Министерство науки и высшего образования

Российской Федерации

Федеральное Государственное

Автономное Образовательное Учреждение

Высшего Образования

Национальный ядерный университет «МИФИ»

Кафедра: «Финансовый Мониторинг»

Научно-исследовательская работа

«Принципы написания Частного Технического задания на разработку системы защиты информации»

Студент Монастырский М. О.

Группа С21-703

Руководитель: Модестов А.А  
Доцент

Кафедра финансового мониторинга

Москва 2023г.

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 подготовить 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 единой 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 обсуждаться конкретные сертифицированные уполномоченными органами СЗИ и будет изложен процесс разработки собственных решений в области защиты информации.

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

Учредить специальную комиссию, отвечающую рекомендациям согласно приложению 2 Методики

В ходе оценки группа должна пройти следующие этапы:



*Рисунок 1. Этапы проведения оценки согласно Методике.*

В качестве базы все этапы основываются на следующих документах:

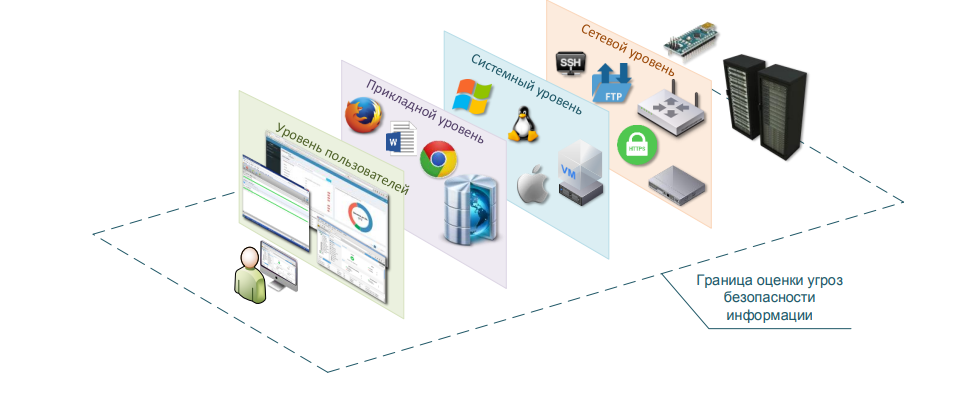
* Список актуальных угроз (<https://bdu.fstec.ru/>);
* Открытые списки векторов атак, такие как ATT&CK;
* Техническое задание на создание компьютерной сети, частные технические задания на создание ее компонентов;
* Данные, предоставляемые Оператору поставщиками услуг, в случае если инфраструктура организации 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;

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.

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**

Основополагающим документов в области определения класса защищенности АС является:   
«Руководящий документ Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации от 30 марта 1992 г.»

Классификация распространяется на все действующие и проектируемые АС учреждений, организаций и предприятий, обрабатывающие конфиденциальную информацию.

Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации.

Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала.

Устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС

Более подробная информация, касающаяся криптографических СЗИ, отражена в утвержденном ФСБ России документе «ПКЗ-2005». Классификация криптографических средств защиты информации ФСБ России определены классы криптографических СЗИ: КС1, КС2, КС3, КВ и КА. К основным особенностям СЗИ класса КС1 относится их возможность противостоять атакам, проводимым из-за пределов контролируемой зоны. При этом подразумевается, что создание способов атак, их подготовка и проведение осуществляется без участия специалистов в области разработки и анализа криптографических СЗИ.

Помимо этого, существует классификация защищенности СВТ, на которую опирается ФСТЭК при утверждении Требований по безопасности информации. Утверждены приказом ФСТЭК России от 2 июня 2020 г. N 76

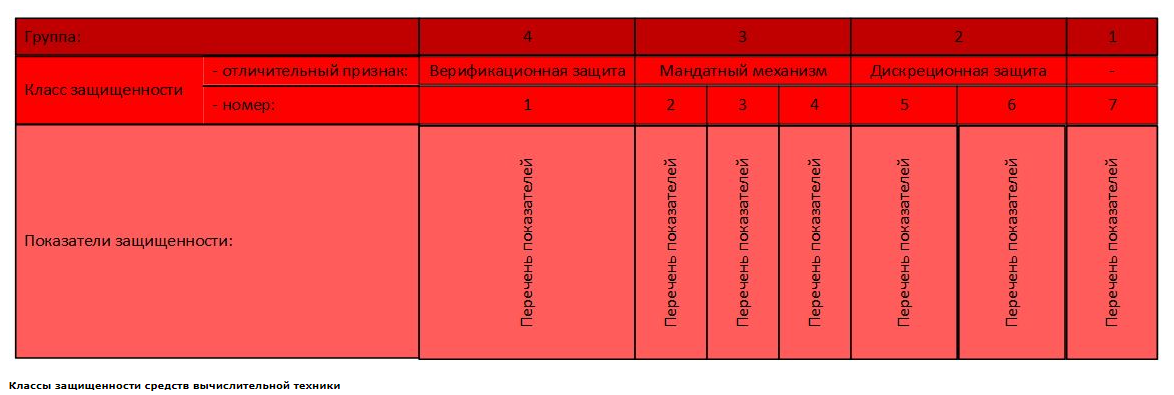
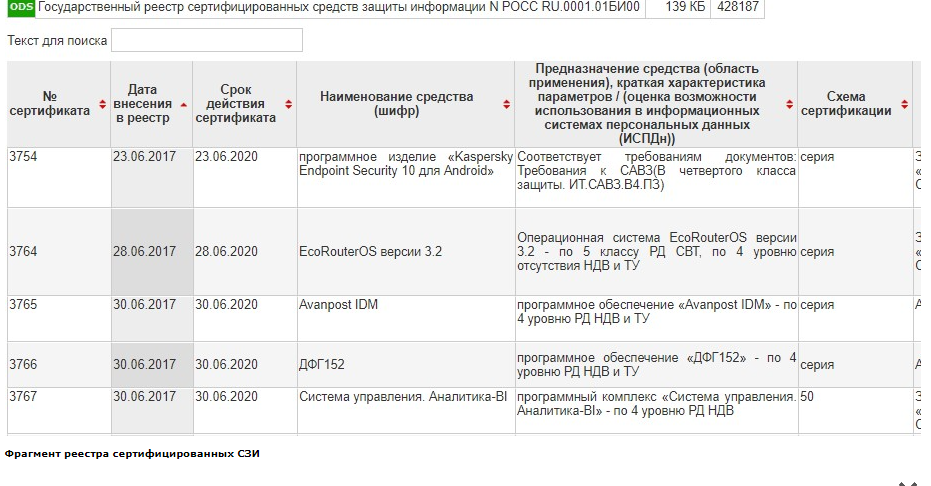


Рисунок 6. Классы защищенности средств вычислительной техники.

Здесь регулятор определил перечень классов защищенности, где первый считается наивысшим классом, а низшим — седьмой. Классы защищенности разделены на группы (рис. 6). Первая группа образована 7 классом. Он устанавливается тем средствам вычислительной техники, которые должны содержать механизмы защиты от НСД к информации, но итоговая защищенность которых ниже защищенности средств 6-го класса. Вторую группу образовывают 6 и 5 классы защищенности. Они отличаются наличием дискреционного управления доступом. Этот механизм позволяет задавать правила доступа пользователей к различным ресурсам, таким как файл, программа и прочее, в которых явно указано, что именно можно делать субъекту: читать содержимое файла, выполнять запуск программы и т. д. Образующие третью группу 4, 3 и 2 классы отличаются реализацией мандатного управления доступом, основанным на использовании классификационных меток. Они позволяют пользователям и ресурсам назначать т. н. классификационные уровни, например, категории секретности обрабатываемой информации. Так, создается иерархическая структура, в которой пользователь может получить доступ к ресурсу в том случае, если его уровень в созданной иерархии не ниже уровня иерархии требуемого ресурса. В случае неиерархической структуры в классификационный уровень пользователя включают те классификационные уровни ресурсов, доступ к которым этому пользователю должен быть обеспечен. При этом в этих средствах вычислительной техники присутствует механизм дискреционного управления доступом, дискреционные правила служат дополнением мандатных. А в состав четвертой группы входил только 1 класс, характеризующийся наличием верифицированной защиты.

# Реализованный механизм защиты должен гарантированно обеспечивать перехват диспетчером доступа всех обращений субъектов доступа к объектам. Перечень предполагаемых к использованию СЗИ

Перечень предлагаемых к использованию СЗИ должен отвечать потребностям организации, выявленным во время оценки угроз безопасности информации, перечень одобренных уполномоченными органами расположен на сайте (<https://reestr.fstec.ru/reg3>) в сети интернет.



*Рисунок 7. Фрагмент реестра сертифированных СЗИ.*

Аналогичный перечень в рамках своей компетенции поддерживает и ФСБ

Основание на разработку собственных СЗИ

Согласно Приказу №17:

«При отсутствии необходимых средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, организуется разработка (доработка) средств защиты информации и их сертификация в соответствии с законодательством Российской Федерации или производится корректировка проектных решений по информационной системе и (или) ее системе защиты информации с учетом функциональных возможностей имеющихся сертифицированных средств защиты информации.»

**Требования к подрядным организациям-исполнителям**

Согласно Постановлению Правительства РФ от 03.02.2012 N 79 (ред. от 03.02.2023) "О лицензировании деятельности по технической защите конфиденциальной информации" (вместе с "Положением о лицензировании деятельности по технической защите конфиденциальной информации».

«Не допускается осуществление деятельности, указанной в абзаце первом настоящего пункта, иностранными юридическими лицами.

4. При осуществлении лицензируемого вида деятельности лицензированию подлежат:

Эксплуатационная документация на систему защиты информации информационной системы разрабатывается с учетом ГОСТ 34.601, ГОСТ 34.201 и ГОСТ Р 51624 и должна в том числе содержать описание:

* структуры системы защиты информации информационной системы;
* состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств;
* правил эксплуатации системы защиты информации информационной системы.

А также сведения об аттестации разработанной СЗИ в уполномоченном органе «Для проведения аттестации информационной системы применяются национальные стандарты, а также методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085.

В настоящей работе обсуждались организационно-правовые моменты, связанные с разработкой частного технического задания на создание средства защиты информации, процесса принятия такого решения, выработки своих собственных решений в случае, если принятые стандартные решения не подходят под задачи и невозможно изменить уже отлаженную архитектуру таким образом, чтобы можно было использовать существующее на рынке аттестованное решение без ущерба производственным процессам, а также процесс аттестации таких решений и результатов разработки.

Кроме этого, в работе были затронуты вопросы, касающиеся обязанностей и требований к исполнителю заказов на выработку подобных решений, вопросы лицензирования деятельности исполнителя.

Все обсуждаемые вопросы были подкреплены соответствующими нормативно правовыми актами и руководящими документами регулирующих Органов Исполнительной Власти.