Министерство науки и высшего образования

Российской Федерации

Федеральное Государственное

Автономное Образовательное Учреждение

Высшего Образования

Национальный ядерный университет «МИФИ»

Кафедра: «Финансовый Мониторинг»

Частное Техническое задание на разработку системы защиты

Студент Монастырский М. О.

Группа С21-703

Москва 2023г.

Оглавление

[Принятые сокращения 3](#_Toc151920891)

[Введение 4](#_Toc151920892)

[Основание разработки 5](#_Toc151920893)

[Исходные данные модернизируемого объекта 6](#_Toc151920894)

[Класс защищенности АС 7](#_Toc151920895)

[Нормативные документы 8](#_Toc151920896)

[Требования к СЗИ 9](#_Toc151920897)

[Перечень предполагаемых к использованию СЗИ 10](#_Toc151920898)

[Основание на разработку собственных СЗИ 11](#_Toc151920899)

[Состав, сроки и содержание проведения работ 12](#_Toc151920900)

[Требования к подрядным организациям-исполнителям 13](#_Toc151920901)

[Перечень предъявляемой заказчику научно-технической продукции и базы 14](#_Toc151920902)

[Заключение 15](#_Toc151920903)

[Источники 16](#_Toc151920904)

# Принятые сокращения и определения

**Система защиты информации (СЗИ)** – средства защиты информации - технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.[[1]](#footnote-1)

**Информационная система(ИС)-** совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств[[2]](#footnote-2)

**ФСТЭК** - Федеральная служба по техническому и экспортному контролю

**ТЗ** – Техническое задание

**ЧТЗ** – Частное Техническое задание

**НПА –** Нормативно-правовой Акт

**ИБ –** Информационная Безопасность

# Введение

Создание всякой сложной системы вне зависимости от ее предназначения есть продукт множества сложных процессов, протекающих параллельно и независимо друг от друга, от исхода каждого такого процесса по отдельности зависит конечный результат в целом. Именно поэтому, для достижения высокой организованности всех задействованных процессов необходимо заранее иметь документ, который позволит всем участникам процесса выстроить образ результата, подкрепленный научно-техническим, организационным и нормативно правовым фундаментом. Только понимание результата может помочь всем участникам выстроить процессы взаимодействия во время разработки и стать базой для эксплуатации разрабатываемых систем. Таким документом может стать техническое задание, поскольку содержит всю необходимую информацию.

В настоящей работе будут рассмотрены организационно-правовые и технические вопросы составления частного технического задания на разработку системы защиты информации, включая такие необходимые для этого процессы как: Построение актуальной модели угроз защиты информации в соответствии с методикой ФСТЭК, построение модели нарушителя в соответствии с вышеупомянутой методикой, и прохождение аттестации ИС, а именно присвоение класса защищенности ИС при вводе таковой в эксплуатацию, также будут рассмотрены конкретные сертифицированные уполномоченными органами, и рассмотрен процесс разработки собственных решений в области защиты информации.

# Основание разработки

# Исходные данные модернизируемого объекта

Для определения исходных данных защищаемого объекта необходимо произвести оценку угроз безопасности исходя из требований Методики.

Учредить специальную комиссию, отвечающую рекомендациям согласно приложению 2 Методики, а именно:

«В состав экспертной группы для оценки угроз безопасности информации рекомендуется включать экспертов (независимо от того, реализуются ли функции обладателя информации, заказчика и оператора в рамках одной или нескольких организаций) от: подразделения по защите информации (обеспечения информационной безопасности); подразделения, ответственного за цифровую трансформацию (ИТ-специалистов); подразделения, ответственного за эксплуатацию сетей связи; подразделения, ответственного за эксплуатацию автоматизированных систем управления; подразделений обладателя информации или оператора, ответственного за выполнение основных (критических) процессов (бизнес-процессов). 36 Состав экспертов по решению обладателя информации или оператора может быть дополнен или уточнен с учетом особенностей области деятельности, в которой функционируют системы и сети. В частности, для оценки угроз безопасности информации, реализация которых может привести к финансовым рискам, рекомендуется привлекать дополнительно специалистов экономических (финансовых) подразделений обладателя информации или оператора. Для организации работы экспертной группы рекомендуется определять специалиста по защите информации (обеспечению информационной безопасности), имеющего стаж работ не менее трех лет и практический опыт оценки информационных рисков. В экспертную группу для оценки угроз безопасности информации рекомендуется включать специалистов, имеющих опыт работы не менее одного года по соответствующему направлению деятельности, в котором проводится оценка угроз безопасности информации. Эксперты должны обладать независимостью, основанной на отсутствии коммерческого и финансового интереса или другого давления, которое может оказать влияние на принимаемые решения. Не рекомендуется формировать экспертную группу из участников, находящихся в прямом подчинении, так как это может негативным образом повлиять на результат определения угроз безопасности информации. В состав экспертной группы должны входить не менее трех экспертов»

В ходе оценки группа должна пройти следующие этапы:



Рисунок 1 Этапы проведения оценки согласно Методике

В качестве базы все этапы основываются на следующих документах:

* Список актуальных угроз (<https://bdu.fstec.ru/>)
* Открытые списки векторов атак, такие как ATT&CK
* Техническое задание на создание компьютерной сети, частные технические задания на создание ее компонентов
* Данные предоставляемые Оператору поставщиками услуг, в случае если инфраструктура организации основана на IaaS и базируется удаленно в облаке на базе сторонней организации
* И другие имеющие ценность в области ИБ

На первом этапе производится анализ потенциальных негативных последствий от реализации возможных угроз, например:

«1)если оператор обрабатывает персональные данные граждан, которые в соответствии с Федеральным законом «О персональных данных» подлежат обязательной защите, одним из возможных негативных последствий от реализации угроз безопасности информации является нарушение конфиденциальности персональных данных, в результате которого будут нарушены права субъектов персональных данных и соответствующие законодательные акты; 2) если оператор обеспечивает транспортировку нефти, одним из возможных негативных последствий от реализации угроз безопасности информации является разлив нефти из нефтепровода, повлекший наступление экологического ущерба; 3) если оператор предоставляет услуги связи, одним из возможных негативных последствий от реализации угроз безопасности информации является непредоставление услуг связи абонентам, повлекшее наступление ущерба в социальной сфере; 4) для оператора по переводу денежных средств одним из возможных негативных последствий от реализации угроз безопасности информации является хищение денежных средств, в результате которого возможны финансовые и репутационные риски.»

Примеры типовых целей и пример оценки целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации составляются согласно Приложениям 6 и 7 Методики.

На Втором этапе проводится инвентаризация систем и сетей, для определения уязвимостей и векторов атаки специфичных для инфраструктуры предприятия.

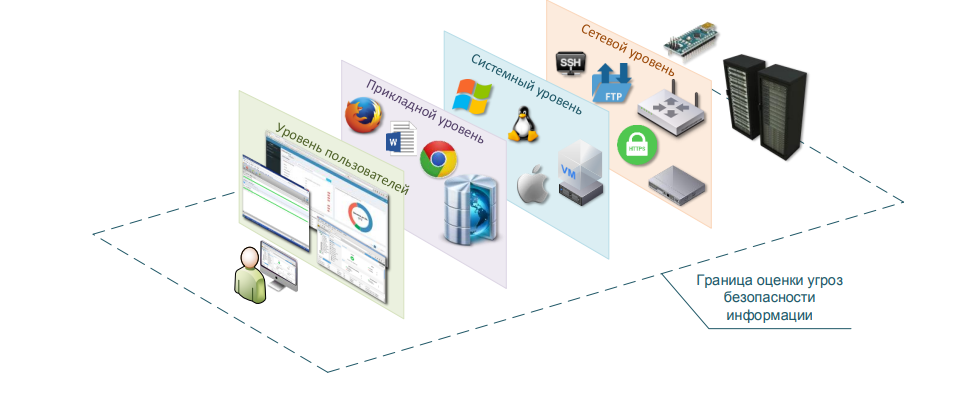


Рисунок 2. Уровни оценки инфраструктуры

На третьем этапе производится обобщение полученной информации и построение на ее основе модели угроз, модели злоумышленника, потенциальных сценариев реализации угрозы



Рисунок 3. Пример реализации угроз безопасности.

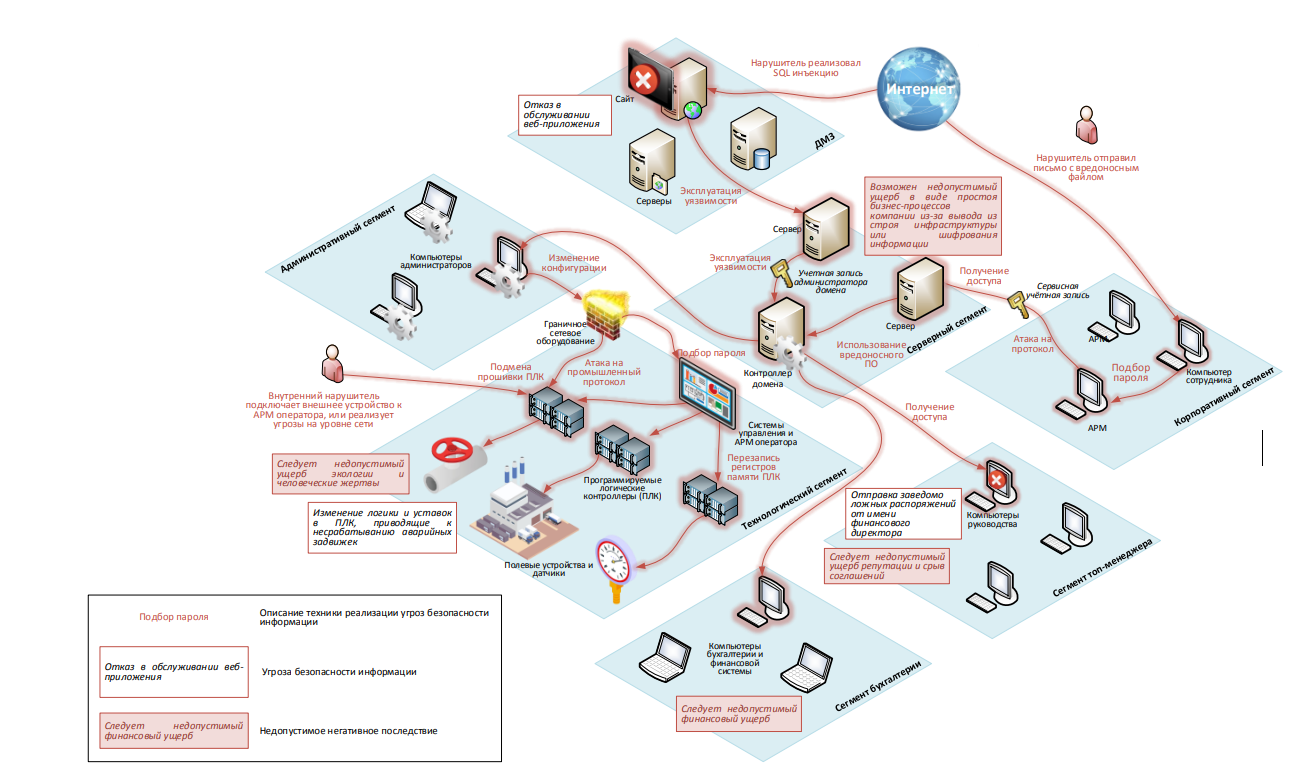


Рисунок 4. Реализация сценария угрозы безопасности

Оценка сложности таких угроз определяется согласно положениям Методики указанным в приложениях.

По результатам построения полученная оценка может быть основой для выявления слабых мест в системах защиты организации и выработке мер по укреплению периметра контролируемой зоны.

# Класс защищенности АС

# Нормативные документы

Основанием для разработки технического задания является п. 15 Приказа ФСТЭК России от 11.02.2013 N 17 (ред. от 28.05.2019) "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"(Далее приказ № 17)

Также основанием для разработки ТЗ является практическая необходимость обеспечения состояния защищенности информации в соответствии с ст. 6,16 149 ФЗ, приказами № 17 и №524(если применим) ФСТЭК и ФСБ соответственно, а также ряда других НПА, таких как:

• Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».  
• Постановление правительства РФ от 1.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».  
• Постановление Правительства Российской Федерации от 15.09.2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».   
• Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»  
• Приказ ФСБ России от 10.07.2014 № 378 «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»   
• Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25.11.1994 г.). • ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».

Помимо этого, основной базой для разработки СЗИ должна является актуальная модель угроз безопасности информации разработанная, содержащаяся и актуализируемая по мере необходимости в соответствии с требованиями Методики оценки угроз безопасности информации ФСТЭК, а также модель нарушителя, выработанная в соответствии с той же методикой, как это было описано выше. Кроме этого, в разработке СЗИ будут те же документы что и при разработке Методики.

# Требования к СЗИ

# Перечень предполагаемых к использованию СЗИ

# Основание на разработку собственных СЗИ

# Состав, сроки и содержание проведения работ

# Требования к подрядным организациям-исполнителям

# Перечень предъявляемой заказчику научно-технической продукции и базы

# Заключение

# Источники

1. Согласно ст. 2 Закона РФ "О государственной тайне" от 21.07.1993 N 5485-1 [↑](#footnote-ref-1)
2. Согласно ст. 2 Федерального закона от 27.07.2006 N 149-ФЗ (ред. от 02.11.2023) "Об информации, информационных технологиях и о защите информации"

   Статья 2. Основные по [↑](#footnote-ref-2)