Тип работы: Лабораторная работа

Предмет: Методы защиты информации

-

Устранение угроз должно подтверждаться либо повторным моделированием угроз (по итогам проведения мероприятий по защите информации), либо документацией (протокол, заключение) по результатам контроля эффективности принятых мер по защите информации на конкретном ЗОИ. Выводы об устранении должны быть по каждой из угроз модели угроз разработанной на стадии аудита и(или) проектирования. Угрозы первого и второго типов могут быть признаны неактуальными при проведении соответствующих мероприятий, описанных в п.2.2.3. настоящих Указаний.
Выявление и устранение угроз безопасности информации необходимо осуществлять в соответствии с требованиями руководящих документов ФСТЭК России.
Выбор, и реализация, в информационных системах мер защиты информации, должны осуществляться в зависимости от класса защищенности информационных систем и уровня защищенности персональных данных, обрабатываемых в информационных системах, а также с учетом угроз безопасности информации применительно ко всем объектам и субъектам доступа на аппаратном, системном, прикладном и сетевом уровнях, в том числе в среде виртуализации и облачных вычислений, связанных с действиями нарушителя с соответствующим потенциалом.
При этом обязательными к учёту и рассмотрению являются следующие угрозы:
- угрозы, перечисленные в НМД ФСТЭК России;
- угрозы, определенные для рассмотрения нормативно-правовым актом правительства автономного округа;
- угрозы, перечисленные в НМД ФСБ России (при защите информации на распределённых объектах информатизации);
- угрозы банка данных угроз и уязвимостей ИБ ФСТЭК России;
- угрозы, выявленные в ходе аналитической работы подразделений по ЗИ МО и Депздрава , рекомендуемые к рассмотрению дополнительно.
Общий порядок создания подсистемы технической защиты информации на объектах информатизации
Структура, состав и основные функции подсистемы ТЗИ определяются исходя из сформированного набора требований по обеспечению ИБ. Набор требований формируется с учётом следующего:
 состава мер, изложенных в нормативно-методических документах ФСТЭК России, для определённого класса (уровня защищённости) ЗОИ (ГИС, ИСПДН);
 модели угроз безопасности информации, разработанной для конкретного ОИ;
 особенностей технологического процесса обработки информации на защищаемом ОИ.
Для обеспечения технической защиты информации и создания подсистемы ТЗИ реализуются ниже следующие этапы:
Предпроектный этап, включающий предпроектное обследование (аудит), разработку технического (частного технического) задания на создание подсистемы технической защиты информации, в том числе моделирование угроз и формирование требований к защите информации, содержащейся в информационной системе.
На предпроектной стадии особое внимание необходимо уделять следующим вопросам:
 соответствию подготовленного исполнителем описания технологического процесса обработки информации реальному положению дел в МО, в том числе в части информационного взаимодействия с другими информационными системами (объектами информатизации), технического сопровождения прикладного ПО в составе ЗОИ, выполнению требований по разграничению прав пользователей к ресурсам ЗОИ;
 определению состава ЗОИ, включая обязательное рассмотрение средств администрирования и управления системным программным обеспечением и средствами защиты информации, средств вычислительной техники, содержащих и создающих ключевую информацию;
 необходимости учета при моделировании УБИ всех угроз (в соответствии с настоящих указаний);
 необходимости учета при моделировании УБИ реально выявленных при первичном тестировании на проникновение угроз;

 правильности определения УБИ и наличия обоснования типа угроз и актуальности (не актуальности) всех угроз.
Частное техническое задание на создание системы защиты информации ЗОИ МО должно содержать:
- разделы, предусмотренные методическими требованиями ФСТЭК России для ИСПДН или ГИС;
- разделы, предусмотренные нормативными актами Аппарата Губернатора автономного округа – , регулирующими вопросы подготовки и согласования технических заданий на поставку товаров, оказание услуг, выполнение работ на поставку систем защиты информации и отдельных их элементов;
- данные о результатах пентестов, реализованных в ходе аудита и программу и методики итогового планируемого тестирования на проникновение (для ТЗ с итоговым контролем эффективности) или программу и методики пентестов предпроектного этапа (для ТЗ на аудит, модерирование угроз и (или) проектирование);
- при содержании в ТЗ работ по сопровождению должно быть приведено детальное распределение полномочий и задач (указанных в п.2.3.2. настоящих Указаний) между Исполнителем и Заказчиком, с целью оценки соответствия требованиям НМД и настоящих Указаний.
В соответствии с нормативными актами аппарата, регулирующими вопросы подготовки и согласования технических заданий на поставку товаров, оказание услуг, выполнение работ на поставку систем защиты информации и отдельных их элементов, частные технические задания подлежат согласованию с управлением защиты информации и специальной документальной связи.
Учитывая особое значение первоначальных этапов (предпроектное обследование, проектирование и подготовка частных технических заданий, анализ защищенности и тестирование на проникновение) на все дальнейшие этапы реализации и отсутствие опыта подготовки ТЗ и формирования требований к системам ЗИ в МО, а также во избежание неэффективного расходования средств на создание систем защиты информации, необходимо чтобы в состав ТЗ к договорам на реализацию указанных первоначальных этапов входил весь перечень вопросов, изложенных в соответствующих разделах настоящих указаний. При реализации договоров (контрактов) на выполнение работ (оказание услуг) по защите информации с единственным поставщиком возможно обращение за консультациями в Управление защиты информации и специальной документальной связи.
Этап проектирования (разработки технических (исполнительных) проектов) подсистемы технической защиты информации ЗОИ.
Особому контролю со стороны МО при приемке работ по проектированию должны подлежать следующие вопросы:
- контроль отсутствия ошибочных трактовок в определении состава защищаемого объекта информатизации и состава объектов защиты, а именно исключение из их числа общесистемного, прикладного, специального программного обеспечения, средств защиты информации и информации о их настройках, в т.ч. ключевой информации, средств управления системным программным обеспечением, средствами и элементами защиты информации объекта информатизации, средств создания и хранения ключевой информации средств криптографической информации, носители ключевой, парольной и аутентифицирующей информации СКЗИ;
- детальное описание технологического процесса обработки информации, в том числе информационного взаимодействия с другими информационными системами (объектами информатизации);
- организация систем обнаружения вторжений и контроля траффика со стороны сетей связи общего пользования и исходящих в сети связи общего пользования;
- информационный обмен между защищенными

-