МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

БЕЗОПАСНОСТЬ СЕТЕЙ ЭВМ

Методические указания по выполнению практических работ
для студентов направления подготовки бакалавриата
10.03.01«Информационная безопасность»

Курск 2017

УДК 621.(076.1)

Составитель: А.Г. Спеваков

Рецензент

Кандидат технических наук, доцент кафедры
«Информационная безопасность» И.В. Калуцкий

Безопасность сетей ЭВМ [Текст]: методические рекомендации по выполнению практических работ/ Юго-Зап. гос. ун-т; сост.: А.Г. Спеваков. – Курск, 2017. – 14 с.: ил. 3. – Библиогр.: с. 14.

Содержат сведения по вопросам практических работ безопасности сетей ЭВМ. Указывается порядок выполнения практических работ, правила содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов направления подготовки бакалавриата 10.03.01 «Информационная безопасность».

Текст печатается в авторской редакции

Подписано в печать . Формат 60х84 1/16.
Усл.печ. л. 1,92. Уч.-изд. л. 1,74. Тираж 100 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г.Курск, ул. 50 лет Октября, 94.

Практическая работа №1
«Стандарты информационной безопасности. Стандарты ISO/IEC 17799:2002 (BS 7799:2000)»

Роль стандартов и спецификаций. Наиболее важные стандарты и спецификации в области информационной безопасности

Специалистам в области информационной безопасности (ИБ) сегодня почти невозможно обойтись без знаний соответствующих стандартов и спецификаций. На то имеется несколько причин.

Формальная состоит в том, что необходимость следования некоторым стандартам (например, криптографическим и/или Руководящим документам Гостехкомиссии России) закреплена законодательно. Однако наиболее убедительны содержательные причины. Во-первых, стандарты и спецификации - одна из форм накопления знаний, прежде всего о процедурном и программно-техническом уровнях ИБ. В них зафиксированы апробированные, высококачественные решения и методологии, разработанные наиболее квалифицированными специалистами. Во-вторых, и те, и другие являются основным средством обеспечения взаимной совместимости аппаратно-программных систем и их компонентов, причем в Internet-сообществе это средство действительно работает, и весьма эффективно.

Отмеченная роль стандартов зафиксирована в основных понятиях закона РФ "О техническом регулировании" от 27 декабря 2002 года под номером 184-ФЗ (принят Государственной Думой 15 декабря 2002 года):

стандарт - документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения;

стандартизация - деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в

сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг.

Примечательно также, что в число принципов стандартизации, провозглашенных в статье 12 упомянутого закона, входит принцип применения международного стандарта как основы разработки национального, за исключением случаев, если "такое применение признано невозможным вследствие несоответствия требований международных стандартов климатическим и географическим особенностям Российской Федерации, техническим и (или) технологическим особенностям или по иным основаниям, либо Российская Федерация, в соответствии с установленными процедурами, выступала против принятия международного стандарта или отдельного его положения". С практической точки зрения, количество стандартов и спецификаций (международных, национальных, отраслевых и т.п.) в области информационной безопасности бесконечно. В курсе рассматриваются наиболее важные из них, знание которых необходимо всем или почти всем разработчикам и оценщикам защитных средств, многим сетевым и системным администраторам, руководителям соответствующих подразделений, пользователям.

Отбор проводился таким образом, чтобы охватить различные аспекты информационной безопасности, разные виды и конфигурации информационных систем (ИС), предоставить полезные сведения для самых разнообразных групп целевой аудитории.

На верхнем уровне можно выделить две существенно отличающиеся друг от друга группы стандартов и спецификаций:

оценочные стандарты, предназначенные для оценки и классификации информационных систем и средств защиты по требованиям безопасности;

спецификации, регламентирующие различные аспекты реализации и использования средств и методов защиты.

Эти группы, разумеется, не конфликтуют, а дополняют друг друга. Оценочные стандарты описывают важнейшие, с точки зрения информационной безопасности, понятия и аспекты ИС,

играя роль организационных и архитектурных спецификаций. Другие спецификации определяют, как именно строить ИС предписанной архитектуры и выполнять организационные требования.

Из числа оценочных необходимо выделить стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем" и его интерпретацию для сетевых конфигураций, "Гармонизированные критерии Европейских стран", международный стандарт "Критерии оценки безопасности информационных технологий" и, конечно, Руководящие документы Гостехкомиссии России. К этой же группе относится и Федеральный стандарт США "Требования безопасности для криптографических модулей", регламентирующий конкретный, но очень важный и сложный аспект информационной безопасности.

Технические спецификации, применимые к современным распределенным ИС, создаются, главным образом, "Тематической группой по технологии Internet" (Internet Engineering Task Force, IETF) и ее подразделением - рабочей группой по безопасности. Ядром рассматриваемых технических спецификаций служат документы по безопасности на IP-уровне (IPsec). Кроме этого, анализируется защита на транспортном уровне (Transport Layer Security, TLS), а также на уровне приложений (спецификации GSS-API, Kerberos). Необходимо отметить, что Internet-сообщество уделяет должное внимание административному и процедурному уровням безопасности ("Руководство по информационной безопасности предприятия", "Как выбирать поставщика Интернет-услуг", "Как реагировать на нарушения информационной безопасности").

В вопросах сетевой безопасности невозможно разобраться без освоения спецификаций X.800 "Архитектура безопасности для взаимодействия открытых систем", X.500 "Служба директорий: обзор концепций, моделей и сервисов" и X.509 "Служба директорий: каркасы сертификатов открытых ключей и атрибутов".

Британский стандарт BS 7799 "Управление информационной безопасностью. Практические правила", полезный для

руководителей организаций и лиц, отвечающих за информационную безопасность, без сколько-нибудь существенных изменений воспроизведен в международном стандарте ISO/IEC 17799.

Таков, на наш взгляд, "стандартный минимум", которым должны активно владеть все действующие специалисты в области информационной безопасности.

Краткие сведения о стандартах и спецификациях

Первым оценочным стандартом, получившим международное признание и оказавшим исключительно сильное влияние на последующие разработки в области информационной безопасности, стал стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем" (Department of Defense Trusted Computer System Evaliation Criteria, TCSEC), более известный (по цвету обложки) под названием "Оранжевая книга".

Без преувеличения можно утверждать, что в "Оранжевой книге" заложен понятийный базис ИБ. Достаточно лишь перечислить содержащиеся в нем понятия: безопасная и доверенная системы, политика безопасности, уровень гарантированности, подотчетность, доверенная вычислительная база, монитор обращений, ядро и периметр безопасности. Исключительно важно и выделение таких аспектов политики безопасности, как добровольное (дискреционное) и принудительное (мандатное) управление доступом, безопасность повторного использования объектов. Последним по порядку, но отнюдь не по значению следует назвать принципы классификации по требованиям безопасности на основе параллельного ужесточения требований к политике безопасности и уровню гарантированности.

После "Оранжевой книги" была выпущена целая "Радужная серия". С концептуальной точки зрения, наиболее значимый документ в ней - "Интерпретация "Оранжевой книги" для сетевых конфигураций" (Trusted Network Interpretation). Он состоит из двух частей. Первая содержит собственно интерпретацию, во второй

описываются сервисы безопасности, специфичные или особенно важные для сетевых конфигураций.

Важнейшее понятие, введенное в первой части, - сетевая доверенная вычислительная база. Другой принципиальный аспект - учет динамичности сетевых конфигураций. Среди защитных механизмов выделена криптография, помогающая поддерживать как конфиденциальность, так и целостность.

Новым для своего времени стал систематический подход к вопросам доступности, формирование архитектурных принципов ее обеспечения.

Упомянем также достаточное условие корректности фрагментирования монитора обращений, являющееся теоретической основой декомпозиции распределенной ИС в объектно-ориентированном стиле в сочетании с криптографической защитой коммуникаций.

Переходя к знакомству с "Гармонизированными критериями Европейских стран", отметим отсутствие в них априорных требований к условиям, в которых должна работать информационная система. Предполагается, что сначала формулируется цель оценки, затем орган сертификации определяет, насколько полно она достигается, т. е. в какой мере корректны и эффективны архитектура и реализация механизмов безопасности в конкретной ситуации. Чтобы облегчить формулировку цели оценки, стандарт содержит описание десяти примерных классов функциональности, типичных для правительственных и коммерческих систем.

В "Гармонизированных критериях" подчеркивается различие между системами и продуктами информационных технологий, но для унификации требований вводится единое понятие - объект оценки.

Важно указание и на различие между функциями (сервисами) безопасности и реализующими их механизмами, а также выделение двух аспектов гарантированности - эффективности и корректности средств безопасности. Руководящие документы (РД) Гостехкомиссии России начали появляться несколько позже, уже после опубликования "Гармонизированных критериев", и, по аналогии с

последними, подтверждают разницу между автоматизированными системами (АС) и продуктами (средствами вычислительной техники, СВТ), но в общем и целом они долгое время следовали в фарватере "Оранжевой книги".

Первое примечательное отклонение от этого курса произошло в 1997 году, когда был принят РД по отдельному сервису безопасности - межсетевым экранам (МЭ). Его основная идея - классифицировать МЭ на основании осуществляющих фильтрацию потоков данных уровней эталонной семиуровневой модели - получила международное признание и продолжает оставаться актуальной.

В 2002 году Гостехкомиссия России приняла в качестве РД русский перевод международного стандарта ISO/IEC 15408:1999 "Критерии оценки безопасности информационных технологий", что послужило толчком для кардинальной и весьма своевременной со всех точек зрения переориентации (вспомним приведенный выше принцип стандартизации из закона "О техническом регулировании"). Конечно, переход на рельсы "Общих критериев" будет непростым, но главное, что он начался.

Среди технических спецификаций на первое место, безусловно, следует поставить документ X.800 "Архитектура безопасности для взаимодействия открытых систем". Здесь выделены важнейшие сетевые сервисы безопасности: аутентификация, управление доступом, обеспечение конфиденциальности и/или целостности данных, а также невозможность отказаться от совершенных действий. Для реализации сервисов предусмотрены следующие сетевые механизмы безопасности и их комбинации: шифрование, электронная цифровая подпись (ЭЦП), управление доступом, контроль целостности данных, аутентификация, дополнение трафика, управление маршрутизацией, нотаризация. Выбраны уровни эталонной семиуровневой модели, на которых могут быть реализованы сервисы и механизмы безопасности. Наконец, детально рассмотрены вопросы администрирования средств безопасности для распределенных конфигураций.

Спецификация Internet-сообщества RFC 1510 "Сетевой сервис аутентификации Kerberos (V5)" относится к более частной, но весьма важной и актуальной проблеме - аутентификации в разнородной распределенной среде с поддержкой концепции единого входа в сеть. Сервер аутентификации Kerberos представляет собой доверенную третью сторону, владеющую секретными ключами обслуживаемых субъектов и помогающую им в попарной проверке подлинности. О весомости данной спецификации свидетельствует тот факт, что клиентские компоненты Kerberos присутствуют в большинстве современных операционных систем. Далее предполагается, что читатель свободно разбирается в особенностях, охарактеризованных выше стандартов и спецификаций.

Краткие аннотации подробно рассматриваемых в курсе стандартов и спецификаций

"Гармонизированные критерии Европейских стран" стали весьма передовым документом для своего времени, они подготовили появление международного стандарта ISO/IEC 15408:1999 "Критерии оценки безопасности информационных технологий" (Evaluationcriteria for IT security), в русскоязычной литературе обычно (но не совсем верно) именуемого "Общими критериями" (ОК).

На сегодняшний день "Общие критерии" - самый полный и современный оценочный стандарт. На самом деле, это метастандарт, определяющий инструменты оценки безопасности ИС и порядок их использования; он не содержит предопределенных классов безопасности. Такие классы можно строить, опираясь на заданные требования.

ОК содержат два основных вида требований безопасности:

функциональные, соответствующие активному аспекту защиты, предъявляемые к *функциям (сервисам) безопасности* и реализующим их механизмам;

требования доверия, соответствующие пассивному аспекту; они предъявляются к технологии и процессу разработки и эксплуатации.

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

Подчеркнем, что безопасность в ОК рассматривается не статично, а в соответствии с жизненным циклом объекта оценки. Кроме того, последний предстает в контексте среды безопасности, характеризующейся определенными условиями и угрозами.

"Общие критерии" способствуют формированию двух базовых видов используемых на практике нормативных документов - это профиль защиты и задание по безопасности.

Профиль защиты представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса.

Задание по безопасности содержит совокупность требований к конкретной разработке, их выполнение позволит решить поставленные задачи по обеспечению безопасности.

В последующей части курса будут детально рассмотрены как сами "Общие критерии", так и разработанные на их основе профили защиты, и проекты профилей.

Криптография – область специфическая, но общее представление о ее месте в архитектуре безопасности и о требованиях к криптографическим компонентам иметь необходимо. Для этого целесообразно ознакомиться с Федеральным стандартом США FIPS 140-2 "Требования безопасности для криптографических модулей" (Security Requirements for Cryptographic Modules). Он выполняет организующую функцию, описывая внешний интерфейс криптографического модуля, общие требования к подобным модулям и их окружению. Наличие такого стандарта упрощает разработку сервисов безопасности и профилей защиты для них.

Криптография как средство реализации сервисов безопасности имеет две стороны: алгоритмическую и интерфейсную. Нас будет интересовать исключительно интерфейсный аспект, поэтому, наряду со стандартом FIPS 140-2, мы рассмотрим предложенную в рамках Internet-сообщества

техническую спецификацию "Обобщенный прикладной программный интерфейс службы безопасности" (GenericSecurity Service Application Program Interface, GSS-API).

Интерфейс безопасности GSS-API предназначен для защиты коммуникаций между компонентами программных систем, построенных в архитектуре клиент/сервер. Он создает условия для взаимной аутентификации общающихся партнеров, контролирует целостность пересылаемых сообщений и служит гарантией их конфиденциальности. Пользователями интерфейса безопасности GSS-API являются коммуникационные протоколы (обычно прикладного уровня) или другие программные системы, самостоятельно выполняющие пересылку данных.

Технические спецификации IPsec [IPsec] имеют, без преувеличения, фундаментальное значение, описывая полный набор средств обеспечения конфиденциальности и целостности на сетевом уровне. Для доминирующего в настоящее время протокола IP версии 4 они носят факультативный характер; в перспективной версии IPv6 их реализация обязательна. На основе IPsec строятся защитные механизмы протоколов более высокого уровня, вплоть до прикладного, а также законченные средства безопасности, в том числе виртуальные частные сети. Разумеется, IPsec существенным образом опирается на криптографические механизмы и ключевую инфраструктуру.

Точно так же характеризуются и средства безопасности транспортного уровня (Transport Layer Security, TLS). Спецификация TLSразвивает и уточняет популярный протокол Secure Socket Layer (SSL), используемый в большом числе программных продуктов самого разного назначения.

В упомянутом выше инфраструктурном плане очень важны рекомендации X.500 "Служба директорий: обзор концепций, моделей и сервисов" (The Directory: Overview of concepts, models and services) и X.509 "Служба директорий: каркасы сертификатов открытых ключей и атрибутов" (The Directory: Public-key and attribute certificate frameworks). В рекомендациях X.509 описан формат сертификатов открытых ключей и атрибутов

- базовых элементов инфраструктур открытых ключей и управления привилегиями.

Как известно, обеспечение информационной безопасности - проблема комплексная, требующая согласованного принятия мер на законодательном, административном, процедурном и программно-техническом уровнях. При разработке и реализации базового документа административного уровня – политики безопасности организации – отличным подспорьем может стать рекомендация Internet-сообщества "Руководство по информационной безопасности предприятия" (Site Security Handbook). В нем освещаются практические аспекты формирования политики и процедур безопасности, поясняются основные понятия административного и процедурного уровней, содержится мотивировка рекомендуемых действий, затрагиваются темы анализа рисков, реакции на нарушения ИБ и действий после ликвидации нарушения. Более подробно последние вопросы рассмотрены в рекомендации "Как реагировать на нарушения информационной безопасности" (Expectations for Computer Security Incident Response). В этом документе можно найти и ссылки на полезные информационные ресурсы, и практические советы процедурного уровня.

При развитии и реорганизации корпоративных информационных систем, несомненно, окажется полезной рекомендация "Как выбирать поставщика Internet-услуг" (Site Security Handbook Addendum for ISPs). В первую очередь ее положений необходимо придерживаться в ходе формирования организационной и архитектурной безопасности, на которой базируются прочие меры процедурного и программно-технического уровней.

Для практического создания и поддержания режима информационной безопасности с помощью регуляторов административного и процедурного уровней пригодится знакомство с британским стандартом BS 7799 "Управление информационной безопасностью. Практические правила" (Code of practice for information security management) и его второй частью BS 7799-2:2002 "Системы управления информационной безопасностью - спецификация с руководством по использованию"

(Information security managementsystems - Specification with guidance for use). В нем разъясняются такие понятия и процедуры, как политика безопасности, общие принципы организации защиты, классификация ресурсов и управление ими, безопасность персонала, физическая безопасность, принципы администрирования систем и сетей, управление доступом, разработка и сопровождение ИС, планирование бесперебойной работы организации.

Можно видеть, что отобранные для курса стандарты и спецификации затрагивают все уровни информационной безопасности, кроме законодательного. Далее мы приступим к их детальному рассмотрению.

Обзор стандарта BS 7799

Продолжая рассмотрение стандартов и спецификаций, относящихся к административному и процедурному уровням информационной безопасности, мы приступаем к изучению двух частей британского стандарта BS 7799, фактически имеющего статус международного (ISO/IEC 17799). Русский перевод первой части опубликован в качестве приложения к информационному бюллетеню Jet Info.

Первая часть стандарта, по-русски именуемая "Управление информационной безопасностью". Практические правила", содержит систематический, весьма полный, универсальный перечень регуляторов безопасности, полезный для организации практически любого размера, структуры и сферы деятельности. Она предназначена для использования в качестве справочного документа руководителями и рядовыми сотрудниками, отвечающими за планирование, реализацию и поддержание внутренней системы информационной безопасности.

Согласно стандарту, цель информационной безопасности - обеспечить бесперебойную работу организации, по возможности предотвратить и/или минимизировать ущерб от нарушений безопасности.

Управление информационной безопасностью позволяет коллективно использовать данные, одновременно обеспечивая их защиту и защиту вычислительных ресурсов.

Подчеркивается, что защитные меры оказываются значительно более дешевыми и эффективными, если они заложены в информационные системы и сервисы на стадиях задания требований и проектирования.

Предлагаемые в первой части стандарта *регуляторы безопасности* разбиты на десять групп:

политика безопасности;

общеорганизационные аспекты защиты;

классификация активов и управление ими;

безопасность персонала;

физической безопасности и безопасность окружающей среды;

администрирование систем и сетей;

управление доступом к системам и сетям;

разработка и сопровождение информационных систем;

управление бесперебойной работой организации;

контроль соответствия требованиям.

В стандарте выделяется десять ключевых регуляторов, которые либо являются обязательными в соответствии с действующим законодательством, либо считаются основными структурными элементами информационной безопасности. К ним относятся:

документ о политике информационной безопасности;

распределение обязанностей по обеспечению информационной безопасности;

обучение и подготовка персонала к поддержанию режима информационной безопасности;

уведомление о случаях нарушения защиты;

антивирусные средства;

процесс планирования бесперебойной работы организации;

контроль за копированием программного обеспечения, защищенного законом об авторском праве;

защита документации;

защита данных;

контроль соответствия политике безопасности.

Для обеспечения повышенного уровня защиты особо ценных ресурсов или оказания противодействия злоумышленнику с исключительно высоким потенциалом нападения могут

потребоваться другие (более сильные) средства, которые в стандарте не рассматриваются.

Следующие факторы выделены в качестве определяющих для успешной реализации системы информационной безопасности в организации:

цели безопасности и ее обеспечение должны основываться на производственных задачах и требованиях. Функции управления безопасностью должно взять на себя руководство организации;

необходима явная поддержка и приверженность к соблюдению режима безопасности со стороны высшего руководства;

требуется хорошее понимание рисков (как угроз, так и уязвимостей), которым подвергаются активы организации, и адекватное представление о ценности этих активов;

необходимо ознакомление с системой безопасности всех руководителей и рядовых сотрудников организации.

Во второй части стандарта BS 7799-2:2002 "Системы управления информационной безопасностью - спецификация с руководством по использованию" предметом рассмотрения, как следует из названия, является система управления информационной безопасностью.

Под *системой управления информационной безопасностью* (СУИБ) (Information Security Management System, ISMS) понимается часть общей системы управления, базирующаяся на анализе рисков и предназначенная для проектирования, реализации, контроля, сопровождения и совершенствования мер в области информационной безопасности. Эту систему составляют организационные структуры, политика, действия по планированию, обязанности, процедуры, процессы и ресурсы.

В основу процесса управления положена четырехфазная модель, включающая:

планирование;

реализацию;

оценку;

корректировку.

По-русски данную модель можно назвать ПРОК (в оригинале - Plan-Do-Check-Act, PDCA). Детальный анализ каждой из выделенных фаз и составляет основное содержание стандарта BS 7799-2:2002.

Тест

1. Первым оценочным стандартом, получившим международное признание и оказавшим исключительно сильное влияние на последующие разработки в области информационной безопасности, стал стандарт более известный (по цвету обложки) под названием ...

а) "Оранжевая книга"

б) "Синяя книга"

в) "Красная книга"

г) "Зеленая книга"

2. В основу процесса управления положена ... модель:

а) двухфазная

б) трехфазная

в) четырехфазная

г) пятифазная

3. На сколько групп разбиты предлагаемые в первой части стандарта BS 7799 регуляторы безопасности?

а) 5

б) 3

в) 8

г) 10

4. В основу процесса управления положена модель, включающая:

а) планирование, реализацию, оценку, корректировку, контроль

б) планирование, реализацию, оценку, контроль

в) планирование, оценку, корректировку, контроль

г) планирование, реализацию, оценку, корректировку

5. Первая часть стандарта BS 7799:

а) рассматривает, как следует из названия, систему управления информационной безопасностью.

б) содержит систематический, универсальный перечень регуляторов безопасности, полезный для организации практически любого размера, структуры и сферы деятельности.

6. Вторая часть стандарта BS 7799:

а) рассматривает, как следует из названия, систему управления информационной безопасностью.

б) содержит систематический, универсальный перечень регуляторов безопасности, полезный для организации практически любого размера, структуры и сферы деятельности.

7. В "Гармонизированных критериях" подчеркивается различие между ..... информационных технологий, но для унификации требований вводится единое понятие - объект оценки.

а) системами и продуктами

б) типами и особенностями

в) видами и подвидами

г) сложностями

8. В каком году Гостехкомиссия России приняла в качестве РД русский перевод международного стандарта ISO/IEC 15408:1999 "Критерии оценки безопасности информационных технологий"?

а) 2000

б) 2002

в) 2003

г) 2005

9. Основная идея РД по отдельному сервису безопасности - межсетевым экранам (МЭ)

а) Классифицировать МЭ на основании осуществляющих фильтрацию потоков данных уровней эталонной семиуровневой модели

б) Различить системы информационных технологий, но для унификации требований уровней эталонной семиуровневой модели

в) Классифицировать МЭ на эффективности и корректности средств безопасности

10. Согласно закону "О техническом регулировании", принципом стандартизации является

а) применение международного стандарта как основы разработки национального стандарта

б) приоритет национальных законодательных и технических актов

в) обеспечение конкурентоспособности российских товаров и услуг на мировом рынке

11. В стандарте BS 7799 не разъясняется следующие понятия или процедуры:

а) безопасность интерфейсов
б) безопасность персонала
в) физическая безопасность

12. Спецификация TLS близка к
а) SSH
б) DNS
в) SSL

13. Сервер аутентификации Kerberos представляет собой ..., владеющую секретными ключами обслуживаемых субъектов и помогающую им в попарной проверке подлинности.
а) одну из сторон
б) третью сторону
в) вторую сторону
г) основную сторону

Темы рефератов

1. Критерий оценки надежности компьютерных систем «Оранжевая книга» (США);
2. Гармонизированные критерии европейских стран;
3. Рекомендации X.800;
4. Германский стандарт BSI;
5. Британский стандарт BS 7799;
6. Стандарт ISO 17799;
7. Стандарт «Общие критерии» ISO 15408;
8. Стандарт COBIT

Практическая работа №2
«Исследование функциональных характеристик локальной вычислительной сети»

Часто администраторы сетей испытывают неудобства, из-за того, что количество централизовано выделенных им номеров сетей недостаточно для того, чтобы структурировать сеть надлежащим образом, например, разместить все слабо взаимодействующие компьютеры по разным сетям.

В такой ситуации возможны два пути. Первый из них связан с получением от NIC дополнительных номеров сетей. Второй способ, употребляющийся более часто, связан с использованием так называемых *масок*, которые позволяют разделять одну сеть на несколько сетей.

IP-адрес – адрес компьютера (32-битное число), состоящий из: номер сети + номер компьютера в сети (адрес узла):

15.30.47.48

Маска подсети необходима для определения того, какие компьютеры находятся в той же подсети; при наложении на IP-адрес (логическая конъюнкция И) дает номер сети:

255.255.255.0 -> FF.FF.FF.0

Маска в двоичном коде всегда имеет структуру: сначала все единицы, затем все нули:

1…10…0

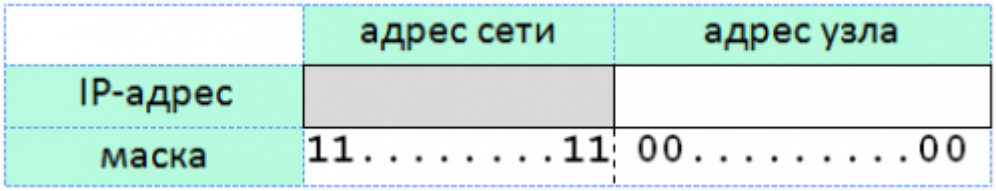

Рис. 2.1. Структура IP-адреса

На рисунке 2.1 та часть IP-адреса, которая соответствует битам маски равным единице, относится к адресу сети, а часть, соответствующая битам маски равным нулю – это числовой адрес компьютера

Таким образом, можно определить каким может быть последнее число маски:

$11111110_2 = 254$ $11100000_2 = 224$

$11111100_2 = 252$ $11000000_2 = 192$

$11111000_2 = 248$ $10000000_2 = 128$

$11110000_2 = 240$ $00000000_2 = 0$

Рис. 2.2. Возможные варианты масок

Если два узла относятся к одной сети, то адрес сети у них одинаковый.

Расчет номера сети по IP-адресу и маске сети

В маске подсети старшие биты, отведенные в IP-адресе компьютера для номера сети, имеют значение 1 (255); младшие биты, отведенные в IP-адресе компьютера для адреса компьютера в подсети, имеют значение 0.

Рис. 2.3. Расчет номера сети по IP-адресу и маске сети

Порядковый номер компьютера в сети

Рис. 2.4. Расчет номера компьютера в сети

Число компьютеров в сети

Количество компьютеров сети определяется по маске: младшие биты маски — нули — отведены в IP-адресе компьютера под адрес компьютера в подсети.

Если маска:

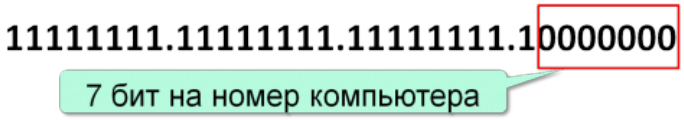

Рис. 2.5. Пример маски компьютера

$2^7 = 128$ адресов

Из них 2 специальных: адрес сети и широковещательный адрес. Значит, 128-2=126 адресов.

Задания

1. Маской подсети называется 32-разрядное двоичное число, которое определяет, какая часть IP-адреса компьютера относится к адресу сети, а какая часть IP-адреса определяет адрес компьютера в подсети. В маске подсети старшие биты, отведенные в IP-адресе компьютера для адреса сети, имеют значение 1; младшие биты, отведенные в IP-адресе компьютера для адреса компьютера в подсети, имеют значение 0.

Если маска подсети 255.255.255.224 и IP-адрес компьютера в сети 162.198.0.157, то порядковый номер компьютера в сети равен_____

2. Маской подсети называется 32-разрядное двоичное число, которое определяет, какая часть IP-адреса компьютера относится к адресу сети, а какая часть IP-адреса определяет адрес компьютера в подсети. В маске подсети старшие биты, отведенные в IP-адресе компьютера для адреса сети, имеют значение 1; младшие биты, отведенные в IP-адресе компьютера для адреса компьютера в подсети, имеют значение 0.

Если маска подсети 255.255.255.192 и IP-адрес компьютера в сети 10.18.134.220, то номер компьютера в сети равен____

3. Маской подсети называется 32-разрядное двоичное число, которое определяет, какая часть IP-адреса компьютера относится к адресу сети, а какая часть IP-адреса определяет адрес компьютера в подсети. В маске подсети старшие биты, отведенные в IP-адресе компьютера для адреса сети, имеют значение 1; младшие биты, отведенные в IP-адресе компьютера для адреса компьютера в подсети, имеют значение 0.

Если маска подсети 255.255.248.0 и IP-адрес компьютера в сети 112.154.133.208, то номер компьютера в сети равен_____

4. Маской подсети называется 32-разрядное двоичное число, которое определяет, какая часть IP-адреса компьютера относится к адресу сети, а какая часть IP-адреса определяет адрес компьютера в подсети. В маске подсети старшие биты, отведенные в IP-адресе компьютера для адреса сети, имеют значение 1; младшие биты,

отведенные в IP-адресе компьютера для адреса компьютера в подсети, имеют значение 0.

Если маска подсети 255.255.224.0 и IP-адрес компьютера в сети 206.158.124.67, то номер компьютера в сети равен_____

5. В терминологии сетей TCP/IP маской подсети называется 32-разрядное двоичное число, определяющее, какие именно разряды IP-адреса компьютера являются общими для всей подсети – в этих разрядах маски стоит 1. Обычно маски записываются в виде четверки десятичных чисел - по тем же правилам, что и IP-адреса. Для некоторой подсети используется маска 255.255.254.0. Сколько различных адресов компьютеров теоретически допускает эта маска, если два адреса (адрес сети и широковещательный) не используют?

6. В терминологии сетей TCP/IP маской подсети называется 32-разрядное двоичное число, определяющее, какие именно разряды IP-адреса компьютера являются общими для всей подсети - в этих разрядах маски стоит 1. Обычно маски записываются в виде четверки десятичных чисел - по тем же правилам, что и IP-адреса. Для некоторой подсети используется маска 255.255.255.192. Сколько различных адресов компьютеров теоретически допускает эта маска, если два адреса (адрес сети и широковещательный) не используют?

7. В терминологии сетей TCP/IP маской подсети называется 32-разрядное двоичное число, определяющее, какие именно разряды IP-адреса компьютера являются общими для всей подсети – в этих разрядах маски стоит 1. Обычно маски записываются в виде четверки десятичных чисел – по тем же правилам, что и IP-адреса. Для некоторой подсети используется маска 255.255.248.0. Сколько различных адресов компьютеров допускает эта маска?

Примечание. На практике для адресации компьютеров не используются два адреса: адрес сети и широковещательный адрес.

8. В терминологии сетей TCP/IP маской подсети называется 32-разрядное двоичное число, определяющее, какие именно

разряды IP-адреса компьютера являются общими для всей подсети - в этих разрядах маски стоит 1. Обычно маски записываются в виде четверки десятичных чисел - по тем же правилам, что и IP-адреса. Для некоторой подсети используется маска 255.255.255.128. Сколько различных адресов компьютеров теоретически допускает эта маска, если два адреса (адрес сети и широковещательный) не используют?

9. Если маска подсети 255.255.252.0 и IP-адрес компьютера в сети 226.185.90.162, то номер компьютера в сети равен_____

10. В терминологии сетей TCP/IP маской подсети называется 32-разрядное двоичное число, определяющее, какие именно разряды IP-адреса компьютера являются общими для всей подсети - в этих разрядах маски стоит 1. Обычно маски записываются в виде четверки десятичных чисел - по тем же правилам, что и IP-адреса. Для некоторой подсети используется маска 255.255.255.224. Сколько различных адресов компьютеров теоретически допускает эта маска, если два адреса (адрес сети и широковещательный) не используют?

11. Если маска подсети 255.255.240.0 и IP-адрес компьютера в сети 232.126.150.18, то номер компьютера в сети равен_____

12. В терминологии сетей TCP/IP маской называется 32-разрядная двоичная последовательность. Маска определяет, какая часть IP-адреса относится к адресу сети, а какая — к адресу самого узла. Обычно маска записывается по тем же правилам, что и IP-адрес.

Определите номер компьютера в сети, если IP-адрес компьютера — 192.112.25.5, а маска подсети — 255.255.240.0

13. В терминологии сетей TCP/IP маской называется 32-разрядная двоичная последовательность. Маска определяет, какая часть IP-адреса относится к адресу сети, а какая — к адресу самого узла. Обычно маска записывается по тем же правилам, что и IP-

адрес. Адрес сети получается в результате применения поразрядной конъюнкции к заданному IP-адресу узла и маске.

Для узла с IP-адресом 218.44.150.15 адрес сети равен 218.44.148.0. Чему равен третий слева байт маски?

14. В терминологии сетей TCP/IP маской называется 32-разрядная двоичная последовательность. Маска определяет, какая часть IP-адреса относится к адресу сети, а какая — к адресу самого узла. Обычно маска записывается по тем же правилам, что и IP-адрес.

Определите номер компьютера в сети, если IP-адрес компьютера — 140.20.110.44, а маска подсети — 255.255.252.0

15. В терминологии сетей TCP/IP маской называется 32-разрядная двоичная последовательность. Маска определяет, какая часть IP-адреса относится к адресу сети, а какая — к адресу самого узла. Обычно маска записывается по тем же правилам, что и IP-адрес. Адрес сети получается в результате применения поразрядной конъюнкции к заданному IP-адресу узла и маске.

Для узла с IP-адресом 185.12.107.15 адрес сети равен 185.12.104.0. Определите наименьшее возможное значение третьего слева байта маски.

16. В терминологии сетей TCP/IP маской называется 32-разрядная двоичная последовательность. Маска определяет, какая часть IP-адреса относится к адресу сети, а какая — к адресу самого узла. Обычно маска записывается по тем же правилам, что и IP-адрес.

Определите номер компьютера в сети, если IP-адрес компьютера — 145.16.2.196, а маска подсети — 255.255.240.0

17. В терминологии сетей TCP/IP маской называется 32-разрядная двоичная последовательность. Маска определяет, какая часть IP-адреса относится к адресу сети, а какая — к адресу самого узла. Обычно маска записывается по тем же правилам, что и IP-адрес.

Определите номер компьютера в сети, если IP-адрес компьютера — 146.146.146.146, а маска подсети — 255.255.252.0

Практическая работа №3
«Построение одноранговой сети»

Одноранговая сеть представляет собой сеть равноправных компьютеров – рабочих станций, каждая из которых имеет уникальное имя и адрес. Все рабочие станции объединяются в рабочую группу. В одноранговой сети нет единого центра управления – каждая рабочая станция сети может отвечать на запросы других компьютеров, выступая в роли сервера, и направлять свои запросы в сеть, играя роль клиента.

Одноранговые сети являются наиболее простым для монтажа и настройки, а также дешевым типом сетей. Для построения одноранговой сети требуется всего лишь несколько компьютеров с установленными клиентскими ОС, и снабженных сетевыми картами. Все параметры безопасности определяются исключительно настройками каждого из компьютеров.

К основным достоинствам одноранговых сетей можно отнести:

простоту работы в них;

низкую стоимость, поскольку все компьютеры являются рабочими станциями;

относительную простоту администрирования.

Недостатки одноранговой архитектуры таковы:

эффективность работы зависит от количества компьютеров в сети;

защита информации и безопасность зависит от настроек каждого компьютера.

Серьезной проблемой одноранговой сетевой архитектуры является ситуация, когда компьютеры отключаются от сети. В этих случаях из сети исчезают все общесетевые сервисы, которые они предоставляли (например, общая папка на диске отключенного компьютера, или общий принтер, подключенный к нему). Администрировать такую сеть достаточно просто лишь при небольшом количестве компьютеров. Если же число рабочих станций, допустим, превышает 25-30 – то это будет вызывать определенные сложности.

Базовые топологии

Топология сети – физическое расположение компьютеров, кабелей и других сетевых компонентов. Она влияет на:

- состав необходимого сетевого оборудования;
- возможность расширения сети (наращиваемость);
- способ управления сетью;
- характеристики и параметры сетевого оборудования.

На практике используются следующие базовые топологии:

1 – шинная;
2 – звездообразная;
3 – кольцевая;
4 – древовидная;
5 – ячеистая.

Все остальные топологии получаются комбинированием базовых.

Темы рефератов

1. Шинная топология локальной вычислительной сети
2. Звездообразная топология локальной вычислительной сети
3. Кольцевая топология локальной вычислительной сети
4. Древовидная топология локальной вычислительной сети
5. Ячеистая топология вычислительной сети

Практическая работа №4

«Критерии оценки защищённости информационных систем»

Классы защищённости автоматизированных систем от несанкционированного доступа к информации разделены на 3 группы:

I-я группа – многопользовательские системы, которые могут одновременно обрабатывать и хранить информацию разных уровней конфиденциальности с различными правами пользователей на доступ к информации. К этой группе относится 5 классов: 1А, 1Б, 1В, 1Г и 1Д.

II-я группа – системы, в которых работает несколько пользователей с одинаковыми правами доступа ко всей информации, которая обрабатывается и хранится на носителях разного уровня конфиденциальности. К этой группе относится 2 класса: 2А и 2Б.

III-я группа – системы, в которых работает один пользователь с абсолютными правами на всю информацию, которая размещена на носителях одного уровня конфиденциальности. К этой группе относится 2 класса: 3А и ЗБ. Самые высокие требования к классу 1А, а самые низкие – к классу ЗБ.

Выделяют 4 подсистемы защиты:

управление доступом;

регистрация и учет;

криптографическое закрытие;

обеспечение целостности.

Наличие методик защиты информации и их поддержка официальными документами составляет достаточно надежную базу защиты информации на регулярной основе. Однако в сегодняшней ситуации защита информации не может быть эффективной по ряду причин:

1. Имеющиеся методики ориентированы на защиту информации только в средствах компьютерных систем, не смотря на устойчивую тенденцию органического сращивания автоматизированных и традиционных технологий обработки информации;

2. Учтены далеко не все факторы, которые оказывают существенное влияние на уязвимость информации, и поэтому и подлежат учету при определении требований к защите;

3. В научном плане имеющиеся методики недостаточно обоснованы, исключая требования к защите информации от утечки по техническим каналам.

Классы защищенности средств компьютерных систем от несанкционированного доступа

Показатели защищенности, установленные руководящими документами Гостехкомиссии, содержат требования по защите средств компьютерных систем (СКС) от несанкционированного доступа к информации.

Совокупность требований описывают классы защищенности СКС, которые делятся на 4 группы:

I-я группа содержит единственный седьмой класс – класс минимальной защищенности.

II-я группа содержит 5-й и 6-й классы – классы избирательной защиты, которая предусматривает контроль доступа определенных субъектов к определенным объектам системы. При этом для каждой соответствующей пары «субъект – объект» определяются разрешенные типы доступа.

III-я группа содержит 2, 3 и 4 классы – полномочная защита, при которой каждому субъекту и объекту системы присваиваются классификационные метки, указывающие их место в соответствующей иерархии. Решение о санкционированности запроса на доступ принимается лишь при одновременном разрешении его избирательными и полномочными правилами разграничения доступа.

IV-я группа включает только 1-й класс – верифицированная защита.

Чтобы присвоить класс защищенности у системы должно быть: руководство администратора и пользователя; тестовая и конструкторская документация.

Факторы, которые влияют на необходимый уровень защиты информации

Рассмотрим классификацию факторов, которые влияют на уровни защиты информации. Факторы классифицируются по 5 признакам:

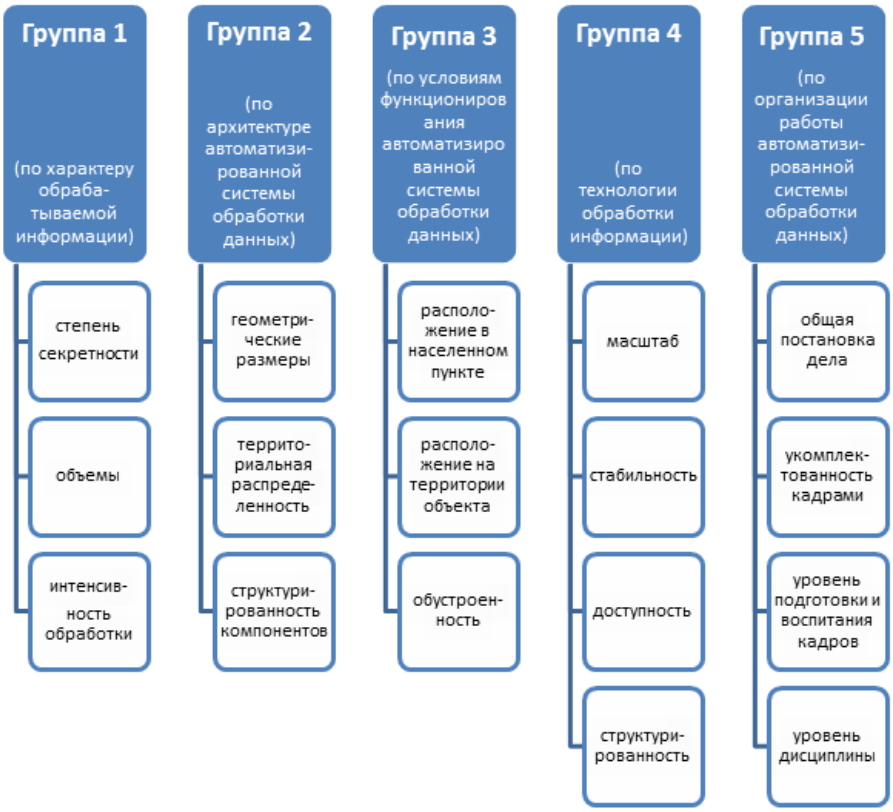

Рис. 4.1. Классификация факторов, влияющих на уровень защиты

Темы рефератов

1. Оценки защищенности на основе модели комплекса механизмов защиты.
2. Семантические показатели защищенности ИС.
3. Нечеткие оценки защищенности информационных систем.
4. Комплексные оценки защищенности ИС.