DOI 10.22394/2073-2929-2023-04-62-72

Финансовое обеспечение мероприятий по защите информации: проблемы и пути решения[1]

Перминова Е. А.
Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация
e-mail: vice.csp@gmail.com
ORCID: 0000-0001-6920-9142

РЕФЕРАТ

Цель. Освещение проблемы обеспечения экономической безопасности в условиях недостаточного финансирования мероприятий по защите информации как со стороны государства, которое устанавливает требования к защите информации ограниченного доступа различных типов, начиная от государственной тайны и заканчивая персональными данными граждан, так и со стороны организаций, которые реализуют указанные требования.

Задачи. Формирование предложений по преодолению трудностей при реализации мероприятий по финансовому обеспечению защиты информации в организациях с целью реализации мероприятий по обеспечению экономической безопасности.

Методология. В настоящей работе с помощью методов факторного, статистического и количественного анализа рассмотрена статистическая информация в сфере финансирования мероприятий по защите информации, оценены параметры финансирования некоторых мероприятий исходя из открытых данных, представленных в Единой информационной системе в сфере закупок, а также оценены положения правовых актов Российской Федерации в сфере информационной безопасности и государственно-частного партнерства и предпринята попытка доказательства наличия проблем в финансировании мероприятий по защите информации.

Результаты. Обосновано, что обеспечение экономической безопасности ЕЭАС (на примере Российской Федерации) на основе финансового обеспечения мероприятий по защите информации является одной из наиболее актуальных проблем в современном цифровом мире. С каждым годом угрозы для безопасности информационных систем становятся все более сложными и утонченными, требуя от организаций и компаний дополнительных усилий и ресурсов для эффективного противодействия. Предложены практические пути решения проблемы финансирования мероприятий по защите информации с целью обеспечения экономической безопасности, используя как возможность расширения государственно-частного партнерства в указанной сфере, так и другие мероприятия, которые могут непосредственно использовать организации.

Выводы. Несмотря на необходимость обеспечения экономической безопасности, многие организации сталкиваются с финансовыми трудностями при осуществлении мероприятий по обеспечению защиты информации. Ограниченные бюджетные средства, неправильное распределение ресурсов, неэффективная стратегия финансирования, трудности в поиске и закупке эффективного российского программного обеспечения и технических средств защиты информации в условиях санкционного воздействия на Российскую Федерацию — все это преграды на пути успешного обеспечения экономической безопасности.

Ключевые слова: экономическая безопасность, государственно-частное партнерство, защита информации, информационные технологии, организация, мероприятия

[1] Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финансового университета при Правительстве Российской Федерации 2023 года по теме «Теоретические основы формирования новой парадигмы управления социально-экономическим, технологическим и финансовым развитием России: междисциплинарный синтез эволюционных и волновых концепций».

Для цитирования: Перминова Е. А. Финансовое обеспечение мероприятий по защите информации: проблемы и пути решения // Евразийская интеграция: экономика, право, политика. 2023. Т. 17. № 4. С. 62–72.
https://doi.org/10.22394/2073-2929-2023-04-62-72

Financial Support for Information Protection Measures: Problems and Solutions

Elena A. Perminova
Financial University under the Government of the Russian Federation, Moscow, Russian Federation
e-mail: vice.csp@gmail.com
ORCID: 0000-0001-6920-9142

ABSTRACT
Aim. Coverage of the problem of ensuring economic security in conditions of insufficient financing of information protection measures both from the state, which establishes requirements for the protection of restricted access information of various types, ranging from state secrets to personal data of citizens, and from organizations that implement these requirements.
Tasks. Formation of proposals to overcome difficulties in the implementation of financial measures to ensure the protection of information in organizations in order to implement measures to ensure economic security.
Methods. In this paper, using the methods of factor, statistical and quantitative analysis, statistical information in the field of financing information protection measures is considered, the parameters of financing some measures are estimated based on open data presented in the Unified Information System in the field of procurement, as well as the provisions of legal acts of the Russian Federation in the field of information security and public-private partnership and an attempt has been made to prove the existence of problems in the financing of information protection measures.
Results. It is proved that ensuring the economic security of nuclear power plants (on the example of the Russian Federation) on the basis of financial support for information protection measures is one of the most pressing problems in the modern digital world. Every year, threats to the security of information systems are becoming more complex and sophisticated, requiring organizations and companies to make additional efforts and resources to effectively counter. Practical ways of solving the problem of financing information protection measures in order to ensure economic security are proposed, using both the possibility of expanding public-private partnership in this area and other measures that organizations can directly use.
Conclusions. Despite the need to ensure economic security, many organizations face financial difficulties in implementing information security measures. Limited budget funds, improper allocation of resources, inefficient financing strategy, difficulties in finding and purchasing effective Russian software and technical means of information protection in the conditions of sanctions impact on the Russian Federation – all these are obstacles to the successful provision of economic security.
Keywords: economic security, public-private partnership, information protection, information technology, organization, events
For citing: Perminova E. A. Financial Support for Information Protection Measures: Problems and Solutions // Eurasian Integration: Economics, Law, Politics. 2023. V. 17. No. 4. P. 62–72. (In Rus.)
https://doi.org/10.22394/2073-2929-2023-04-62-72

Введение

Обеспечение экономической безопасности в современном мире является одной из приоритетных задач, на решение которой нацелены большинство имеющихся ресурсов, находящихся в распоряжении как государства в целом, так и хозяйствующих субъектов в частности.

С точки зрения ЕАЭС в условиях беспрецедентного давления на государства-члены со стороны ряда недружественных государств и интеграционных объединений в виде введения санкций на Россию и Беларусь и запугивания других членов вводом санкций при усилении сотрудничества с Россией обеспечение экономической безопасности является одной из важнейших задач как на уровне Евразийской экономической комиссии, так и на уровне суверенного руководства государств-членов.

В связи с большим объемом информации в данной статье в качестве объекта рассмотрения будет представлена Российская Федерация, как наиболее влиятельная страна с точки зрения развития информационных технологий и функционирования системы защиты информации и обеспечения экономической безопасности. В конце статьи будет коротко представлен обзор документов других государств — членов ЕАЭС с точки зрения обеспечения экономической безопасности и реализации мероприятий по защите информации.

Защита информации как один из элементов экономической безопасности

В России вопросам обеспечения экономической безопасности посвящен указ Президента РФ от 13.05.2017 № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» (далее — Стратегия экономической безопасности).

В соответствии с терминами, представленными в Стратегии экономической безопасности, под экономической безопасностью понимается состояние защищенности национальной экономики от внешних и внутренних угроз, при котором обеспечиваются экономический суверенитет страны, единство ее экономического пространства, условия для реализации стратегических национальных приоритетов Российской Федерации[1].

В указанной стратегии определено, что одним из элементом обеспечения экономической безопасности является реализация информационных мер, которые осуществляются органами государственной власти, органами местного самоуправления и Центральным банком Российской Федерации во взаимодействии с институтами гражданского общества.

Одним из вызовов экономической безопасности является слабая инновационная активность, отставание в области разработки и внедрения новых и перспективных технологий (в том числе технологий цифровой экономики).

В статье О. П. Чечина отмечено, что «Приоритетной задачей обеспечения экономической безопасности, особенно в быстроменяющихся внешних условиях, является прогнозирование угроз и рисков, к реализации которых необходимо готовиться на постоянной основе. Всеобъемлющим глобальным вызовом является тенденция эволюции цифрового мира» [9, с. 93].

Современная мировая ситуация в условиях цифрового мира характеризуется все более частым использованием нестандартных подходов к нанесению экономического ущерба государству с использованием информационных технологий, в результате чего ведущие позиции занимают так называемые информационно-экономические войны, которые несколько десятилетий назад использовались крайне ограниченно. Данные войны основаны на развитии информационных технологий и, как абсолютно верно отмечают Т. А. Шаклеина и А. А. Байков, являются «революцией в военном деле» [3, с. 243].

В современном мире, даже в самой технологически отсталой стране, люди, у которых имеется Интернет, а, согласно Digital 2022 Global Overview Report [Там же], таких в 2022 г. на Земле было 5,16 млрд чел., или 64,4% населения, так или иначе задействованы в нацеленных на их сознание целенаправленных дезориентирующих событиях. Но главное внимание со стороны специальных служб государств уделяется нанесению ущерба экономической безопасности России за счет совершения целенаправленных компьютерных атак на инфраструктуру организаций и предприятий.

В РФ в последние несколько лет защите информации, как одному из основных элементов обеспечения экономической безопасности, уделяется особо большое внимание. Развитие технологий и все боль-

[1] Указ Президента РФ от 13.05.2017 № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» // Собрание законодательства РФ. 15.05.2017. № 20. Ст. 2902.

шая зависимость от цифровых систем приводит к увеличению угроз и рисков в сфере экономической и информационной безопасности. Д. В. Таловерова в своей статье характеризует современное состояние информационной безопасности следующим образом: «Информационное пространство, глобальная сеть Интернет становятся новой реальностью, где, с одной стороны, совершенно новые объекты преступлений входят в структуру ранее неизвестных нам составов преступлений, а с другой — современные информационные технологии выступают в качестве новых способов и средств совершения уже хорошо известных нам преступлений» [6, с. 45]. В связи с этим необходимость проведения мероприятий по защите информации становится неотъемлемой частью деятельности как государства, так и организаций с целью обеспечения экономической безопасности Российской Федерации.

Анализ проблемных вопросов по обеспечению защиты информации

Однако проведение таких мероприятий требует финансового обеспечения. Ведь для эффективной защиты информации в экономических системах необходимо обеспечить не только наличие современного оборудования и программного обеспечения, но и обучение персонала, а также проведение аудита и мониторинга системы информационной безопасности. Все это требует значительных финансовых затрат.

При этом на уровне законодательства, а также регуляторов необходимости регулирования финансового обеспечения защиты информации уделяется крайне мало внимания.

В ГОСТ 50922-2006[1] выделено четыре вида обеспечения защиты информации: правовая защита информации, техническая защита информации, криптографическая защита информации и физическая защита информации. В данном документе не выделен такой вид обеспечения защиты информации, как финансовое обеспечение.

Определяющим законом, который выделяет два основных типа информации: общедоступная информация и информация, доступ к которой ограничен федеральными законами (информация ограниченного доступа), а также устанавливает необходимость защиты информации ограниченного доступа, является Закон об информации, информационных технологиях и о защите информации[2]. В ст. 9 указанного закона неявным образом выделены следующие типы информации ограниченного доступа: государственная тайна, коммерческая тайна, служебная тайна, профессиональная тайна, персональные данные, а также иные виды тайн.

При этом четкий порядок финансирования мероприятий по защите информации ограниченного доступа определен только для государственной тайны в ст. 29 Закона о государственной тайне[3].

Для остальных видов информации ограниченного доступа ни в федеральных законах, ни в подзаконных актах порядок финансового обеспечения защиты информации не определен.

Все это приводит к тому, что для любого руководителя организации финансирование мероприятий по защите информации является одной из основных проблем, т. к. данная деятельность, с точки зрения любого руководителя, не приносит никакой прибыли, но требует больших финансовых вложений для выполнения требований законодательства и подзаконных актов по защите информации.

Основным подходом при защите информации является то, что защищаемая информация должна приносить определенную пользу ее собственнику и оправдывать затрачиваемые на ее защиту средства [8, с. 31].

---

[1] ГОСТ 50922-2006 Защита информации. Основные термины и определения : нац. стандарт Российской Федерации, утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст, введен взамен ГОСТ Р 50922-96, дата введения 01.02.2008 [Электронный ресурс] // Каталог национальных стандартов. URL: https://www.rst.gov.ru/portal/gost/home/standarts/catalognational?portal:componentId=3503536e-2ac1-4753-8ed1-09a92fee02de&portal:isSecure=false&portal:portletMode=view&navigationalstate=JBPNS_rO0ABXdPAAplbnRpdHlOYW1lAAAAAQALRE9DVU1FTlRfMTEABmFjdGlvbgAAAAEABnNlYXJjaAAIZW50aXR5SWQAAAABAAUxMjgwOAAHX19FT0ZfXw** (дата обращения: 14.10.2023).

[2] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 31.07.2023) // Собрание законодательства РФ. 31.07.2006. № 31 (часть 1). Ст. 3448.

[3] Закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне» (ред. от 04.08.2023) // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 21.09.1993. № 38. Ст. 1480.

При этом, с точки зрения руководителя организации, защищаемая информация, например персональные данные работников, или объекты, которые отнесены к критической информационно инфраструктуре Российской Федерации, большой ценности не имеют. С экономической точки зрения (если не считать штрафы, и то достаточно условно, т. к. в большинстве случаев штрафы по сравнению с масштабом экономического оборота организации и не такие большие) сама организация не будет терпеть никаких убытков, если будут разглашены персональные данные работников, но при этом на системы защиты этих персональных данных для выполнения требований законодательства и подзаконных актов о защите персональных данных руководитель организации вынужден выделять достаточно большие ресурсы. Только содержание штата подразделений по защите информации обходится организации в несколько десятков миллионов рублей в год, не говоря уже о стоимости технических средств защиты информации, которые могут достигать достаточно внушительных сумм, не считая затрат на их обслуживание.

Напрямую подтвердить указанную информацию достаточно затруднительно, т. к. в большинстве случаев затраты компаний на обеспечение информационной безопасности являются закрытыми данными, как минимум выполняя требования ст. 3 Закона о коммерческой тайне[1].

Но в открытых публикациях на официальном сайте Единой информационной системы в сфере закупок[2] можно найти, какую сумму организации готовы заплатить подрядчикам для разработки и обслуживания систем защиты информации. В таблице представлены примеры тендеров при поиске поставщиков в сфере защиты информации. В таблице представлены примеры тендеров при поиске поставщиков в сфере защиты информации.

Таблица

Примеры тендеров при поиске поставщиков в сфере защиты информации[3]

Table. Examples of tenders when searching for suppliers in the field of information security

Организация, осуществляющая размещение тендера	Наименование тендера	Начальная цена тендера, руб.
ФГУП «Государственная корпорация по организации воздушного движения в Российской Федерации»	Оказание услуг по технической поддержке системы защиты информации локальной вычислительной сети филиала «Аэронавигация Северо-Запада» с присоединенными Сыктывкарским, Воркутинским, Печорским, Усинским и Ухтинским ЦОВД, включая закупку сертификатов технической поддержки и техническое сопровождение присоединенных ЦОВД	53 028 680,00
Фонд пенсионного и социального страхования Российской Федерации	Оказание услуг по периодическому контролю обеспечения уровня защищенности информации, содержащейся в Федеральной государственной информационной системе «Федеральный реестр инвалидов»	4 236 420,00
Межрегиональная инспекция Федеральной налоговой службы по централизованной обработке данных	Поставка оборудования для обеспечения защиты конфиденциальной информации	366 985 800,00
ФГУП «Объединенный эколого-технологический и научно-исследовательский центр по обезвреживанию РАО и охране окружающей среды»	Поставка ПАК ViPNet Coordinator для нужд филиала «Уральский территориальный округ» ФГУП «РАДОН»	1 831 500,00
Департамент города Москвы по конкурентной политике	Поставка программного обеспечения для защиты информации	126 860 596,15

В таблице исключительно для примера представлена лишь малая часть тендеров. При вводе в строке поиска запроса «система защиты информации» Портал госзакупок выдает более 30 тыс. записей.

Представленные в таблице примеры показывают, что при поиске подрядчиков в сфере защиты информации организации готовы выплачивать миллионы, а иногда и сотни миллионов рублей. При этом

[1] Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (ред. от 14.07.2022) // Собрание законодательства РФ. 09.08.2004. № 32. Ст. 3283.

[2] Официальный сайт Единой информационной системы в сфере закупок [Электронный ресурс]. URL: https://zakupki.gov.ru/epz/main/public/home.html (дата обращения: 15.10.2023).

[3] Составлено автором по результатам анализа официального сайта Единой информационной системы в сфере закупок.

необходимо обратить внимание, что в Единой информационной системе в сфере закупок тендеры размещают в основном государственные организации, которые выполняют требования законодательства Российской Федерации о закупках[1]. И финансирование указанных мероприятий, как правило, осуществляется из средств федерального бюджета.

Но остается открытым вопрос, что делать коммерческим организациям, которые, основываясь на ч. 1 ст. 50 Гражданского кодекса Российской Федерации[2], преследуют в качестве основной цели деятельности извлечение прибыли? Почему владелец коммерческой организации должен тратить собственные деньги на деятельность, которая априори не приносит прибыль (особенно в сфере защиты персональных данных), а является заведомо убыточной и только из-за того, что законодатель и регулятор требуют это делать, но при этом ни законодатель, ни регулятор не озадачиваются вопросом, а на какие финансовые средства владелец коммерческой организации сможет обеспечить реализацию требований по защите информации?

Конечно, можно уповать на гражданскую сознательность руководителей и владельцев организаций, опираясь на то, что сфера защиты информации очень важна. И несомненно, большинство руководителей это понимают, учитывая то, что в случае инцидентов информационной безопасности возникают не только финансовые риски, а также различного рода репутационные издержки, когда компания не сможет выполнить взятые на себя обязательства, а также есть вероятность потери клиентской базы и изыскивают средства на реализацию мероприятий по защите информации, что подтверждают аналитические исследования. Так, по данным фонда «Центр стратегических разработок», объем российского рынка продуктов и услуг в сфере информационной безопасности по итогам 2022 г. достиг 193,3 млрд руб., увеличившись на 4% в сравнении с 2021 г. [8, с. 6], а по итогам 2023 г. прогнозируемый рост рынка составит 31%, достигнув суммы 252 млрд руб. [5, с. 17].

Но столь оптимистичные прогнозы говорят только о том, что руководители организаций будут вынуждены изыскивать средства из собственных бюджетов, что в большинстве случаев делается достаточно неохотно.

При этом государство готово в 2023 г. выделить на продукты и услуги в области информационной безопасности в рамках федерального проекта «Информационная безопасность» только 139,35 млрд руб.[3]

Поэтому одной из основных проблем финансового обеспечения мероприятий по защите информации является недостаточное финансирование данных мероприятий, причем это касается и государственных организаций.

Многие руководители организаций склонны экономить на безопасности информации, относя эту задачу к второстепенным или незначительным. В результате такой подход может привести к серьезным последствиям: утечке конфиденциальной информации, хакерским атакам, потере доверия клиентов и парализации бизнеса.

Особенно эти утечки касаются такой чувствительной информации, как персональные данные. По данным Аналитического центра информационной безопасности компании InfoWathc, в России в первом полугодии 2023 г. общее количество утечек информации сократилось на 17,5% по сравнению со вторым полугодием 2022 г. [7, с. 6], при этом количество утечек записей о персональных данных в первом полугодии 2023 г. увеличилось на 72% по сравнению со вторым полугодием 2022 г. [Там же, с. 7] (рисунок 1).

---

[1] Федеральный закон от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (ред. от 04.08.2023) // Собрание законодательства РФ. 08.04.2013. № 14. Ст. 1652; Федеральный закон от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» (ред. от 04.08.2023) // Собрание законодательства РФ. 25.07.2011. № 30 (часть 1). Ст. 4571.

[2] Гражданский кодекс Российской Федерации, часть 1 от 30.11.1994 № 52-ФЗ (ред. от 24.07.2023) (с изм. и доп., вступ. в силу с 04.08.2023) // Собрание законодательства РФ. 05.12.1994. № 32. Ст. 3301.

[3] Паспорт федерального проекта «Информационная безопасность» (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28.05.2019 № 9) (Приложение № 5 к протоколу) [Электронный ресурс] // Информационно-правовой портал «Гарант.ру». URL: https://base.garant.ru/72302278/ (дата обращения: 14.10.2023).

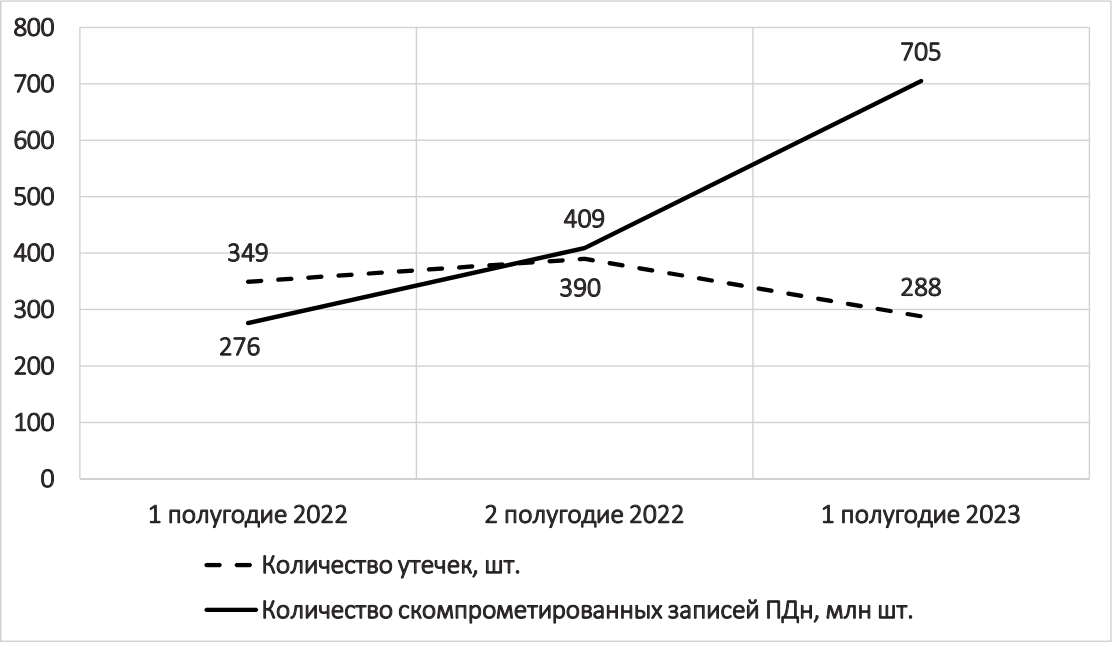

Рис. Количество утечек и количество скомпрометированных записей персональных данных (ПДн)[1]

Fig. Number of leaks and number of compromised personal data records

Еще одной распространенной проблемой является неэффективное использование имеющихся финансовых ресурсов. Часто организации тратят большие суммы на закупку и установку современных технических средств защиты информации, однако не обеспечивают его должное функционирование из-за недостатка квалифицированных специалистов или неправильной настройки. В результате финансовые вложения оказываются напрасными, а защита информации остается уязвимой.

Также стоит отметить проблему быстрого устаревания технологий и программного обеспечения в сфере информационной безопасности. Развитие ИТ-технологий происходит со стремительной скоростью, и то, что было актуально еще год назад, может устареть или быть неэффективно. В сфере информационной безопасности постоянно появляются новые угрозы и атаки, поэтому необходимо постоянно обновлять систему защиты и внедрять новые технологии. Обновление систем требует значительных затрат как на приобретение нового оборудования и программного обеспечения, так и на переподготовку персонала. Однако без этих мероприятий риск компрометации информации значительно возрастает.

Еще одной проблемой является сложность определения реальной стоимости финансовых потерь от возможных инцидентов в сфере информационной безопасности. Многие организации трудно оценивают возможный ущерб, который может быть причинен в результате утечки информации или хакерской атаки. Это затрудняет принятие обоснованных решений по финансовому обеспечению мероприятий по защите информации и может привести к недостаточному выделению средств на эти цели.

В связи с вышеуказанными проблемами необходимо искать пути решения финансового обеспечения мероприятий по защите информации.

Предложения по решению проблем финансового обеспечения мероприятий по защите информации

Несомненно, главным способом полноценной реализации мероприятий в сфере защиты информации является привлечение главного интересанта и регулятора в этой сфере — государства.

[1] Составлено автором по результатам анализа источника [5].

Именно поэтому необходима поддержка организаций со стороны государства по приобретению оборудования и программного обеспечения, входящего в состав средств защиты информации.

Данный фактор не противоречит Стратегии экономической безопасности, в пп. 3 п. 18 указано, что одной из основных задач по реализации направления, касающегося создания экономических условий для разработки и внедрения современных технологий, стимулирования инновационного развития, а также совершенствования нормативно-правовой базы в этой сфере, является расширение государственной поддержки научно-технической и инновационной деятельности, а также формирование благоприятных условий для привлечения частных инвестиций в эту сферу, в том числе с использованием механизмов государственно-частного партнерства[1].

В [1] отмечено: «Одним из видов данной поддержки является взаимодействие между государством и бизнесом в рамках государственно-частного (муниципально-частного) партнерства (ГЧП, МЧП) для решения задач на взаимовыгодных условиях».

В п. 1 ст. 3 закона «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации» (далее — Закон о ГЧП)[2] определено, что под государственно-частным партнерством, муниципально-частным партнерством понимается юридически оформленное на определенный срок и основанное на объединении ресурсов, распределении рисков сотрудничество публичного партнера, с одной стороны, и частного партнера, с другой стороны, которое осуществляется на основании соглашения о государственно-частном партнерстве, муниципально-частном партнерстве, заключенных в соответствии с настоящим федеральным законом в целях привлечения в экономику частных инвестиций, обеспечения органами государственной власти и органами местного самоуправления доступности товаров, работ, услуг и повышения их качества.

Поэтому для эффективной реализации мероприятий по финансовому обеспечению защиты информации органам государственной власти (публичным партнерам) необходимо оказывать поддержку частным партнерам, соответствующим требованиям ст. 5 Закона о ГЧП, для приобретения дорогостоящего оборудования и программного обеспечения.

Все это не противоречит п. 1 ст. 7 Закона о ГЧП, где указано, что объектами соглашения могут быть:

- программы для электронных вычислительных машин (программы для ЭВМ), базы данных, информационные системы (в том числе государственные информационные системы) и (или) сайты в информационно-телекоммуникационной сети «Интернет» или других информационно-телекоммуникационных сетях, в состав которых входят такие программы для ЭВМ и (или) базы данных, либо совокупность указанных объектов (объекты информационных технологий), либо объекты информационных технологий и имущество, технологически связанное с одним или несколькими такими объектами и предназначенное для обеспечения их функционирования или осуществления иной деятельности, предусмотренной соглашением (технические средства обеспечения функционирования объектов информационных технологий);
- совокупность зданий, частей зданий или помещений, объединенных единым назначением с движимым имуществом, технологически связанным с объектами информационных технологий, и предназначенных для автоматизации с использованием программ для ЭВМ и баз данных процессов формирования, хранения, обработки, приема, передачи, доставки информации, обеспечения доступа к ней, ее представления и распространения (центры обработки данных).

Именно опираясь на положения Закона о ГЧП, органы государственной власти смогут оказывать различного рода поддержку бизнесу для закупки необходимого оборудования, программного обеспечения, средств и систем защиты информации.

---

[1] Указ Президента РФ от 13.05.2017 № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» // Собрание законодательства РФ. 15.05.2017. № 20. Ст. 2902.

[2] Федеральный закон от 13.07.2015 № 24-ФЗ «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» (ред. от 04.08.2023) (с изм. и доп., вступ. в силу с 01.04.2024) // Собрание законодательства РФ. 20.07.2015. № 29 (часть 1). Ст. 4350.

Также для решения проблем финансового обеспечения мероприятий по защите информации организациям следует придерживаться следующих рекомендаций:

1) оптимизация расходов на защиту информации. Одним из первых шагов по обеспечению финансирования мероприятий по защите информации является оптимизация расходов. Это может быть достигнуто путем анализа текущих затрат на защиту информации, выявления неэффективных механизмов или систем, а также использования новых технологий и инструментов, которые позволяют снизить затраты без потери качества защиты;

2) поиск внешних источников финансирования. Для успешного финансирования мероприятий по защите информации можно обратиться к внешним источникам финансирования, таким как гранты от государственных организаций или неправительственных организаций, инвестиции от частных инвесторов или партнерство с другими компаниями. Важно провести анализ и выбрать наиболее подходящие источники финансирования, учитывая специфику мероприятий по защите информации;

3) создание внутренней финансовой базы. Для обеспечения стабильного финансирования мероприятий по защите информации можно создать внутреннюю финансовую базу, которая будет выделять средства на эти цели. Это может быть реализовано путем создания специального бюджета на защиту информации, включение расходов на защиту в общий бюджет организации или использование доходов от деятельности организации для финансирования данных мероприятий.

Заключение

В качестве вывода можно отметить, что в настоящее время обеспечение экономической безопасности на основе реализации мероприятий по информационной безопасности становится все более актуальной и важной проблемой. Развитие технологий и увеличение объемов передаваемой и хранимой информации требует более эффективных мер по ее защите.

В статье [4, с. 65] сказано, что для достижения максимальных успехов в инновационном развитии передовых отраслей Российской Федерации необходимо активно диверсифицировать имеющиеся собственные высокотехнологичные проекты с целью получения максимальной прибыли и создания имиджа высокоразвитого, конкурентоспособного государства.

Что касается других государств — членов ЕАЭС, можно отметить, что вопросы обеспечения экономической безопасности и информационной безопасности рассматриваются на уровне законов и подзаконных актов.

В Республике Армения указанные вопросы рассмотрены в Стратегии национальной безопасности, принятой в 2020 г.

В Республике Беларусь рассмотрению вопросов экономической и информационной безопасности посвящена Концепция национальной безопасности Республики Беларусь, принятая в 2010 г., которая в скором времени будет заменена на новую концепцию, проект которой опубликован на правовом портале Республики Беларусь[1].

В Республике Казахстан вопросы обеспечения экономической и информационной безопасности регулируются законом от 06.01.2012 № 527-IV «О национальной безопасности Республики Казахстан».

В Киргизской Республике указанные вопросы регулируются законом от 26.02.2003 № 44 «О национальной безопасности», а также Концепцией национальной безопасности Кыргызской Республики, утвержденной указом Президента от 20.12.2021 УП № 570.

Литература

1. *Агеев А. И., Кузьмин О. В., Перминова Е. А.* Информационная безопасность автоматизированных систем управления производственными и технологическими процессами объектов критической инфор-

[1] Постановление совета безопасности Республики Беларусь от 06.03.2023 № 1 «О рассмотрении проекта новой Концепции национальной безопасности Республики Беларусь» [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. URL: https://pravo.by/document/?guid=3871&p0=P223s0001 (дата обращения: 30.11.2023).

мационной инфраструктуры Российской Федерации : учебное пособие. М. : МНИИПУ ИНЭС, 2021. 156 с.
2. *Кашников Б. Н.* Теория справедливой войны: критика основных начал // Этическая мысль. 2019. Т. 19. № 2. С. 152–167. EDN: WEOAWU. DOI: 10.21146/2074-4870-2019-19-2-152-167
3. Мегатренды: Основные траектории эволюции мирового порядка в XXI веке : учебник / под. ред. Т. А. Шаклеиной, А. А. Байкова. 2-е изд., испр. и доп. М. : Аспект Пресс, 2017. 448 с. EDN: WZVJFZ
4. *Перминова Е. А.* Стимулирование инновационного развития регионов Российской Федерации в рамках стратегических инвестиционных проектов // Евразийская интеграция: экономика, право, политика. 2022. № 1 (39). С. 57–67. EDN: YNVVVB. DOI: 10.22394/2073-2929-2022-01-57-67
5. Прогноз развития рынка кибербезопасности в Российской Федерации на 2023–2027 годы. Аналитический отчет // Фонд «Центр стратегических разработок» (ЦСР). Июль, 2023. 24 с.
6. *Таловерова Д. В.* Проблемы обеспечения безопасности критической информационной инфраструктуры // Сборник статей V Всероссийской научно-технической конференции молодых ученых, аспирантов, магистрантов и студентов «Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности». Таганрог, 2019. 606 с.
7. Утечки информации ограниченного доступа в мире и России, первое полугодие 2023 г. Аналитический отчет // Экспертно-аналитический центр InfoWatch. 2023. 17 с.
8. *Цуканова О. А., Смирнов С. Б.* Экономика защиты информации : учебное пособие. СПб. : СПб ГУИТМО, 2007. 59 с.
9. *Чечин О. П.* Цифровая трансформация в концепции экономической безопасности // Экономические науки. 2019. № 7 (176). С. 92–97. EDN: JWLROU. DOI: 10.14451/1.176.92
10. *Кетр S.* Digital 2022: Global Overview Report, 26 January 2022 [Электронный ресурс] // Datareportal. 26.01.2022. URL: https://datareportal.com/reports/digital-2022-global-overview-report (дата обращения: 24.03.2023).

Об авторе:

Перминова Елена Александровна, ведущий научный сотрудник Института глобальных исследований факультета международных экономических отношений Федерального государственного образовательного бюджетного учреждения высшего образования «Финансовый университет при Правительстве Российской Федерации» (Москва, Российская Федерация), кандидат экономических наук;
e-mail: vice.csp@gmail.com; ORCID: 0000-0001-6920-9142

References

1. Ageev A. I., Kuzmin O. V., Perminova E. A. Information Security of Automated Control Systems of Production and Technological Processes of Objects of Critical Information Infrastructure of the Russian Federation : Textbook. Moscow : MNIIPU INES, 2021. 156 p. (In Rus.)
2. Kashnikov B. N. Just War Theory: The Critique of the Foundations // Ethical Thought [Eticheskaya mysl']. 2019. Vol. 19. No. 2. P. 152–167. (In Rus.) EDN: WEOAWU. DOI: 10.21146/2074-4870-2019-19-2-152-167
3. Megatrends: The Main Trajectories of the Evolution of the World Order in the XXI Century : Textbook / ed. by T. A. Shakleina, A. A. Baykova. 2nd ed., ispr. and add. Moscow : Aspect Press, 2017. 448 p. (In Rus.) EDN: WZVJFZ
4. Perminova E. A. Stimulation of Innovative Development of Regions of the Russian Federation within the Framework of Strategic Investment Projects // Eurasian Integration: Economics, Law, Politics [Evraziiskaya integratsiya: ekonomika, pravo, politika]. 2022. No. 1 (39). P. 57–67. (In Rus.) EDN: YNVVVB. DOI: 10.22394/2073-2929-2022-01-57-67
5. Forecast of the Development of the Cybersecurity Market in the Russian Federation for 2023–2027. Analytical Report // Center for Strategic Research Foundation (CSR). July, 2023. 24 p. (In Rus.)

6. Taloverova D. V. Problems of Ensuring the Security of Critical Information Infrastructure // Collection of articles of the V All-Russian Scientific and Technical Conference of Young scientists, postgraduates, undergraduates and students "Fundamental and Applied Aspects of Computer Technology and Information Security". Taganrog, 2019. 606 p. (In Rus.)
7. Leaks of Restricted Access Information in the World and Russia, the First Half of 2023. Analytical Report // Expert and Analytical Center InfoWatch. 2023. 17 p. (In Rus.)
8. Tsukanova O. A., Smirnov S. B. Economics of Information Protection : Textbook. St. Petersburg : SPb GUITMO, 2007. 59 p. (In Rus.)
9. Chechin O. P. Digital Transformation in Economic Security Concept // Economic Sciences [Ekonomicheskie nauki]. 2019. No. 7 (176). P. 92–97. (In Rus.) EDN: JWLROU. DOI: 10.14451/1.176.92
10. Kemp *S.* Digital 2022: Global Overview Report, 26 January 2022 [Electronic resource] // Datareportal. 26.01.2022. URL: https://datareportal.com/reports/digital-2022-global-overview-report (accessed: 24.03.2023).

About the author:

Elena A. Perminova, Leading Researcher of the Institute of Global Studies of the Faculty of International Economic Relations of the Federal State Budgetary Educational Institution of Higher Education "Financial University under the Government of the Russian Federation" (Moscow, Russian Federation), PhD in Economics;
e-mail: vice.csp@gmail.com; ORCID: 0000-0001-6920-9142