ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ имени А.Ф.МОЖАЙСКОГО

Кафедра математического и программного обеспечения

УТВЕРЖДАЮ

Начальник 27 кафедры

полковник

С. Войцеховский

«___» _____ 20__ г.

Автор: старший преподаватель 27 кафедры
кандидат технических наук
подполковник С.Краснов

Лекция № 5

по учебной дисциплине
«Защита информации»
на тему

Тема: «ЛИЦЕНЗИРОВАНИЕ, СЕРТИФИКАЦИЯ И АТТЕСТАЦИЯ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ КАК ФОРМЫ ГОСУДАРСТВЕННОГО РЕГУЛИРОВАНИЯ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

по дисциплине: «Защита информации»

Рассмотрено и одобрено
на заседании кафедры № 27
« ___ » августа 201__ г.

протокол № __

Санкт-Петербург 201_

Содержание занятия и время

Введение……13-15 мин.

Учебные вопросы (основная часть):

1. Лицензирование в области защиты информации. – 20 мин.
2. Сертификация средств защиты информации – 20 мин.
3. Аттестация объектов информатизации. – 30 мин.

Заключение……....5-7 мин.

Литература:

1. план-конспект.
2. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – 252 с.
3. Воробьев Е.Г., Войцеховский С.В., Марковский А.С. Подготовка объекта информатизации к аттестации по требованиям безопасности. / под ред. Н.М.Михайлова. – СПб., ООО «Издательский дом Афина», 2006. – 89 с.
4. Инженерно-техническая защита информации: учеб. Пособие для студентов, обучающихся по специальностям в обл. информ. безопасности / А.А. Торокин. – М.: Гелиос АРВ, 2005.

Материально-техническое обеспечение:

1. Наглядные средства обучения - доска, мел. проектор.

Организационно-методические указания:

Во введении сформулировать тему лекции, цель и название изучаемых вопросов. При этом в течение 10 мин. произвести опрос курсантов по пройденному материалу в виде летучки № 2.

Метод проведения занятия – рассказ. В основной части сконцентрировать внимание курсантов на особенностях лицензирования деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, необходимости сертификации средств защиты информации, основными лицензионными требованиями и условиями, частотой и особенностями проведения аттестационных испытаний.

За 3 – 5 мин. до конца занятия делаю обобщающие выводы, задаю контрольные вопросы для проверки, как военнослужащие усвоили тему занятия:

1. Для чего необходимо лицензирование деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну?
2. Для чего необходима сертификация средств защиты информации?
3. Перечислите основные лицензионные требования и условия.
4. Для чего проводится аттестация объектов информатизации?
5. Кто имеет право проводить аттестационные испытания?
6. Как часто проводится аттестация?

Отвечаю на вопросы по теме занятия, даю задание на самоподготовку.

Лекция № 5

Лицензирование, сертификация и аттестация в области защиты информации как формы государственного регулирования применения информационных технологий.

В условиях повсеместной информатизации основных процессов жизнедеятельности страны информационная сфера становится не только неотъемлемой частью общественной жизни, но и во многом определяет направления социально - политического и экономического развития государства. Поскольку состояние защищённости информационной среды в ключевых областях деятельности экономики в целом является в значительной степени определяющим фактором безопасности государства, то в этом случае информационная безопасность выходит на передний план и становится важной и неотъемлемой составной частью общей стратегии национальной безопасности Российской Федерации. В соответствии с Указом Президента РФ от 31.12.2015 года № 683 "Стратегия национальной безопасности Российской Федерации") информационная безопасность является составной частью национальной безопасности Российской Федерации.

Среди угроз государству в информационной сфере, наиболее критичных по своим последствиям, следует выделить угрозы нарушения таких свойств информации, как целостность, конфиденциальность и доступность вследствие утечки информации по техническим каналам, несанкционированного доступа к информации, а также специальных воздействий в целях её уничтожения, искажения или блокирования доступа к ней.

Среди методов обеспечения безопасности информации, отмеченных в Доктрине информационной безопасности Российской Федерации (Указ Президента РФ № 646 от 02.12.2016), одно из важных мест занимают сертификация средств защиты информации по требованиям безопасности информации и лицензирование деятельности в области защиты информации.

В. 1 Лицензирование в области защиты информации

Полный перечень видов деятельности в области защиты информации, подлежащих обязательному государственному лицензированию, определён в Законе Российской Федерации "О государственной тайне" (№ 5485-1 от 21.07.93, ред. 29.07.2018 г.) и Федеральном законе "О лицензировании отдельных видов деятельности" (№ 99 от 22 апреля 2011 г., ред. 4 мая 2011 г.).

В законе "О государственной тайне" определены лицензируемые виды деятельности в области защиты информации, содержащей сведения, отнесённые к государственной тайне, а в Законе "О лицензировании отдельных видов деятельности" - в области защиты конфиденциальной информации.

В ст. 27 Закона "О государственной тайне" указано, что допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляется путём полученья ими лицензий в порядке, устанавливаемом Правительством РФ. Во исполнение данной статьи закона Правительством РФ было принято Постановление "О лицензировании отдельных видов деятельности" (№ 957 от 21.11.2011 г.), в котором утвержден перечень федеральных органов исполнительной власти, осуществляющих лицензирование конкретных видов деятельности.

Согласно этому Перечню, лицензии выдаются на основании результатов специальных экспертиз организаций-заявителей, располагающих производственно - испытательной базой, нормативно-методической документацией, научным и инженерно-техническим персоналом. ФСТЭК России в пределах своей компетенции осуществляет лицензирование деятельности предприятий, учреждений и организаций, связанной с созданием средств технической защиты информации и осуществлением мероприятий и (или) оказанием услуг в области защиты информации.

Основные лицензионные требования и условия

В соответствии с вышеперечисленными законодательными документами основными лицензионными требованиями и условиями являются:

- Соответствие производственных помещений, производственного, испытательного и контрольно-измерительного оборудования техническим нормам и требованиям, установленным государственными стандартами, руководящими и нормативно-методическими документами по защите информации.
- Использование сертифицированных (аттестованных по требованиям безопасности информации) автоматизированных систем, обрабатывающих конфиденциальную, а также средств защиты такой информации.
- Осуществление деятельности специалистами, имеющими высшее профессиональное образование по специальностям "Компьютерная безопасность", "Комплексное обеспечение информационной безопасности автоматизированных систем", "Информационная безопасность телекоммуникационных систем" либо прошедшими переподготовку по вопросам защиты информации.
- Использование третьими лицами программ для электронно-вычислительных машин или баз данных только на основании договора с их правообладателем.

Государственная система лицензирования деятельности в области защиты информации включает в себя две составляющие: допуск предприятий и организаций к оказанию услуг по защите информации и контроль качества и эффективности оказываемых услуг в процессе их деятельности.

Таким образом, лицензирование деятельности в области защиты информации как государственного контроля призвано обеспечить не только допуск организаций, соответствующих определённым требованиям и условиям, к осуществлению указанных видов деятельности, но и, как следствие, повышение качества непосредственно мероприятий и услуг по технической защите информации.

В. 2 Сертификация средств защиты информации

Постоянное усложнение средств и систем обработки информации, программных продуктов увеличивает вероятность возникновения непреднамеренных дефектов, которые могут исказить информацию или повлиять на процесс её обработки, вместе с тем нельзя исключить возможность преднамеренного воздействия на информацию, как в условиях недобросовестной конкуренции, так и информационного противоборства.

Для того, чтобы защита информации была максимально эффективна, средства её обработки и защиты должны соответствовать определённым требованиям, подтверждённым объективной и независимой оценкой. Одной из форм такой оценки соответствия требованиям нормативных документов по защите информации является сертификация.

В Законе "О государственной тайне" установлено, что средства защиты должны иметь сертификат, удостоверяющий соответствие требованиям по защите.

Постановлением Правительства РФ "О сертификации средств защиты информации" (№ 608 от 26.06.95) были определены федеральные органы по сертификации: Гостехкомиссия России, ФАПСИ, ФСБ России, Минобороны России, СВР. Координация деятельности систем сертификации средств защиты информации возложена на Межведомственную комиссию по защите государственной тайны.

Таким образом, Гостехкомиссия России является одним из элементов общероссийской системы сертификации средств защиты информации и выполняет эти функции в пределах своей компетенции.

Структура системы сертификации

Обязательной сертификации подлежат защищённые технические, программно-технические, программные средства, системы связи, сети и системы вычислительной техники, средства защиты и средства контроля эффективности защиты, а также технические и программные средства, предназначенные для обработки информации с ограниченным доступом, в том числе и иностранного производства.

Организационную структуру системы сертификации средств защиты информации по требованиям безопасности информации образуют:

- Государственный орган по сертификации продукции
- Аккредитованные органы по сертификации продукции
- Аккредитованные испытательные центры (лаборатории)
- Заявители (разработчики, изготовители, поставщики, заказчики, потребители продукции).

Государственный орган по сертификации продукции отвечает за организацию обязательной государственной сертификации, создание системы сертификации и установление правил сертификации, а также организует разработку нормативно - методических документов, на соответствие которым проводится сертификация, и утверждает их.

В качестве органов по сертификации могут быть аккредитованы организации и предприятия, обладающие необходимой компетентностью и отвечающие установленным требованиям, в том числе государственные органы, акционерные общества, общества с ограниченной ответственностью и другие организации.

Процесс аккредитации исключительно важен и является официальным признанием технической компетентности и независимости субъекта от разработчиков, изготовителей, поставщиков и потребителей продукции. В ходе этого процесса осуществляется передача необходимых функций по сертификации аккредитуемому органу.

Испытательные центры (лаборатории) проводят испытания конкретной продукции или предварительную проверку производства и готовят необходимые технические заключения и протоколы испытаний.

Заявители (разработчики, изготовители, поставщики) несут ответственность за обеспечение соответствия продукции требованиям, по которым она была сертифицирована, и пронимают необходимые меры по обеспечению стабильности характеристик, определяющих безопасность информации.

Технология сертификации

При сертификации могу подтверждаться как отдельные характеристики, так и весь комплекс характеристик продукции, связанных с обеспечением безопасности информации. В зависимости от назначения продукция подтверждается на соответствие требованиям по защите информации от следующих угроз:

- Несанкционированного доступа (действия), в том числе от компьютерных вирусов.
- Утечки информации за счёт побочных электромагнитных излучений и наводок (ПЭМИН).
- Утечки информации или воздействия на неё за счёт специальных устройств, встроенных в технические и программные средства.

Выбор схемы сертификации зависит от технических характеристик продукции, подвергающейся проверке, и условий её производства. Основными схемами сертификации продукции на соответствие требованиям по безопасности информации являются:

- Для единичных образцов - проведение испытаний образцов продукции.
- Для партии продукции - проведение испытаний выборки образцов продукции из партии.
- Для серийного производства - аттестация производства, проведение типовых испытаний образцов продукции и последующий надзор за стабильностью характеристик сертифицированной продукции, обеспечивающих (определяющих) выполнение этих требований.

По согласованию с органом по сертификации могут быть использованы и другие схемы сертификации, применяемые в международной практике.

Испытания проводятся в испытательных центрах (лабораториях), аккредитованных Гостехкомиссией России. Выбор испытательного центра проводится исходя из принципа его независимости от заявителя, обеспечивающего объективность результатов испытаний.

В отдельных случаях по согласованию с органом по сертификации допускается проведение испытаний на испытательной базе разработчика (изготовителя) продукции. При этом орган по сертификации определяет условия, необходимые для обеспечения объективности результатов испытаний.

На основе полученных в ходе испытаний протоколов орган по сертификации принимает решение о выдаче сертификата на продукцию, проводит работы по его оформлению и регистрации в государственном реестре. Расходы по проведению всех видов работ по сертификации продукции по требованиям безопасности информации относятся на себестоимость продукции и оплачиваются заявителем.

Органы по сертификации и испытательные центры (лаборатории) несут ответственность за выполнение возложенных на них функций по обеспечению режима конфиденциальности и соблюдения, авторских прав при испытаниях продукции.

Совершенствование нормативно-методической базы

Сертификация продукции на соответствие требованиям безопасности информации базируется на основе действующей системы стандартизации и нормативно - технической документации по безопасности информации. Однако в настоящее время в связи с принятием Федерального закона "О техническом регулировании" (№ 184 от 27.12.02) и изменением принципов технического регулирования, стандартизации и оценки соответствия возникла острая необходимость выработки общей политики в области обеспечения безопасности информационных технологий и построения целостной системы нормативно - методических документов, которые составили бы основу для деятельности различных органов, действующих в сфере обеспечения безопасности информационных технологий.

Фундаментом для совершенствования нормативно-методической базы оценки безопасности информационных технологий должен стать ГОСТ Р ИСО/МЭК 15408-2002, принятый решением Госстандарта России и вступающий в силу с 1 января 2004 г. Одновременно планируется разработка следующих нормативно-методических документов, направленных на организацию сертификации средств защиты информации в соответствии с методологией этого ГОСТа:

- Руководство по разработке профилей защиты и заданий по безопасности.
- Руководство по регистрации профилей защиты.
- Положение по организации разработки, испытаний, производства и эксплуатации безопасных информационных технологий.
- Методология (типовые методики) оценки.

Указанный пакет документов, наряду с собственно профилями защиты, должен составить базу для совершенствования системы нормативно-методических документов Гостехкомиссии России по безопасности информационных технологий.

В. 3. Аттестация объектов информатизации

Прогрессивной формой оценки систем информационных технологий, или объектов информатизации, является их аттестация. Под аттестацией объектов информатизации понимается комплекс организационно - технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" - подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утверждённых Гостехкомиссией России.

Объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, а также ведения секретных переговоров, подлежат обязательной аттестации по требованиям защиты информации. К таким объектам относятся:

- Средства и системы информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных, технические средства приёма, передачи и обработки информации (телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео-, смысловой и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прокладное программное обеспечение), используемые для обработки секретной информации.
- Технические средства и системы, не обрабатывающие непосредственно секретную информацию, но размещённые в помещениях, где обрабатывается (циркулирует) секретная информация.
- Выделенные помещения, предназначенные для ведения секретных переговоров или в которых размещены средства закрытой телефонной связи.

Аттестация объектов информатизации на соответствие требованиям безопасности информации вызвана необходимостью официального подтверждения эффективности комплекса используемых на конкретном объекте мер и средств защиты информации. Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта в реальных условиях эксплуатации с целью оценки соответствия использованного комплекса мер и средств защиты требуемому уровню безопасности информации.

Аттестационные испытания

Аттестационные испытания осуществляются аттестационной комиссией, формируемой аккредитованным Гостехкомиссией России органом по аттестации из компетентных специалистов в необходимых для конкретного объекта информатизации направлениях защиты информации, по согласованной с заявителем программе испытаний.

Органы по аттестации несут ответственность за выполнение возложенных за них функций, обеспечение сохранности государственной тайны, а также за соблюдение авторских прав разработчиков аттестуемых объектов информатизации и их компонентов.

При проведении аттестационных испытаний применяются следующие методы проверок и испытаний:

Экспертно-документальный метод.

- Измерение и оценка уровней защищённости для отдельных технических средств и каналов утечки информации.
- Проверка функций или комплекса функций защиты информации от несанкционированного доступа (НСД) с помощью тестирующих средств, а также путём пробного запуска средств защиты информации от НСД и наблюдения за их выполнением.
- Проверка на попытку "взлома" систем защиты информации.

Программа испытаний разрабатывается на основе анализа исходных данных об объекте информатизации и должна включать необходимые виды испытаний, определённые методическими рекомендациями для соответствующих групп объектов информатизации (выделенные помещения, автоматизированные системы, системы связи и т.д.), а также определять сроки, условия и методики проведения испытаний.

Программа испытаний может уточниться и корректироваться в процессе испытаний по согласованию с заявителем и руководителем аттестационной комиссии.

На сегодняшний день Гостехкомиссией России аккредитовано более 170 органов по аттестации объектов информатизации. Объём ежегодно проводимых ими работ по аттестации составляет порядка 2000 объектов информатизации. Статистические данные по аттестованным объектам информатизации в федеральных округах

Принцип работы программного инструментального средства для проведения сертификационных испытаний СЗИ НСД – «**Анализатор уязвимостей НКВД**».

Специальное программное инструментальное средство для проведения сертификационных испытаний СЗИ НСД, работающих в среде ОС Windows 9x, установленных на платформе x.86.

Называется это средство – «Анализатор уязвимостей НКВД, версия 2.1».

В частности, проверки выполнения требований по «изоляции модулей» с помощью указанного Анализатора производятся следующим образом:

Тестовая программа анализатора запрещает аппаратные прерывания ОС и производит контрольную запись в область памяти, используемую драйверами ОС. Затем производится контрольное чтение записанных данных и восстановление первоначального состояния системы.

Если контрольное чтение подтверждает запись в область системных модулей, делается вывод о возможности нарушения изоляции модулей (по факту возможности доступа из прикладного процесса к модулям ОС в оперативной памяти ПЭВМ). В противном случае делается вывод о корректности работы механизма изоляции модулей испытываемого СЗИ НСД.

При указанных проверках по существу проверяется:

- Реализация в СЗИ НСД функций контроля защищенности системных таблиц памяти при работе процессора в защищенном режиме;
- Реализация в СЗИ НСД функций установки и контроля привилегий прерываний в системной таблице прерываний;
- Реализация в СЗИ НСД функций контроля в системных таблицах привилегий и параметров областей памяти в создаваемых селекторах;
- Реализация в СЗИ НСД механизма проверки правильности выполнения ядром ОС своих функций;

Проверки выполнения СЗИ НСД требований РД по обеспечению «дискреционного принципа контроля доступа» с помощью указанного Анализатора производятся следующим образом.

А) При проверке возможности доступа к защищенному файлу документированными функциями ОС (явными действиями пользователя):

Тестовая программа анализатора запрашивает у оператора путь к контрольному защищенному файлу известного содержания, все виды доступа к которому для оператора запрещены. Далее производится перебор документированных функций ОС, работающих с файлами.

Если использование какой-либо функции позволило прочитать контрольный файл и подтвердилась его подлинность, то делается вывод о возможности несанкционированного доступа к данным, т.е. нарушении ПРД, реализуемых средством защиты. В противном случае считается, что механизм, реализующий ПРД, работает корректно в отношении документированных функций ОС.

Б) При проверке возможности доступа к защищенному файлу программными средствами анализатора (скрытыми действиями пользователя с использованием собственных программных средств):

Тестовая программа анализатора запрашивает у оператора путь к контрольному защищенному файлу известного содержания, все виды доступа к которому для оператора запрещены (если путь не был указан в предыдущем тесте). Далее производится попытка чтения файла с помощью встроенного в анализатор драйвера работы с контроллером ЖМД.

В случае успешного чтения и подтверждения его подлинности делается вывод о возможности нарушении ПРД скрытыми действиями пользователя (с использованием собственных программных средств). В противном случае механизм, реализующий ПРД в КСЗ, функционирует правильно в отношении использования собственных драйверов пользователя для работы с устройствами.

В) При проверке доступа к защищенному файлу **путем обхода драйверов СЗИ НСД** (скрытыми действиями пользователя):

Тестовая программа анализатора запрашивает у оператора путь к контрольному защищенному файлу известного содержания, все виды доступа к которому для оператора

запрещены (если путь не был указан в предыдущем тесте). Далее производится попытка обращения к базовым драйверам ОС Windows в обход драйверов СЗИ НСД с целью чтения контрольного файла. В случае успешного чтения и подтверждения его подлинности делается вывод о нарушении ПРД. В противном случае механизм, реализующий ПРД в СЗИ НСД, функционирует правильно и не допускает обхода драйверов СЗИ НСД.

При указанных проверках по существу проверяется:

- Наличие и эффективность реализованного в СЗИ НСД механизма перехвата функций работы ОС с файловой системой;
- Реализация СЗИ НСД механизмов полномочного разграничения доступа к контроллерам различных устройств ПЭВМ для любых драйверов ОС на уровне системных таблиц процессора.

Проверка других показателей защищенности проводится с помощью указанного Анализатора на аналогичном, системном уровне.

«Анализатор уязвимостей НКВД, версия 2.1» предназначен для оценки выполнения СЗИ НСД показателей защищенности СВТ от НСД с 6 по 1 класс включительно.

Поскольку при сертификации хоть СЗИ НСД, хоть ОС, имеющих встроенные функции защиты, должны проверяться механизмы «монитора обращений», реализованные в абстрактной или физической машине (ПЭВМ), то сертификационные испытания этих объектов оценки тождественны сертификационным испытаниям защищенного автоматизированного рабочего места, созданного на базе ПЭВМ, при отсутствии установленных прикладных программ.

В этих условиях, определенных нормативными документами Гостехкомиссии России, на сегодняшнем этапе будут играть важнейшую роль средства автоматизации проверок – программные инструментальные средства – Анализаторы такого уровня, как при проведении сертификационных, так и аттестационных испытаний.

Старший преподаватель 27 кафедры
подполковник С.Краснов