ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ ИМЕНИ А.Ф. МОЖАЙСКОГО

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 № 3
по учебной дисциплине
«Защита информации»
на тему
«**Основные документы по защите информации**»

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

протокол № __

Санкт-Петербург 201_

Содержание занятия и время

ВСТУПИТЕЛЬНАЯ ЧАСТЬ – 5 МИН.
ОСНОВНАЯ ЧАСТЬ:
1. Международные стандарты – 40 мин.
2. Законы РФ, указы Президента РФ, ГОСТЫ. Документы ФСТЭК в области защиты информации – 40 мин.

ЗАКЛЮЧИТЕЛЬНАЯ ЧАСТЬ – 3-5 МИН.

Цель лекции: Ознакомить курсантов с требованиями руководящих документов в области защиты информации.

Литература:

1. Доктрина «Информационной безопасности РФ» от 02 декабря 2016 г., указ президента РФ №646.
2. Военная доктрина РФ.
3. ФЗ РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ (в редакции 2012 года).
4. ФЗ РФ «О государственной тайне» от 21 июля 1993 года.
5. ФЗ РФ «О персональных данных» от 27 июля 2006 года.
6. Указ Президента РФ «О мерах по обеспечению информационной безопасности РФ при использовании ИТКС международного информационного обмена» от 17 марта 2008 г.
7. Указ Президента РФ «Об утверждении Перечня сведений конфиденциального характера» от 6 марта 1997 г.
8. Указ Президента РФ «Об утверждении Перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г.
9. Указ Президента РФ № 537 «О стратегии национальной безопасности РФ до 2020 года» от 12 мая 2009 года.
10. Приказ ФСТЭК России «Об утверждении требований к обеспечению защиты информации в АСУ производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а так же на объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» от 14 марта 2014 года.
11. Совместный приказ ФСТЭК России, ФСБ России и Минкомсвязи России «Об утверждении Порядка проведения классификации информационных систем персональных данных» от 31 декабря 2013 г.
12. Приказ ФСТЭК России «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 года.
13. Приказ ФСТЭК России «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11 февраля 2013 года.
14. Приказ ФСТЭК России «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования» от 31 августа 2010 года.
15. Положение «По аттестации объектов информатизации по требованиям безопасности информации» от 25 ноября 1994 г.
16. Методический документ «Меры защиты информации в государственных информационных системах» утвержден ФСТЭК России 11 февраля 2014 года.

17. Руководящий документ. Приказ председателя Гостехкомиссии России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» от 19 июня 2002 года.
18. Руководящий документ. Приказ председателя Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей» от 4 июня 1999 года.
19. Руководящий документ. Приказ председателя Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от НСД. Показатели защищенности от НСД к информации» от 25 июня 1997 года.
20. Руководящий документ. Приказ председателя Гостехкомиссии России «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации» от 30 марта 1992 года.
21. Руководящий документ. Приказ председателя Гостехкомиссии России «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации» от 30 марта 1992 года.
22. Руководящий документ. Приказ председателя Гостехкомиссии России «Защита от НСД к информации. Термины и определения» от 30 марта 1992 года.
23. Руководящий документ. Приказ председателя Гостехкомиссии России «Концепция защиты средств вычислительной техники и АС от НСД к информации» от 30 марта 1992 года.

Материально техническое обеспечение:

1. Технические средства обучения: ПЭВМ, мультимедиа проектор, экран, программное обеспечение.
2. Приложения (слайды).
3. Наглядные средства обучения – доска, мел.

Организационно-методические указания:

Во введении сформулировать тему лекции, цель и название изучаемых вопросов. При этом произвести опрос курсантов по пройденному материалу.

Применяемым методическим приемом является рассказ.

В основной части сконцентрировать внимание курсантов на основных руководящих документах в области ЗИ.

В заключительной части обобщить изложенный материал и осуществить контрольный опрос.

1. Назовите основные группы руководящих документов?
2. Перечислите международные стандарты?
3. Расшифруйте аббревиатуру «ФСТЭК» ?

Отвечаю на вопросы по теме занятия, даю задание на самостоятельную подготовку – ознакомиться и законспектировать:

1. РД «Межсетевые экраны. Показатели защищённости от НСД».
2. РД «Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей».
3. РД «Защита от НСД к информации. Термины и определения».

Лекция № 3

«ОСНОВНЫЕ ДОКУМЕНТЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ».

В. 1 Основные международные стандарты.

Основными международными стандартами в области защиты информации являются:

- критерии оценки доверенных компьютерных систем министерства обороны ("Оранжевая книга" Министерства обороны США) [10];
- согласованные критерии оценки безопасности информационных технологий европейских стран [11];
- международный стандарт ISO/IEC 17799:2000 (BS 7799-1) "Управление информационной безопасностью - Информационные технологии. - Information technology- Information security management";
- международный стандарт "Общие критерии безопасности информационных технологий" (ОК) ISO/IEC 15408 на данный момент признается одним из наиболее функциональных стандартов в сфере информационной безопасности (ИБ).

Критерии оценки надежных компьютерных систем. Данный труд, называемый чаще всего по цвету обложки "Оранжевой книгой", опубликован в августе 1983 года.

"Оранжевая книга" поясняет понятие безопасной системы, которая "управляет, посредством соответствующих средств, доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, писать, создавать и удалять информацию". Очевидно, однако, что абсолютно безопасных систем не существует, что это абстракция. Любую систему можно "взломать", если располагать достаточно большими материальными и временными ресурсами. Есть смысл оценивать лишь степень доверия, которое разумно оказать той или иной системе.

В "Оранжевой книге" надежная система определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

Степень доверия, или надежность систем, оценивается по двум основным критериям:

Политика безопасности – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь имеет право оперировать с определенными наборами данных. Чем надежнее система, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы, обеспечивающие безопасность системы. Политика безопасности – это активный компонент защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

Гарантированность – мера доверия, которая может быть оказана архитектуре и реализации системы. Гарантированность может проистекать как из тестирования, так и из проверки (формальной или нет) общего замысла и исполнения системы в целом и ее компонентов.

Гарантированность показывает, насколько корректны механизмы, отвечающие за проведение в жизнь политики безопасности. Гарантированность можно считать пассивным компонентом защиты, надзирающим за самими защитниками.

В "Оранжевой книге" определяется четыре уровня безопасности (надежности) – D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. В настоящее время он содержит две подсистемы управления доступом для компьютеров. По мере перехода от уровня C к A к надежности систем предъявляются все более жесткие требования.

Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием надежности. Таким образом, всего имеется шесть классов безопасности – C1, C2, B1, B2, B3, A1. Чтобы система в результате процедуры сертификации могла быть отнесена к некоторому классу, ее политика безопасности и гарантированность должны удовлетворять определенным в документе требованиям.

Согласованные критерии Европейских стран. Следуя по пути интеграции, Европейские страны в 1991 году приняли согласованные критерии оценки безопасности информационных технологий (Information Technology Security Evaluation Criteria, ITSEC).

Европейские Критерии рассматривают следующие составляющие информационной безопасности:

- конфиденциальность, то есть защиту от несанкционированного получения информации;
- целостность, то есть защиту от несанкционированного изменения информации;

- доступность, то есть защиту от несанкционированного удержания информации и ресурсов.

В Критериях проводится различие между системами и продуктами. Система – это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении. Продукт – это аппаратно-программный "пакет", который можно купить и по своему усмотрению встроить в ту или иную систему.

Таким образом, с точки зрения информационной безопасности основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно определить и изучить сколь угодно детально, а продукт должен быть рассчитан на использование в различных условиях.

Гарантированность затрагивает два аспекта – эффективность и корректность средств безопасности. При проверке эффективности анализируется соответствие между целями, сформулированными для объекта оценки, и имеющимся набором функций безопасности. Точнее говоря, рассматриваются вопросы адекватности функциональности, взаимной согласованности функций, простоты их использования, а также возможные последствия эксплуатации известных слабых мест защиты. Кроме того, в понятие эффективности входит способность механизмов защиты противостоять прямым атакам (мощность механизма). Определяется три градации мощности – базовая, средняя и высокая.

Под *корректностью* понимается правильность реализации функций и механизмов безопасности. В Критериях определяется семь возможных уровней гарантированности корректности – от E0 до E6 (в порядке возрастания). Уровень E0 обозначает отсутствие гарантированности (аналог уровня D "Оранжевой книги"). При проверке корректности анализируется весь жизненный цикл объекта оценки — от проектирования до эксплуатации и сопровождения.

Общая оценка системы складывается из минимальной мощности механизмов безопасности и уровня гарантированности корректности.

Международный стандарт ISO/IEC 17799:2000 (BS 7799-1) «Управление информационной безопасностью - Информационные технологии»

Он был разработан на основе первой части Британского стандарта BS 7799-1:1995 ("Практические рекомендации по управлению информационной безопасностью") и относится к новому поколению стандартов информационной безопасности компьютерных информационных систем. Текущая версия стандарта ISO/IEC 17799:2000 (BS 7799-1:2000) рассматривает следующие актуальные вопросы обеспечения информационной безопасности организаций и предприятий:

1. Необходимость обеспечения информационной безопасности.
2. Основные понятия и определения информационной безопасности.
3. Политика информационной безопасности компании.
4. Организация информационной безопасности на предприятии.
5. Классификация и управление корпоративными информационными ресурсами.
6. Кадровый менеджмент и информационная безопасность;
7. Физическая безопасность.
8. Администрирование безопасности корпоративных информационных систем.
9. Управление доступом.
10. Требования по безопасности к корпоративным информационным системам в ходе их разработки, эксплуатации и сопровождения.
11. Управление бизнес-процессами компании с точки зрения информационной безопасности.
12. Внутренний аудит информационной безопасности компании.

Так, например, раздел «***Кадровый менеджмент и информационная безопасность***» включает в себя следующие подразделы:

1. **Включение в должностные обязанности каждого сотрудника задач по обеспечению информационной безопасности**

   Обеспечить строгое выполнение всеми сотрудниками своих обязанностей по отношению к безопасности информации: халатное отношение к этим вопросам (так называемый человеческий фактор) может свести на нет все вложения в эту область и обречь на неудачу все попытки обеспечить безопасность компании.
2. **Заключение соглашений о соблюдении режима информационной безопасности со всеми сотрудниками**

   При приеме на работу необходимо подписать специальное соглашение о конфиденциальности, запрещающее сотруднику разглашать информацию, начиная с определенного уровня (грифа) секретности. В подобном юридически проработанном соглашении, необходимо учесть степень ответственности за его невыполнение сотрудником компании, а также период действия соглашения, в том числе и после увольнения сотрудника
3. **Условия работы персонала**

   При приеме на работу новых сотрудников необходимо, чтобы они ознакомились и подписали:

- письменную формулировку их должностных обязанностей;
- письменную формулировку прав доступа к ресурсам компании (в том числе и информационным);
- соглашение о конфиденциальности;
- специальные соглашения о перлюстрации всех видов служебной корреспонденции (мониторинг сетевых данных, телефонных переговоров, факсов и т.д.).

Любые компоненты корпоративной сети могут использоваться пользователями только для выполнения своих служебных обязанностей.

Использование компонентов сети не по назначению, нарушающее требования инструкций, приказов и распоряжений руководства компании (Директора, Технического Директора, руководителей подразделений), а также использование, которое наносит вред компании, в зависимости от тяжести наступивших последствий может повлечь за собой дисциплинарную (включая увольнение), административную или уголовную ответственность.

4. **Наладить постоянный процесс повышения уровня технической грамотности и информированности пользователей в области информационной безопасности.** Для этого необходимо регулярное проведение тренингов, посвященных общим правилам информационной защиты.
5. **Разработать однозначно воспринимаемый порядок действий в случае критических ситуаций.**

К ***физической безопасности*** стандарт относит следующие мероприятия:

1. **Контроль физического доступа**

   Во-первых, все посетители безопасного периметра должны контролироваться, время и дата входа и выхода должны быть записаны.

   Во-вторых, персонал должен носить хорошо видимые идентификаторы. Идентификатор сразу же позволяет выявить незнакомца, который каким-либо образом проник в контролируемый периметр, а также автоматически повышает бдительность сотрудников.
2. **Безопасность офисов, комнат и средств**

   Во-первых, ключевые информационные системы должны быть расположены так, чтобы исключить случайный доступ к ним неавторизованных лиц.

   Во-вторых, здания должны быть обычными и показывать своим внешним видом минимум своего назначения. Выполнение этого требования позволит ввести в заблуждение потенциального злоумышленника и скроет от посторонних глаз назначение того или иного здания компании.

   В-третьих, оборудование, предназначенное для ликвидации неисправностей и резервные копии должны храниться на безопасном удалении от основного объекта во избежание уничтожения при происшествии на основном объекте.
3. **Месторасположение и защита оборудования**

   Оборудование должно располагаться с учетом минимизации доступа в рабочее помещение лиц, не связанных с обслуживанием этого оборудования.

   Политика компании должна содержать категорический запрет на прием пиши, напитков и курение вблизи оборудования.

   Необходимость постоянного мониторинга оборудования для раннего обнаружения признаков, которые могут повлечь за собой отказ системы является очевидным требованием - видео наблюдение, постоянный контроль за пожарными датчиками позволят вовремя обнаружить возможную неисправность.

   Требование предусмотреть возможные воздействия от происшествий на соседних объектах позволит заранее оценить возможный ущерб и спланировать контр аварийные мероприятия.
4. **Безопасность кабельной системы**

   Выполнение требования по разделению трасс силовых и коммуникационных кабелей позволит избежать появления наведенных электромагнитных помех в последних. Более того, в ряде стран совместная прокладка таких кабелей запрещена правилами пожарной безопасности.
5. **Безопасное уничтожение отработавшего оборудования**

   Жесткий контроль за дальнейшей судьбой всего списываемого оборудования является необходимым условием любой политики безопасности. Особенно стоит обратить внимание на требование обязательного уничтожения (или безопасной перезаписи информации) устройств хранения информации, содержащих ценную информацию.

Вторая часть стандарта BS 7799-2:2000 "Спецификации систем управления информационной безопасностью" определяет возможные функциональные спецификации корпоративных систем управления информационной безопасностью с точки зрения их проверки на соответствие требованиям первой части данного стандарта. В соответствии с положениями этого стандарта также регламентируется процедура аудита информационных корпоративных систем.

Комплексный учет показателей предполагает комплексный подход к аудиту, когда на соответствие определенным правилам проверяется не только программно-техническая составляющая информационной безопасности компьютерной системы, но и организационно-административные меры по ее обеспечению.

Сущность аудита безопасности на соответствие системы управления информационной безопасностью компании требованиям стандарта заключается в проверке выполнения каждого положения стандарта ISO 17799. По каждому такому положению проверяющие должны ответить на два вопроса: выполняется ли данное требование, и если нет, то каковы причины невыполнения? На основе ответов составляется «Ведомость соответствия», основная цель которой – аргументированное обоснование имеющихся отклонений информационной безопасности от требований стандарта ISO 17799.

В результате должны быть проверены: организация информационной безопасности компании, обязанности по обеспечению информационной безопасности сотрудников всех должностей, наличие документированной политики и стратегии информационной безопасности для компании, и, в частности, документированной стратегии и общих положений подхода к оцениванию и управлению рисками. По результатам успешно выполненного аудита компании или ее информационной системы и подсистемы информационной безопасности осуществляется выдача сертификатов на соответствие стандарту ISO/IEC 17799:2000 (BS 7799-1:2000), которые считаются действительными в течение 3 лет.

Появление проекта международного стандарта **"Общие критерии оценки безопасности информационных технологий" ISO 15408** явилось качественно новым этапом в развитии нормативной базы оценки безопасности информационных технологий (ИТ).

Общие критерии (ОК) обобщили содержание и опыт использования Оранжевой книги, развили уровни гарантии оценки Европейских критериев, воплотили в реальные структуры концепцию профилей защиты Федеральных критериев США.

Главные достоинства Общих критериев — полнота и систематизация требований безопасности, гибкость в применении и открытость для последующего развития. Разработка этого международного стандарта велась совместными усилиями США, Канады, Франции, Германии, Нидерландов и Великобритании. В последствии к проекту присоединился ряд других стран.

В январе 1996 года была выпущена версия 1.0 Общих критериев, в мае 1998 года - версия 2.0 , а **4 июня 1999 года** международная организация по стандартизации **утвердила** в качестве **международного стандарт**а **ISO/IEC 15408** (ИСО/МЭК 15408). “Критерии оценки безопасности информационных технологий”.

Общие критерии разработаны таким образом, чтобы удовлетворить потребности трех групп специалистов: разработчиков, оценщиков и пользователей объекта оценки. Под объектом оценки (ОО) понимается аппаратно-программный продукт или информационная система. К таким объектам относятся, например, операционные системы, вычислительные сети, распределенные системы, прикладные программы.

К рассматриваемым в ОК аспектам безопасности относятся: защита от несанкционированного доступа, модификации или потери доступа к информации при воздействии угроз, являющихся результатом случайных или преднамеренных действий. Защищенность от этих трех типов угроз обычно называют конфиденциальностью, целостностью и доступностью.

Некоторые аспекты безопасности ИТ находятся вне рамок ОК:

- ОК не охватывают оценку административных мер безопасности;
- в ОК не рассматривается оценка технических аспектов безопасности ИТ типа побочных электромагнитных излучений;
- ОК формулируют только критерии оценки и не содержат методик самой оценки;
- в ОК не входят критерии для оценки криптографических методов защиты информации.

Общие критерии предполагается использовать как при задании требований к продуктам и системам ИТ, так и при оценке их безопасности на всех этапах жизненного цикла.

ОК состоят из следующих частей:

Часть 1. "Представление и общая модель". Определяются общая концепция, принципы и цели оценки безопасности ИТ. Приведены категории специалистов, для которых ОК представляют интерес.

Часть 2. "Требования к функциям безопасности". Приведены требования к функциям безопасности и определен набор показателей для оценки безопасности информационных технологий. Каталоги части 2 содержат наборы требований, сгруппированные в семейства и классы.

Часть 3. "Требования гарантированности безопасности". Приведены требования к гарантиям безопасности, сгруппированные в семейства, классы и уровни. Определены также критерии оценки для Профилей защиты и Заданий по безопасности.

Часть 4. "Предопределенные профили защиты". Приведены примеры профилей защиты, включающих функциональные требования и требования гарантированности. Ряд подобных требований присутствовал в предшествующих критериях (ITSEC, CTCPEC, FC, TCSEC), другие впервые представлены в данном документе. Предполагается, что в конечном счете часть 4 станет каталогом профилей защиты, которые прошли процесс регистрации.

Часть 5. "Процедуры регистрации". Определит процедуры регистрации профилей защиты и их поддержки в международном регистре.

В. 2 Основные нормативно правовые акты РФ по защите информации.

Будущее России, её экономики, благосостояния населения, наряду с промышленным потенциалом и природными богатствами зависит от информационных и телекоммуникационных технологий, информационных ресурсов, а также от способности государства обеспечить их эффективную защиту.

Необходимость защиты информационных ресурсов, информационных и телекоммуникационных систем вытекают из требований Правительства РФ, которые нашли отражение в целом ряде нормативных правовых актов в области ИБ, в том числе в «Доктрине ИБ РФ».

Все нормативно-правовые акты РФ по защите информации можно разделить на три составляющие:

1. •Указы Президента РФ, федеральные законы и постановления Правительства РФ имеющие отношение к защите информации.
2. •Руководящие документы ФСТЭК (Гостехкомиссии) России.
3. •Государственные стандарты в области защиты информации.

Документы относящиеся к первой составляющей перечислены на слайде № 6. А более подробно рассмотрены на слайдах № 7 – 20.

Документы относящиеся к первой составляющей перечислены на слайдах № 21, 22. А более подробно рассмотрены на слайдах № 23 – .

В 1992 году Государственная техническая комиссия при Президенте Российской Федерации опубликовала пять Руководящих документов, посвященных проблеме защиты от несанкционированного доступа (НСД) к информации [1-5]. Позже был принят ряд других документов [6-9]. В 2004 г. на основе Государственной технической комиссии создана Федеральная служба по техническому и экспортному контролю (ФСТЭК России) (Указ Президента Российской Федерации от 16.08.2004 г. № 1085). Однако все руководящие документы Гостехкомиссии России, опубликованные ранее, продолжают действовать в РФ до выхода новых документов ФЭСТЭК России. Рассмотрим важнейшие из них.

Идейной основой набора Руководящих документов является ***"Концепция защиты СВТ и АС от НСД к информации"*** [1]. Концепция излагает систему взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от НСД, являющейся частью общей проблемы безопасности информации.

В Концепции различаются понятия средств вычислительной техники (СВТ) и автоматизированной системы. Концепция предусматривает существование двух относительно самостоятельных и, следовательно, имеющих отличие направлений в проблеме защиты информации от НСД. Это – направление, связанное с СВТ, и направление, связанное с АС.

Отличие двух направлений порождено тем, что СВТ разрабатываются и поставляются на рынок лишь как элементы, из которых в дальнейшем строятся функционально ориентированные АС, и поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации.

Помимо пользовательской информации при создании АС появляются такие отсутствующие при разработке СВТ характеристики АС, как полномочия пользователей, модель нарушителя, технология обработки информации.

Существуют различные способы покушения на защиту информации – радиотехнические, акустические, программные и т. п. Среди них НСД выделяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС.

Под *штатными средствами* понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

В Концепции формулируются следующие основные принципы защиты от НСД к информации:

- Защита СВТ обеспечивается комплексом программно-технических средств.
- Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.
- Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.
- Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).

- Неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты.
- Защита АС должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.

Концепция ориентируется на физически защищенную среду, проникновение в которую посторонних лиц считается невозможным, поэтому нарушитель определяется как субъект, имеющий доступ к работе с штатными средствами АС и СВТ как части АС.

Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ. Выделяется четыре уровня этих возможностей. Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

Первый уровень определяет самый низкий уровень возможностей ведения диалога в АС — запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

В своем уровне нарушитель является специалистом высшей квалификации, знает все о АС и, в частности, о системе и средствах ее защиты.

В качестве главного средства защиты от НСД к информации в Концепции *рассматривается система разграничения доступа* (СРД) субъектов к объектам доступа. Основными функциями СРД являются:

- реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;
- реализация ПРД субъектов и их процессов к устройствам создания твердых копий;
- изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;
- управление потоками данных с целью предотвращения записи данных на носители несоответствующего грифа;
- реализация правил обмена данными между субъектами для АС и СВТ, построенных по сетевым принципам.

Кроме того, Концепция предусматривает наличие обеспечивающих средств для СРД, которые выполняют следующие функции:

- идентификацию и опознание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;
- регистрацию действий субъекта и его процесса;
- предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;
- реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление после НСД;
- тестирование;
- очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;
- учет выходных печатных и графических форм и твердых копий в АС;
- контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.

Технические средства защиты от НСД, согласно Концепции, должны оцениваться по следующим основным параметрам:

- степень полноты охвата ПРД реализованной СРД и ее качество;
- состав и качество обеспечивающих средств для СРД;
- гарантии правильности функционирования СРД и обеспечивающих ее средств.

Классификация СВТ по уровню защищенности от НСД

В данном Руководящем документе [2] устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс — седьмой, самый высокий — первый.

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

- первая группа содержит только один седьмой класс;
- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;

- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

На слайде № 23 приведена таблица распределения показателей защищенности по шести классам СВТ.

Обозначения:

« - » – нет требований к данному классу;

« + » – новые или дополнительные требования;

« = » – требования совпадают с требованиями к СВТ предыдущего класса.

Седьмой класс присваивают СВТ, к которым предъявлялись требования по защите от НСД к информации, но при оценке защищенность СВТ оказалась ниже уровня требований шестого класса.

При *дискреционном контроле* доступа для каждой пары (субъект – объект) в правилах разграничения доступа должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ (объекту).

Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов).

Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов.

Основой *мандатного принципа* разграничения доступа служат специальные классификационные метки, присваиваемые каждому субъекту и каждому объекту доступа, отражающие их место в соответствующей иерархии. Посредством этих меток субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т.п.), являющиеся комбинациями иерархических и неиерархических категорий.

КСЗ при вводе новых данных в систему должен запрашивать и получать от санкционированного пользователя классификационные метки этих данных. При санкционированном занесении в список пользователей нового субъекта должно осуществляться сопоставление ему классификационных меток. Внешние классификационные метки (субъектов, объектов) должны точно соответствовать внутренним меткам (внутри КСЗ).

Классификация АС по уровню защищенности от НСД

В данном Руководящем документе [3] 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.

Третья группа классифицирует АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса — 3Б и 3А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности.

Группа содержит два класса — 2Б и 2А.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС.

Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А.

На слайде № 24, 25 представлены требования ко всем девяти классам защищенности АС.

Межсетевые экраны. Показатели защищенности от НСД

Настоящий руководящий документ [6] устанавливает классификацию межсетевых экранов (МЭ) по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

Устанавливается пять классов защищенности МЭ. Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации.

Самый низкий класс защищенности – пятый, применяемый для безопасного взаимодействия АС класса 1Д с внешней средой, четвертый - для 1Г, третий - 1В, второй - 1Б, самый высокий - первый, применяемый для безопасного взаимодействия АС класса 1А с внешней средой.

Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей

В данном Руководящем документе [7] устанавливается классификация программного обеспечения (ПО) средств защиты информации (СЗИ), в том числе и встроенных в общесистемное и прикладное ПО, по уровню контроля отсутствия в нем недекларированных возможностей.

Под недекларированными возможностями понимаются функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации. Реализацией недекларированных возможностей, в частности, являются программные закладки.

Классификация распространяется на ПО, предназначенное для защиты информации ограниченного доступа. Устанавливается четыре уровня контроля отсутствия недекларированных возможностей. Каждый уровень характеризуется определенной минимальной совокупностью требований.

Самый высокий уровень контроля – первый, достаточен для ПО, используемого при защите информации с грифом «ОВ».

Второй уровень контроля достаточен для ПО, используемого при защите информации с грифом «СС».

Третий уровень контроля достаточен для ПО, используемого при защите информации с грифом «С».

Самый низкий уровень контроля – четвертый, достаточен для ПО, используемого при защите конфиденциальной информации.

Уровень контроля определяется выполнением заданного настоящим РД набора требований, предъявляемого:

- к составу и содержанию документации, представляемой заявителем для проведения испытаний ПО СЗИ;
- к содержанию испытаний.

Специальные требования и рекомендации по технической защите конфиденциальной информации

В руководящем документе СТР-К [8] приводятся основные термины и определения по защите информации, а также устанавливается порядок организации работ, указываются требования и рекомендации по обеспечению технической защиты информации с ограниченным доступом (конфиденциальная информация), не содержащей сведений составляющих государственную тайну, на территории Российской Федерации.

Документ включает следующие шесть разделов:

1. Термины, определения и сокращения.
2. Общие положения.
3. Организация работ по защите информации.
4. Требования и рекомендации по защите речевой информации.
5. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники.
6. Рекомендации по обеспечению защиты информации, содержащейся в негосударственных информационных ресурсах, при взаимодействии абонентов с информационными сетями общего пользования.

Планируемое вступление России во Всемирную торговую организацию и вхождение в мировое информационное сообщество предполагает, что необходимо принимать документы, имеющие аналогичные или близкие к ним критерии оценки безопасности информационных технологий. В этой связи при аппарате Совета Безопасности Российской Федерации была создана рабочая группа из представителей Гостехкомиссии России, ФАПСИ, ФСБ, Минобороны России и других структур, где рассматривалась возможность применения в России методологии стандарта ISO 15408. По результатам работы этой группы межведомственной комиссией Совета Безопасности по информационной безопасности было принято решение о проведении практической апробации в системе сертификации Гостехкомиссии России нормативных документов в области ЗИ, разработанных в соответствии с методологией указанного международного стандарта.

Гостехкомиссией России организована разработка на базе международных стандартов комплекса государственных стандартов в области управления безопасностью информационных технологий, а также ряда нормативных и методических документов, соответствующих используемой в международной практике нормативно-методической базе. Это разработанный

Гостехкомиссией России и принятый постановлением Госстандарта России от 4 апреля 2002 г. №133-СТ государственный стандарт ГОСТ Р ИСО/МЭК №15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», а также руководящий документ Гостехкомиссии России с аналогичным названием.

Критерии оценки безопасности информационных технологий

В России в 2002 году внедрена адаптированная 3 версия международного стандарта ISO/IEC 15408 (см. раздел 1.4) – **«Критерии оценки безопасности информационных технологий»**. Этот руководящий документ (РД) [9] содержит систематизированный каталог требований безопасности информационных технологий (ИТ) порядок и методические рекомендации по его использованию при задании требований, разработке, оценке и сертификации продуктов и систем ИТ по требованиям безопасности информации.

Руководящий документ состоит из трех частей.

Часть 1. «Введение и общая модель» определяет виды требований безопасности (функциональные и требования доверия), основные конструкции представления требований безопасности (профиль защиты, задание по безопасности) и содержит основные методические положения по оценке безопасности ИТ.

Часть 2. «Функциональные требования безопасности» содержит универсальный систематизированный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам. Она содержит каталог всех функциональных компонентов, семейств и классов.

Часть 3. «Требования доверия к безопасности» устанавливает совокупность компонентов доверия как стандартный способ выражения требований доверия к объекту оценки (ОО). Содержит каталог всех компонентов, семейств и классов доверия. Кроме того, в этой части определены критерии оценки профилей защиты и заданий по безопасности и представлены оценочные уровни доверия (ОУД), которые определяют предопределенную ГОСТ Р ИСО/МЭК 15408-2002 шкалу ранжирования доверия к ОО.

Требования безопасности, содержащиеся в настоящем РД, могут уточняться и дополняться по мере совершенствования правовой и нормативной базы, развития информационных технологий и совершенствования методов обеспечения безопасности. Внесение изменений в РД осуществляется в порядке, устанавливаемом Гостехкомиссией России.

Правовой основой для создания систем полномасштабного электронного документооборота стали разработка и принятие Федерального закона «Об электронной цифровой подписи».

Для обеспечения технологической основы создания упомянутых систем Федеральное агентство завершило работу по созданию новой версии стандарта электронной цифровой подписи (ЭЦП) ГОСТ Р -34.10-01. Криптографическую основу стандарта составили алгоритмы с операциями в группе точек эллиптических кривых. Стандарт введен в действие с 1 июля 2002 г. Высокие криптографические качества нового стандарта обеспечивают должный уровень защищенности документов от подделки подписи в течение многих десятков лет даже с учетом развития вычислительной техники и соответствующих математических методов анализа. Практика показала, что скоростные и технические характеристики реализации нового алгоритма выработки и проверки электронной цифровой подписи существенно превосходят характеристики старого стандарта. В частности, время вычисления электронной цифровой подписи микроконтроллером, используемым в российских интеллектуальных картах, не превышает 300 миллисекунд, чего нельзя было достичь при реализации предыдущего стандарта ЭЦП.

Достижение надежной защищенности информации, в том числе и конфиденциальной, будет в XXI веке важнейшим фактором обеспечения национальной безопасности России.

Государственные стандарты:

Государственные нормативные документы по стандартизации

ГОСТ Р ИСО/МЭК 15408-1 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. 2002 г.

ГОСТ 29339-92 Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений и наводок при ее обработке средствами вычислительной техники. Общие технические требования

ГОСТ РВ 50170-92 Противодействие иностранной технической разведке. Термины и определения

ГОСТ Р 50543-93 Конструкции базовые несущие средств вычислительной техники. Требования по Обеспечению защиты информации и электромагнитной совместимости методом экранирования

ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования

ГОСТ Р 50752-95 Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений и наводок при ее обработке средствами вычислительной техники. Методы испытаний

ГОСТ РВ 50859-96 Противодействие иностранной технической разведке. Документация по защите образца военной техники от иностранных технических разведок. Общие положения

ГОСТ Р 50922-96. Защита информации. Основные термины и определения

ГОСТ РВ 50934-96 Защита информации. Организация и содержание работ по защите информации об образцах военной техники от технических разведок. Общие положения

ГОСТ Р 50972-96 Защита информации. Радиомикрофон. Технические требования к защите от утечки секретной информации

ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство

ГОСТ Р 51189-98 Средства программные систем вооружения. Порядок разработки

ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

ГОСТ Р 51583-00 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения

ГОСТ Р 51624-00 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования

ГОСТ Р ИСО 7498-1-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель

ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации

ГОСТ 6.38-90 Система организационно-распорядительной документации. Требования к оформлению

ГОСТ 6.10-84 Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники, ЕСКД, ЕСПД и ЕСТД

ГОСТ 29339-92 Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений и наводок при ее обработке средствами вычислительной техники. Общие технические требования

В. 3 Приказы МО РФ, командующего КВ, командира части по защите компьютерной информации.

В настоящее время в ВС РФ действуют следующие **приказы МО** по защите информации:

1. № 392 МО РФ от 2004 г. «О мерах по обеспечению информационной безопасности В ВС РФ при использовании международных сетей (Интернет)».
2. Приказ Министра обороны Российской Федерации № 190 от 13.05.02 г. «О принятии на снабжение ВС РФ защищенных ОС МСВС 3.0, СУБД «Линтер-ВС» 6.0 и комплекса программных средств обеспечения повседневной деятельности должностных лиц КП «Офис» 1.0».

Действующие приказы **командующего Космическими войсками**:

1. № 40 от 2004 г. «Об утверждении инструкции по обеспечению защиты объектов (средств) вычислительной техники Космических войск и информации от воздействия компьютерных вирусов».

Перечень организационных документов по ОБИ

на объекте вычислительной техники (в ЛВС)

№ п/п	Наименование документа
1.	Приказ командира части о вводе в эксплуатацию (о закреплении технических средств объекта ВТ за должностными лицами)
2.	Перечень защищаемых ресурсов объекта ВТ (ЛВС)
3.	Таблица разграничения доступа к защищаемым ресурсам объекта ВТ(ЛВС)
4.	Инструкция по организации паролирования (раздел в инструкции по ОБИ)
5.	Акт проверки функционирования системы защиты информации в ЛВС
6.	Список должностных лиц, имеющих право работать на АРМ
7.	Функциональные обязанности должностных лиц по ОБИ
8.	Годовой план практических мероприятий по ОБИ на объекте ВТ
9.	Сводный перечень задач, решаемых на объекте ВТ
10.	Разрешение на автоматизированное производство расчётов
11.	Частная инструкция по ОБИ на объекте ВТ
12.	Методические указания (инструкция оператору) по выполнению задачи
13.	Инструкция по действиям личного состава объекта ВТ на случай стихийного бедствия, а также угрозе нападения противника
14.	Инструкция по стиранию информации с магнитных носителей информации
15.	Журнал учёта машинных носителей информации
16.	Журнал предварительного учёта формируемых бумажных носителей информации и документов
17.	Журнал учёта стирания информации
18.	Список лиц, имеющих право вскрывать помещение объекта ВТ
19.	Журнал сдачи под охрану помещений объекта ВТ
20.	Перечень опечатываемых технических средств объекта ВТ
21.	Схема (маршрутная или технологическая карта) опечатывания технических средств объекта ВТ
22.	Акт (доклад) внутренней проверочной комиссии части о ежегодной проверке вопросов состояния ОБИ на объекте ВТ
23.	Акт на уничтожение машинных носителей информации и документов (стирание секретной информации)
24.	Карточка учёта выдачи машинных носителей информации
25.	Акт категорирования ЛВС (объекта ВТ)
26.	Сертификат соответствия или предписание на эксплуатацию
27.	Заключение (сертификат) о проведении специальной проверки (для ТСПИ иностранного или совместного производства)

28.	Проектная документация в части спецзащиты
29.	Протоколы замеров величины сопротивления заземления
30.	Акт проведения скрытых работ
31.	Аттестат соответствия, выдаваемый при вводе объекта в эксплуатацию
32.	Формуляр по защите информации от утечки по техническим каналам
33.	Акт спецобследования комиссией части