Научная статья
УДК 34
https://doi.org/10.24412/2073-0454-2024-2-72-76
EDN: https://elibrary.ru/hmgmxk
NIION: 2003-0059-2/24-999
MOSURED: 77/27-003-2024-02-198

Особенности обеспечения безопасности информационной инфраструктуры Российской Федерации в условиях нестабильных международных отношений

Борис Николаевич Комахин
Московский университет МВД России имени В.Я. Кикотя, Москва, Россия, komakhin@yandex.ru

Аннотация. Исследуется комплекс мер обеспечения безопасности информационной инфраструктуры Российской Федерации в условиях активных угроз со стороны недружественных стран. Анализируются различные сферы утечки информации. Рассмотрены современные возможности защиты информации и информационных систем. Раскрываются особенности правового регулирования при использовании искусственного интеллекта в различных сферах. Сформированы положения обеспечения безопасности информационной инфраструктуры.

Ключевые слова: активные угрозы, информационная безопасность, компьютерные технологии, информационная война, санкции, искусственный интеллект, инновационное развитие

Для цитирования: Комахин Б. Н. Особенности обеспечения безопасности информационной инфраструктуры Российской Федерации в условиях нестабильных международных отношений // Вестник Московского университета МВД России. 2024. № 2. С. 72–76. https://doi.org/10.24412/2073-0454-2024-2-72-76. EDN: HMGMXK.

Original article

Features of ensuring the security of the information infrastructure of the Russian Federation in conditions of unstable international relations

Boris N. Komakhin
Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Moscow, Russia, komakhin@yandex.ru

Abstract. The complex of measures to ensure the security of the information infrastructure of the Russian Federation in the conditions of active threats from unfriendly countries is studied. Various areas of information leakage are analyzed. Modern possibilities of protection of information and information systems are considered. The peculiarities of legal regulation in the use of artificial intelligence in various spheres are revealed. Provisions for ensuring the security of information infrastructure are formed.

Keywords: active threats, information security, computer technology, information warfare, sanctions, artificial intelligence, innovative development

For citation: Komakhin B. N. Features of ensuring the security of the information infrastructure of the Russian Federation in conditions of unstable international relations. Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2024;(2):72–76. (In Russ.). https://doi.org/10.24412/2073-0454-2024-2-72-76. EDN: HMGMXK.

Сложившаяся в современном мире ситуация, когда коллективный запад во главе с Соединенными Штатами Америки создает активную угрозу террористического характера, угрожающую безопасности людей и государств в различных уголках земного шара, все в большей мере проявляется необходимость защищать не только территориальные границы России, но и информационные ресурсы, а также системы, предназначенные для обеспечения информационной безопасности.

В это же время, обостряющиеся конфликты, столкновение территориальных, политических и экономических интересов стран никак не способствует тому, чтобы государства эффективно и на взаимной основе осуществляли сотрудничество друг с другом в передовых развивающихся направлениях, обменивались необходимой информацией, различными достижениями, новейшими открытиями и показателями.

С внедрением компьютерных технологий во все сферы деятельности государственных органов, служб

(в том числе и правоохранительных), в различные отрасли промышленности, бизнеса, науки и техники, с большим вниманием требует отнестись к Указу Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

Следует учитывать, что ежегодно увеличивается утечка всевозможных данных из различных компьютерных информационных систем, финансовых и медицинских организаций, сфер энергетики и науки, сервисов онлайн-продаж, поставщиков логистических услуг, служб доставки еды, промышленных товаров и продажи билетов, утечка информации происходит даже из правоохранительных и государственных органов и силовых структур. И такая тенденция продолжает увеличиваться, так как это становится дополнительным заработком для хакеров и инсайдеров.

Кроме того, все увеличивающаяся санкционная политика западного мира приводит нашу страну к изоляции от новых современных зарубежных технологий в области импортных средств защиты информации, запрет на приобретение и использование иностранных программно-аппаратных комплексов, а также недостаточное количество высококвалифицированных кадров в данной сфере не позволяет своевременно, быстро и в полной мере устранять все угрозы информационной безопасности.

Информация занимает все более важное место в обществе, так как не только появляются новые средства ее сбора, хранения, обработки и распространения, но информация все более активно используется гражданами и организациями. Кроме того, меняется и отношение общества к самой информации. Сегодня информация во многом определяет направления развития всего общества и государства. В связи с этим актуальными являются вопросы обеспечения информационной безопасности.

Неслучайно в настоящее время активно используется термин «информационная война». Стоит отметить, что данное понятие уже достаточно прочно вошло в оборот не только в России и недружественных нам стран, но и в иных государствах. Информационные войны разрушают принятые в международных союзах и организациях нормы и принципы, и в определенной степени диктуют собственные правила игры и развитие международных отношений. Поэтому проблема защиты информации и информационных систем приобретает все большую актуальность и необходимость комплексного исследования административно-правового регулирования отношений в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации на базе современного административного законодательства, с учетом требований новых современных технических средств, организационных и юридических мероприятий, которые могут обеспечить информационную безопасность в современных непростых условиях.

Вопросы обеспечения информационной безопасности в нашей стране регулируют многие нормативные акты, среди которых Конституция Российской Федерации, акты информационного права, административного и уголовного права и пр. В настоящее время соответствующие нормы содержатся в большинстве действующих нормативных актов. Формирование соответствующего законодательства в рассматриваемой сфере является одной из приоритетных задач государства, так как новые угрозы информационной безопасности требуют принятия соответствующих мер. Современные информационные технологии должны внедряться совместно с мерами по обеспечению информационной безопасности, так как только так можно выявить информационные угрозы.

В связи с тем, что в настоящее время информационная среда быстро развивается, государственные органы должны иметь возможность вовремя реагировать на угрозы и принимать необходимые меры для их предотвращения.

Российский законодатель за нарушения требований по обеспечению защиты информации предусмотрел административную и уголовную ответственность для всех субъектов соответствующих правоотношений, т. е. к ответственности могут быть привлечены не только граждане и организации, но и государственные и муниципальные органы власти и подведомственные им учреждения. Дифференциация ответственности осуществляется на основе критерия тяжести причиненного вреда. Также с целью компенсации вреда могут применяться и меры гражданско-правовой ответственности.

Таким образом, если проанализировать нормативные акты, обеспечивающие информационную безопасность, то можно сделать вывод, что на сегодняшний день сформирована достаточно крепкая ос-

нова для последующего обеспечения информационной безопасности России. В результате принятие все новых законов отходит на второй план, а наиболее важной задачей в исследуемой сфере становится увеличение качества существующих законодательных актов.

Следует учитывать, что в настоящее время идет быстрое внедрения компаниями искусственного интеллекта в свою деятельность и, как справедливо отмечает Н. Д. Эриашвили и А. В. Минаков, «искусственный интеллект широко применяют в банковской сфере, на транспорте, в промышленности и в электронной коммерции. Наиболее значимыми технологиями последних лет являются электронная почта, интернет, гаджеты, компьютерное (машинное) зрение, интернет вещей, технологии беспроводной связи, беспилотные автомобили, машинное обучение, виртуальная и дополнительная реальность, облачные вычисления, блокчейн» [1, с. 114], что оказывает весьма сильное влияние на государство и общество, а также на каждого отдельного человека.

Этот процесс уже давно является вполне материальным и обусловленным политическими аспектами и превращается в огромную индустрию с огромным вложением денежных средств. В то же время, значимость обеспечения безопасности информационной инфраструктуры не только большого бизнеса, но и Российской Федерации в целом во всех сферах, где используется искусственный интеллект, все увеличивается. Поэтому требуется адекватное правовое регулирование, с учетом положений закона о защите данных, обучение соответствующих кадров (в том числе научных), разработка антимонопольной политики в данном направлении.

Разработчики систем, обеспечивающих защиту безопасности информационной инфраструктуры, все больше обращают внимание на то, что в современных условиях видеоаналитика и видеонаблюдение являются самыми популярными средствами обеспечения безопасности повседневной жизни жителей больших городов, предприятий и учреждений через установку видеокамер. На улицах, на транспорте, в местах скопления людей и на различных охраняемых объектах с использованием Интернета и обработки полученной информации с помощью искусственного интеллекта.

Формирующаяся политика в данном направлении включает в себя не только наблюдение за происходящими событиями на фиксируемой видеокамерами территории, но и обеспечение вычислительных задач по обнаружению интересующих объектов, их сопровождение с захватом изображений высокой четкости, бесконтактная проверка, обнаруживающая высокую температуру тела и обеспечивающая обнаружение заболевших людей, а также видеофиксация и распознание в режиме реального времени интересующих компетентные органы событий, обработка полученных данных, резервное копирование и осуществление последующих действий в соответствии с поставленными задачами требует высокой надежности, автоматизированной оптической проверки, необходимой конфиденциальности и недопущения утечки информации к субъектам, которые могут ее использовать в своих противоправных намерениях.

В целях обеспечения безопасности информационной инфраструктуры необходимо учитывать, что современные компьютерные устройства подвержены критической уязвимости по целому ряду использованных продуктов; неточности могут возникать из-за некорректной обработки пользовательских данных, которые считываются из памяти устройства; возможно использование хакерами root-права (доступ к файлам, действиям оперативной системы и ее внутренним функциям) на устройство, воспользовавшись доступом к операционной системе; уязвимость позволяет неавторизованному пользователю удаленно выполнять код на скомпрометированных устройствах и т. д.

Следует согласиться с С. И. Макаренко, что «атакующие информационно-технические воздействия ориентированы на непосредственное воздействие на информацию, системы ее сбора, передачи, хранения, обработки и представления, а также на используемые в этих системах информационные технологии, как правило, с целью снижения уровня информационной безопасности или эффективности функционирования» [2, с. 189].

Чтобы защитить информационную инфраструктуру от возможных несанкционированных проникновений со стороны как хакерских атак, так и внешних воздействий, необходимо внедрение интеллектуальной автоматизации, объединяющей разнообразные высокоразвитые технологии и сервисы для выполнения различных производственных задач, направленные на повышение производительности в сложившихся непростых условиях.

При организации данного направления требуется соединение между использованием возможностей искусственного интеллекта (машиной) и человеком, как решающего фактора при принятии окончательного решения, например, человеко-машинный интерфейс (ЧМИ — это методы и средства обеспечения непосредственного взаимодействия между оператором и технической системой, представляющих возможности оператору управлять этой системой и контролировать ее работу [3, с. 64]), поиск неисправностей в системе обеспечения безопасности, мониторинг и автоматизацию собираемой информации, проверку и наблюдение за окружающей средой, интеграцию разработанного производственного плана, управление складскими запасами, базами данных и приложениями для обработки различных сведений.

Для того, чтобы субъекты, обеспечивающие информационную безопасность как в предпринимательстве, так и в различных государственных сферах, могли функционировать и развиваться, требуются эффективные методы конкуренции на рынках, с учетом развития современных информационных технологий. Именно информационные технологии в настоящее время являются наиболее эффективным средством защиты общества и государства, так как они используются во всех отраслях и сферах. Поэтому в мире происходит постоянное изменение существующих социальных и экономических условий, разрабатываются и внедряются в практику важные научные и технические достижения, к которым нам необходимо своевременно получать доступ в полном объеме, чтобы обеспечить своевременную информационную безопасность всем государственным и коммерческим ресурсам. Как отмечает А. А. Фатьянов, «средства получения необходимой информации из различных источников, подключенных к сети Интернет и передающих сигналы в радиоэфир, показывают экспоненциальный рост своего совершенствования. И в этих условиях важным является не только обозначение круга защищаемой информации, но и выстраивание действенных механизмов защиты этих сведений в различных информационных средах» [4, с. 405].

В настоящее время, считаем необходимым обеспечение безопасности информационной инфраструктуры всех сфер деятельности Российской Федерации определить как стратегический ресурс общества и государства, так как она позволяет осуществлять эффективный процесс развития без постороннего вмешательства недружеских сил. Она выполняет ведущую роль и стала обязательным важным фактором производства. Обеспечив своевременную и в полном объеме безопасность информационной инфраструктуры и ее инновационное развитие, относящуюся к тем средствам, при помощи которых можно существенно снизить затраты на производство необходимой продукции, товаров и услуг. Стоит отметить, что важность обеспечения безопасности информационной инфраструктуры в настоящее время все повышается, что обусловливается происходящими в мире изменениями как в политической и социальной сферах, так и в экономической деятельности. Субъекты экономической деятельности сейчас могут эффективно функционировать и развиваться только при наличии необходимого обеспечения безопасности информационной инфраструктуры.

Подводя итог изложенному, можно сделать выводы, что на сегодняшний день сформирована достаточно крепкая основа для последующего обеспечения информационной безопасности России. Как уже отмечалось выше, в результате принятия все новых законов наиболее важной задачей в исследуемой сфере становится увеличение качества существующих законодательных актов. В связи с тем, что в настоящее время информационная среда быстро развивается, государственные органы должны иметь возможность вовремя реагировать на угрозы и принимать необходимые меры для их предотвращения.

Обеспечение безопасности информационной инфраструктуры представляет собой создание системы активной защиты всех органов власти, физических и юридических лиц использующих информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, а также компьютерные сети и сети электросвязи.

Важным способом обеспечения безопасности информационной инфраструктуры в настоящее время является разработка новых российских продуктов, создание самостоятельных платформ, посредством которых передается информация, создание собственных средств связи и программного обеспечения, а также подготовка новых специалистов в сфере информационной безопасности, что в резуль-

тате позволит не только защитить данные, но и снизить зависимость нашей страны от зарубежных государств.

Список источников

1. Эриашвили Н. Д., Минаков А. В. Внедрение цифровых технологий в различные сферы национального хозяйства и формирование глобального цифрового пространства // Вестник Московской академии Следственного комитета Российской Федерации. 2022. № 4. С. 112–124.

2. Макаренко С. И. Защита компьютерных сетей и телекоммуникаций : учеб. пособие. СПб : Наукоемкие технологии, 2024.

3. Курочкин М. А., Ясинская Ю. В., Пантюхин О. И. Человеко-машинный интерфейс и его применение в системах управления // Неделя науки Санкт-Петербургского государственного морского технического университета. 2021. № 1-1.

4. Фатьянов А. А. Служебная тайна как элемент обеспечения национальной безопасности России // Сибирское юридическое обозрение. 2023. Т. 20. № 4. С. 397–405.

References

1. Eriashvili N. D., Minakov A. V. The introduction of digital technologies in various spheres of the national economy and the formation of a global digital space // Bulletin of the Moscow Academy of the Investigative Committee of the Russian Federation. 2022. № 4. P. 112–124.

2. Makarenko S. I. Protection of computer networks and telecommunications : textbook. St. Petersburg : High-tech Technologies, 2024.

3. Kurochkin M. A., Yasinskaya Yu. V., Pantyukhin O. I. Human-machine interface and its application in control systems // Science Week of St. Petersburg State Maritime Technical University. 2021. № 1-1.

4. Fatyanov A. A. Official secrets as an element of ensuring national security of Russia // Siberian Legal Review. 2023. Vol. 20. № 4. P. 397–405.

Библиографический список

1. Ломанов Е. Н., Комахин Б. Н., Поздняков Е. В. и др. Цифровизация управления : антикоррупционный курс административных и финансовых правоотношений: учеб. пособие // под общ. ред. В. А. Прокошина. М. : Юстиция, 2018.

Bibliographic list

1. Lomanov E. N., Komakhin B. N., Pozdnyakov E. V. and others. Digitalization of management : anti-corruption course of administrative and financial legal relations: studies the manual // under the general editorship of V. A. Prokoshin. M. : Justice, 2018.

Информация об авторе

Б. Н. Комахин — профессор кафедры административного права Московского университета МВД России имени В.Я. Кикотя, доктор юридических наук, доцент, заслуженный сотрудник органов внутренних дел Российской Федерации.

Information about the author

B. N. Komakhin — Professor of the Department of Administrative Law of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Doctor of Legal Sciences, Associate Professor, Honored Employee of the Internal Affairs Bodies of the Russian Federation.

Статья поступила в редакцию 31.01.2024; одобрена после рецензирования 18.03.2024; принята к публикации 04.04.2024.

The article was submitted 31.01.2024; approved after reviewing 18.03.2024; accepted for publication 04.04.2024.