УДК 004.057
DOI 10.21685/2587-7704-2020-5-1-6

Open Access | RESEARCH ARTICLE

# Применение средств защиты информации для реализации мер защиты, установленных специальными нормативными документами Федеральной службы по техническому и экспертному контролю

***А. Г. Фатеев***
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

**Аннотация**. Проведен обзор мер защиты и их базовых наборов, установленных приказами ФСТЭК России № 17 и № 21 для защиты информационных систем. Выполнено сравнение мер защиты и их базовых наборов для выявления отличий. Проанализированы возможности реализации мер защиты информации посредством использования различных типов средств защиты информации. В результате установлено, что для реализации мер защиты требуется использование нескольких средств защиты различного типа. Определены недостатки такого подхода и рассмотрен один из вариантов решения этой проблемы, предлагаемый разработчиками средств защиты информации.

**Ключевые слова**: мера защиты, базовый набор, информационная система, средство защиты информации, реестр сертифицированных средств защиты информации.

# The use of information security tools to implement protection measures specified by the FSTEC regulatory acts

***A. G. Fateev***
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

**Abstract**. A review of protection measures and their basic sets specified by Orders of FSTEC of Russia No. 17 and No. 21 on information system security is carried out. A comparison of protection measures and their basic sets to identify differences is performed. The possibilities of implementing information protection measures through the use of various types of information security tools are analyzed. As a result, it was found that the implementation of protection measures requires the use of a number of various security tools. The disadvantages of this approach are identified, and an option for solving this problem proposed by the developers of information security tools is considered.

**Keywords**: protection measure, basic set, information system, information security tool, registry of certified information security tools.

В настоящее время действуют приказы Федеральной службы по техническому и экспортному контролю, которые устанавливают требования по защите информационных систем персональных данных (ИСПДн) [1] и государственных информационных систем (ГИС) [2]. Эти требования представлены в виде мер защиты информации, которые необходимо реализовать в соответствующей ин-

формационной системе (ИС) для обеспечения безопасности обрабатываемой информации. В каждом из перечисленных документов приводится перечень мер защиты, а также устанавливается классификация ИС посредством определения классов или уровней защищенности. Их может быть четыре, как для ИСПД, или три, как для ГИС. Каждому из уровней классификации ИС соответствует определенный минимальный набор мер защиты, который должен обеспечить безопасность обрабатываемой информации.

Сравнение полных наборов требований показывает, что количественно они почти не отличаются.

Приказ Федеральной службы по техническому и экспортному контролю № 17 от 11 февраля 2013 г. [2] содержит 13 групп мер защиты, которые должны обеспечивать:

– идентификацию и аутентификацию субъектов доступа и объектов доступа. Включает семь мер защиты;

– управление доступом субъектов доступа к объектам доступа. Включает 17 мер защиты;

– ограничение программной среды. Включает четыре меры защиты;

– защиту машинных носителей информации. Включает восемь мер защиты;

– регистрацию событий безопасности. Включает восемь мер защиты;

– антивирусную защиту. Включает две меры защиты;

– обнаружение (предотвращение) вторжений. Включает две мер защиты;

– контроль (анализ) защищенности информации. Включает пять мер защиты;

– целостность информационной системы и информации. Включает восемь мер защиты;

– доступность информации. Включает семь мер защиты;

– защиту среды виртуализации. Включает десять мер защиты;

– защиту технических средств. Включает пять мер защиты;

– защиту информационной системы, ее средств, систем связи и передачи данных. Включает 30 мер защиты.

Общее количество мер защиты – 113.

Приказ № 21 [1] определяет состав мер по обеспечению безопасности персональных данных (ПДн), реализуемых в рамках системы защиты ПДн с учетом актуальных угроз безопасности ПДн и применяемых информационных технологий, в который входят те же меры, которые определены и приказом №17 [2]. К ним добавлены еще две группы мер защиты:

– выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ИС и (или) к возникновению угроз безопасности ПДн (инциденты), и реагирование на них;

– управление конфигурацией информационной системы и системы защиты ПДн.

Общее количество мер защиты, определенных приказом № 21, – 119.

Сравнение перечней мер защиты, установленных этими приказами, показывает, что большей частью меры защиты, определенные приказами № 17 [2] и № 21 [1], совпадают. Однако есть отличия по некоторым группам мер защиты. Например, количество мер защиты, относящихся к идентификации и аутентификации субъектов доступа и объектов доступа в приказе № 17 [2], составляет семь. Приказ № 21 [1] устанавливает шесть мер защиты, относящихся к идентификации и аутентификации субъектов доступа и объектов доступа. В приложении 2 к приказу № 21 [1] отсутствует такая мера, как ИАФ.7 Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа. Для меры регистрации событий безопасности приказом № 17 [2] определена мера РСБ.8 Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в ИС, которая не определена приказом № 21 [1]. В состав мер обеспечения доступности приказом № 17 [2] включены такие меры, как ОДТ.6 Кластеризация ИС и (или) ее сегментов и ОДТ.7 Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации. Приказом № 21 [1] эти меры не определены.

Существенно отличаются меры по защите ИС, ее средств, систем связи и передачи данных. Так, приказом № 17 [2] определено 30 мер защиты, а приказом № 21 [1] только 20. Сравнение этих мер защиты показывает, что меры с ЗИС.1 по ЗИС.20, определенные каждым приказом, полностью совпадают. Приказом № 17 [2] установлены меры защиты с идентификаторами с ЗИС.21 по ЗИС.30, которые не определены приказом № 21 [1].

Кроме того, следует отметить, что приказом № 21 [1] установлены меры защиты, которые не определены приказом № 17 [2]. Это меры по выявлению инцидентов и реагированию на них (шесть мер защиты) и меры по управлению конфигурацией ИС и системы защиты (четыре меры защиты).

Полностью совпадают такие меры защиты, как управление доступом, ограничение программной среды, защита машинных носителей, антивирусная защита, обнаружение вторжений, контроль (анализ) защищенности, обеспечение целостности, защита среды виртуализации и защита технических средств.

Количественная оценка сравнения мер защиты, установленных приказами № 17 [2] и № 21 [1], показывает, что совпадают 99 мер защиты. Отличаются эти два приказа в 24 мерах защиты.

Каждый приказ определяет классификацию ГИС и ИСПДн. В приложении 1 к приказу № 17 [2] устанавливается три класса защищенности ГИС. Для каждого из трех классов приведены базовые наборы мер защиты. Базовые наборы мер защиты для каждого класса защищенности являются основой для определения того набора мер защиты, который должен быть реализован для защиты ГИС и выполнения предъявляемых к ней требований с учетом класса защищенности, характеристик ГИС, информационных технологий, особенностей функционирования, сформированной модели угроз и других требований. Для ГИС, класс защищенности которых определяется как третий (самый низкий), базовый набор включает 48 мер защиты. Некоторые меры защиты в этот набор не входят, например меры защиты по обнаружению вторжений. Из состава других мер включено по одной или две меры. В состав базового набора мер защиты для второго класса защищенности ГИС входят 76 мер. В состав базового набора мер защиты для первого класса защищенности ГИС входят 83 меры.

Аналогично для классификации ИСПДн используются уровни защищенности ПДн, которых установленных четыре. Соответственно, в приложении к приказу № 21 [1] определено четыре базовых набора мер защиты ПДн. Базовый набор для четвертого уровня защищенности ПДн включает 27 мер защиты. Базовый набор для третьего уровня защищенности ПДн включает 41 меру защиты. Базовый набор для второго уровня защищенности ПДн включает 66 мер защиты. Базовый набор для первого уровня защищенности ПДн включает 69 мер защиты. Некоторые меры защиты в базовые наборы для уровней защищенности не включены. Например, меры по защите машинных носителей информации не входят в базовый набор для четвертого уровня. Меры по обнаружению вторжений не входят в базовые наборы для четвертого третьего уровней.

Выбор мер защиты для ИСПДн определяется не только базовым набором. Окончательный список мер защиты определяется с учетом характеристик ИСПДн системы, информационных технологий, особенностей функционирования ИСПДн, модели угроз и требований к защите ПДн, установленных нормативными правовыми актами в области обеспечения безопасности ПДн и защиты информации. Таким образом, к базовому набору для установленного уровня защищенности добавляются дополнительные меры защиты. Также могут исключаться меры защиты, если в ИСПДн не применяются информационные технологии, требующие использование некоторых мер. Например, если в ИСПДн не применяются технологии виртуализации, то нет необходимости в использовании мер по защите среды виртуализации.

Приказами № 17 [2] и № 21 [1] также устанавливается необходимость применять для реализации мер защиты средства защиты информации, в том числе программные (программно-аппаратные) средства, имеющие необходимые функции безопасности. Эти средства защиты информации должны быть сертифицированы по обязательным требованиям по безопасности информации, установленным нормативными правовыми актами, или требованиям, указанным в технических условиях (заданиях по безопасности). В настоящее время существует ряд систем сертификации, в рамках которых действуют документы, устанавливающие требования, на соответствие которым сертифицируются средства защиты информации (СЗИ). Средства защиты информации от НСД и ряд других категорий сертифицируется в системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00. Эта система действует на основании Положения о системе сертификации средств защиты информации, утвержденного приказом ФСТЭК России от 3 апреля 2018 г. № 55 [3]. Федеральным органом сертификации является ФСТЭК. Сведения о средствах защиты информации заносятся в Государственный реестр сертифицированных средств защиты информации, размещенный на официальном сайте ФСТЭК [4]. Таким образом, при выборе средств защиты информации, которые могут применяться для реализации мер защиты, установленных приказами № 17 [2] и № 21 [1], следует выбирать их только из тех средств, которые имеют действующий сертификат, подтверждающий соответствие обязательным требованиям по защите информации.

Процесс определения мер защиты информации, которые необходимо реализовать для обеспечения безопасности ГИС или ИСПДн, включает несколько этапов. Первый этап – определение базового набора мер защиты информации для установленного класса защищенности ГИС или уровня защищенности ПДн в соответствии с базовыми наборами мер защиты информации. Второй этап – адаптация базового набора мер защиты информации применительно к структурно-функциональным

характеристикам ГИС или ИСПДн, информационным технологиям, особенностям функционирования. Третий этап – уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включенных в модель угроз безопасности информации. Четвертый этап – дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации. В результате выполнения этих четырех этапов формируется окончательный набор мер защиты, которые должны быть реализованы для защиты ГИС или ИСПДн. При этом базовый набор может претерпеть существенные изменения. К нему только могут быть добавлены необходимые меры защиты, но также исключены те меры, которые не соответствуют особенностям ГИС или ИСПДн. Именно такой окончательный набор мер защиты и должен реализовываться с применением сертифицированных средств защиты информации. Таким образом, перед оператором ИС и администратором безопасности возникает задача выбора программных (программно-аппаратных) средств, имеющих необходимые функции безопасности.

Оценка перечня мер защиты, определенного в приложениях к приказам № 17 [2] и № 21 [1], показывает, что для их реализации потребуется несколько различных средств защиты информации. Например, для реализации мер по идентификации и аутентификации субъектов доступа и объектов доступа потребуется применять средства защиты информации от несанкционированного доступа (НСД). Для реализации мер по управлению доступом субъектов доступа к объектам доступа потребуется применять как СЗИ от НСД, так и межсетевые экраны. Эти средства защиты потребуются для реализации мер защиты, связанных с управлением информационными потоками между сегментами сетей и контролем удаленного доступа. Для реализации мер защиты по ограничению программной среды, защите машинных носителей информации, регистрации событий безопасности также потребуется применить СЗИ от НСД. Но для реализации таких мер, как антивирусная защита, обнаружение вторжений, анализ защищенности, потребуется применение соответствующих средств, а именно средств антивирусной защиты, систем обнаружения атак и вторжений, средств анализа защищенности (сканеров уязвимостей). Для реализации мер по обеспечению целостности и доступности потребуется применять как СЗИ от НСД, так и специализированные средства контроля и фиксации целостности, средства резервного копирования, межсетевые экраны и другие средства, позволяющие разбивать ИС на сегменты. Реализация мер по защите среды виртуализации также потребует применения как СЗИ от НСД, межсетевых экранов, средств резервного копирования, так и применения средств защиты информации, которые разработаны для применения именно в средах виртуализации и учитывают особенности их функционирования. Также подобные специальные средства защиты могут применяться для контроля действий администраторов и пользователей при работе с объектами среды виртуализации – виртуальными машинами и др. Для реализации мер по защите ИС, ее средств, систем связи и передачи данных также потребуется несколько типов СЗИ. К ним следует отнести СЗИ от НСД, межсетевые экраны, средства обеспечения доверенной загрузки операционной системы, средства построения виртуальных частных сетей (VPN), средства контроля доступа к аппаратным ресурсам. Меры по выявлению инцидентов и реагирование на них, а также управлению конфигурацией ИС и СЗИ могут быть реализованы посредством СЗИ от НСД. Они наряду с мерами по защите технических средств реализуются организационно.

В результате проведенного анализа возможностей реализации мер защиты, определенных приказами № 17 [2] и № 21 [1], можно сделать вывод о том, что потребуется использовать несколько типов СЗИ. В их число входят СЗИ от НСД, межсетевые экраны, средства антивирусной защиты и др. Если рассматривать базовые наборы мер защиты для четвертого уровня защищенности ПДн или третьего класса защищенности, ГИС не позволяют применить какой-то один тип СЗИ. Это как минимум СЗИ от НСД, межсетевой экран, средство антивирусной защиты. При оценке реализации мер защиты необходимо учесть и возможности операционной системы, установленной на защищаемом компьютере. В перечне функций также присутствуют идентификация и аутентификация, межсетевой экран, регистрация событий (аудит) и др. Но ОС может не иметь сертификат соответствия требованиям безопасности. Также функции, реализуемые специальными СЗИ, предоставляют больше возможностей по сравнению с функциями ОС. Поэтому возможности применения функций защиты информации, реализуемых ОС, ограниченны.

Необходимость использовать для защиты ИС нескольких типов СЗИ приводит к возникновению нескольких проблем. Во-первых, необходимо приобретать эти СЗИ и необходимые лицензии. Во-вторых, потребуется провести обучение навыкам работы с каждым СЗИ как администраторов, так

и пользователей. В-третьих, при установке на один компьютер нескольких СЗИ, как правило, возникают конфликты при их совместном функционировании.

Ни один из разработчиков СЗИ не выпускает всю номенклатуру СЗИ, которые позволяли бы реализовывать различные меры защиты информации. При этом разные разработчики не обеспечивают совместимость разрабатываемых ими СЗИ со средствами защиты от других разработчиков. Такие СЗИ от НСД, как Аккорд, DallasLock, Secret Net и ряд других, обладающих широким набором функций защиты, не реализуют антивирусную защиту, анализ защищенности, обнаружение вторжений и другие меры защиты. Поэтому администратору безопасности при установке, настройке и последующей эксплуатации приходится решать задачу настройки и конфигурирования различных СЗИ так, чтобы они не влияли друг на друга. В качестве примера можно привести блокирование работы ядра СЗИ от НСД Secret Net антивирусом Касперского. При этом процесс ядра выгружается из памяти и удаляется исполняемый файл, обеспечивающий работу ядра СЗИ. Для корректной работы СЗИ от НСД Secret Net необходимо при конфигурировании антивируса Касперского создать список доверенных процессов, в который включить процессы, запускаемые при загрузке СЗИ от НСД Secret Net. Решение подобной задачи приводит к дополнительным затратам времени. Кроме того, в процессе функционирования при изменении параметров работы могут возникать сбои в работе СЗИ, вызванные взаимным влиянием, ранее не проявлявшиеся.

Решением этой проблемы является переход от разработки СЗИ, которые являются специализированными и решающими ограниченный набор задач, к решениям (программным или программно-аппаратным), представляющим собой комплекс средств защиты или отдельных компонентов. Эти решения должны создаваться одним разработчиком, что позволяет избежать негативного влияния различных СЗИ друг на друга. Программно-аппаратные средства защиты информации, реализующие такие решения, должны быть построены по модульному принципу. В их основе может лежать ядро системы защиты и модули, реализующие основной набор функций, для соответствия обязательным требованиям по ЗИ, установленным документами ФСТЭК. Кроме того, в состав таких СЗИ могут включаться другие модули и компоненты, реализующие функции защиты в соответствии с требованиями по защите информации, например, функции антивирусной защиты, обеспечения безопасного межсетевого взаимодействия и др. Подобная архитектура позволит гибко конфигурировать СЗИ, выбирая компоненты, выполняющие функции, необходимые для реализации требуемых мер защиты. При изменении требований и необходимости реализовать дополнительные меры защиты можно приобретать лицензии только на те компоненты, которые необходимы для их реализации.

В результате построение СЗИ как решений позволит операторам ИС выбирать конфигурацию СЗИ, необходимую для решения задачи реализации мер защиты, установленных приказами ФСТЭК. Например, если перед оператором стоит задача реализовать меры защиты для какого-либо класса защищенности ГИС с учетом внесенных изменений, он может выбрать СЗИ и приобрести лицензию только на те компоненты, которые выполняют необходимые функции.

Анализ рынка СЗИ и предложений от разработчиков с учетом сведений, приведенных в Государственном реестре сертифицированных средств защиты информации [4], показывает, что на сегодняшний день единственным СЗИ, которое может рассматриваться как решение, является система защиты информации (ЗИ) Secret Net Studio. Эта система ЗИ включает базовый набор политик (базовую защиту), а также набор защитных подсистем, которые реализуют функции защиты в соответствии с требованиями руководящих документов ФСТЭК. Кроме того, в состав системы ЗИ Secret Net Studio могут входить компоненты антивирусной защиты, компоненты обнаружения вторжений, межсетевой экран, защита локальных дисков и функция криптозащиты. Их использование требует приобретения отдельных лицензий. При использовании всего набора компонент из состава одной системы ЗИ Secret Net Studio отпадает необходимость в приобретении отдельного средства антивирусной защиты, межсетевого экрана и др. Такой подход к разработке СЗИ позволяет избежать всех отмеченных выше по тексту проблем. Еще одним преимуществом является возможность использования системы ЗИ Secret Net Studio как решения задачи обеспечения безопасности ГИС и ИСПДн в соответствии с приказами № 17 [2] и № 21 [1]. Разработчики предоставляют рекомендации по набору используемых компонентов для каждого типа ИС, а также предоставляют рекомендации по настройке системы ЗИ с учетом класса защищенности ГИС и уровня защищенности ПДн.

Оценивая возможности применения системы ЗИ Secret Net Studio следует отметить, что подобные решения были бы для операторов ИС более полезны по сравнению с отдельными специализированными СЗИ. Они позволяют сократить затраты времени на конфигурирование и решить многие другие проблемы, связанные с использованием набора СЗИ от разных разработчиков. В настоящее время, кроме системы ЗИ Secret Net Studio, других аналогичных систем разработчиками не предлагается.

**Библиографический список**

1. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : Приказ ФСТЭК России от 18 февраля 2013 г. № 21 : [зарегистрировано в Минюсте России 14.05.2013 № 28375] // КонсультантПлюс.
2. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : Приказ ФСТЭК России от 11 февраля 2013 г. № 17 : [зарегистрировано в Минюсте России 31.05.2013 № 28608] // КонсультантПлюс.
3. Положение о системе сертификации средств защиты информации : [утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55] // КонсультантПлюс.
4. Государственный реестр сертифицированных средств защиты информации № РОСС RU.0001.01БИ00. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00 (дата обращения: 21.10.2019).

**Образец цитирования:**

Фатеев, А. Г. Применение средств защиты информации для реализации мер защиты, установленных специальными нормативными документами Федеральной службы по техническому и экспертному контролю / А. Г. Фатеев // Инжиниринг и технологии. – 2020. – Vol. 5(1). – С. 1–6. – DOI 10.21685/2587-7704-2020-5-1-6.