, г. Тюмень

Alena A. Popkova, Candidate of Sociology, Associate Professor at the Department of Marketing and Government Administration, Industrial University of Tyumen, popkovaaa@tyuiu.ru, ORCID: https://orcid.org/0000-0002-8507-8151

Konstantin V. Parfenov, Postgraduate at the Department of Marketing and Government Administration, Industrial University of Tyumen

Arsen R. Alborov, Applicant at the Department of Marketing and Government Administration, Industrial University of Tyumen

Статья поступила в редакцию 29.10.2024; одобрена после рецензирования 06.11.2024; принята к публикации 12.11.2024.
The article was submitted 29.10.2024; approved after reviewing 06.11.2024; accepted for publication 12.11.2024.