БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2026. – № 2 (121). – 50–67

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2026-2-50-67

РАЗРАБОТКА ПОДХОДА К АВТОМАТИЗАЦИИ ВЫБОРА МЕР ЗАЩИТЫ ГИС В ПЕРЕХОДНЫЙ ПЕРИОД*

Е.Е. КОРОТКОВА[1], В.В. СЕЛИФАНОВ[2]

[1] *РФ, 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, лаборант кафедры защиты информации. E-mail: iza.korotkova@gmail.com*
[2] *РФ, 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E- mail: sfo1@mail.ru*

Статья посвящена проблеме проектирования систем защиты информации государственных информационных систем (ГИС) в условиях изменения нормативной базы. Проведен сравнительный анализ приказов ФСТЭК России № 17 и № 117, выявлены ключевые усложнения в части расширения области регулирования, появления новых категорий мер защиты и ужесточения требований к отчетности. Обосновывается необходимость перехода от экспертного проектирования к автоматизированному ввиду усложнения требований, динамичности угроз и дефицита квалифицированных кадров. Представлен алгоритм автоматизированного сопоставления параметров ГИС с базой данных угроз (БДУ) ФСТЭК, а также архитектурное решение сервиса для автоматической генерации проектной документации.

Ключевые слова: ГИС, Приказ ФСТЭК № 117, Приказ ФСТЭК № 17, защита информации, модель угроз, меры защиты, БДУ ФСТЭК, средства защиты информации

ВВЕДЕНИЕ

С вступлением в силу приказа ФСТЭК России № 117 смещается акцент со статичного проектирования систем защиты в сторону более динамичного управления безопасностью. Новые требования расширяют область действия, детализируют процессы и процедуры защиты информации, увеличивают объем используемых мер. Высокая детализация требований ведет к росту трудозатрат и повышает риск ошибок из-за человеческого фактора. В условиях дефицита кадров и необходимости оперативного реагирования на изменения обстановки вопрос автоматизации процессов выходит на передний план.

* Статья получена 27 апреля 2026 г.

В статье приводится анализ Приказа ФСТЭК № 117, а также уже действующих и проектируемых методических документов и предлагаются меры по автоматизации процессов моделирования угроз и подбору средств защиты информации (СЗИ) в условиях перехода на новые требования и постоянные изменения обстановки (от обновления техник и тактик атак до обновления реестров сертифицированных СЗИ).

1. СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРИКАЗОВ ФСТЭК № 17 И № 117

Приказ № 117 сохраняет базовую структуру требований к защите информации, но существенно развивает их содержание, предлагая более детализированные и обширные меры безопасности. Проведенный анализ позволяет выделить несколько ключевых направлений изменений.

1.1. РАСШИРЕНИЕ ОБЛАСТИ ДЕЙСТВИЯ

Одним из ключевых изменений, вносимых Приказом № 117, является расширение круга информационных систем, на которые распространяются его требования. Если ранее Приказ № 17 регулировал вопросы создания и ввода в действие систем защиты информации преимущественно для ГИС [1–3], то новая редакция охватывает более широкий перечень объектов.

Действие Приказа № 117 распространяется:

– на государственные информационные системы, обрабатывающие информацию ограниченного доступа;

– иные информационные системы государственных органов;

– информационные системы государственных унитарных предприятий и государственных учреждений;

– муниципальные информационные системы.

Для некоторых указанных систем ранее уже существовали отдельные требования по аттестации. При этом Приказ № 117 впервые устанавливает унифицированный подход к их защите, предъявляя единые, более детализированные и строгие требования.

Расширение области действия напрямую повлияло на состав применяемых мер защиты и порядок их реализации.

1.2. ЭВОЛЮЦИЯ МЕР ЗАЩИТЫ И ПОЯВЛЕНИЕ НОВЫХ КАТЕГОРИЙ

Изменение круга регулируемых систем повлекло за собой пересмотр подходов к регламентации стадий и этапов ввода СЗИ в эксплуатацию. Ранее Приказ ФСТЭК № 17 содержал требования к стадиям и этапам работ по вводу

в действие СЗИ информационных систем. Приказ ФСТЭК № 117 таких требований не содержит, а ссылается на другие нормативные акты: для ГИС применяются требования ПП РФ № 676, к иным ИС применяется ГОСТ Р 51583–2014 [4–7]. Ниже представлена таблица сравнения.

Таблица 1

Table 1

Сравнение стадий и этапов работ по вводу в действие СЗИ ИС

Comparison of stages and phases of work on the commissioning of information security systems

Группа этапов	ПП РФ 676	ГОСТ Р 51583	Приказ ФСТЭК № 17
Подготовка и установка	Этап отсутствует	Комплектация АС	Установка и настройка средств ЗИ ИС
	Этап отсутствует	Строительно-монтажные работы	
Настройка и внедрение	Пусконаладочные работы	Пусконаладочные работы	Этап отсутствует
	Этап отсутствует	Подготовка объекта автоматизации к вводу АС в действие	Разработка организационно-распорядительных документов по ЗИ
			Внедрение организационных мер ЗИ
	Этап отсутствует	Подготовка персонала	Этап отсутствует
Испытания	Проведение предварительных испытаний	Проведение предварительных испытаний	Предварительные испытания системы ЗИ ИС
	Проведение опытной эксплуатации	Проведение опытной эксплуатации	Опытная эксплуатация системы ЗИ ИС
	Этап отсутствует	Этап отсутствует	Анализ уязвимостей ИС и принятие мер ЗИ по их устранению
Завершающие мероприятия	Проведение приемочных испытаний	Проведение приемочных испытаний	Приемочные испытания системы ЗИ ИС

Применение различных нормативных актов для регламентации стадий и этапов ввода СЗИ в эксплуатацию в зависимости от типа системы усложняет

процесс проектирования и внедрения. Введенное разделение на государственные и иные информационные системы, а также отсутствие жесткой регламентации этапов для последних создает риск возникновения ошибок.

Другим важным изменением, вносимым Приказом № 117, является введение требований к организационной структуре системы защиты информации. Ключевым последствием стало расширение сферы действия ПП РФ № 1272. Если ранее документ распространялся только на субъекты критической информационной инфраструктуры (КИИ), то теперь Приказ № 117 делает его требования обязательными для более широкого круга организаций, подпадающих под действие приказа [8–10]. Это обязывает такие организации привести свои системы защиты в соответствие с ПП РФ № 1272 (рис. 1), что унифицирует и ужесточает требования к информационной безопасности для многих субъектов, ранее не охваченных регулированием.

Рис. 1. Организационная структура в Приказе ФСТЭК № 117 [11]

Fig. 1. Organizational structure in the FSTEC order № 117 [11]

Что касается состава мер и мероприятий защиты, то в Приказе № 117 отсутствует их полный перечень. Однако даже базовый набор претерпел существенные изменения. Появились следующие группы мер:

- защита виртуализации и облачных вычислений;
- защита технологий контейнерных сред и их оркестрации;
- защита сервисов электронной почты;
- защита веб-технологий;

– защита программных интерфейсов взаимодействия приложений;
– защита конечных устройств;
– защита мобильных устройств;
– защита технологий интернета вещей;
– защита точек беспроводного доступа;
– обнаружение и предотвращение вторжений на сетевом уровне;
– сегментация и межсетевое экранирование;
– защита каналов передачи данных и сетевого взаимодействия.

Сравнение базового перечня мероприятий представлено в табл. 2.

Таблица 2
Table 2

Сравнение мероприятий защиты информации в приказах № 17 и № 117
Comparison of information security measures in orders № 17 and № 117

Приказ ФСТЭК России № 17 (было)	Приказ ФСТЭК России № 117 (стало)
Выявление и оценка угроз безопасности информации (УБИ)	Обеспечение разработки безопасного ПО
Контроль конфигураций ИС	Обеспечение физической защиты ИС
Управление уязвимостями	Обеспечение непрерывности функционирования ИС при возникновении нештатных ситуаций
Управление обновлениями	Повышение уровня знаний и информированности пользователей по вопросам ЗИ
Обеспечение ЗИ при обработке, хранении и обращении с информацией ограниченного доступа	Обеспечение ЗИ при взаимодействии с подрядными организациями
Обеспечение ЗИ при применении конечных устройств	Обеспечение защиты от компьютерных атак, направленных на отказ в обслуживании
Обеспечение ЗИ при применении мобильных устройств	Обеспечение ЗИ при использовании искусственного интеллекта
Обеспечение ЗИ при удаленном доступе пользователей к ИС	Реализация в ИС мер по их защите и защите содержащейся в них информации
Обеспечение ЗИ при беспроводном доступе пользователей к ИС	Проведение контроля уровня защищенности информации, содержащейся в ИС
Обеспечение ЗИ при предоставлении пользователям привилегированного доступа	Обеспечение непрерывного взаимодействия с ГосСОПКА на информационные ресурсы РФ
Обеспечение мониторинга ИБ	–

Исчерпывающий перечень мер и мероприятий содержится в соответствующем методическом документе. В нем описано 96 мер и 18 мероприятий, из них для 42 и 15 соответственно установлены требования к документированию.

Для реализации этих мер требуется применение различных сертифицированных средств защиты информации. По состоянию на май 2026 года в реестре ФСТЭК России зарегистрировано 1919 СЗИ, в реестре ФСБ России – 833 СЗИ, в реестре Минцифры России – 30 313 единиц отечественного программного обеспечения (ПО). При этом СЗИ и ПО должны корректно функционировать совместно.

В настоящее время существует широкий спектр требований к СЗИ. В рамках системы сертификации ФСТЭК России действует 13 типов требований, которые не охватывают все необходимые виды средств. Например, отсутствуют требования к средствам идентификации и аутентификации, анализа уязвимостей, SIEM-системам и другим классам. Такие средства сертифицируются на соответствие уровню доверия, что не отражает их функциональные возможности и дополнительно усложняет выбор и обоснование применения средств защиты.

При выборе СЗИ также необходимо учитывать возможности нарушителя. Соответствующие требования приведены в табл. 3.

Таблица 3

Table 3

Требования к средствам защиты информации

Requirements for information security tools

Вид требования	Класс 1	Класс 2	Класс 3
СВТ (средства вычислительной техники)	5-й уровень доверия	5-й уровень доверия	5-й уровень доверия
СЗИ	4-й уровень доверия	5-й уровень доверия	6-й уровень доверия
УД (устройства доверенной загрузки)	4-й уровень доверия	5-й уровень доверия	6-й уровень доверия
Уровень возможностей нарушителя (Приказ № 117)	Высокий	Повышенный	Базовый
Уровень возможностей нарушителя (Приказ № 17)	Высокий	Усиленный базовый	Базовый

Кроме того, в Приказе № 117 установлены меры по обязательному выполнению требований эксплуатационной документации и организации технической поддержки. В этой части Приказ № 117 полностью совпадает с Приказом ФСТЭК № 239, устанавливающим требования к защите значимых объектов КИИ [12–15].

Увеличение числа критериев выбора средств, а также отсутствие четких требований к реализуемому функционалу значительно повышает трудоемкость проектирования систем защиты информации. Это требует внедрения процессов автоматизации фильтрации применяемых мер.

Помимо изменений в составе мер и процедур их внедрения, Приказ № 117 вводит новые подходы к оценке состояния защиты информации.

1.3. ОЦЕНКА СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Приказ № 117 вводит два ключевых показателя оценки соответствия: уровень защищенности (количественная оценка, выражаемая коэффициентом защищенности, $К_{зи}$) и уровень зрелости (качественная оценка процессов обеспечения защиты информации, $П_{зи}$). Первый контролируется не реже одного раза в полгода с обязательной отчетностью во ФСТЭК России. Второй проверяется не реже одного раза в два года.

Приказ устанавливает требования к регулярной отчетности. Необходимо проводить контроль уровня защищенности, мониторинг безопасности и иные мероприятия, перечисленные в табл. 4 [11, 16, 17]. В связи с этим возникает потребность в регулярной обработке больших объемов данных.

На май 2026 года в БДУ ФСТЭК России содержится 227 угроз и 83 991 уязвимость. Ожидается, что темпы роста этих показателей будут увеличиваться. В ходе проектирования системы защиты информации специалисты должны учитывать все возможные способы реализации угроз безопасности, что требует обработки огромного количества вариантов. При таком объеме данных традиционный «ручной» подход становится неэффективным.

Помимо увеличения количества отчетных документов новый приказ вводит нормативные сроки для ряда процессов. Стоит отметить, что для некоторых процессов, например устранения уязвимостей, установленные сроки могут потребовать привлечения сотрудников в нерабочее время.

Таблица 4
Table 4

Отчетность во ФСТЭК
Reporting to FSTEC

Пункт Приказа № 117	Что отправляется	Периодичность	Срок предоставления
32	Оценка показателя защищенности ($К_{зи}$)	Один раз в 6 месяцев	5 рабочих дней
32, 73	Оценка показателя уровня зрелости ($П_{зи}$)	Один раз в 2 года	5 рабочих дней
36	Модель угроз (техническое задание) со ссылкой на ПП РФ 676 (только для ГИС)	При создании	–
38	Информация о найденных уязвимостях, отсутствующих в БДУ	При обнаружении	5 рабочих дней
49	Последний в текущем году отчет по результатам мониторинга либо итоговый отчет за текущий год	Ежегодно	–
65, 73	Аттестационные материалы (Приказ ФСТЭК России № 77)	При аттестации	5 рабочих дней
65, 73	Протоколы контроля защиты информации (Приказ ФСТЭК России № 77)	Один раз в 2 года (для аттестованных ИС)	–
67	Отчет по результатам проведения контроля уровня защищенности	Один раз в 3 года или после инцидента	5 рабочих дней

Таблица 5
Table 5

Сроки выполнения процессов
Process execution times

Пункт Приказа № 117	Процесс	Срок выполнения
38	Устранение уязвимостей	От 24 часов до 7 календарных дней
53	Восстановление функционирования	От 24 часов до 4 недель
55	Проверка возможности восстановления выполнения значимых функций с использованием резервных копий	Один раз в 2 года
57	Оценка уровня знаний	Один раз в 3 года или после контрольных испытаний

1.4. СИНТЕЗ ПРОБЛЕМАТИКИ

Проведенный сравнительный анализ приказов № 17 и № 117 демонстрирует существенное увеличение объема и детализации требований к защите ГИС. Переход к динамическому управлению безопасностью, расширение круга регулируемых систем и значительное увеличение объема отчетности создают условия, в которых автоматизация процессов становится критически важной.

Количество актуальных угроз и выявляемых уязвимостей исключает возможность их качественной «ручной» обработки. Автоматизация в этом сегменте должна быть направлена на непрерывное сопоставление архитектурных и технологических параметров ГИС с актуальными данными об угрозах.

С учетом появления новых мер и мероприятий, а также изменения подходов к их группировке процесс их выбора значительно усложнился. Автоматизация позволяет перейти от субъективных экспертных оценок к формализованному алгоритмическому сопоставлению.

Анализ реестров Минцифры, ФСТЭК и ФСБ выявил наличие тысяч наименований ПО и СЗИ при отсутствии единых функциональных требований к ряду их классов. В этих условиях автоматизированная система должна выступать в роли фильтра, сопоставляющего функциональные возможности средств защиты с требованиями к уровням доверия и спецификой архитектуры ГИС.

Таким образом, выявленное усложнение нормативных требований, рост числа угроз и многообразие средств защиты обосновывают необходимость перехода от экспертного проектирования к формализованному алгоритмическому подходу. Описание структуры и логики такого алгоритма приведено в следующем разделе.

2. АЛГОРИТМ АВТОМАТИЗИРОВАННОГО СОПОСТАВЛЕНИЯ ПАРАМЕТРОВ ГИС И МЕР ЗАЩИТЫ

С учетом выявленных ранее проблем разработан общий алгоритм работы сервиса проектирования систем защиты информации ГИС. Алгоритм включает пять основных этапов: 1) сбор общей информации, 2) построение модели угроз, 3) определение мер защиты, 4) выбор СЗИ и 5) генерация отчета. При реализации в виде программного обеспечения каждый этап выполняется отдельным одноименным модулем (рис. 2).

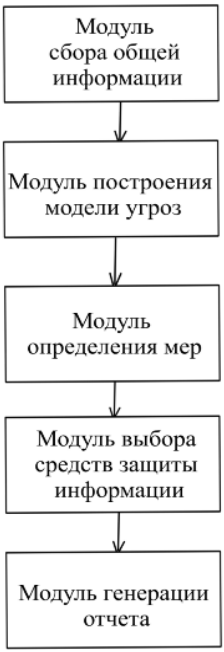

Рис. 2. Структура программы

Fig. 2. Program structure

2.1. ЭТАП СБОРА ОБЩЕЙ ИНФОРМАЦИИ

Первый этап предназначен для формирования цифрового паспорта ГИС, а также определения ее класса защищенности. На основе входных параметров автоматически определяется требуемый класс защищенности ГИС (К1, К2 или К3). Сформированные на этом этапе данные служат основой для всех последующих шагов.

2.2. ЭТАП ФОРМИРОВАНИЯ МОДЕЛИ УГРОЗ

Этот этап представляет собой центральный аналитический блок, интегрированный с актуальными базами данных угроз. Его цель – из всего множества УБИ выделить только те, которые актуальны для конкретной ГИС с заданными архитектурными, технологическими и режимными характеристиками.

На основе класса защищенности и ценности информации система автоматически назначает потенциал нарушителя: базовый, повышенный или высокий. Дополнительно учитываются особенности архитектуры – они могут повышать уровень нарушителя. Модель нарушителя включает его предполагаемые навыки, ресурсы, время, местонахождение (внешний/внутренний) и легальный статус доступа.

Выполняется импорт актуальной версии БДУ. Из общего перечня отбираются только те, которые удовлетворяют совокупности формальных критериев: соответствие типу нарушителя, технологическая совместимость, наличие канала реализации, ценность информации. Фильтрация выполняется по формализованным правилам, заданным в базе знаний системы. Это позволяет исключить заведомо неприменимые угрозы и сократить перечень с сотен до десятков релевантных записей. Для каждой отобранной угрозы из БДУ ФСТЭК система автоматически сопоставляет соответствующие техники и тактики.

Для каждой пары «угроза – техника» с учетом архитектуры ГИС и модели нарушителя автоматически генерируется типовой сценарий реализации в виде последовательности действий нарушителя. Сценарии не являются творческим описанием, а собираются из шаблонных фрагментов, что обеспечивает воспроизводимость и пригодность для последующей автоматической проверки мер защиты.

Полученная модель угроз передается на следующий этап для выбора соответствующих мер защиты.

2.3. ЭТАП ВЫБОРА И АДАПТАЦИИ МЕР ЗАЩИТЫ

На основе класса защищенности ГИС и требований Приказа № 117 автоматически формируется базовый перечень технических и организационных мер защиты.

Из этого перечня исключаются меры, которые неприменимы к данной ГИС. Каждое исключение сопровождается автоматически генерируемым обоснованием, что важно для последующей экспертной оценки.

Результатом этапа является комплексный перечень технических и организационных мер защиты информации, адаптированный под специфику ГИС, ее класс, актуальные угрозы и технологический стек. Перечень оформляется в виде требований технического задания на систему защиты информации.

Сформированный перечень мер служит основой для подбора конкретных средств защиты.

2.4. ЭТАП ПОДБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Входными параметрами для этого этапа являются перечень требуемых мер защиты и класс защищенности ГИС. Система обращается к внутренней базе знаний СЗИ, которая содержит актуальные сведения о продуктах, сертифицированных ФСТЭК России и ФСБ России: функциональные возможности, классы защиты, номера и сроки действия сертификатов, версии.

Каждая требуемая мера защиты сопоставляется с функциональными возможностями доступных СЗИ. Автоматически проверяются наличие и актуальность действующих сертификатов для предложенных средств, а также их соответствие требуемому классу защищенности ГИС.

Выходные данные этапа – спецификация оборудования и программного обеспечения, включающая наименования продуктов, их версии, сертификационные данные и обоснование выбора.

Сформированная спецификация вместе со всеми накопленными данными поступает на финальный этап.

2.5. ЭТАП ГЕНЕРАЦИИ ПРОЕКТНОЙ И ОТЧЕТНОЙ ДОКУМЕНТАЦИИ

Финальный этап обеспечивает формирование полного пакета документов. На этом шаге используются все данные, полученные на предыдущих этапах, и применяются предопределенные шаблоны, соответствующие требованиям ФСТЭК России. Кроме того, формируются отчеты, необходимые для предоставления во ФСТЭК России. Все сгенерированные документы экспортируются в форматах .docx и/или .pdf.

ЗАКЛЮЧЕНИЕ

Приведенный в первом разделе анализ положений Приказа ФСТЭК России № 117 в сравнении с Приказом № 17 демонстрирует значительное усложнение и расширение требований к защите государственных информационных систем. Эти изменения затрагивают все стадии жизненного цикла системы защиты информации – от проектирования до эксплуатации и контроля.

В условиях динамичного обновления нормативной базы, постоянного появления новых угроз и дефицита квалифицированных специалистов традиционные «ручные» подходы к проектированию систем защиты становятся неэффективными, трудозатратными и подверженными ошибкам.

Предложенный во втором разделе алгоритм позволяет автоматизировать построение актуальной модели угроз на основе БДУ ФСТЭК России, подбор мер защиты и сертифицированных средств защиты информации, а также генерацию необходимой проектной и отчетной документации.

Внедрение такого автоматизированного подхода даст организациям возможность снизить трудоемкость работ и минимизировать риски, связанные с человеческим фактором.

СПИСОК ЛИТЕРАТУРЫ

1. Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений».

2. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

3. *Заугольков И.А., Исаева О.В., Рожнова Е.А.* Комплексное обеспечение защиты информации ограниченного доступа в мировом суде // Материалы пула научно-практических конференций, Сочи, 04–08 января 2025 г. – Керчь, 2025. – С. 154–159.

4. ГОСТ Р 51583–2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения: дата введения 2014–09–01. – М.: Стандартинформ, 2014. – 13 с.

5. *Вялых С.А., Ульянов В.А.* Актуальные вопросы технической защиты информации в государственных информационных системах регионального уровня // Информатика: проблемы, методы, технологии: материалы XXV Международной научно-практической конференции им. Э.К. Алгазинова, Воронеж, 12–13 февраля 2025 г. – Воронеж, 2025. – С. 501–510.

6. *Киреева Н.В., Кузнецова Д.В., Шамина Ю.И.* Современные методы обеспечения информационной безопасности // Актуальные проблемы информатики, радиотехники и связи: материалы XXXI Российской научно-технической конференции, Самара, 01–02 февраля 2024 г. – Самара, 2024. – С. 101–103.

7. Постановление Правительства РФ от 6 июля 2015 г. № 676 «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».

8. Постановление Правительства РФ от 15 июля 2022 г. № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)».

9. *Попова В.В., Булаев В.Д., Галицкий П.А.* Системный подход к построению комплексной защиты информации на объектах критической информационной инфраструктуры. Создание Единой централизованной федеральной телекоммуникационной сети // Безопасность личности, общества и государства: теоретико-правовые аспекты: сборник научных статей XVII Международной научной конференции обучающихся образовательных организаций высшего образования, проводимой в рамках IV Санкт-Петербургского международного молодежного научного форума «Северная Пальмира: территория возможностей», Санкт-Петербург, 30 мая 2024 года. – СПб., 2024. – С. 1694–1703.

10. *Милько Д.С., Данеев А.В.* Множество вариантов решений для задачи выбора мер защиты объектов критической информационной инфраструктуры // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2023. – Т. 26, № 1. – С. 82–90. – DOI: 10.21293/1818-0442-2023-26-1-82-90.

11. *Селифанов В., Ситьков И.* Информационная безопасность 2.0: что изменится с новым приказом ФСТЭК России. – URL: https://infotecs.ru/press-center/events/informatsionnaya-bezopasnost-2-0-chto-izmenitsya-s-novym-prikazom-fstek-rossii/ (дата обращения: 15.12.2024).

12. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

13. *Павлов Е.О.* Подходы к обеспечению безопасности объектов критической информационной инфраструктуры // Журнал высоких гуманитарных технологий. – 2024. – № 3 (6). – С. 32–38.

14. Обеспечение безопасности государственных информационных систем как объектов критической информационной инфраструктуры / Г.П. Гавдан, А.А. Голубев, А.Г. Голубев, И.Ю. Жуков, Э.П. Рыбалко // Безопасность информационных технологий. – 2025. – Т. 32, № 3. – С. 26–43. – DOI: 10.26583/bit.2025.3.03.

15. *Гончаренко М.Д., Холкина К.С.* Безопасность критической информационной инфраструктуры // Научное и техническое творчество молодежи: материалы Всероссийской научно-практической конференции с международным участием, Новосибирск, 19–20 апреля 2023 г. Ч. 5 (дополнительная). – Новосибирск, 2023. – С. 200–208.

16. *Михиенко О.В., Ламонина Л.В., Смирнова О.Б.* К вопросу о кибербезопасности критической информационной инфраструктуры // Инновационные технологии в АПК как фактор развития науки в современных условиях: сборник XIV Международной научно-практической конференции, посвященной 75-летию факультета Технического сервиса в АПК (факультет механиза-

ции сельского хозяйства Омского сельскохозяйственного института им. С.М. Кирова), Омск, 27 ноября 2025 г. – Омск, 2025. – С. 787–791.

17. *Замилов А.Р.* Автоматизация контроля состояния безопасности объектов критической информационной инфраструктуры // Радиоэлектроника, электротехника и энергетика: тезисы докладов Тридцатой Международной научно-технической конференции студентов и аспирантов. – М., 2024. – С. 344.

Короткова Елизавета Евгеньевна, лаборант кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – разработка систем автоматизации процессов. E-mail: iza.korotkova@gmail.com

Селифанов Валентин Валерьевич, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – информационная безопасность. E-mail: sfo1@mail.ru

DOI: 10.17212/2782-2230-2026-2-50-67

Development of an approach to automating the selection of GIS protection measures during the transition period*

E.E. Korotkova[1], V.V. Selifanov[2]

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, laboratory assistant of the Department of Information Security. E-mail: iza.korotkova@gmail.com*

[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, Senior Lecturer at the Department of Information Security. E-mail: sfo1@mail.ru*

This article examines the design of information security systems for government information systems (GIS) in the context of changing regulatory frameworks. A comparative analysis of FSTEC of Russia Orders № 17 and № 117 is provided, identifying key challenges related to the expansion of the regulatory scope, the emergence of new categories of security measures, and stricter reporting requirements. The need for a transition from expert-based to automated design is substantiated in light of increasingly complex requirements, dynamic threats, and a shortage of qualified personnel. An algorithm for automated comparison of GIS parameters with the FSTEC Threat Database (TDB) and other sources

* *Received 27 April 2026.*

is presented, along with an architectural solution for a service for the automatic generation of design documentation.

Keywords: GIS, FSTEC order №117, FSTEC order № 17, information protection, threat model, protective measures, FSTEC TDB, information security tools

REFERENCES

1. Order of the FSTEC of Russia of 04.11.2025, N 117 "On approval of requirements for the protection of information contained in state information systems, other information systems of state bodies, state unitary enterprises, and state institutions". (In Russian).

2. Order of the FSTEC of Russia of 11.02.2013, N 17 "On approval of requirements for the protection of information not constituting state secrets contained in state information systems". (In Russian).

3. Zaugolkov I.A., Isaeva O.V., Rozhnova E.A. Kompleksnoe obespechenie zashchity informatsii ogranichennogo dostupa v mirovom sude [Comprehensive protection of restricted access information in the world court]. *Materialy pula nauchno-prakticheskikh konferentsii* [Proceedings of the pool of scientific and practical conferences], Sochi, January 04–08, 2025. Kerch, 2025, pp. 154–159.

4. GOST R 51583–2014. *Zashchita informatsii. Poryadok sozdaniya avtomatizirovannykh sistem v zashchishchennom ispolnenii. Obshchie polozheniya* [State Standard R 51583–2014. Information protection. Sequence of protected operational system formation. General]. Moscow, Standartinform Publ., 2014. 13 p.

5. Vyalykh S.A., Ul'yanov V.A. [Actual issues of technical protection of information in state information systems at the regional level]. *Informatika: problemy, metody, tekhnologii* [Informatics: problems, methods, technologies]. Materials of the XXV International Scientific and Practical Conference named after E.K. Al-Gazinov, Voronezh, February 12–13, 2025, pp. 501–510. (In Russian).

6. Kireeva N.V., Kuznetsova D.V., Shamina Yu.I. [Modern methods of ensuring information security]. *Aktual'nye problemy informatiki, radiotekhniki i svyazi* [Actual problems of computer science, radio engineering and communications]. Proceedings of the XXXI Russian Scientific and Technical Conference, Samara, February 01–02, 2024, pp. 101–103. (In Russian).

7. Decree of the Government of the Russian Federation dated July 6, 2015 N 676 "On the requirements for the procedure for the creation, development, commissioning, operation and decommissioning of state information systems and the further storage of information contained in their databases". (In Russian).

8. Decree of the Government of the Russian Federation dated July 15, 2022 N 1272 "On approval of the model regulation on the deputy head of the body (organization) responsible for ensuring information security in the body (organization)

and the model regulation on the structural unit in the body (organization) ensuring information security of the body (organization)". (In Russian).

9. Popova V.V., Bulaev V.D., Galitskii P.A. [A systematic approach to building comprehensive information protection at critical information infrastructure facilities. Co-building of the Unified centralized Federal Telecommunication network]. *Bezopasnost' lichnosti, obshchestva i gosudarstva: teoretiko-pravovye aspekty* [Security of the individual, society and the state: theoretical and legal aspects]. Collection of scientific articles of the XVII International Scientific conference of students of educational institutions of higher education, St. etersburg, 2024, pp. 1694–1703. (In Russian).

10. Milko D.S., Daneev A.V. Mnozhestvo variantov reshenii dlya zadachi vybora mer zashchity ob"ektov kriticheskoi informatsionnoi infrastruktury [Multiple of solutions for the choosing measures task to cybersecurity of critical infrastructure]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki = Proceedings of Tomsk State University of Control Systems and Radioelectronics*, 2023, vol. 26, no. 1, pp. 82–90. DOI: 10.21293/1818-0442-2023-26-1-82-90.

11. Selifanov V., Sit'kov I. *Informatsionnaya bezopasnost' 2.0: chto izmenitsya s novym prikazom FSTEK Rossii* [Information security 2.0: what will change with the new order of the FSTEC of Russia. Available at: https://infotecs.ru/press-center/events/informatsionnaya-bezopasnost-2-0-chto-izmenitsya-s-novym-prikazom-fstek-rossii/ (accessed 15.12.2024).

12. Order of the FSTEC of Russia of 25.12.2017, N 239 "On approval of requirements for ensuring the security of significant objects of critical information infrastructure of the Russian Federation". (In Russian).

13. Pavlov E.O. Podkhody k obespecheniyu bezopasnosti ob"ektov kriticheskoi in-formatsionnoi infrastruktury [Approaches to ensuring the security of critical information infrastructure facilities]. *Zhurnal vysokikh gumanitarnykh tekhnologii = Hi-Hume Journal*, 2024, no. 3 (6), pp. 32–38.

14. Gavdan G.P., Golubev A.A., Golubev A.G., Zhukov I.Y., Rybalko A.P. Obespechenie bezopasnosti gosudarstvennykh informatsionnykh sistem kak ob"ektov kriticheskoi informatsionnoi infrastruktury [Managing the security of government information systems as critical information infrastructure objects]. *Bezopasnost' informatsionnykh tekhnologii = IT Security (Russia)*, 2025, vol. 32, no. 3, pp. 26–43. DOI: 10.26583/bit.2025.3.03.

15. Goncharenko M.D., Kholkina K.S. [Safety of critical information infrastructure]. *Nauchnoe i tekhnicheskoe tvorchestvo molodezhi* [Scientific and technical creativity of youth]. Materials of the All-Russian Scientific and Practical Conference with international participation, Novosibirsk, April 19–20, 2023, pp. 200–208. (In Russian).

16. Mikhienko O.V., Lamonina L.V., Smirnova O.B. [On the issue of cybersecurity of critical information infrastructure]. *Innovatsionnye tekhnologii v APK, kak faktor razvitiya nauki v sovremennykh usloviyakh* [Innovative technologies in agriculture as a factor in the development of science in modern conditions]. Collection of the XIV International Scientific and Practical Conference, Omsk, 2025, pp. 787–791. (In Russian).

17. Zamilov A.R. [Automation of security monitoring of critical information infrastructure facilities]. *Radioelektronika, elektrotekhnika i energetika* [Radio electronics, electrical engineering and power engineering]. Abstracts of the Thirtieth International Scientific and Technical Conference of Students and Postgraduates, Moscow, 2024, p. 344. (In Russian).

Для цитирования:

Короткова Е.Е., *Селифанов В.В.* Разработка подхода к автоматизации выбора мер защиты ГИС в переходный период // Безопасность цифровых технологий. – 2026. – № 2 (121). – С. 50–67. – DOI: 10.17212/2782-2230-2026-2-50-67.

For citation:

Korotkova E.E., Selifanov V.V. Razrabotka podkhoda k avtomatizatsii vybora mer zashchity GIS v perekhodnyi period [Development of an approach to automating the selection of GIS protection measures during the transition period]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2026, no. 2 (121), pp. 50–67. DOI: 10.17212/2782-2230-2026-2-50-67.