АНАЛИЗ НОВЫХ ТРЕБОВАНИЙ К ЗАЩИТЕ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Лукоянов А.А., специалист по информационной безопасности,

АНО «Проектный офис по развитию туризма и гостеприимства Москвы»,

г. Москва, Россия

Аннотация. В работе рассмотрены новые требования к защите информации в информационных системах, установленные в результате актуализации нормативного регулирования ФСТЭК России. Проведен сравнительный анализ ранее действовавших и новых требований ФСТЭК России к организации защиты информации в информационных системах, выбору и реализации мер защиты, оценке состояния защиты информации и учету современных информационных технологий. Новые требования ориентируют операторов информационных систем на более последовательное управление защитой информации и дополняют традиционные меры защиты положениями, связанными с применением облачных вычислений, контейнерных сред, программных интерфейсов, мобильных устройств и искусственного интеллекта. Закреплено требование к периодической оценке состояния защиты информации на основе показателя защищенности и показателя уровня зрелости, что требует регулярного совершенствования защиты информационных систем на протяжении их жизненного цикла.

Ключевые слова: защита информации, информационная система, ФСТЭК России, требования, меры защиты, мониторинг, искусственный интеллект.

Введение. Развитие государственных и иных значимых информационных систем сопровождается усложнением архитектуры, ростом интеграционных связей, применением облачных и контейнерных технологий, API (Application Programming Interface), мобильных устройств и сервисов на основе искусственного интеллекта. В этих условиях защита информации должна рассматриваться как непрерывное управление защищенностью, включающее выявление угроз, управление уязвимостями и обновлениями, мониторинг событий безопасности и оценку состояния защиты.

Долгое время базовым документом являлся приказ ФСТЭК России от 11 февраля 2013 г. № 17, устанавливавший требования к защите информации в государственных информационных системах [5]. Приказ ФСТЭК России от 11 апреля 2025 г. № 117 расширил область применения требований и применяется с 1 марта 2026 г.; одновременно приказ № 17 признается утратившим силу [6].

Целью статьи является анализ новых требований к защите информации на основе сопоставления прежнего и нового подходов ФСТЭК России. Приказ № 17 был ориентирован на создание, эксплуатацию и аттестацию системы защиты информации в государственных информационных системах [5].Ключевым элементом прежнего подхода являлась классификация информационной системы по требованиям защиты информации. Класс защищенности определялся с учетом значимости обрабатываемой информации и масштаба системы, после чего выбирался базовый набор мер защиты, уточняемый по модели угроз, архитектуре и условиям функционирования информационной системы [5]. Меры защиты в приказе № 17 были сгруппированы по

направлениям: идентификация и аутентификация, управление доступом, ограничение программной среды, защита носителей информации, регистрация событий безопасности, антивирусная защита, обнаружение вторжений, контроль защищенности, обеспечение целостности и доступности, защита среды виртуализации, технических средств и сетевого взаимодействия [5].

Новые требования приказа ФСТЭК России № 117 расширяют область применения и распространяются не только на государственные информационные системы, но и на иные информационные системы государственных органов, государственных унитарных предприятий и государственных учреждений [6]. Существенным отличием является переход к регулярному управлению деятельностью по защите информации, включающему планирование и реализацию мероприятий, оценку состояния защиты, а также совершенствование применяемых мер [6].

В новых требованиях появляется формализованная оценка состояния защиты информации. Она должна проводиться на основе показателя защищенности

, характеризующего текущее состояние защиты от базового уровня угроз, и показателя уровня зрелости

, определяющего достаточность и эффективность проводимых мероприятий по защите информации [6]. Значения указанных показателей должны определяться с применением методических документов ФСТЭК России. В связи с этим особое значение приобретает методический документ «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах», утвержденный ФСТЭК России 12 апреля 2026 г. [4].

Таблица 1 — Сравнительный анализ прежнего и нового подходов к защите информации в информационных системах

Критерий сравнения		
Приказ	**ФСТЭК**	**России**
17		

Приказ	**ФСТЭК**	**России**
1	**1**	**7**

Область применения		
Основной акцент сделан на	государственных информационных системах, содержащих инфо	
Требования установлены для	государственных информационных систем, иных информационны	
Логика организации защиты		
Защита строилась вокруг этапов	создания системы защиты: формирование требований, разр	

Введена логика управления	деятельностью по защите информации: планирование, проведен		
Классификация	и выбор мер		
Класс защищенности определялся	по значимости информации и масштабу информационной		
Сохраняются классы защищенности,	но дополнительно устанавливается связь мер с уровнем в		
Состав групп мер	защиты		
Использовались группы мер:	идентификация и аутентификация, управление доступом, ограни		
Перечень базовых мер дополнен	блоками: защита облачных,	API,	,
Оценка состояния	защиты		
Контроль защищенности	проводился в рамках эксплуатации и аттестационных мероприятий,		
Введены показатели		и	, исп

Мониторинг процессов информационной безопасности

Регистрация событий и мониторинг рассматривались как элементы эксплуатации системы защ

Мероприятия по мониторингу ИБ выделены как самостоятельный процесс, предусматривающи

Управление уязвимостями и обновлениями

Анализ уязвимостей и управление обновлениями включались в процессы внедрения и эксплу

Управление уязвимостями, контроль конфигураций и управление обновлениями выделены в

Технологии искусственного интеллекта

Отдельные требования к применению искусственного интеллекта в составе информационных

Предусмотрены требования к защите информации при использовании ИИ: контроль запросов

Обобщенная характеристика требований

Подход был преимущественно ориентирован на выбор и реализацию мер защиты, подготовку

Подход дополняется постоянной оценкой состояния защиты, зрелости процессов, отчетность

Сравнительный анализ,приведенный в табл.1 показывает, что новые требования сохраняют преемственность с прежним подходом: классы защищенности, модель угроз, базовые меры защиты, аттестация и применение сертифицированных средств защиты информации остаются значимыми элементами обеспечения безопасности. Вместе с тем приказ № 117 уточняет и расширяет требования к организации защиты информации. Если прежний документ был в большей степени ориентирован на построение системы защиты и подтверждение ее соответствия, то новые требования предусматривают постоянное управление процессами защиты информации и регулярную оценку их результативности.Особое значение имеет введение показателей и : показатель защищенности

характеризует текущее состояние защиты информации, а показатель уровня зрелости

— достаточность и эффективность проводимых мероприятий по защите информации. Практическая ценность такого подхода состоит в том, что оператор получает инструмент не только для фиксации факта реализации отдельных мер, но и для оценки степени зрелости деятельности по защите информации. Это позволяет формировать план совершенствования защиты на основе измеримых результатов, а не только по итогам разовых проверок.

Направлением развития требований является учет современных технологий. В приказе № 117 отдельно выделены облачные вычисления, контейнерные среды, веб-технологии, API, мобильные устройства, интернет вещей, беспроводный доступ, DDoS-защита и использование искусственного интеллекта [6]. Это отражает переход современных информационных систем к распределенной и интегрированной архитектуре, зависящей от внешних сервисов и программных компонентов.

Отдельно в новых требованиях выделены положения о защите информации при использовании моделей искусственного интеллекта. Они предусматривают защиту от несанкционированного доступа и воздействия через наборы данных, модели ИИ, их параметры, процессы и сервисы обработки данных, а также контроль шаблонов запросов и ответов, допустимых тематик и реагирование на недостоверные ответы [6]. Практическая реализация приказа № 117 должна рассматриваться совместно с методическим документом ФСТЭК России от 12 апреля 2026 г., который определяет состав и содержание мероприятий и мер защиты информации [4].

Заключение.Проведенный анализ показывает, что новые требования к защите информации отражают развитие подходов к обеспечению защищенности информационных систем. Основные изменения связаны с расширением области применения требований, повышением роли внутренних стандартов и регламентов, выделением процессов управления уязвимостями, обновлениями и конфигурациями, развитием мониторинга, введением показателей защищенности и уровня зрелости, а также учетом облачных вычислений, контейнерных сред, API, мобильных устройств и искусственного интеллекта.

Практическое значение новых требований заключается в переходе от разового подтверждения соответствия к регулярному управлению защищенностью информационных систем. Это предполагает актуализацию внутренних документов, пересмотр моделей угроз, адаптацию мер защиты к архитектуре конкретной информационной системы, организацию мониторинга, расчет показателей защищенности и уровня зрелости, а также планирование мероприятий по совершенствованию защиты информации.

Литература

1. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. М.: Стандартинформ, 2014.

2. ГОСТ Р 56939-2024. Защита информации. Разработка безопасного программного обеспечения. Общие требования. М.: Российский институт стандартизации, 2024.

3. ГОСТ Р 59547-2021. Защита информации. Мониторинг информационной безопасности. Общие положения. М.: Стандартинформ, 2021.

4. Методический документ «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах»: утв. ФСТЭК России 12.04.2026 // Официальный сайт ФСТЭК России. URL: https://fstec.ru (дата обращения: 02.05.2026).

5. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»: утратил силу с 01.03.2026 // Официальный сайт ФСТЭК России. URL: https://fstec.ru (дата обращения: 02.05.2026).

6. 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»: зарегистрирован в Минюсте России 16.06.2025 № 82619 // Официальный интернет-портал правовой информации. URL: https://publication.pravo.gov.ru (дата обращения: 02.05.2026).

7. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. № 31, ч. I. Ст. 3448.