Программно-аппаратная защита информации

Лекция 4. Формализованные требования к программно-аппаратной защите информации

2020

Лекция 4. Формализованные требования к программно- аппаратной защите информации

Учебные вопросы:

1. Политика и показатели безопасности СВТ и АС.
2. Формализованные требования ФСТЭК к средствам вычислительной техники и автоматизированным системам по защите информации.
3. Новое поколение нормативно-технических документов по безопасности информации.

Литература

Основная:

1. РД «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации»: утв. Гостехкомиссией России. – М.: Изд-во стандартов, 1992.
2. РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»: утв. Гостехкомиссией России. – М.: Изд-во стандартов, 1992.
3. Стандарт ИСО/МЭК 27000.
4. Стандарт ИСО/МЭК 15408.
5. Казарин О.В., Забабурин А.С. Программно-аппаратные средства защиты информации. Защита программного обеспечения. Учебник и практикум для вузов (серия специалист), 312 с. 2018 г.
6. Нестеров С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров ; Политех. - М. : Юрайт, 2017. - 321 с.

Литература

Дополнительная:

1. Куватов В. И., Синещук Ю. И., Смирнов А. С. Безопасность информациионных систем и защита информации в МЧС России. (учебное пособие) . - СПб.: СПбУ ГПС МЧС России, 2010. 378 с.
2. Куватов В. И., Пантиховский О. В., Синещук Ю. И., Обеспечение безопасности информации в АСУ. (учебное пособие). - СПб.: ВМИРЭ, 2011г.320 с.
3. Платонов В. В. Программно-аппаратные средства защиты информации. –М.: Издательский центр «Академия», 2013 г. – 331 с.
4. Синадский Н. И. Специализированные программно-аппаратные средства защиты информации. Учебное пособие. -Екатеринбург: Уральский государственный университет им. М. Горького, 2008 г. – 237 с.
5. Котухов М.М., Калашников А.О., Кубанков А.Н. Информационная безопасность. Учебное пособие. М.: Издание Академия IBS, 2008.- 148 с.

Введение

Безопасность информационных систем (ИС) — это состояние, определяющее защищенность обрабатываемой информации и ресурсов от действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способность ИС выполнять предписанные функции без нанесения неприемлемого ущерба объектам и субъектам информационных отношений. Ранее мы убедились, что пространство угроз компьютерной информации велико и разнообразно. Столь же велики и разнообразны программно-аппаратные методы и средства противодействия этим угрозам. Поэтому задача выбора средств и методов противодействия угрозам, осуществляемая на этапе обоснования проекта системы защиты информации, не является тривиальной. В настоящее время в России и в мире наибольшее распространение получили два подхода к решению этой задачи.

1. Политика и показатели безопасности СВТ и АС.

Задачи защиты компьютерной информации и требования к системе защиты объективны, порождены практическим опытом эксплуатации СВТ, АС и во многом близки, как для больших распределенных вычислительных систем, так и для одиночных ПК, работающих в одно- или многопользовательском режиме.

Политика безопасности это совокупность принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности. ПБ оформляется в виде документа (набора документов), который должен быть доступен всем сотрудникам, и, в первую очередь, отвечающим за обеспечение режима информационной безопасности на предприятии. Этот документ определяет основные цели политики информационной безопасности и область ее применения, а также ее значение как механизма, позволяющего сотрудникам предприятия коллективно использовать информацию.

Руководящие документы ГТК (ФСТЭК) предлагают *две основных группы показателей (критериев)* защищенности информации: показатели защищенности средств вычислительной техники (СВТ) от НСД и критерии защищенности автоматизированных систем (АС) обработки данных.

При создании АС появляются такие отсутствующие у СВТ характеристики, как:

- пользовательская информация;
- полномочия пользователей;
- модель нарушителя;
- технология обработки информации.

В отдельный класс выделяются требования по защите СВТ и АС от НСД к информации с использованием межсетевых экранов и систем обнаружения вторжений.

2.Формализованные требования к средствам вычислительной техники

Требования к защите СВТ формализуют условия защищенности отдельно взятого средства (ОС, СУБД, приложения и пр.). Классификацию СВТ по уровню защищенности от НСД устанавливает руководящий документ (РД), утвержденный России 1992 «Средства Гвычислительной техники. Защита от в информации. Показатели защищенностиот НСД к информации». к Данный Р устанавливает классификацию отдельно взятых СВТ (ОС, Д приложения) по уровню защищенности СУБД, от НСД к информациина перечня показателейбазе защищенности и совокупности описывающих требований. Конкретные ихперечни показателей определяют классы защищенности СВТ и описываются совокупностью требований. Установлено семь классов защищенности СВТ от НСД к информации.

Документация на СВТ должна включать в себя:

- Краткое руководство для пользователя с описанием способов использования КСЗ и его интерфейса с пользователем.

- Руководство по КСЗ. Данный документ адресован администратору защиты и должен содержать: описание контролируемых функций, руководство по генерации КСЗ, описание старта СВТ и процедур проверки правильности старта.
- Тестовая документация. Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ и результатов тестирования.
- Конструкторская (проектная) документация. Должна содержать общее описание принципов работы СВТ, общую схему КСЗ, описание интерфейсов КСЗ с пользователем и интерфейсов частей КСЗ между собой, описание механизмов идентификации и аутентификации.

Требования к защите АС формализуют условия защищенности объекта с учетом:

- совокупности механизмов защиты, реализуемых установленными на защищаемом объекте средствами, включая ОС, СУБД (если есть), приложениями, добавочными механизмами защиты (если есть);
- дополнительных организационных мер, принимаемых для безопасного функционирования АС.

Классификация автоматизированных систем и требования по защите информации отражены в РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»: утв. Гостехкомиссией России. – М.: Изд-во стандартов, 1992. В этом документе основные меры для защиты от НСД автоматизированных систем группируют в четыре подсистемы:

- управления доступом,
- регистрации и учета,
- криптографической,
- обеспечения целостности.

Все перечисленные требования должны обеспечиваться средствами самой компьютерной системы автоматически. Каждый сотрудник предприятия должен быть вынужден гарантированно выполнять требования политики безопасности, а не только под воздействием силы приказов и распоряжений начальников. На предприятии *должен быть организован такой режим функционирования АС*, который просто не позволит пользователю работать с конфиденциальными данными в незащищенном режиме.

Перечисленные выше требования защиты АС от НСД вытекают из опыта, здравого смысла и давно существующего порядка работы с конфиденциальной информацией (на бумажных или электронных носителях). Этот набор требований далеко не полон, не противоречит официальным руководящим документам, однако он не затрагивает специальных вопросов проектирования комплекса защиты информации, параметров функциональности средств и механизмов защиты, разработки необходимой документации, тестирования СЗИ, контроля защищенности АС.

Соответствие между классами АС и степенями конфиденциальности информации:

- классы 1А, 2А, 3А включают АС, на которых обрабатываются сведения, составляющие государственную тайну, до сведений с грифом "особой важности";
- класс 1Б включает АС, на которых обрабатываются сведения, составляющие государственную тайну, до сведений с грифом "совершенно секретно";
- класс 1В включает АС, на которых обрабатываются сведения, составляющие государственную тайну, до сведений с грифом "секретно";
- классы 1Г, 2Б, 3Б включают АС, на которых обрабатываются сведения, составляющие конфиденциальную информацию - служебная тайна;
- классы 1Г, 1Д, 2Б, 3Б включают АС, на которых обрабатываются сведения, составляющие конфиденциальную информацию - персональные данные, коммерческая тайна.

Гриф сведений	Государственная тайна			Конфиденциальная информация	
	Особой важности	Сов. сек-ретно	Секрет-но	Служеб-ная тайна	Персон. данные, коммерч. тайна
Классы АС	1А, 2А, 3А	1Б	1В	1Г, 2Б, 3Б	1Г, 1Д, 2Б, 3Б

Требования к уровням отсутствия недекларированных возможностей

Недекларированные возможности это функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности и целостности обрабатываемой информации.

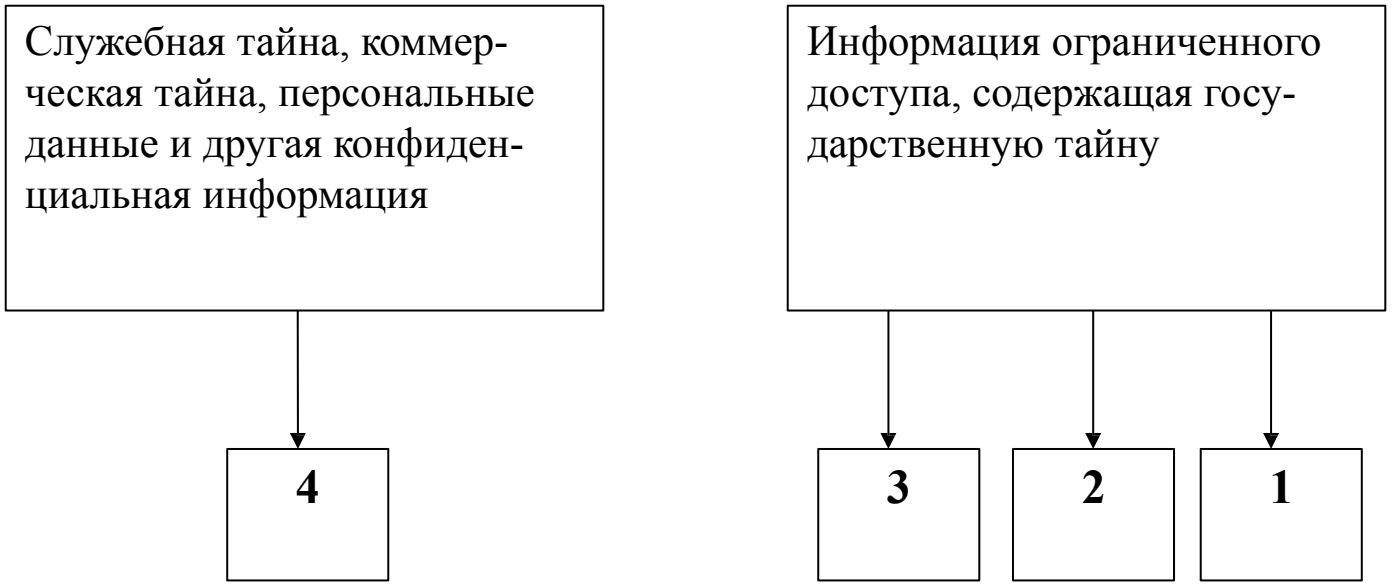

Рис. 1. Классификация по степени соответствия уровня контроля недекларированных возможностей уровням защищенности от НСД

3.Новое поколение нормативно-технических документов по защите информации.

3.1.Общие критерии информационной безопасности. Стандарты ИСО/МЭК 15408

Одним из наиболее важных международных документов в области информационной безопасности является международный стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий», сокращенно называемый часто «Общие критерии». На самом деле ISO/IEC 15408 является метастандартом, определяющим инструменты оценки безопасности информационных систем и порядок их использования. Он содержит обобщенный опыт ряда государств в области информационной безопасности и подвергается постоянным уточнениям и доработкам.

***«Общие критерии» представлены в виде*:**

- национального стандарта ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасных информационных технологий. Часть I. Введение и общая модель». Утвержден приказом Росстандарта РФ от 15.11.2012 г. № 814-ст.
- национального стандарта ГОСТ Р 15408-2-2013. ИСО/МЭК Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасных информационных технологий. Часть 2. Функциональные требования безопасности». Утвержден приказом Росстандарта РФ от 8.11.2013 г. № 1339-ст.
- национального стандарта ГОСТ Р 15408-3-2013. ИСО/МЭК Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасных информационных технологий. Часть 3. Требования доверия к безопасности». Утвержден приказом Росстандарта РФ от 8.11.2013 г. № 1340-ст.
- РД ФСТЭК Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. 2002 г.

3.2. *Стандарты управления информационной безопасностью ИСО/МЭК* 27000

В США и страны Европы в вопросах информационной безопасности, наряду с нормативным подходом, основанным на стандарте ИСО/МЭК 15408, повсеместно применяют рисковую модель, в основе которой лежит стандарт ИСО/МЭК 27000. Все бизнес-процессы зарубежных компаний, применяющих этот стандарт, однозначно описаны и исполняются строго «по учебнику». Благодаря этому руководители систем информационной безопасности четко понимают, какие инциденты могут возникнуть, с какой вероятностью и что они за собой повлекут.

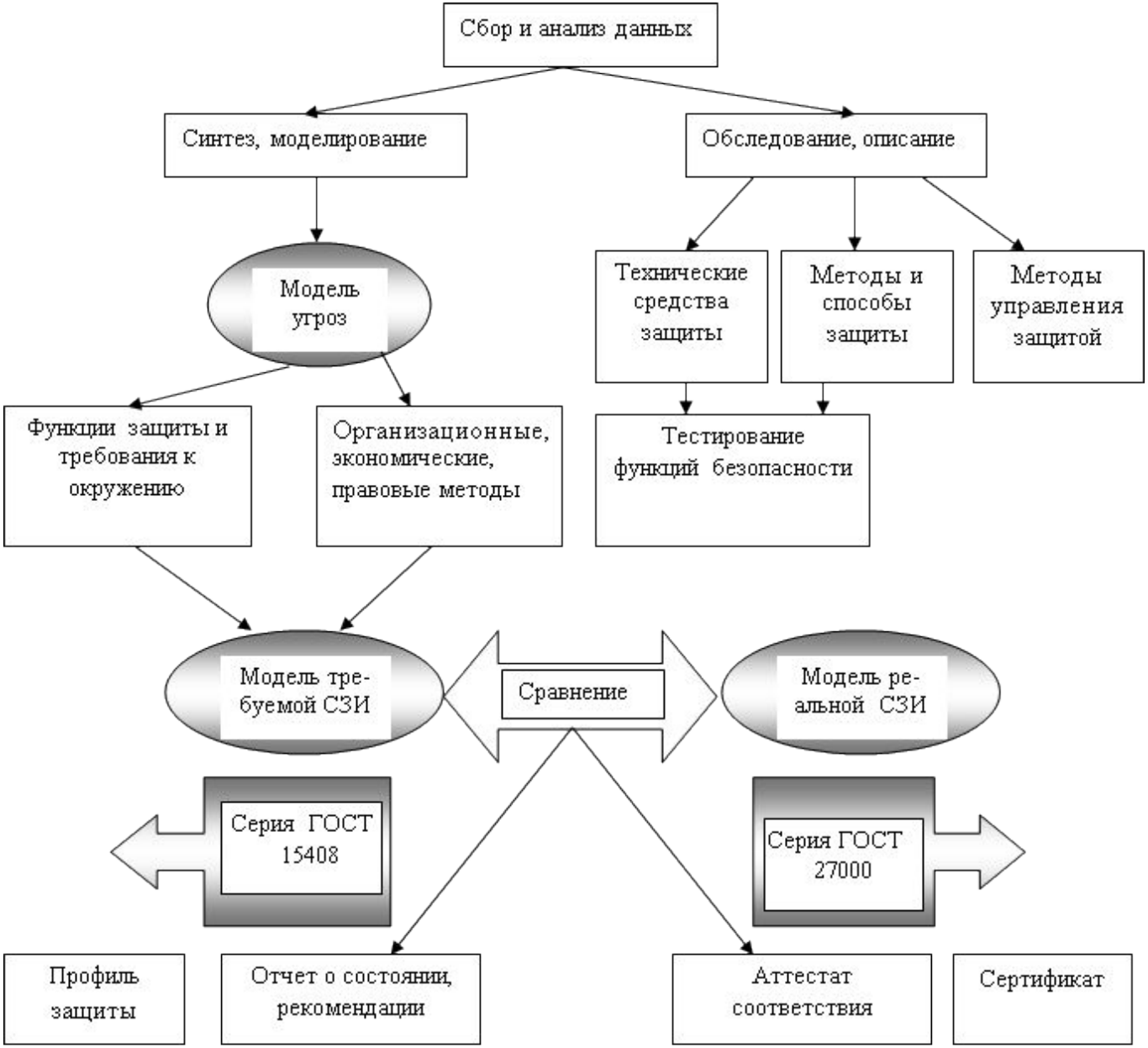

Рис. 1. Методика проведения аудита безопасности

Новое поколение стандартов в области защиты информации отличается как от предыдущего поколения, так и от Руководящих документов ФСТЭК России большей формализацией процесса обеспечения безопасности и достижения более комплексным учетом качественно и количественно проверяемых и управляемых показателей информационной безопасности. Комплексный учет предполагает комплексный подход к управлению безопасностью, когда на соответствие определенным правилам проверяется не только программно-аппаратная составляющая защиты информации, но и организационно-административные меры по ее обеспечению.

Предлагаемый в стандарте метод аудита является а прогностическим, выводыего носят вероятностно-прогностический характер. Принципиально отличаются документы, возникающие по результатам аудита.

Заключение

В данной лекции мы рассмотрели формализованные требованияк средствам вычислительной техники и автоматизированным системам. Также здесь крассмотрены основные нормативно-технические документы по безопасности информации нового поколения, касающиеся, прежде всего, защиты средств вычислительной техники и автоматизированных систем. Приведено назначение и краткое описание этих документов