УДК 004.056.5 URL: https://ptsj.bmstu.ru/catalog/icec/insec/1029.html

АНАЛИЗ ОРГАНИЗАЦИОННО-ПРАВОВЫХ АСПЕКТОВ ЭКСПЛУАТАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

В.Е. Соколовский sokolovskiyve@student.bmstu.ru
Е.В. Глинская glinskaya@bmstu.ru
SPIN-код: 5430-3023

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Проанализированы основные нормативные требования, предъявляемые к средствам защиты информации при создании систем обеспечения информационной безопасности государственных информационных систем, информационных систем персональных данных и информационных систем значимых объектов критической информационной инфраструктуры. Зафиксированы требования к средствам защиты для различных категорий защищаемой информации. Выделены зоны ответственности регуляторных органов в части формирования требований к средствам защиты информации, используемых в организациях для создания защищенных информационных систем. Показаны отличия в требованиях к средствам защиты информации в зависимости от категорий обрабатываемой информации, подлежащей защите. Определены ограничения для применения средств защиты информации иностранного производства при создании защищенных информационных систем организации и условия проведения аттестационных испытаний создаваемых систем обеспечения информационной безопасности.

Ключевые слова: информационная безопасность, государственные информационные системы, класс защищенности, уровень защищенности, средства защиты информации, Федеральная служба по техническому и экспортному контролю, Федеральная служба безопасности, значимый объект критической информационной инфраструктуры, аттестационные испытания

Введение. В настоящее время в Российской Федерации наблюдается устойчивая тенденция к увеличению объема и значимости информации, обрабатываемой в различных информационных системах [1–4]. В статье рассмотрены требования по защищенности информационных ресурсов и нормативные документы, выполнение которых необходимо для обеспечения защиты информации в организациях.

Обеспечение информационной безопасности (ИБ), как состояния защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз[1], способных нанести ущерб интересам личности, обще-

[1] Указ Президента РФ «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05.12.2016 № 646.

 ISSN 2541-8009

ства, государства (национальным интересам), является актуальной проблемой, стоящей перед организациями различных форм собственности[2].

Согласно учебному пособию [5], к основным видам защиты информации наряду с физической и правовой относятся техническая и криптографическая защита.

В РФ на государственном уровне сформулированы подходы[3] к обеспечению ИБ, под которой понимается деятельность, обеспечивающая конфиденциальность, доступность и целостность информации[4] для следующих целей:

– государственных информационных систем (ГИС);

– информационных систем персональных данных (ИСПДн)[5];

– информационных систем значимых объектов критической информационной инфраструктуры (ЗО КИИ)[6];

– защиты информации, отнесенной организацией к категории коммерческой тайны[7].

Требования федеральных законов РФ в части состава и содержания организационных и технических мер по обеспечению ИБ ГИС, ИСПДн, информационных систем ЗО КИИ, автоматизированных систем управления производственными и технологическими процессами раскрываются в постановлениях Правительства РФ[8] и приказах регуляторов[9].

---

[2] ГОСТ Р 50922–2006. Защита информации. Основные термины и определения.

[3] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

[4] ГОСТ Р ИСО/МЭК 27000–2021. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.

[5] Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ.

[6] Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.

[7] Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ.

[8] Постановление Правительства РФ «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» от 06.07.2015 № 676; постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119; постановление Правительства РФ «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» от 08.02.2018 № 127.

[9] Приказ ФСТЭК России «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11.02.2013 № 17; приказ ФСТЭК «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 № 21; приказ

Анализ законодательства РФ в области обеспечения ИБ свидетельствует, что установленные требования направлены на создание в организации, обрабатывающей информацию, подлежащую защите, системы менеджмента ИБ, под которой понимают часть общей системы менеджмента, основанной на подходе бизнес-рисков при создании, внедрении, функционировании, мониторинге, анализе, поддержке и улучшении ИБ организации[10].

Непосредственное применение средств защиты информации должно соответствовать условиям, установленным в пределах своей компетенции Правительством РФ, Федеральной службой по техническому и экспортному контролю (ФСТЭК) и Федеральной службой безопасности (ФСБ) РФ. Например, согласно п. 1 (2), 7 постановления Правительства РФ «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации», средства защиты информации для ГИС должны соответствовать установленному классу защищенности ГИС по требованиям о защите информации.

Порядок классификации ГИС определен в приказе ФСТЭК России «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». В зависимости от установленного класса защищенности (первый класс — самый высокий, третий — самый низкий) должны применяться соответствующие средства защиты информации, удовлетворяющие ряду требований:

– быть сертифицированы в системе сертификации ФСТЭК РФ;

– соответствовать установленному ФСТЭК РФ классу.

ФСТЭК России «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» от 25.12.2017 № 239; приказ ФСБ России «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» от 10.07.2014 № 378; Приказ ФСБ России «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств» от 24.10.2022 № 524; приказ ФСТЭК «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (с изменениями и дополнениями)» от 14.02.2014 № 31.

[10] ГОСТ Р ИСО/МЭК 27001–2021. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

 ISSN 2541-8009

Например, согласно п. 26 этого приказа:

– в информационных системах 1-го класса защищенности применяются средства защиты информации не ниже 4-го класса;

– в информационных системах 2-го класса защищенности применяются средства защиты информации не ниже 5-го класса;

– в информационных системах 3-го класса защищенности применяются средства защиты информации 6-го класса.

Соответствие средства защиты информации вышеуказанным требованиям фиксируется в сертификате соответствия средства защиты информации установленного ФСТЭК РФ образца. Сведения о сертифицированных средствах защиты информации, кроме того, размещаются в государственном реестре сертифицированных средств защиты информации на официальном сайте ФСТЭК РФ (https://reestr.fstec.ru/reg3).

Однако применение сертифицированных средств защиты информации не является достаточным условием для обеспечения ИБ, например, в составе ГИС.

Согласно п. 13, 17 приказа ФСТЭК России «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», перед вводом ГИС в эксплуатацию необходимо провести комплекс аттестационных мероприятий, в результате которых подтверждается соответствие системы защиты информации ГИС установленным регуляторным требованиям. Выполнение требований по сертификации средств защиты информации также является необходимым для защиты информации, обрабатываемой в информационных системах ЗО КИИ согласно п. 2 постановления Правительства РФ «Об утверждении требований к программному обеспечению, в том числе в составе программно-аппаратных комплексов, используемому органами государственной власти, заказчиками, осуществляющими закупки»[11].

Кроме того, в соответствии с положениями п. 1 подп. б указа Президента РФ «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»[12], с 1 января 2025 г. не разрешается использование иностранного программного обеспечения в составе ЗО КИИ. То есть, помимо выполнения требований

[11] Постановление Правительства РФ «Об утверждении требований к программному обеспечению, в том числе в составе программно-аппаратных комплексов, используемому органами государственной власти, заказчиками, осуществляющими закупки» от 22.08.2022 № 1478.

[12] Указ Президента РФ «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» от 30.03.2022 № 166.

к сертификации, программное обеспечение средства защиты информации должно быть российского производства. Вместе с тем применение иностранных средств защиты информации для обеспечения ИБ в ИСПДн, при условии, что ИСПДн не является ЗО КИИ и не входит в состав ГИС, законодательными и регуляторными мерами в настоящее время не ограничивается.

Необходимо отметить, что согласно п. 29.2, п. 29.3.1 постановления Правительства РФ «О лицензировании деятельности по технической защите конфиденциальной информации»[13,] прикладное программное обеспечение, планируемое к внедрению в рамках создания (модернизации или реконструкции, ремонта) ЗО КИИ и обеспечивающее выполнение его функций по назначению должно соответствовать требованиям по безопасной разработке программного обеспечения. Подходы к безопасной разработке программного обеспечения как составляющей системы обеспечения ИБ рассматриваются в различных публикациях, в том числе в [6].

В соответствии с постановлением Правительства РФ «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию; приказом ФАПСИ «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»[14], в отношении криптографических средств защиты информации также определены требования по сертификации и применимости в соответствии с установленными классами (уровнями) защищенности для ГИС (ИСПДн).

Вопросы эксплуатации технических и криптографических средств защиты информации для собственных нужд организации объединяет необходи-

[13] Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

[14] Постановление Правительства РФ от 16 апреля 2012 г. № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию; приказ ФАПСИ «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» от 13.06.2001 № 152.

 ISSN 2541-8009

мость соблюдения правил применения (настройки), изложенных в соответствующих руководствах (инструкциях) администраторов. При условии, что организация оказывает услуги по технической (криптографической) защите информации сторонним организациям, такой вид деятельности необходимо лицензировать в установленном ФСТЭК (ФСБ) РФ порядке.

Отличительной особенностью применения в организации средств криптографической защиты информации (шифровальных средств), сертифицированных ФСБ РФ, с целью обработки и передачи по каналам связи информации с ограниченным доступом, подлежащей в соответствии с законодательством РФ обязательной защите и не содержащей сведений, составляющих государственную тайну, является необходимость строго следования регуляторным требованиям.

Порядок применения в организации физических средств (железных дверей, замков, решеток и т. п.) для защиты информации с ограниченным доступом, подлежащей в соответствии с законодательством РФ обязательной защите и не содержащей сведений, составляющих государственную тайну, приказами ФСТЭК РФ строго не определен.

Заключение. Анализ положений нормативных документов в области обеспечения ИБ свидетельствует, что установленные требования направлены на создание в организации, обрабатывающей информацию, подлежащую защите, соответствующей системы обеспечения ИБ. Требования, предъявляемые к составу и характеристикам применяемых средств защиты информации, определяются в соответствии с установленным классом (уровнем, категорией) защищенности информационной системы. Выполнение требований к защищенности информационной системы в установленных нормативными требованиями случаях подтверждается в ходе аттестационных испытаний созданных систем обеспечения ИБ.

Литература

[1] Трофимов В.В., Ильина О.П., Кияев В.И. и др. *Информационные технологии*. Москва, Изд-во Юрайт, 2025, 546 с.

[2] Швецов А.Н. «*Информационное общество»: теория и практика становления в мире и в России*. Москва, URSS, 2021, 304 с.

[3] Суворова Г.М. *Информационная безопасность*. Москва, Изд-во Юрайт, 2025, 277 с.

[4] Родичев Ю.А. *Информационная безопасность. Национальные стандарты Российской Федерации*. Санкт-Петербург, Питер, 2023, 384 с.

[5] Вострецова Е.В. *Основы информационной безопасности*. Екатеринбург, Изд-во Урал. ун-та, 2019, 204 с.

[6] Соколовский В.Е., Глинская Е.В. Безопасная разработка программного обеспечения как составляющая системы обеспечения информационной безопасности. *Политехнический молодежный журнал*, 2024, № 3. URL: https://ptsj.bmstu.ru/catalog/icec/insec/979.html (дата обращения 09.09.2024).

Поступила в редакцию 24.10.2024

Соколовский Владислав Евгеньевич — студент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Глинская Елена Вячеславовна — старший преподаватель кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Басараб Михаил Алексеевич, доктор физико-математических наук, заведующий кафедрой «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:
Соколовский В.Е., Глинская Е.В. Анализ организационно-правовых аспектов эксплуатации средств защиты информации в организации. *Политехнический молодежный журнал*, 2025, № 01 (96). URL: https://ptsj.bmstu.ru/catalog/icec/insec/1029.htmll

 ISSN 2541-8009

ANALYZING ORGANIZATIONAL AND LEGAL ASPECTS OF THE INFORMATION SECURITY TOOLS OPERATION IN THE ORGANIZATION

V.E. Sokolovsky sokolovskiyve@student.bmstu.ru
E.V. Glinskaya glinskaya@bmstu.ru
SPIN-code: 5430-3023

Bauman Moscow State Technical University, Moscow, Russian Federation

The paper analyzes the main regulatory requirements imposed on the information security tools in creating information security systems for the state information systems, personal data information systems, and information systems of significant objects of the critical information infrastructure. It states requirements for security tools in various categories of the protected information. The paper identifies areas of responsibility for the regulatory bodies in terms of forming requirements for the information security tools used in the organizations to create the secure information systems. It shows the differences in requirements for the information security tools depending on the categories of processed information to be protected. The paper defines restrictions to using the foreign-made information security tools when creating a secure information system for the organization and conditions for conducting certification tests of the created information security systems.

Keywords: information security, state information systems, protection class, protection level, information security tools, Federal Service for Technical and Export Control, Federal Security Service, significant object of critical information infrastructure, certification tests

Received 24.10.2024

Sokolovsky V.E. — Student, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Glinskaya E.V. — Senior Lecturer, Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — Basarab M.A., Dr. Sci. (Phys. & Math.), Head of the Department of Information Security, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:
Sokolovsky V.E., Glinskaya E.V. Analyzing organizational and legal aspects of the information security tools operation in the organization. *Politekhnicheskiy molodezhnyy zhurnal*, 2025, no. 01 (96). (In Russ.). URL: https://ptsj.bmstu.ru/catalog/icec/insec/1029.html

