ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
Сибирский колледж транспорта и строительства

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

МДК.03.02 Безопасность компьютерных сетей
для специальности
09.02.06 Сетевое и системное администрирование

Иркутск 2022

Фонд оценочных средств разработан в соответствии с ФГОС СПО по специальности 09.02.06 Сетевое и системное администрирование, утвержденного приказом Министерства образования и науки Российской Федерации от 09.12.2016 N 1548, на основе рабочей программы дисциплины МДК.03.02 Безопасность компьютерных сетей профессионального модуля ПМ.03.

РАССМОТРЕНО:
Цикловой методической
комиссией специальности 09.02.06
Сетевое и системное
администрирование
«08» июня 2022 г.
Председатель: _____/Саквенко Т.В.

УТВЕРЖДАЮ:
Заместитель директора по УВР
_____/А.П.Ресельс
«09» июня 2022 г.

Согласовано:

Ведущий специалист «Института информационных технологий и кибербезопасности »

_____С.В. Бахвалов

Разработчик: Панина В.Е.- преподаватель Сибирского колледжа транспорта и строительства ФГБОУ ВО «Иркутский государственный университет путей сообщения»

СОДЕРЖАНИЕ

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

В результате освоения дисциплины обучающийся должен уметь: выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств, использовать схемы послеаварийного восстановления работоспособности сети, эксплуатировать технические средства сетевой инфраструктуры, осуществлять диагностику и поиск неисправностей технических средств, выполнять действия по устранению неисправностей в части, касающейся полномочий техника, тестировать кабели и коммуникационные устройства, выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, правильно оформлять техническую документацию, наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных, устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту.

В результате освоения дисциплины обучающийся должен знать: архитектуру и функции систем управления сетями, стандарты систем управления, задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией, средства мониторинга и анализа локальных сетей, классификацию регламентов, порядок технических осмотров, проверок и профилактических работ, правила эксплуатации технических средств сетевой инфраструктуры, расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры, методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных, основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем (ИС), требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных, основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем.

Общие компетенции и /или профессиональные компетенции (их компоненты, составные части, уровень освоения), формирующиеся в процессе освоения дисциплины:

Код	Название компетенций
ОК1	Выбирать способы решения задач профессиональной деятельности, применительно к различным кон текстам
ОК2	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК3	планировать и реализовывать собственное профессиональное и личностное развитие.
ОК4	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК5	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного кон текста.
ОК 6	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 9	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 11	Планировать предпринимательскую деятельность в профессиональной сфере.
ПК 3.1	Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.
ПК 3.2	Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.
ПК 3.3	Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации.

ПК 3.4	Участвовать в разработке схемы после аварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.
ПК 3.5	Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.
ПК 3.6	Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.

Программа воспитания в рабочей программе профессионального модуля отражается через содержание направлений воспитательной работы, разбитых на следующие воспитательные модули:

Модули программы воспитания	Содержание модуля программы воспитания
Модуль 1 «Профессионально-личностное воспитание»	*Цель модуля:* создание условий для удовлетворения потребностей обучающихся в интеллектуальном, культурном и нравственном развитии в сфере трудовых и социально-экономических отношений посредством профессионального самоопределения. *Задачи модуля:* – развитие общественной активности обучающихся, воспитание в них сознательного отношения к труду и народному достоянию; – формирование у обучающихся потребности трудиться, добросовестно, ответственно и творчески относиться к разным видам трудовой деятельности. – формирование профессиональных компетенций; – формирование осознания профессиональной идентичности (осознание своей принадлежности к определённой профессии и профессиональному сообществу); – формирование чувства социально-профессиональной ответственности, усвоение профессионально-этических норм;

	– осознанный выбор будущего профессионального развития и возможностей реализации собственных жизненных планов; – формирование отношения к профессиональной деятельности как возможности участия в решении личных, общественных, государственных, общенациональных проблем.
Модуль 2 «Гражданско-патриотическое воспитание»	*Цель модуля:* развитие личности обучающегося на основе формирования у обучающихся чувства патриотизма, гражданственности, уважения к памяти защитников Отечества и подвигам Героев Отечества, закону и правопорядку. *Задачи модуля:* – формирование знаний обучающихся о символике России; – воспитание у обучающихся готовности к выполнению гражданского долга и конституционных обязанностей по защите Родины; – формирование у обучающихся патриотического сознания, чувства верности своему Отечеству; – развитие у обучающихся уважения к памяти защитников Отечества и подвигам Героев Отечества, историческим символам и памятникам Отечества; – формирование российской гражданской идентичности, гражданской позиции активного и ответственного члена российского общества, осознающего свои конституционные права и обязанности, уважающего закон и правопорядок, обладающего чувством собственного достоинства, осознанно принимающего традиционные национальные и общечеловеческие гуманистические и демократические ценности; – развитие правовой и политической культуры обучающихся, расширение конструктивного участия в принятии решений,

	затрагивающих их права и интересы, в том числе в различных формах общественной самоорганизации, самоуправления, общественно значимой деятельности; развитие в молодежной среде ответственности, принципов коллективизма и социальной солидарности; – формирование приверженности идеям интернационализма, дружбы, равенства, взаимопомощи народов; воспитание уважительного отношения к национальному достоинству людей, их чувствам, религиозным убеждениям; – формирование установок личности, позволяющих противостоять идеологии экстремизма, национализма, ксенофобии, коррупции, дискриминации по социальным, религиозным, расовым, национальным признакам и другим негативным социальным явлениям; – формирование антикоррупционного мировоззрения.
Модуль 3 «Физическая культура и здоровьесбережение»	*Цель модуля:* формирование у обучающихся чувства бережного отношения к культурному наследию и традициям многонационального народа России, культуры здоровья, безопасного поведения, стремления к здоровому образу жизни и занятиям спортом, воспитание психически здоровой, физически развитой и социально-адаптированной личности. *Задачи модуля:* – формирование способности к духовному развитию, реализации творческого потенциала в учебной, профессиональной деятельности на основе нравственных установок и моральных норм, непрерывного образования, самовоспитания и универсальной духовно-нравственной компетенции - «становиться лучше»; – формирование у обучающихся ответственного отношения к своему здоровью и потребности в здоровом образе

	жизни, физическом самосовершенствовании, занятиях спортивно-оздоровительной деятельностью, развитие культуры безопасной жизнедеятельности, профилактику наркотической и алкогольной зависимости, табакокурения и других вредных привычек; – формирование бережного, ответственного и компетентного отношения к физическому и психологическому здоровью - как собственному, так и других людей, умение оказывать первую помощь, развитие культуры здорового питания.
Модуль 4 «Культурно-творческое воспитание»	*Цель модуля:* создание условий для самоопределения и социализации обучающихся на основе социокультурных, духовно-нравственных ценностей и принятых в российском обществе правил и норм поведения в интересах человека, семьи, общества и государства, формирование у обучающихся уважения к старшему поколению. *Задачи модуля:* – воспитание здоровой, счастливой, свободной личности, формирование способности ставить цели и строить жизненные планы; – реализация обучающимися практик саморазвития и самовоспитания в соответствии с общечеловеческими ценностями и идеалами гражданского общества; – формирование позитивных жизненных ориентиров и планов; – формирование у обучающихся готовности и способности к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности; – формирование выраженной в поведении нравственной позиции, в том числе способности к сознательному выбору добра,

	нравственного сознания и поведения на основе усвоения общечеловеческих ценностей и нравственных чувств (чести, долга, справедливости, милосердия и дружелюбия); – развитие культуры межнационального общения; – формирование уважительного отношения к родителям и старшему поколению в целом, готовности понять их позицию, принять их заботу, готовности договариваться с родителями и членами семьи в решении вопросов ведения домашнего хозяйства, распределения семейных обязанностей; – воспитание ответственного отношения к созданию и сохранению семьи на основе осознанного принятия ценностей семейной жизни; – формирование толерантного сознания и поведения в поликультурном мире, готовности и способности вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения.
Модуль 5 «Экологическое воспитание»	*Цель модуля:* формирование у обучающихся чувства бережного отношения к живой природе и окружающей среде, культурному наследию и традициям многонационального народа России. *Задачи модуля:* – развитие у обучающихся экологической культуры, бережного отношения к родной земле, природным богатствам России и мира, понимание влияния социально-экономических процессов на состояние природной и социальной среды; – воспитание чувства ответственности за состояние природных ресурсов, формирование умений и навыков разумного природопользования, нетерпимого отношения к действиям, приносящим вред экологии; приобретение опыта эколого-направленной деятельности;

	– воспитание эстетического отношения к миру, включая эстетику быта, научного и технического творчества, спорта, общественных отношений; – формирование мировоззрения, соответствующего современному уровню развития науки и общественной практики, основанного на диалоге культур, а также на признании различных форм общественного сознания, предполагающего осознание своего места в поликультурном мире; – формирование чувства любви к Родине на основе изучения культурного наследия и традиций многонационального народа России.

2. КОМПЛЕКТ КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫХ МАТЕРИАЛОВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

Тема 1. Введение в информационную безопасность.

Задание 1. Вопросы для обсуждения

1. Определение информационной безопасности, угроз, уязвимости. Цели защиты.

2. Характеристики информации, применительно к задачам защиты. Физические и экономические характеристики. Взаимосвязь между стоимостями.

3. Информационная безопасность в условиях функционирования в России глобальных сетей.

4. Тенденции развития преступлений в сфере информационных технологий.

5. Internet как среда для компьютерных преступлений.

Задание 2. Практическая работа.

Практическая работа 1. Методы поиска и сбора информации.

1. Поисковые системы. Методика поиска.

2. Рассылки, тематические форумы, информационные листы.

3. Домашние страницы. Методика отбора и восстановления материала.

4. Возможности использования иноязычных ресурсов.

Тема 2. Задачи и методы информационной безопасности.

Задание 1. Вопросы для обсуждения

1. Основные задачи информационной безопасности.

2. Основные методы обеспечения защиты информационной системы. Законодательные, административные, технические. Классификация

методов.

Задание 2. Практическая работа.

Практическая работа 1. Методика устранения компьютерной информации.

1. Физическая организация жестких дисков.

2. Методы восстановления информации.

3. Обзор современных средств устранения компьютерной информации.

4. Действующие стандарты и законы об уничтожении информации.

Тема 3. Угрозы информационной безопасности.

Задание 1. Вопросы для обсуждения

1. Ключевые свойства информации. Понятие угрозы. Секретность, конфиденциальность, доступность. Определение и классификация угроз.

2. Угроза нарушения конфиденциальности. Служебная и предметная информация. Непрерывность защиты.

3. Угроза нарушения целостности. Статическая и динамическая целостность. Примеры нарушений целостности.

4. Угроза отказа служб. Классификация угроз и методы минимизации последствий.

Задание 2. Практическая работа.

Практическая работа 1. Целесообразность усиления обороны.

1. Экономическая эффективность программного обеспечения.

2. Методика принятия решения об усилении защиты информации.

Задание 3. Тестирование

1. К субъектам информационной системы не относится …

А. Владелец;

Б. Пользователь;

В. Регулятор;

Г. Собственник;

2. Информационная система – это …

А. набор программных и технических средств;

Б. упорядоченную совокупность документов и информационных технологий, реализующих информационные процессы;

В. упорядоченная совокупность документов, относящихся к определенной области;

Г. набор программных средств, относящихся к одной задаче.

3. Несанкционированный доступ – это …

А. доступ или воздействие с нарушением правил доступа;

Б. изменение пароля с правами администратора;

В. доступ в незащищенную систему пользователя;

Г. изменение пароля доступа в систему пользователем.

4. К конфиденциальной информации не относится …

А. служебная тайна;

Б. персональные данные;

В. государственная тайна;

Г. коммерческая тайна.

5. Что не относится к непреднамеренным воздействиям?

А. воздействия из-за ошибок пользователя;

Б. сбой технических средств;

В. сбой программных средств;

Г. внедрение вируса в автоматическом режиме.

6. Целью защиты информации является …

А. предотвращение экономического ущерба собственнику, владельцу или пользователю информации;

Б. предотвращения доступа в информационную систему нелегитимным пользователям;

В. недопущение распространения конфиденциальной информации;

Г. соблюдение политики безопасности и выполнение правил хранения информации.

7. Что не является характеристикой информации?

А. статичность;

Б. тип доступа;

В. время отклика;

Г. стоимость создания.

8. Какая стоимостная характеристика информации совпадает с себестоимостью информации?

А. стоимость создания;

Б. стоимость потери конфиденциальности;

В. стоимость скрытого нарушения целостности;

Г. стоимость утраты.

9. Время жизни информации – это …

А. время, пока информация хранится в информационной системе;

Б. время, пока информация актуальна;

В. время, пока информация интересна для злоумышленников;

Г. время, пока стоимость создания информации выше стоимость потери.

10. Каков максимальный срок хранения документов с грифом "секретно"?

А. 5 лет;

Б. 10 лет;

В. неограничен;

Г. до тех пор, пока информация не будет скомпрометирована.

11. Что не относится к задачам информационной безопасности?

А. целостность и секретность;

Б. электронная подпись и датирование;

В. устойчивость связи и определение трафика;

Г. неотказуемость и анонимность.

12. Право на использование некоторого ресурса – это …

А. уполномочивание;

Б. контроль доступа;

В. право собственности;

Г. сертификация.

13. Какие методы реализуют контроль соблюдения установленного порядка к защищаемой информации?

А. правовые;

Б. административные;

В. технические;

Г. все перечисленные.

14. Какие методы не относятся к обеспечению информационной безопасности?

А. принуждение и побуждение;

Б. управление доступом и регламентация;

В. маскировка и препятствие;

Г. скрытый доступ и копирование сообщений.

15. Методами защиты с "черным ящиком" называют …

А. методы, не имеющие математического обоснования стойкости;

Б. "слепые" полуавтоматические методы;

В. криптографические методы;

Г. методы, реализованные на аппаратном уровне.

Тема 4. Потенциальные противники и атаки.

Задание 1. Вопросы для обсуждения

1. Виды противников или "нарушителей".

2. Виды и каналы утечки информации. Непосредственные и косвенные каналы. Каналы, предполагающие изменение структуры информационной структуры.

3. Классификация атак.

4. Сетевые атаки.

Задание 2. Практическая работа.

Практическая работа 1.. Уязвимости Windows.

1. Недостатки архитектуры операционных систем семейства Windows.

2. Основные виды уязвимостей: статистика их обнаружения и устранения.

3. Описание методик атак, использующих уязвимости операционной системы семейства Windows.

4. Рекомендации по настройке операционной системы для увеличения обороноспособности

Тема 5. Основные положения теории информационной безопасности информационных систем.

Задание 1. Вопросы для обсуждения

1. Подходы к обеспечению информационной безопасности. Формулирование основных положений информационных положений.

2. Принципы обеспечения информационной безопасности. Системность, комплексность, непрерывность, разумная достаточность, гибкость, открытость алгоритмов, простота применения.

3. Формальные модели доступа к данным. Классификация моделей.

4. Дискреционная модель.

5. Мандатная модель.

6. Монитор безопасности и его функции.

Задание 2. Практическая работа.

Практическая работа 1.. Уязвимости Linux-систем.

1. Понятие открытого программного обеспечения, Преимущества и недостатки.

2. Алгоритма защиты информации, используемые в Linux.

3. Основные типы уязвимости и возможности их минимизации.

Практическая работа 2. Защита от копирования переносных носителей.

1. Методики защиты программных и установочных дисков.

2. Методика защиты дисков с данными.

3. Система защиты StarForce.

4. Современные средства защиты видеодисков.

5. Описание некоторых методологий взлома переносных носителей.

Тема 6. Политика безопасности информационных систем.

Задание 1. Вопросы для обсуждения

1. Административный уровень защиты информации.

2. Разделение политики безопасности по уровням. Описание функций административного уровня безопасности.

3. Разработка и реализация политики безопасности.

4. Функции политики безопасности по уровням. Вопросы, решаемые при разработке политики безопасности.

5. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

6. Выявление недостатков этих операционных систем, приводящих к снижению уровня безопасности.

7. Анализ способов нарушений безопасности.

Задание 2. Практическая работа.

Практическая работа 1.. Модели распространения программного обеспечения и

связанные с этим задачи защиты программ.

1. Модели распространения программ.

2. Выбор модели распространения.

3. Методики защиты программного обеспечения.

4. Выбор методики в зависимости от выбранной модели распространения.

Практическая работа 1.. Аппаратные ключи защиты.

1. Основные виды аппаратных ключей.

2. Методики обхода аппаратных ключей.

3. Недостатки аппаратных ключей

Задание 3. Тестирование

1. Попытка реализации угрозы – это …

А. уязвимость;

Б. атака;

В. конфиденциальность;

Г. взлом.

2. Что не является примером нарушения статической целостности

информации?

А. ввод неверных данных;

Б. несанкционированное изменение данных;

В. изменение программного модуля вирусом;

Г. внесение дополнительных пакетов в сетевой трафик.

3. Угроза утечки информации ограниченного доступа, хранящейся в информационной системе или передающейся по каналам связи – это …

А. угроза нарушения конфиденциальности;

Б. угроза нарушения целостности;

В. угроза отказа служб;

Г. все перечисленные.

4. Какая угроза отказа служб устраняется административно-правовыми методами?

А. отказ пользователей;

Б. отказ программного обеспечения;

В. нарушение работ систем связи;

Г. разрушение и повреждение помещений.

5. Высококвалифицированного специалиста, стремящегося обойти защиту компьютерной системы, вне зависимости от того, получает ли он от этого коммерческую выгоду, и преследуются ли по закону его действия, называют:

А. FREEker;

Б. HACKer;

В. SLASHer;

Г. CRACKer.

6. Что не относится к косвенным каналам утечки информации?

А. перехват побочного электромагнитного излучения;

Б. использование подслушивающих средств;

В. сбор производственных отходов с информацией;

Г. дистанционное видеонаблюдение.

7. Что относится к каналам, предполагающим изменение элементов информационной структуры?

А. намеренное копирование файлов и носителей информации;

Б. маскировка под других пользователей, путём похищение идентифицирующей их информации;

В. хищение носителей информации;

Г. незаконное подключение специальной регистрирующей аппаратуры к устройствам связи.

8. Какая направленность атак неверно сформулирована?

А. атаки на уровне операционной системы;

Б. атаки на уровне системного администратора;

В. атаки на уровне сетевого программного обеспечения;

Г. атаки на уровне систем управления базами данных.

9. Захват ресурсов с помощью хакерских программ, бомбардировка запросами сервера и аналогичные атаки относятся к виду:

А. отказ в обслуживании;

Б. превышения полномочий;

В. модификация потока данных;

Г. создание ложного потока данных.

10. Наиболее защищенным элементом информационной системы обычно

является …

А. Операционная система;

Б. Персонал;

В. Система управления базами данных;

Г. Сетевые подключения.

11. Что не относится к принципам информационной безопасности?

А. открытость алгоритмов и механизмов защиты;

Б. простота применения защитных мер;

В. разумная достаточность;

Г. организованность по уровням.

12. В какой модели доступа отношения «субъекты-объекты» представлены в виде матрицы доступа?

А. мандатной;

Б. модели Биба;

В. дискреционной;

Г. распределённой.

13. В какой модели используются метки секретности?

А. мандатной;

Б. модели Биба;

В. дискреционной;

Г. распределённой.

14. Как по-другому называется монитор безопасности?

А. системный монитор;

Б. администраторский монитор;

В. диспетчер доступа;

Г. диспетчерский монитор.

15. Какой из принципов информационной безопасности требует проверки на соответствие стандартам средств защиты?

А. Системность;

Б. Комплексность;

В. Разумная достаточность;

Г. Открытость алгоритмов и механизмов защиты.

Тема 7. Организационно-правовые методы информационной безопасности.

Задание 1. Вопросы для обсуждения

1. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

2. Уровни правового обеспечения информационной безопасности.

3. Место информационной безопасности экономических систем в национальной безопасности страны.

4. Основные принципы обеспечения безопасности.

5. Концепция информационной безопасности.

6. Доктрина информационной безопасности России.

7. Четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

8. Основные задачи обеспечения информационной безопасности. Правовые методы обеспечения информационной безопасности

Задание 2. Практическая работа.

Практическая работа 1. Защита от потери информации и отказов программных

средств.

1. Резервное копирование – правила проведения.

2. Архивация данных.

3. Организация бесперебойного питания компьютерной системы.

4. Аппаратные средства дублирования информации.

Тема 8. Основные понятия криптографии.

Задание 1. Вопросы для обсуждения

1. Определение базовых понятий. Понятие криптографии, шифра, ключа, взлома шифра.

2. Задачи и методы криптографии. Секретность, аутентификация, целостность,

неоспоримость.

3. Виды шифров. Симметричны, ассиметричные, блочные и потоковые шифры. Принцип Керкхоффса.

4. Криптографические примитивы. Хэш-функция и её применения. Генераторы псевдослучайных чисел.

Задание 2. Практическая работа.

Практическая работа 1.. Виды шифров. Методика кодирования.

1. Подстановочные шифры. Шифр Цезаря.

2. Перестановочные шифры. Табличное шифрование с ключевым словом.

3. Смешанные шифры. Матричный способ.

4. Шифр Тритемиуса.

5. Криптоанализ. Частотный и статистический анализ.

6. Самостоятельная работы – методики шифрования и расшифрования

Практическая работа 2. Криптосистемы DES и RSA.

1. Введение в комбинаторику.

2. Алгоритм шифрования DES.

3. Введение в теорию сравнений.

4. Алгоритм шифрования RSA.

Тема 9. Криптографические протоколы.

Задание 1. Вопросы для обсуждения

1. Понятие протокола. Определение протокола, условия протоколов. Виды протоколов.

2. Основные криптографические протоколы. Схема обмена ключами, аутентификация, распределение ответственности, цифровая подпись. Вспомогательные криптографические протоколы.

3. Электронная цифровая подпись. Задачи, решаемые цифровой подписью. Схема создания и проверки электронной цифровой подписи.

4. Модели основных криптоаналитических атак.

5. Атака методом сведения к середине. Словарная атака.

6. Четыре основных подхода к анализу криптографических протоколов.

Задание 2. Практическая работа.

Практическая работа 1. Шифры Эль-Гамаля и Rijndael. ГОСТ.

1. Шифр Эль-Гамаля. Алгоритм работы. Основные достоинства и недостатки.

2. Шифр Rijndael. Циклическое преобразование, особенности использования.

3. ГОСТ. Основные требования. Отличия от DES. Преимущества и недостатки.

Практическая работа 2. Алгоритмы распределения ключей.

1. Протоколы распределения ключей.

2. Выработка секретных ключей по Диффи-Хеллману.

3. Распределение ключей с помощью асимметрических систем шифрования.

4. Взаимное подтверждение подлинности при обмене сообщениями в сети.

Задание 3. Тестирование

1. Что является основной целью административного уровня безопасности?

А. отладка монитора безопасности;

Б. формирование политики безопасности;

В. реализация дискреционной модели;

Г. реализация мандатной модели.

2. К какому уровню политике безопасности относятся вопросы, касающиеся отдельных аспектов организации?

А. верхнего уровня;

Б. административного уровня;

В. среднего уровня;

Г. нижнего уровня.

3. Выберите лишний шаг в процедуре разработки политики информационной безопасности.

А. разработка желаемой политики безопасности;

Б. выбор системы защиты;

В. стандартизация системы защиты;

Г. определение требований, не реализованных системой защиты.

4. Что не относится к недостаткам операционных систем семейств Windows?

А. невозможно встроенными средствами гарантированно удалять остаточную информацию;

Б. невозможно встроенными средствами обеспечить полноту системы;

В. не обеспечивается регистрация выдачи документов на "твёрдую копию", а также некоторые другие требования к регистрации событий;

Г. невозможно в общем случае обеспечить замкнутость (или целостность)

программной среды.

5. Какие методы несанкционированного доступа является наиболее распространёнными в операционной системе Windows?

А. Позволяющие несанкционированно запустить исполняемый код;

Б. Позволяющие обойти установленные разграничения прав доступа;

В. Троянские программы;

Г. Позволяющие осуществить несанкционированные операции чтения/записи файловых и других объектов.

6. Наиболее распространёнными методами несанкционированного доступа в операционной системе Unix является …

А. Позволяющие несанкционированно запустить исполняемый код;

Б. Позволяющие обойти установленные разграничения прав доступа;

В. Троянские программы;

Г. Позволяющие осуществить несанкционированные операции чтения/записи файловых и других объектов.

7. Что не относится к основным принципам обеспечения национальной безопасности?

А. взаимная ответственность личности, общества и государства по обеспечению безопасности;

Б. законность;

В. соблюдение баланса между сферами ответственности личности, общества и государства;

Г. соблюдение баланса жизненно важных интересов личности, общества и государства.

8. К правовым методам обеспечения информационной безопасности не относят

…

А. определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;

Б. определение ответственности физических и юридических лиц за несанкционированный доступ к информации;

В. определение уровней безопасностей в информационных системах;

Г. определение ответственности физических и юридических лиц за противоправное раскрытие конфиденциальной информации.

9. Какой документ представляет собой совокупность взглядов на цели, задачи и

принципы и основные направления обеспечения информационной безопасности Российской Федерации:

А. Конституция Российской Федерации;

Б. Концепция национальной безопасности Российской Федерации;

В. Доктрина информационной безопасности Российской Федерации;

Г. Федеральный закон "Об информации, информатизации и защите информации".

10. К какому уровню правового обеспечения информационной безопасности относятся Постановления Правительства Российской Федерации:

А. первому;

Б. второму;

В. третьему;

Г. четвертому.

11. Основной задачей криптоанализа является …

А. компрометация ключа;

Б. получение открытого текста без знания ключа;

В. получение шифртекста без знания ключа;

Г. получение ключа из шифртекста.

12. Что не относится к задачам криптографии?

А. аутентификация;

Б. целостность;

В. системность;

Г. неоспоримость.

13. Как называются криптографические алгоритмы, для которых ключ зашифрования не совпадает с ключом расшифрования?

А. блочные;

Б. поточные;

В. симметричные;

Г. ассиметричные.

14. В чем суть принципа Керкхоффса?

А. в криптосистеме должен использоваться сменный элемент, называемый ключом, и секретность шифра обеспечивается секретностью ключа шифрования;

Б. устойчивость криптосистемы обратно пропорциональна интегральной мощности используемых для взлома компьютеров;

В. устойчивость криптосистемы полиномиально зависит от длины используемого ключа;

Г. в криптосистеме шифрование должно осуществляться посимвольно, причем каждый следующий символ не должен зависеть от предыдущих.

15. Класс односторонних функций, применяемых в криптографии, называется …

А. генераторы случайных чисел или рнд-функция;

Б. функции Керкхоффса или крфс-функция;

В. сингл-функция;

Г. хэш-функция.

Тема 10. Программно-технические методы защиты.

Задание 1. Вопросы для обсуждения

1. Программно-аппаратные средства.

2. Понятие информационного сервиса безопасности.

3. Виды сервисов безопасности.

4. Основные методы идентификации и аутентификации.

5. Биометрические показатели пользователей и возможности их применения. Основные методики идентификации по биометрическим показателям. Недостатки идентификации по биометрическим показателям.

6. Сервисы управления доступом. Матрица списков доступа. Анализ дискреционного и мандатного доступа.

7. Протоколирование и аудит.

8. Журнал аудита. Активный аудит.

9. Основы защиты корпоративных экономических информационных систем.

10.Основные положения обмена информацией в открытых сетях. Понятие межсетевого экрана. Программные средства защиты Internet-подключений.

Задание 2. Практическая работа.

Практическая работа 1.. Навесная защита.

1. Методика установки протекторов.

2. Особенности работы протекторов.

3. Методика обхода протектора.

4. Недостатки протекторов.

Практическая работа 2. Защита информации на уровне баз данных.

1. Концептуальные вопросы построения уровней защиты систем управления базами данных.

2. Обязанности администратора по защите баз данных от несанкционированного доступа.

3. Общее понятие о целостности базы данных. Типы ошибок, ведущих к нарушению целостности.

4. Проблема непротиворечивости при параллельной обработке данных.

5. Восстановление базы данных. Особенности восстановления распределенной базы данных.

Тема 11. Защита данных и сервисов от воздействия вредоносных программ.

Задание 1. Вопросы для обсуждения

1. Вирусы. Виды вирусов.

2. Классификации вирусов.

3. Антивирусное программное обеспечение.

4. Методики обнаружения вирусов и виды антивирусного программного обеспечения. Недостатки антивирусов.

5. Защита системы электронной почты.

6. Спам. Методики работы спам-фильтров.

Задание 2. Практическая работа.

Практическая работа 1.. Вредоносное программное обеспечение.

1. Программы-шпионы. Защита от программ шпионов.

2. Троянские программы.

3. "Черви", методики проникновения.

4. Вирусы, алгоритмы работы.

5. Антивирусное программное обеспечение: рекомендуемые настройки, правила использования.

6. Стратегия заблаговременной подготовки к эффективной ликвидации последствий вирусной эпидемии.

Тема 12. Стандарты обеспечения информационной безопасности.

Задание 1. Вопросы для обсуждения

1. Критерии безопасности компьютерных систем министерства обороны США

(“Оранжевая книга”).

2. Руководящие документы Гостехкомиссии России.

3. Классы защищенности, группы и классы пользователей, их права и возможности.

4. Международные стандарты информационной безопасности. Стандарт ISO/IEC 15408 "Общие критерии". Описание требований безопасности и характеристик угроз.

5. Классы функциональных требований. Классификационная статистика.

Тема 13. Основные технологии построения защищённых экономических информационных систем.

Задание 1. Вопросы для обсуждения

1. Общие принципы построения защищенных систем.

2. Цели защищенных информационных систем: безопасность, безотказность, деловая добросовестность.

3. Средства разработки и правила их реализации.

4. Основные средства, методика их реализации, практические аспекты функционирования.

5. Фундаментальные проблемы, возникающие при построении защищенных

информационных систем.

Задание 2. Практическая работа.

Практическая работа 1. Особенности защиты информации при работе в локальной сети.

1. Средства управления сетями.

2. Программные средства обеспечения защиты информации в локальной сети.

3. Обязанности администратора сети, относящиеся к безопасности информации.

Практическая работа 2. Программные средства защиты информации для корпоративных сетей.

1. Брандмауэры: виды и варианты использования.

2. Средства организации виртуальных частных сетей.

3. Средства обнаружения сетевых атак.

4. Средства защиты электронных сообщений с помощью цифровой подписи.

Практическая работа 3. Безопасная работа в Internet.

1. Выбор сайтов для посещения.

2. Настройка встроенных средств защиты информации современных браузеров.

3. Обработка сообщений электронной почты. Спам-фильтры.

4. Ограничение доступа из локальной сети в Internet с помощью proxyсерверов.

5. Типы межсетевых экранов, их достоинства и недостатки.

Задание 3. Тестирование.

1. Как называется последовательность шагов, которые предпринимают стороны для совместного решения задачи, требующей применение криптографических методов:

А. криптографические алгоритмы;

Б. криптографические протоколы;

В. криптографические функции;

Г. криптографические обмены.

2. Уберите несуществующий криптографический протокол.

А. Протокол с наблюдением;

Б. Протокол с арбитражем;

В. Протокол с судейством;

Г. Самоутверждающийся протокол.

3. Что не относится к основным криптографическим протоколам?

А. обмен ключами;

Б. депонирование ключей;

В. цифровая подпись;

Г. распределение ответственности.

4. С помощью какого типа криптографических алгоритмов реализуется электронная цифровая подпись?

А. блочных;

Б. поточных;

В. симметричных;

Г. ассиметричных.

5. Что не является видом криптоаналитической атаки?

А. словарная атака;

Б. брутфорсе-атака;

В. блицкриг-атака;

Г. метод сведения к середине.

6. Что не относится к основным преимуществам программных средств защиты?

А. простота тиражирования;

Б. простота доступа к ресурсам;

В. простота применения;

Г. гибкость настройки.

7. Что не является видом сервисов безопасности?

А. превентивные меры;

Б. проективные меры;

В. меры по выявлению нарушений;

Г. меры восстановления режимы безопасности.

8. Что не является методом идентификации?

А. использование парольной фразы;

Б. метод "рукопожатия";

В. метод "встречного приветствия";

Г. использование смарт-карт.

9. Какая система идентификации по биометрическим показателям является наиболее распространённой?

А. по отпечаткам пальцев;

Б. по сетчатке глаза;

В. по голосу;

Г. по клавиатурному почерку.

10. Какой сервис позволяет контролировать действия субъектов над информационными объектами?

А. сервис контроля пользователей;

Б. сервис управления доступом;

В. системный сервис;

Г. пользовательский сервис.

11. Как называется анализ накопленной системной информации, проводимый оперативно или периодически?

А. аудит;

Б. протоколирование;

В. идентификация;

Г. систематизация.

12. К какому виду ошибок относится пропуск атак на информационные системы?

А. ошибки первого рода;

Б. ошибки второго рода;

В. ошибки третьего рода;

Г. ошибки четвертого рода.

13. Что не относится к потенциальным угрозам безопасности информации в локальных вычислительных сетях?

А. несанкционированный доступ в локальную вычислительную систему со стороны штатных компьютеров;

Б. несанкционированный доступ со стороны линий связи;

В. нештатные административно-правовые ситуации;

Г. аварийные ситуации с оборудованием.

14. Как называются программные или аппаратные средства разграничения доступа между сегментами локальной вычислительной сети?

А. антивирусный экран;

Б. межсетевые экраны;

В. транспортный узел;

Г. сигнально-аппаратный узел.

15. Как называют вид компьютерных вирусов, которые действуют самостоятельно и не внедряются в тела других файлов?

А. "трояны";

Б. стелс-вирусы;

В. полиморфы;

Г. "черви".

Тематика рефератов

1. Аппаратные ключи HASP.

2. Аппаратные ключи Alladin.

3. Уязвимости Windows 2000 и методики их нейтрализации.

4. Уязвимости Windows XP и методики их нейтрализации.

5. Уязвимости Windows Vista и методики их нейтрализации.

6. Криптографическая система DES. Алгоритм работы.

7. Криптографическая система RSA. Алгоритм работы.

8. Программа, реализующая шифра Цезаря, на языке Delphi.

9. Программа, реализующая шифра Тритемиуса, на языке Delphi.

10. Система защиты от копирования Star Force.

11. Методики защиты видеодисков.

12. Использование и настройка firewall.

13. Возможности удаленного взлома компьютерной системы. Методы противодействия.

14. Настройка средств защиты при выходе в Internet.

15. История развития криптографии и методик криптоанализа.

16.Обзор современных методик и аппаратуры для удаленного считывания информации с персонального компьютера.

17. Методики защиты информации, составляющей государственную тайну.

ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ

ВОПРОСЫ К ЭКЗАМЕНУ

1. Стоимостные характеристики информации и их соотношения.

2. Internet как среда для компьютерных преступлений.

3. Основные задачи информационной безопасности.

4. Основные методы обеспечения защиты информационной системы.

5. Определение и классификация угроз.

6. Потенциальные противники: классификация и характеристика.

7. Каналы утечки информации.

8. Классификация атак и их характеристики.

9. Сетевые атаки: основные виды.

10. Формулирование основных положений информационных положений.

11. Принципы обеспечения информационной безопасности.

12. Формальные модели доступа к данным.

13. Монитор безопасности и его функции.

14. Политика безопасности информационных систем

15. Таксономия нарушений информационной безопасности вычислительной системы.

16. Уровни правового обеспечения информационной безопасности.

17. Доктрина информационной безопасности России.

18. Задачи и методы криптографии.

19. Виды шифров. Принцип Керкхоффса.

20. Основные криптографические протоколы.

21. Модели основных криптоаналитических атак.

22. Основные аппаратные средства защиты. Основные программные средства защиты.

23. Основные методы идентификации и аутентификации.

24. Сервисы управления доступом.

25. Протоколирование и аудит. Задачи аудита.

26. Основы защиты Internet-подключений.

27. Вирусы. Виды вирусов.

28. Антивирусное программное обеспечение.

29. Стандарты обеспечения информационной безопасности.

30. Общие принципы построения защищенных систем.