МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению практических работ
по дисциплине

ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Направление подготовки	10.03.01 Информационная безопасность
Профиль	Комплексная защита объектов информатизации
Квалификация выпускника	бакалавр
Форма обучения	очная
Учебный план	2020 г.

Пятигорск, 2020 г.

ВВЕДЕНИЕ

Методические указания содержат курс практических работ по дисциплине «Основы управления информационной безопасностью» направленный на изучение принципов функционирования и элементной базы вычислительных систем.

Содержащиеся в данном пособии сведения теории, методические указания и рекомендации по выполнению практических работ позволяют использовать его в качестве дополнительного пособия для закрепления курса лекций.

СОДЕРЖАНИЕ

ПРАКТИЧЕСКАЯ РАБОТА №1

«Основополагающие документы в области информационной безопасности»

Цель работы: изучить основополагающие документы в области информационной безопасности и российские и международные, которые используются в России.

1. Теоретическая часть

1. Рекомендации X.800.

Основополагающим документом в области защиты распределенных систем стали рекомендации X.800 — документ довольно обширный.

Основная особенность этого документа – распределение функций обеспечения ИБ по уровням OSI/

Распределение функций безопасности по уровням эталонной семиуровневой модели OSI

Функции безопасности	Уровень модели OSI						
	1	2	3	4	5	6	7
Аутентификация	-	-	+	+	-	-	+
Управление доступом	-	-	+	+	-	-	+
Конфиденциальность соединения	+	+	+	+	-	+	+
Конфиденциальность вне соединений	-	+	+	+	-	+	+
Выборочная конфиденциальность	-	-	-	-	-	+	+
Конфиденциальность трафика	+	-	+	-	-	-	+
Целостность с восстановлением	-	-	-	+	-	-	+
Целостность без восстановления	-	-	+	+	-	-	+
Избирательная целостность	-	-	-	-	-	-	+
Целостность вне соединения	-	-	+	+	-	-	+
Неотказуемость	-	-	-	-	-	-	+

Механизмы безопасности

- Шифрование;
- Электронная (цифровая) подпись;
- Механизмы управления доступом;
- Механизмы контроля целостности данных;
- Механизмы аутентификации;

- Механизмы дополнения трафика;
- Механизмы управления маршрутизацией;
- Механизмы подтверждения подлинности;

2. Критерии оценки надежных компьютерных систем ("Оранжевая книга" Министерства обороны США).

Данный труд, называемый чаще всего по цвету обложки "Оранжевой книгой", был впервые 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, 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.

Надежность системы

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
- Гарантированность

Политика безопасности

Это 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.

Основными элементами политики безопасности являются

- Произвольное управление доступом;
- Безопасность повторного использования объектов;
- Метки безопасности;

- Принудительное управление доступом;
- Подотчетность.

Гарантированность

Это мера доверия, которая может быть оказана архитектуре и реализации системы. Гарантированность показывает, насколько корректны механизмы, отвечающие за проведение в жизнь политики безопасности. Гарантированность можно считать пассивным компонентом защиты, надзирающим за самими защитниками.

Важным средством обеспечения безопасности является механизм подотчетности (протоколирования). Надежная система должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом, то есть анализом регистрационной информации.

Концепция надежной вычислительной базы является центральной при оценке степени гарантированности, с которой систему можно считать надежной. Надежная вычислительная база — это совокупность защитных механизмов системы (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности.

Классы безопасности

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 ПК.

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 приводимым ниже требованиям.

Оранжевая книга	Классы безопасности					
Надежность системы		C1	C2	B1	B2	B3	A1	
1. Политика безопасности						
1.1 Произвольное управление доступом	+	+	=	=	+	=
1.2 Повторное использование объектов		+	=	=	=	=
1.3.1 Метки безопасности			+	+	=	=
1.3.2 Целостность меток безопасности			+	+	=	=
1.4 Принудительное управление доступом			+	+	=	=
1.5 Подотчетность						
1.5.1 Идентификация и аутентификация	+	+	+	=	=	=

1.5.2	Предоставление надежного пути				+	+	=
1.5.3	Аудит		+	+	+	+	=

3. Интерпретация "Оранжевой книги" для сетевых конфигураций.

Вводится новое понятие — сетевая надежная вычислительная база, распределенный аналог надежной вычислительной базы изолированных систем. Сетевая надежная вычислительная база формируется из всех частей всех компонентов сети, обеспечивающих информационную безопасность. Надежная сетевая система должна обеспечивать такое распределение защитных механизмов, чтобы общая политика безопасности проводилась в жизнь несмотря на уязвимость коммуникационных путей и на параллельную, асинхронную работу компонентов.

Интерпретация предусматривает различные варианты распределения сетевой надежной вычислительной базы по компонентам и, соответственно, различные варианты распределения механизмов управления доступом.

В частности, некоторые компоненты, закрытые от прямого доступа пользователей (например, коммутаторы пакетов, оперирующие на третьем уровне семиуровневой модели OSI), могут вообще не содержать подобных механизмов.

Идентификация групп пользователей может строиться на основе сетевых адресов хостов или (под)сетей. В то же время регистрационный журнал должен содержать достаточно информации для ассоциирования действий с конкретным пользователем. Сетевой адрес может являться частью глобального идентификатора пользователя.

В принципе возможен централизованный контроль доступа, когда решения принимает специальный сервер авторизации. Возможен и смешанный вариант, когда сервер авторизации разрешает соединение двух хостов, а дальше в дело вступают локальные механизмы хоста, содержащего объект доступа.

Аналогично, идентификация и аутентификация пользователей может производиться как централизованно (соответствующим сервером), так и локально — той системой, с которой пользователь непосредственно взаимодействует. Возможна передача идентификационной и аутентификационной информации между хостами (чтобы избавить пользователя от многократной аутентификации). При передаче аутентификационная информация должна быть защищена не слабее, чем на каждом из компонентов сетевой конфигурации.

В качестве еще одного отличительного момента Интерпретации нужно отметить повышенное внимание к целостности информации вообще и меток безопасности в частности. Для контроля целостности меток и для их защиты от нелегального изменения в Интерпретации рекомендуется широкое использование криптографических методов. Далее, чтобы принудительное управление доступом в распределенной конфигурации имело смысл, совокупность уровней секретности и категорий должна поддерживаться централизованно. В этом одно из принципиальных отличий от произвольного управления доступом.

Новым по сравнению с Оранжевой книгой является рассмотрение вопросов доступности. Сетевой сервис перестает быть доступным, когда пропускная способность коммуникационных каналов падает ниже минимально допустимого уровня или сервис не в состоянии обслуживать запросы. Удаленный ресурс может стать недоступным и вследствие нарушения равноправия в

обслуживании пользователей. Надежная система должна быть в состоянии обнаруживать ситуации недоступности, уметь возвращаться к нормальной работе и противостоять атакам на доступность.

4. Гармонизированные критерии Европейских стран.

Европейские страны приняли согласованные критерии оценки безопасности информационных технологий (Information Technology Security Evaluation Criteria, ITSEC). опубликованные в июне 1991 года от имени соответствующих органов четырех стран — Франции, Германии, Нидерландов и Великобритании.

Принципиально важной чертой Европейских Критериев является отсутствие априорных требований к условиям, в которых должна работать информационная система.

Так называемый спонсор, то есть организация, запрашивающая сертификационные услуги, формулирует цель оценки, то есть описывает условия, в которых должна работать система, возможные угрозы ее безопасности и предоставляемые ею защитные функции. Задача органа сертификации — оценить, насколько полно достигаются поставленные цели, то есть насколько корректны и эффективны архитектура и реализация механизмов безопасности в описанных спонсором условиях.

Европейские Критерии рассматривают следующие составляющие информационной безопасности:

1. конфиденциальность, то есть защиту от несанкционированного получения информации;
2. целостность, то есть защиту от несанкционированного изменения информации;
3. 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.

В Европейских Критериях средства, имеющие отношение к информационной безопасности, рассматриваются на трех уровнях детализации. Наиболее абстрактный взгляд касается лишь целей безопасности. На этом уровне мы получаем ответ на вопрос, зачем нужны функции безопасности. Второй уровень содержит спецификации функций безопасности. Мы узнаем, какая функциональность на самом деле обеспечивается. Наконец, на третьем уровне содержится информация о механизмах безопасности. Мы видим, как реализуется декларированная функциональность.

Спецификации функций безопасности — важнейшая часть описания объекта оценки. Критерии рекомендуют выделить в этих спецификациях разделы со следующими заголовками:

1. Идентификация и аутентификация.
2. Управление доступом.
3. Подотчетность.
4. Аудит.
5. Повторное использование объектов.
6. Точность информации.
7. Надежность обслуживания.
8. Обмен данными.

Набор функций безопасности может специфицироваться с использованием ссылок на заранее определенные классы функциональности.

В Европейских Критериях таких классов десять. Пять из них (F-C1, F-C2, F-B1, F-B2, F-B3) соответствуют классам безопасности "Оранжевой книги".

5. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий".

Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран, он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба. Данный стандарт часто называют "Общими критериями" (ОК).

"Общие критерии" на самом деле являются метастандартом, определяющим инструменты оценки безопасности ИС и порядок их использования.

В отличие от "Оранжевой книги", ОК не содержат предопределенных "классов безопасности". Такие классы можно строить, исходя из требований безопасности, существующих для конкретной организации и/или конкретной информационной системы.

ОК содержат два основных вида требований безопасности:

1. функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;
2. требования доверия, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации.

Требования безопасности предъявляются, а их выполнение проверяется для определенного объекта оценки - аппаратно-программного продукта или информационной системы.

Очень важно, что безопасность в ОК рассматривается не статично, а в привязке к жизненному циклу объекта оценки. Выделяются следующие этапы:

1. определение назначения, условий применения, целей и требований безопасности;
2. проектирование и разработка;
3. испытания, оценка и сертификация;
4. внедрение и эксплуатация.

В ОК объект оценки рассматривается в контексте среды безопасности, которая характеризуется определенными условиями и угрозами.

В свою очередь, угрозы характеризуются следующими параметрами:

1. источник угрозы;
2. метод воздействия;
3. уязвимые места, которые могут быть использованы;
4. ресурсы (активы), которые могут пострадать.

Уязвимые места могут возникать из-за недостатка:

1. в требованиях безопасности;
2. в проектировании;
3. в эксплуатации.

Слабые места по возможности следует устранить, минимизировать или хотя бы постараться ограничить возможный ущерб от их преднамеренного использования или случайной активизации.

С точки зрения технологии программирования в ОК использован устаревший библиотечный (не объектный) подход. Чтобы, тем не менее, структурировать пространство требований, в "Общих критериях" введена иерархия класс – семейство – компонент - элемент.

Классы определяют наиболее общую, "предметную" группировку требований (например, функциональные требования подотчетности).

Семейства в пределах класса различаются по строгости и другим нюансам требований.

Компонент - минимальный набор требований, фигурирующий как целое.

Элемент - неделимое требование.

Между компонентами ОК могут существовать зависимости. Они возникают, когда компонент сам по себе недостаточен для достижения цели безопасности. Вообще говоря, не все комбинации компонентов имеют смысл, и понятие зависимости в какой-то степени

компенсирует недостаточную выразительность библиотечной организации, хотя и не заменяет объединение функций в содержательные объектные интерфейсы.

Формируется два вида нормативных документов: профиль защиты и задание по безопасности.

Профиль защиты (ПЗ) представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (например, операционные системы на компьютерах в правительственных организациях).

Задание по безопасности содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

В ОК нет готовых классов защиты. Сформировать классификацию в терминах "Общих критериев" - значит определить несколько иерархически упорядоченных (содержащих усиливающиеся требования) профилей защиты, в максимально возможной степени использующих стандартные функциональные требования и требования доверия безопасности.

Выделение некоторого подмножества из всего множества профилей защиты во многом носит субъективный характер. По целому ряду соображений (одним из которых является желание придерживаться объектно-ориентированного подхода) целесообразно, на наш взгляд, сформировать сначала отправную точку классификации, выделив базовый (минимальный) ПЗ, а дополнительные требования компоновать в функциональные пакеты.

Функциональный пакет - это неоднократно используемая совокупность компонентов, объединенных для достижения определенных целей безопасности. "Общие критерии" не регламентируют структуру пакетов, процедуры верификации, регистрации и т.п., отводя им роль технологического средства формирования ПЗ.

Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) возможностям. Производные профили получаются из базового путем добавления необходимых пакетов расширения, то есть подобно тому, как создаются производные классы в объектно-ориентированных языках программирования.

Функциональные требования сгруппированы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в "Общих критериях" представлено 11 функциональных классов, 66 семейств, 135 компонентов. Это, конечно, значительно больше, чем число аналогичных сущностей в "Оранжевой книге".

Перечислим классы функциональных требований ОК:

1. идентификация и аутентификация;

2. защита данных пользователя;

3. защита функций безопасности (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);

4. управление безопасностью (требования этого класса относятся к управлению атрибутами и параметрами безопасности);

5. аудит безопасности (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);

6. доступ к объекту оценки;

7. приватность (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);

8. использование ресурсов (требования к доступности информации);

9. криптографическая поддержка (управление ключами);

10. связь (аутентификация сторон, участвующих в обмене данными);

11. доверенный маршрут/канал (для связи с сервисами

безопасности).

"Общие критерии" - очень продуманный и полный документ с точки зрения функциональных требований. В то же время, хотелось бы обратить внимание и на некоторые недостатки.

Первый - это отсутствие объектного подхода. Функциональные требования не сгруппированы в осмысленные наборы (объектные интерфейсы), к которым могло бы применяться наследование. Подобное положение, как известно из технологии программирования, чревато появлением слишком большого числа комбинаций функциональных компонентов, несопоставимых между собой.

В современном программировании ключевым является вопрос накопления и многократного использования знаний. Стандарты - одна из форм накопления знаний. Подход в ОК сужает круг фиксируемых знаний, усложняет их корректное использование.

К сожалению, в "Общих критериях" отсутствуют архитектурные требования, что является естественным следствием программистского подхода "снизу вверх". Технологичность средств безопасности, следование общепризнанным рекомендациям по протоколам и программным интерфейсам, а также апробированным архитектурным решениям, таким как менеджер/агент, - необходимые качества изделий информационных технологий, предназначенных для поддержки критически важных функций, к числу которых, безусловно, относятся функции безопасности. Без рассмотрения интерфейсных аспектов системы оказываются нерасширяемыми и изолированными. С практической точки зрения это недопустимо.

Каждый элемент требований доверия принадлежит одному из трех типов:

1. действия разработчиков;

2. представление и содержание свидетельств;

3. действия оценщиков.

Всего в ОК 10 классов, 44 семейства, 93 компонента требований доверия безопасности.
Перечислим классы:

1. разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации);

2. поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки);

3. тестирование;

4. оценка уязвимостей (включая оценку стойкости функций безопасности);

5. поставка и эксплуатация;

6. управление конфигурацией;

7. руководства (требования к эксплуатационной документации);

8. поддержка доверия (для поддержки этапов жизненного цикла после сертификации);

9. оценка профиля защиты;

10. оценка задания по безопасности.

6. Руководящие документы по защите от несанкционированного доступа Гостехкомиссии при Президенте РФ.

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

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

1. Защита СВТ обеспечивается комплексом программно-технических средств.

2. Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

3. Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

4. Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).

5. 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.

6. 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.

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

Основными функциями СРД являются:

1. реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;

2. реализация ПРД субъектов и их процессов к устройствам создания твердых копий;

3. изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;

4. управление потоками данных с целью предотвращения записи данных на носители несоответствующего грифа;

5. 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:

1. идентификацию и опознание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;

2. регистрацию действий субъекта и его процесса;

3. предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;

4. реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление после НСД;

5. тестирование;

6. очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;

7. учет выходных печатных и графических форм и твердых копий в АС;

8. 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:

1. степень полноты охвата ПРД реализованной СРД и ее качество;

2. состав и качество обеспечивающих средств для СРД;

3. гарантии правильности функционирования СРД и обеспечивающих ее средств.

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:

1. первая группа содержит только один седьмой класс;
2. вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
3. третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
4. четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

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.

2. Практическое задание

Изучить в интернете один из основополагающих документов, рассмотренных выше и составить краткий конспект этого документа.

3. Содержание отчета

1. Титульный лист
2. Содержание
3. Практическое задание
4. Конспект документа
5. Выводы

ПРАКТИЧЕСКАЯ РАБОТА № 2

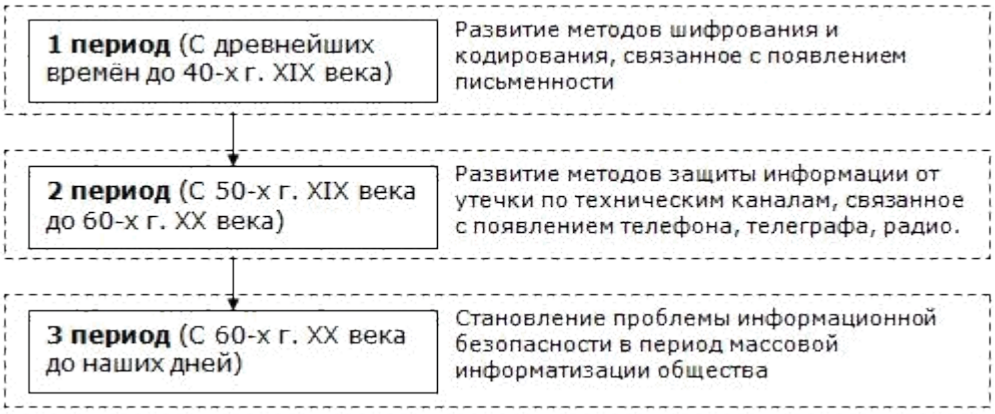
«Обеспечение информационной безопасности в ведущих зарубежных странах»

Цель работы: ознакомление с основными принципами обеспечения информационной безопасности в ведущих зарубежных странах.

1. Теоретическая часть

Обеспечение защиты информации волновало человечество всегда. В процессе эволюции цивилизации менялись виды информации, для её защиты применялись различные методы и средства.

Процесс развития средств и методов защиты информации можно разделить на три относительно самостоятельных периода:



Наблюдаемые в последние годы тенденции в развитии информационных технологий могут уже в недалеком будущем привести к появлению качественно новых (информационных) форм борьбы, в том числе и на межгосударственном уровне, которые могут принимать форму информационной войны, а сама информационная война станет одним из основных инструментов внешней политики, включая защиту государственных интересов и реализацию любых форм агрессии. Это является одной из причин, почему полезно ознакомиться с основными принципами обеспечения ИБ в ведущих зарубежных странах.

Другая причина заключается в том, что большинство применяемых на территории РФ средств и методов обеспечения ИБ основаны на импортных методиках и строятся из импортных компонентов, которые были разработаны в соответствии с нормами и требованиями по обеспечению ИБ стран-изготовителей. В связи с этим, прежде чем приступить к изучению непосредственно технологий и средств обеспечения ИБ, следует познакомиться с политикой ИБ ведущих зарубежных стран.

2. Практическое задание

1. Подготовить краткий доклад по заданному вопросу (см. вариант), используя учебное пособие Аверченкова, В.И. «Системы защиты информации в ведущих зарубежных странах» и другие доступные источники информации.
2. Заполнить таблицу «Системы обеспечения ИБ в ведущих зарубежных странах» (см. вариант) на основе подготовленного материала, а также докладов других студентов.
3. Провести анализ собранной информации и сделать выводы.

3. Содержание отчета

1. Титульный лист
2. Содержание
3. Практическое задание
4. Таблица «Системы обеспечения ИБ в ведущих зарубежных странах»

5. Выводы

4. Варианты

Вариант – номер по списку в журнале.

Вариант	Страна	Основные принципы обеспечения ИБ	Основные документы в области обеспечения ИБ	Структура государственных органов обеспечения национальной ИБ
1	**США**			
2	**Италия**			
3	**Великобритания**			
4	**Швеция**			
5	**Франция**			
6	**Германия**			
7	**Китай**			
8	**Япония**			
9	**Швейцария**			
10	**Испания**			
11	**Канада**			
12	**Австралия**			
13	**Бразилия**			
14	**Аргентина**			
15	**Корея**			

ПРАКТИЧЕСКАЯ РАБОТА № 3

«Пакеты антивирусных программ»

Цель работы: ознакомление с основными функциями, достоинствами и недостатками современного антивирусного ПО.

1. Теоретическая часть

На сегодняшний день перечень доступных антивирусных программ весьма обширен. Они различаются как по цене, так и по своим функциональным возможностям. Наиболее мощные (и, как правило, наиболее дорогие) антивирусные программы представляют собой на самом деле пакеты специализированных утилит, способных при совместном их использовании обеспечить разностороннюю защиту компьютерной системы.

Большинство современных антивирусных пакетов выполняют следующие функции:

- сканирование памяти и содержимого дисков;
- сканирование в реальном режиме времени с помощью резидентного модуля;

- распознавание поведения, характерного для компьютерных вирусов;
- блокировка и/или удаление выявленных вирусов;
- восстановление зараженных информационных объектов;
- принудительная проверка подключенных к корпоративной сети компьютеров;
- удаленное обновление антивирусного программного обеспечения и баз данных через Интернет;
- фильтрация трафика Интернета на предмет выявления вирусов в передаваемых программах и документах;
- выявление потенциально опасных Java-апплетов и модулей ActiveX;
- ведение протоколов, содержащих информацию о событиях, касающихся антивирусной защиты и др.

2. Практическое задание

1. Подготовить краткий доклад по заданному вопросу (см. вариант), используя любые доступные источники информации.

Рекомендация: Собранный материал будет наиболее актуальным, если включить в него данные, полученные практическим путем. Для этого при возможности, установите демонстрационную версию заданного пакета ПО и протестируйте ее в течении нескольких дней.

2. Заполнить таблицу «Пакеты антивирусных программ» на основе подготовленного материала, а также докладов других студентов.

3. Провести анализ собранной информации и сделать выводы.

3. Содержание отчета

1. Титульный лист
2. Содержание
3. Практическое задание
4. Таблица "Пакеты антивирусных программ"
5. Выводы

4. Варианты

Вариант – номер по списку в журнале.

Пакет антивирусного ПО	Основные функции	Достоинства	Недостатки

Антивирус Касперского			
Антивирус Dr.Web для Windows			
Panda Antivirus			
ESET NOD32 Антивирус			
avast! Free Antivirus			
Avira AntiVir Personal			
Norton AntiVirus			
Trend Micro Internet Security			
Microsoft Security Essentials			
McAfee VirusScan			

Список использованных источников и рекомендуемой литературы:

1. **Аверченков В.И.** Системы защиты информации в ведущих зарубежных странах – М. : ФЛИНТА, 2011. – 224 с.
2. **Гатчин Ю.А., Климова Е.В**. Основы информационной безопасности: учебное пособие. – СПб: СПбГУ ИТМО, 2009. – 84 с.

3. **Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.** Технические средства и методы защиты информации: Учебник для вузов / – М.: ООО «Издательство Машиностроение», 2009 – 508 с.
4. **Нестеров С. А**. Информационная безопасность и защита информации: Учеб. пособие. – СПб.: Изд-во Политехн. ун-та, 2009. – 126 с.
5. **Чефранова А.О., Игнатов В.В., Уривский А.В. и др**. Технология построения VPN: курс лекций: Учебное пособие.- Москва: Прометей, 2009. -180 с.
6. **Шаньгин В. Ф.** Защита информации в компьютерных системах и сетях - М: ДМК Пресс, 2012. - 596 с.
7. Федеральный закон «Об информации, информатизации и защите информации». Собрание законодательства Российской Федерации 20.02.1995г.: Официальное издание. – М.: Юридическая литература; Администрация Президента Российской Федерации, 1995. – с. 1213-1225.
8. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 3 «Методы менеджмента безопасности информационных технологий».
9. Международный стандарт ISO/IEC 27000:2005 Информационные технологии. Методы обеспечения безопасности. Определения и основные принципы./ http://www.27000.org/
10. Международный стандарт. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы правления информационной безопасностью. Требования (BS 7799-2:2005)./ http://www.27000.org/
11. Международный стандарт. ISO/IEC 27002:2005 Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью./ http://www.27000.org/
12. Международный стандарт. ISO/IEC 27003:2005 Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью./ http://www.27000.org/
13. Международный стандарт. ISO/IEC 27004:2005 Информационные технологии. Методы обеспечения безопасности. Измерение эффективности системы управления информационной безопасностью./ http://www.27000.org/
14. Международный стандарт. ISO/IEC 27005:2005 Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности./ http:// www.27000.org/

15. Международный стандарт. ISO/IEC 27006:2005 Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью./ http://www.27000.org/
16. Международный стандарт. ISO/IEC 27007:2005 Информационные технологии. Методы обеспечения безопасности. Руководство для аудитора систем управления информационной безопасностью./ http://www.27000.org/