электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 621.391

Обзор методического документа "Меры защиты информации в государственных информационных системах", утвержденного ФСТЭК России 11 февраля 2014 г.

***Якубов Р.Ж.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Цирлов В.Л., к.т.н, доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
bauman@bmstu.ru

Введение

В данной работе приводится краткий обзор и описание методического документа "Меры защиты информации в государственных информационных системах", утвержденного ФСТЭК России 11 февраля 2014 г.

Данный методический документ предназначен для детализации организационных и технических мер защиты информации в соответствии с "Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах", утвержденными приказом ФСТЭК РФ от 11 февраля 2013 г. № 17.

Основной целью создания "Мер защиты информации" стало подробное описание мер безопасности, определенных в приказе № 17, но также не были обойдены вниманием некоторые другие пункты.

Целью работы являлось рассмотрение методического документа, как вспомогательного средства при создании системы защиты информации в государственных учреждениях. Был проведен анализ документа и составлено краткое описание для ознакомления с его общей структурой и принципами работы с ним.

Классификация информационной системы

Первым шагом определения требований безопасности к информационной системе является определение ее класса защищенности, определяемого совокупностью уровня значимости информации и масштабом самой системы. В данном разделе описаны

принципы определения уровня значимости информации и масштабов системы. Классы защищенности системы определяются в соответствии с таблицей 1.

Уровень значимости (УЗ) - это степень возможного ущерба для обладателя информации и оператора от нарушения конфиденциальности, целостности или доступности данных, причем для каждого из этих трех свойств определяется собственная степень ущерба. Информация получает уровень значимости, равный наибольшей степени ущерба среди трех свойств безопасности. (УЗ 1 - высокий уровень ущерба, У З4 - степень ущерба не может быть определена, но информацию необходимо защитить в соответствии с законодательством РФ).

Для определения степени возможного ущерба могут применяться национальные стандарты и (или) методические документы, разработанные и утвержденные ФСТЭК.

Масштаб информационной системы определяется назначением и распределением сегментов информационной системы.

Информационная система имеет федеральный масштаб, если она функционирует на территории Российской Федерации (в пределах федерального округа) и имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях.

Информационная система имеет региональный масштаб, если она функционирует на территории субъекта Российской Федерации и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях.

Информационная система имеет объектовый масштаб, если она функционирует на объектах одного федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

Таблица 1

Классы защищенности систем

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3
УЗ 4	К3	К3	К3

Определение угроз безопасности информации в информационной системе

После классификации системы предполагается создание модели угроз безопасности. Эффективность принимаемых мер защиты зависит от качества определения угроз безопасности информации для определенной системы в конкретных условиях ее функционирования.

Предлагается определять угрозы безопасности информации(УБИ) по следующему принципу:

УБИ = [возможности нарушителя; уязвимости информационной системы; способ реализации угрозы; последствия реализации угрозы].

Также в документе даются рекомендации по созданию модели угроз безопасности конкретной системы, с упоминанием того, что для определения угроз безопасности должны быть использованы методические документы, разработанные и утвержденные ФСТЭК.

Выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации

Выполнение инструкций, предоставленных в данном разделе, является конечной ступенью создания системы информационной безопасности в соответствии с приказом №17. Основной целью создания данного методического документа является помощь в грамотном выборе мер защиты и их реализации в конкретной системе. Она заключается в подробном разборе каждой из предполагаемой мер защиты, представленном в приказе ФСТЭК от 11 февраля 2013 г. № 17.:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение(предотвращение) вторжений;
- контроль(анализ) защищенности информации;
- обеспечение целостности информационной системы и информации;
- обеспечение доступности информации;
- защита среды виртуализации;
- защита технический средств;

- защита информационной системы, ее средств и систем связи и передачи данных.

Однако, описание вышеперечисленных средств расположено в 3 главе документа "Содержание мер защиты информации в информационной системе", обращение к которой предполагается по ходу работы с разделом 2.3 ("Выбор мер защиты информации"). Сам он посвящен описанию механизма создания набора мер защиты информации, заточенного под конкретную систему.

Этот механизм состоит из 5 ступеней, выполняемых поочередно:

1. Определяется базовый набор мер защиты информации для установленного класса защищенности информационной системы;
2. Адаптация базового набора мер защиты, с учетом целей, задач защиты информации, применяемых информационных технологий и структурно-функциональных характеристик информационной системы;
3. Уточнение адаптированного базового набора мер защиты информации, проводящееся с учетом результатов оценки его возможности адекватно блокировать все угрозы безопасности, включенные в модель угроз безопасности информации, или снизить вероятность из реализации.
4. Дополнение уточненного адаптированного базового набора мер защиты информации, целью которого является выполнение требований иных нормативных правовых актов в области защиты информации.
5. Применение компенсирующих мер защиты информации, необходимых при невозможности реализации по тем или иным причинам некоторых пунктов в сформированном наборе.

Создание и реализация эффективной системы защиты информации и является конечной целью работы с приказом №17 об утверждении Требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

Содержание мер защиты информации в информационной системе

Для полноценного описания данного методического документа необходимо предоставить структуру описания мер защиты информации. Она довольно проста.

В описание каждой меры входят три кратких пункта:

- Требования к реализации.
- Требования к усилению.

- Содержание базовой меры.

Требования к реализации - это общие требования(или инструкции) при внедрении данной меры. Например, в случае ИАФ.1 (идентификация и аутентификация пользователей, являющихся работниками оператора) расписано, кто является внутренним пользователем системы, и показаны главные аспекты, на которые стоит обращать внимание при внедрении меры.

Также в описании каждой меры даны **требования к усилению**, позволяющие качественно повысить уровень безопасности при их реализации. В случае все того же ИАФ.1, предлагается ввести многофакторную(двухфакторную) аутентификацию, механизм одноразовых паролей. Следует заметить, что меры усиления применяются на этапе уточнения адаптированного базового набора мер защиты информации, и их применение зависит от класса защищенности системы.

Внедрение требований к усилению соответствующей меры происходит добровольно или в обязательном порядке, в зависимости от таблицы "содержание базовой меры защиты информации". Если применение какого-либо требования не включено в эту таблицу, то решение о его включении в систему происходит по решению обладателя информации, заказчика и (или) оператора для повышения уровня защищенности информации.

В конце описания каждой меры безопасности дается таблица "**содержание базовой меры защиты информации**". В качестве примера в таблице 2 дается содержание базовой меры ИАФ.1.

Таблица 2

Содержание базовой меры защиты информации

Мера защиты информации	Класс защищенности информационной системы			
	4	3	2	1
ИАФ.1	+	+	+	+
Усиление ИАФ.1			1а, 2а, 3	1а, 2а, 3, 4

Заключение

В целом, методический документ мог быть полнее. Так, раздел классификации информационной системы практически дублирует приказ № 17, да и практически весь документ не несет значительного объема информации, способного существенно помочь

при реализации системы защиты информации(за исключением раздела содержания мер защиты информации).

В документе отсутствует описание базовой модели угроз, и, при более чем подробном описании мер защиты, отсутствуют приоритеты по их реализации.

При этом, подробное описание мер защиты информации является довольно интересной частью документа, позволяющей примерно ознакомиться с необходимыми работами и конкретными требованиями к каждой меры. Несмотря на это, в остальной части документа отсутствует конкретика, и необходимо активно пользоваться иными методическими документами при разработке системы(например, при создании модели угроз).

Таким образом, обращение к методическому документу необходимо для доступа к разделу 3 ("Содержание мер защиты информации"), но раздел 2 довольно неплохо описан и в исходном приказе № 17.

Список литературы

1. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [текст]: приказ ФСТЭК России № 17. 2013. 37 с.
2. Меры защиты информации в государственных информационных системах [текст]: Методический документ ФСТЭК России. 2014. 176 с.
3. Прозоров А. 15 замечаний на проект документа ФСТЭК по защите ГосИС (и ПДн) Режим доступа: http://80na20.blogspot.ru/2013/12/15.html (дата обращения 06.03.2014).