Аннотация к рабочей программе дисциплины «Защита информации в компьютерных сетях»

Цель преподавания дисциплины

Дисциплина «Защита информации в компьютерных сетях» изучается с целью обучить студентов принципам построения компьютерных сетей, основным угрозам информационного обмена в них, а также средствами их устранения.

Задачи изучения дисциплины

- изучения технологии построения компьютерных сетей;
- изучение основных угроз компьютерным сетями методов их реализации;
- изучение технологий обеспечения безопасности информации на верхних уровнях модели взаимодействия открытых систем.

Компетенции, формируемые в результате освоения дисциплины

Способность осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учётом предъявляемых к ним требованиям
качества обслуживания и функционирования (ПК-7)
Способность выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и
восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и
систем (ПК-14).

Разделы дисциплины

Настройка компьютерной сети. Организация защиты совместно используемых сетевых ресурсов. Анализ кадров ethernet. Технологии маршрутизации. Работа протоколов транспортного уровня udp и tcp. Сертификаты для безопасного сетевого взаимодействия.
Защита соединений Брандмауэры. Протоколы аутентификации.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
(наименование ф-та полностью)
информатики
Т.А. Ширабакина
(подпись, инициалы, фамилия)
«01» 02 2017г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации в компьютерных сетях
(наименование дисциплины)

направление подготовки (специальность) 10.05.02
(шифр согласно ФГОС
Информационная безопасность телекоммуникационных систем
и наименование направление подготовки (специальности)

Защита информации в системах связи и управления
наименование профиля, специализации или магистерской программы)

форма обучения очная
(очная, очно-заочная, заочная)

Курск – 2017

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования специальности подготовки 10.05.02 Информационная безопасность телекоммуникационных систем и на основании учебного плана специальности подготовки 10.05.02 Информационная безопасность телекоммуникационных систем (специализация Защита информации в системах связи и управления), одобренного Учёным советом университета, протокол № 5 «30» 01 2017 г.

Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по специальности 10.05.02 Информационная безопасность телекоммуникационных систем на заседании кафедры информационной безопасности № «9» 01.02 2017.

Зав. кафедрой ИБ Таныгин М.О.

Разработчик программы
доцент кафедры ИБ Спеваков А.Г.

Директор научной библиотеки Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, одобренного Ученым советом университета протокол № 1 «25» авг 2017 г. на заседании кафедры ИБ Таныгин М.О.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, одобренного Ученым советом университета протокол №5 «30» 01 2017 г. на заседании кафедры И5, протокол №12 от 29.06.18г.
(наименование кафедры, дата, номер протокола)

Зав. кафедрой Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана специальности подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, одобренного Ученым советом университета протокол № « » 20 г. на заседании кафедры информационной безопасности 27.06.2019 №11
(наименование кафедры, дата, номер протокола)

Зав. кафедрой к.т.н. доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол №7 «30» 01 2017 г. на заседании кафедры информационной безопасности протокол №1 от 31.08.2020г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол №9 «26» 03 2018 г. на заседании кафедры информационной безопасности протокол №11 от 28.06.21г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности протокол №11 от 30.06.22г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.05.02 «Информационная безопасность телекоммуникационных систем», одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности протокол №1 от 30.08.22г.

(наименование кафедры, дата, номер протокола)

Зав. кафедрой

---

1. Цель и задачи дисциплины, планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

1.1. Цель дисциплины

Дисциплина «Защита информации в компьютерных сетях» изучается с целью обучить студентов принципам построения компьютерных сетей, основным угрозам информационного обмена в них, а также средствами их устранения.

1.2. Задачи дисциплины

– изучения технологии построения компьютерных сетей;

– изучение основных угроз компьютерным сетями методов их реализации;

– изучение технологий обеспечения безопасности информации на верхних уровнях модели взаимодействия открытых систем.

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательный программы

Обучающиеся должны **знать:**

- технологию построения защищенных компьютерных сетей;
- состав и оборудование компьютерных сетей;
- протоколы взаимодействия, используемые в компьютерных системах;
- номенклатуру и характеристики средств обеспечения сетевой безопасности;
- принципы функционирования средств обеспечения сетевой безопасности;

уметь:

- производить оценку угроз безопасности различным вариантам компьютерных сетей;
- выполнять практические работы по настройке механизмов обеспечения безопасной работы в компьютерных системах;

владеть:

-навыками работы со средствами обеспечения безопасности компьютерных систем;

- навыками сопоставления защитных механизмов, характерных для определённого уровня модели взаимодействия открытых систем с имеющимися на рынке средствами обеспечения сетевой безопасности.

У обучающегося формируются следующие компетенции:

Способность осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учётом предъявляемых к ним требованиям качества обслуживания и функционирования (ПК-7)

способность выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем (ПК-14).

2. Указание места дисциплины в структуре образовательной программы

«Защита информации в компьютерных сетях» представляет дисциплину с индексом Б1.В.ДВ.9.2 вариативной части учебного плана направления подготовки 10.05.02 Информационная безопасность телекоммуникационных систем, изучаемую на 5 курсе в 9 семестре.

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоёмкость (объём) дисциплины составляет 4 зачётные единицы (з.е.), 108 академических часов.

Таблица 3.1 – Объём дисциплины по видам учебных занятий

Общая трудоемкость дисциплины	144
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	54,15
лекции	18
лабораторные занятия	18
практические занятия	18
экзамен	0,15
зачет	
курсовая работа (проект)	
расчетно-графическая (контрольная) работа	
Аудиторная работа (всего):	54
в том числе:	
лекции	18
лабораторные занятия	18
практические занятия	18
Самостоятельная работа обучающихся (всего)	54
Контроль/экз (подготовка к экзамену)	36

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Настройка компьютерной сети	Общие сведения о компьютерных сетях, состав и и оборудование компьютерных сетей. Технические характеристики
2.	Организация защиты совместно используемых сетевых ресурсов	Виды совместно используемых ресурсов, задачи совместного использования сетевых ресурсов. Методы обращения к сетевым ресурсам. Штатные средства защиты совместных сетевых ресурсов операционных систем. Решения сторонних производителей
3.	Анализ кадров ethernet	Задачи анализа пакетов данных, передаваемых по сети. Угрозы, которые несёт анализ кадров со стороны злоумышленника. Средства анализа трафика, их функциональные возможности
4.	Технологии маршрутизации	Задачи маршрутизации сообщений и кадров. Средства маршрутизации, особенности маршрутизации пакетов различных типов.
5.	Работа протоколов транспортного уровня udp и tcp	Структура кадров протоколов транспортного уровня. Угрозы информации на транспортном уровне. Области применения протоколов, преимущества и ндостатки протоколов
6.	Сертификаты для безопасного сетевого взаимодействия	Назначение сертификатов при сетевом взаимодействии. Принципы работы цифровых сертификатов. Жизненный цикл сертификата. Протоколы проверки сертификатов, используемые при сетевом взаимодействии
7.	Защита соединений	Стандарт IPsec. Режимы тунеллирования данных, Структура кадра пакета защищённого соединения. Алгоритмы установления защищённого соединения. Виртуальные частные сети: назначение, испольуемые технологии, используемые алгоритмы
8.	Брандмауэры	Назначение и принципы работы МСЭ. Виды МСЭ. Реализация МСЭ средствами операционных систем. МСЭ сторонних разработчиков. Уязвимости и ограничения примения МСЭ
9.	Протоколы аутентификации	Общая схема аутентификации пользователей компьютерных сетей. Протоколы аутентификации, используемые в компьютерных сетях. Используемые криптографические схемы аутентификации. Протокол Kerberos

Таблица 4.2 – Содержание дисциплины и его методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности	Учебно-методические	Формы текущего контроля успеваемости	Компетенции

		лек, час	№, лаб.	№, пр.	материалы	(*по неделям семестра*)	
1	2	3	4	5	6	7	8
1.	Настройка компьютерной сети	2		1	О-1-3 Д-4,6	С,Т	ПК-7, ПК-14
2.	Организация защиты совместно используемых сетевых ресурсов	2		1	О-1,2 Д-4-7	С,Т	ПК-7, ПК-14
3.	Анализ кадров ethernet	2	1		О-1,2 Д-5,9	С,Т	ПК-14
4.	Технологии маршрутизации	2	2		О-1,3 Д-4,8	С,Т	ПК-14
5.	Работа протоколов транспортного уровня udp и tcp	2	2		О-1,3 Д-4,7	С,Т	ПК-14
6.	Сертификаты для безопасного сетевого взаимодействия	2			О-1,2 Д-4,10	С	ПК-14
7.	Защита соединений	2			О-1,2 Д-4,6	С,Т	ПК-7, ПК-14
8.	Брандмауэры	2		2	О-1,2 Д-7,8	С	ПК-7, ПК-14
9.	Протоколы аутентификации	2	3		О-1-3 Д-4,9	С	ПК-14

С – собеседование, Т – тест.

4.2 Лабораторные работы и (или) практические занятия

4.2.1 Лабораторные работы

Таблица 4.2.1 – Лабораторные работы

№	Наименование лабораторной работы	Объем, час.
1.	Контроль потоков конфиденциальной информации	6
2.	Настройка и создание локальной сети Ethernet	6
3.	Организация локальной сети на базе ОС WINDOWS	6
Итого		18

4.2.2 Практические работы

Таблица 4.2.1 – Практические занятия

№	Наименование лабораторной работы	Объем, час.
1.	Исследование сетевых возможностей ОС Linux.	9
2.	Сетевые фильтры.	9
Итого		18

4.3 Самостоятельная работы студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№ раздела (Тема)	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Настройка компьютерной сети	2 неделя	6

2.	Организация защиты совместно используемых сетевых ресурсов	4 неделя	6
3.	Анализ кадров ethernet	6 неделя	6
4.	Технологии маршрутизации	8 неделя	6
5.	Работа протоколов транспортного уровня udp и tcp	10 неделя	6
6.	Сертификаты для безопасного сетевого взаимодействия	12 неделя	6
7.	Защита соединений	14 неделя	6
8.	Брандмауэры	16 неделя	6
9.	Протоколы аутентификации	18 неделя	6
Итого			54

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;
- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;
- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;
- путем разработки:

– методических рекомендаций, пособий по организации самостоятельной работы студентов;

– вопросов к экзамену, тестовых заданий;

– методических указаний к выполнению лабораторных работ, к практическим зантиям и т.д.

типографией университета:

– помощь авторам в подготовке и издании научной, учебной и методической литературы;

– удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6. Образовательные технологии. Технологии использования воспитательного потенциала дисциплины

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены выполнение практикоориентированных заданий в ходе лабораторных занятий.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объём, час.
1	2	3	4
1.	Выполнение работы «Контроль потоков конфиденциальной информации»	Выполнение студентом интерактивных заданий по типовым вариантам контроля информационных потоков в компьютерных сетях	3
2.	Выполнение работы «Настройка и создание локальной сети Ethernet»	Выполнение студентом интерактивных заданий по развёртыванию ЛВС различной конфигурации	3
3.	Выполнение работы «Организация локальной сети на базе ОС WINDOWS»	Выполнение студентом настройки сетевых компонентов операционной системы Windows	6
4.	Выполнение работы «Исследование сетевых возможностей ОС Linux»	Выполнение студентом настройки сетевых компонентов операционной системы Linux	6
5.	Выполнение работы «Сетевые фильтры»	Выполнение студентом интерактивных заданий контролю сетевых соединений	6
	Итого		24

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для лабораторных занятий содержания,

демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и производства;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, (командная работа, разбор конкретных ситуаций)*;*

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплины

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код и содержание компетенции	Этапы* формирования компетенций и дисциплины (модуле), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
способность осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учётом предъявляемых к ним требованиям качества обслуживания и		Безопасность операционных систем	Измерения в телекоммуникационных системах Защита информации в компьютерных сетях Системы и сети радиосвязи Системы и сети мобильной связи Конструкторская практика

функционирования (ПК-7)			Преддипломная практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
способность выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем (ПК-14)		Информационная безопасность телекоммуникационных систем	Антенны и распространение радиоволн Аппаратные средства телекоммуникационных систем Техническая защита информации Программно-аппаратные средства обеспечения информационной безопасности Защита информации в системах беспроводной связи Защита информации в компьютерных сетях Администрирование защищенных телекоммуникационных систем Практика по получению профессиональных умений и опыта профессиональной деятельности Эксплуатационная практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

**Этапы для РПД всех форм обучения определяются по учебному плану очной формы обучения следующим образом:*

Этап	Учебный план очной формы обучения/ семестр изучения дисциплины		
	Бакалавриат	Специалитет	Магистратура

Начальный	1-3 семестры	1-3 семестры	1 семестр
Основной	4-6 семестры	4-6 семестры	2 семестр
Завершающий	7-8 семестры	7-10 семестры	3-4 семестр

7.2 Описание показателей и критериев оценивания компетенций на различных этапах формирования, описание шкал оценивания

Код компетенции/этап *(указывается название этапа из п 7.1)*	Показатели оценивания компетенций	Критерии шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно»)	Продвинутый уровень («хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ПК-7 /завершающий	*1.Доля освоенных обучающимся знаний, умений навыков от общего объема ЗУН, установленных в п.1.ЗРПД* *2.Качество освоенных обучающимися знаний, умений, навыков* *3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях*	**Знает:** Основные правила организации защиты компьютерных сетей. **Умеет:** В недостаточной форме находить правильные средства для обеспечения информационной безопасности компьютерных сетей. **Владеет:** Навыками организации работы отдельных компонентов компьютерных сетей.	**Знает:** Основные принципы обеспечения защиты информации компьютерных сетей. **Умеет:** Осуществлять выбор средств обеспечения информационной безопасности компьютерных сетей. **Владеет:** навыками эксплуатации компьютерных сетей.	**Знает:** Глубокие знания в области инструментальных средств обеспечения защиты информации компьютерных сетей. **Умеет:** Осуществлять рациональный выбор средств обеспечения информационной безопасности компьютерных сетей. **Владеет:** Умелыми навыками эксплуатации компьютерных сетей и средств их защиты
ПК-14/ завершающий	*1.Доля освоенных обучающимся знаний,*	**Знает:** Номенклатуру и функционал средств защиты	**Знает:** Принципы обмена информацией в компьютерных	**Знает:** Полный спектр технологий организации

	умений навыков от общего объема ЗУН, установленных в п.1.ЗРПД *2.Качество освоенных обучающимися знаний, умений, навыков* *3. Умение применять знания, умения, навыки в типовых и нестандартных ситуациях*	компьютерных сетей. **Умеет:** Выполнять основные технологические операции по обслуживанию компонентов компьютерных сетей, отвечающих за безопасность. **Владеет:** Проведения основных технологических операций со средствами защиты информации в компьютерных сетях.	сетях. **Умеет:** Эксплуатировать компоненты компьютерных систем с учётом знаний о протоколах обмена информацией в них. **Владеет:** Эксплуатации и настройки комплексом программных средств поддержания инфраструктуры компьютерных сетей.	компьютерных сетей. **Умеет:** Реагировать инциденты безопасности, возникающие в процессе эксплуатации компьютерных сетей. **Владеет:** Навыками реализации комплексной политики информационной в компьютерных сетях.

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология форматирования	Оценочные средства		Описание шкал оценивания
				наименование	№ заданий	
1	2	3	4	5	6	7
1.	Настройка компьютерной сети	ПК-7, ПК-14	Лекция, СРС, практическое занятие	Собеседование, тест, вопросы к п.р №1		Согласно табл. 7.2
2.	Организация защиты совместно используемых сетевых ресурсов	ПК-14	Лекция, СРС, практическое занятие	Собеседование, тест, вопросы к п.р №1		Согласно табл. 7.2

3.	Анализ кадров ethernet	ПК-14	Лекция, СРС, лабораторная работа	Собесе-дование, тест, вопросы к л.р №1		Согласно табл. 7.2
4.	Технологии маршрутизации	ПК-14	Лекция, СРС, лабораторная работа	Собесе-дование, тест, вопросы к л.р №2		Согласно табл. 7.2
5.	Работа протоколов транспортного уровня udp и tcp	ПК-14	Лекция, СРС, лабораторная работа	Собесе-дование, тест, вопросы к л.р №2		Согласно табл. 7.2
6.	Сертификаты для безопасного сетевого взаимодействия	ПК-14	Лекция, СРС,	Собесе-дование		Согласно табл. 7.2
7.	Защита соединений	ПК-7, ПК-14	Лекция, СРС	Собесе-дование, тест		Согласно табл. 7.2
8.	Брандмауэры	ПК-7, ПК-14	Лекция, СРС, практическое занятие	Собесе-дование, вопросы к п.р №2		Согласно табл. 7.2
9.	Протоколы аутентификации	ПК-14	Лекция, СРС, лабораторная работа	Собесе-дование, вопросы к л.р №3		Согласно табл. 7.2

Примеры типовых контрольных заданий для текущего контроля

Вопросы для собеседования

– Перечислите действия, необходимые для организации локальной компьютерной сети.

– Назовите основные компоненты, входящие в состав сетевого адаптера.

– Назовите известные Вам скорости и режимы передачи данных, используемые в сетевых адаптерах, поддерживающих тот либо иной вариант технологии Ethernet.

– Перечислите системные ресурсы, потребляемые сетевыми адаптерами.

Тесты для контроля знаний

Выберите типы доступа для сетевых дисков и папок, определяемых в операционной системе Windows:

а) чтение; б) чтение и выполнение; в) изменение; г) запись; д) полный доступ; е) просмотр; ж) список содержимого папки.

Какой из сетевых компонентов Windows обеспечивает возможность предоставления ним сетевых ресурсов?

а) адаптер; б) сетевой протокол; в) клиент; г) служба.

Какой из сетевых компонентов Windows отвечает за адресацию узлов сети на сетевом уровне?

а) адаптер; б) сетевой протокол; в) клиент; г) служба.

Полностью оценочные средства представлены в учебно-методическом комплексе дисциплины.

Типовые задания для промежуточной аттестации

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%).

Для проверки *знаний* используются вопросы и задания в закрытой форме (с выбором одного или нескольких правильных ответов).

Умения, навыки и компетенции проверяются с помощью задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов. Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулирующих следующими нормативными актами университета:

- Положение П 02.016 – 2015 «О балльно-рейтинговой системе оценки качества освоений образовательных программ»;
- методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля* по дисциплине в рамках действующей в университете бально-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
1	2	3	4	5
Выполнение работы «Контроль потоков конфиденциальной информации»	2	Выполнил, но «не защитил»	5	Выполнил, и «защитил»
Выполнение работы «Настройка и создание локальной сети Ethernet»	2	Выполнил, но «не защитил»	5	Выполнил, и «защитил»
Выполнение работы «Организация локальной сети на базе ОС WINDOWS»	2	Выполнил, но «не защитил»	5	Выполнил, и «защитил»
Выполнение работы «Исследование сетевых возможностей ОС Linux»	2	Выполнил, но «не защитил»	5	Выполнил, и «защитил»
Выполнение работы «Сетевые фильтры»	4	Выполнил, но «не защитил»	6	Выполнил, и «защитил»
СРС	12		22	
Итого	24		48	
Посещаемость	0		16	
Экзамен	0		36	
Итого	24		100	

При итоговом контроле (экзамен) в форме бланкового теста студенту предлагается 15. В каждом вопросе один правильный ответ. Полученную итоговую сумму условных баллов (максимум 15) переводят в баллы на экзамене (максимум 36) путём умножения на 2.4 и округления до целого значения. Пример билета в тестовой форме приведён в приложении А

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1) Баканов В.М. Сетевые технологии: Учебное пособие. - М.: МГУПИ, 2008. - 105 с. [Электронный ресурс]: http://window.edu.ru/resource/182/58182

2) Комагоров В.П. Архитектура сетей и систем телекоммуникации: учебное пособие / В.П. Комагоров; Томский политехнический университет. - Томск: Изд-во Томского политехнического университета, 2011. - 154 с. [Электронный ресурс]: http://window.edu.ru/resource/074/79074

3) Олифер В. Г., Компьютерные сети. Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е

изд. - Санкт-Петербург : Питер, 2015. - 943 с. - (Учебник для вузов). - Библиогр.: с. 917 . - Алф. указ.: с. 918

8.2 Дополнительная учебная литература

4) Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с.: ил.

5) Хорев А.А. Способы и средства защиты информации. Учебн. пособие. – М.: МО РФ, 2000. – 316 с.

6) Грибунин В. Г., Чудовский В. В. Комплексная защита информации на предприятии: Учебн. пособие.- М.: Академия, 2009.- 416 с.

7) Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Учебн. пособие.- М.: Форум: Инфра-М, 2010.- 592 с.

8) Чепиков О. Средства аутентификации – выбор между рисками, удобством и стоимостью //Информационная безопасность. – 2004. №3

9) Применение сканеров для анализа защищенности компьютерных сетей: Материалы курса. – М.: Учебный центр «Информзащита», 2009.

10) Ньюман Д. Системы предотвращения сетевых атак //Сети. №16. – 2006.

8.3 Перечень методических указаний

1. Спеваков А.Г. Контроль потоков конфиденциальной информации: методические указания по выполнению лабораторной работы (учебно-методическая разработка) / Курск:, Юго-Зап. гос. ун-т, 2013. 36 с.

2. Спеваков А.Г. Настройка и создание локальной сети Ethernet: методические указания по выполнению лабораторной работы (учебно-методическая разработка) / Курск:, Юго-Зап. гос. ун-т, 2010. 54 с..

3. Калуцкий И.В., Максаков А.А., Мезенцева Н.А. Организация локальной многофункциональной сети на базе ОС WINDOWS SERVER 2012: методические указания по выполнению лабораторных и практических работ (учебно-методическая разработка) / Курск:, Юго-Зап. гос. ун-т, 2016. 47 с.

4. Калуцкий И.В., Гефнер В.В. Исследование сетевых возможностей ОС Linux: методические указания по выполнению лабораторных и практических работ:методические указания к лабораторной работе (учебно-методическая разработка) / Курск:, Юго-Зап. гос. ун-т, 2013. 23 с.

5. Калуцкий И.В., Пономарев С.В., Сетевые фильтры: методические указания по выполнению лабораторной работы (учебно-методическая разработка) / Курск:, Юго-Зап. гос. ун-т, 2014 25 с.

8.4 Другие учебно-методические материалы

9. Перечень ресурсов информационно-телекаммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/

2. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/

3. Википедия. Свободная энциклопедия [официальный сайт]. Режим доступа: https://ru.wikipedia.org/

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Защита информации в компьютерных сетях» являются лекции и практические и лабораторные занятия. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают лабораторные занятия, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Лабораторному занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

По согласованию с преподавателем или по его заданию студенты готовить рефераты по отдельным темам дисциплины, выступать на занятиях с докладами. Основу докладов составляет, как правило, содержание подготовленных студентами рефератов.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по лабораторным работам, а также по результатам докладов.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Безопасность жизнедеятельности»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами

пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

GNS3 - графический симулятор сети (свободное ПО) - https://www.gns3.com/ ; Wireshark - программа-анализатор трафика для компьютерных сетей Ethernet (Бесплатная, GNU General Public License) - https://www.wireshark.org/ ; Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал», Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,Windows 7, договор IT000012385, Oracle Virtualbox (Бесплатная, GNU General Public License), редактор двоичных файлов Free Hex Editor Neo, (Свободное ПО http://www.hhdsoftware.com/free-hex-editor), открытая среда разработки программного обеспечения Lazarus (Свободное ПО http://www.lazarus.freepascal.org/) Microsoft Visual Studio 2010 Professional Договор IT000012385, ОС Ubuntu (Бесплатная, GNU GPLv3)

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (10 шт) CPU AMD-Phenom, ОЗУ 16 GB, HDD 2 Tb, монитор Aok 21”. Проекционный экран на штативе; Мультимедиацентр: ноут- букASUSX50VLPMD-T2330/14"/1024Mb/160Gb/сумка/ проектор inFocusIN24+

13. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место,

передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14. Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	изменённых	заменённых	аннулированных	новых			
1		4, 14			2	23.08.18	

ПРИЛОЖЕНИЕ А Образец экзаменационного билета в тестовой форме

ЮГО-ЗАПАДНЫЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ	
Факультет ФиПИ Специальность 10.05.02 курс 5, семестр 9 Дисциплина **«Защита информации в компьютерных сетях»**	Утверждено на заседании кафедры ИБ, Протокол № __ от ____ 201__ г. Зав. кафедрой _____ М.О. Таныгин

1. Как правильно указать только хост 172.16.30.55 в списке доступа IP.
?. 172.16.30.55 0.0.0.255
?.172.16.30.55 0.0.0.0
?. any 172.16.30.55
?. host 172.16.30.55
? 0.0.0.0 172.16.30.55

2. В компании реализована следующая схема аутентификации:
Пользователь во время регистрации в системе, в качестве пароля использует число;
данное число пользователь рассчитывает по некой формуле, где используются текущие значения даты и времени.
К какой из перечисленных технологий аутентификации относится данная схема?
?) Аутентификация с использованием сертификатов
?) Мультифакторная аутентификация
?) Аутентификация с использованием многоразовых паролей
?) Аутентификация с использованием одноразовых паролей
?) Биометрическая аутентификация

3. В компании разрабатывается схема аутентификации пользователей. Были выработаны следующие требования:
Клиент должен проходить аутентификацию единожды, после этого прозрачно получать доступ к любым разрешенным ресурсам, в независимости от их местонахождения;
протокол аутентификации должен быть платформенно-независимым;
аутентификация должна быть централизованной.

Какой из перечисленных протоколов аутентификации позволит решить поставленную задачу?
?) SPAP
?) EAP
?) PAP
?) CHAP
?) Kerberos

4. Каким из перечисленных недостатков обладает система аутентификации Kerberos?
?) Невозможность использования дополнительных Kerberos серверов для снижения (балансировки) нагрузки
?) Использование простых криптографических алгоритмов
?) Централизованное хранение всех секретных ключей системы
?) Отсутствие достаточной поддержки со стороны производителей операционных систем и программного обеспечения
?) Сильное увеличение загрузки сети

5. Сотрудникам требуется организовать удаленное подключение к внутренней сети компании на базе VPN. Руководство компании выдвинуло основные требования безопасности этих подключений:
Обеспечение конфиденциальности данных;
обеспечение целостности данных;
защита от повторения.
Какой из перечисленных протоколов позволит реализовать выполнение данных требований?
?) SSL

?) L2TP
?) PPTP
?) EAP
?) TLS

6. Принято решение внедрить систему обнаружения атак (Intrusion Detection System). Основная задача системы - своевременно предотвращать изменения, вносимые в критически важные системные файлы.

Какой тип систем обнаружения вторжений позволит решить поставленную задачу?
?) Системы контроля целостности (System Integrity Verifiers)
?) Мониторы регистрационных (журналов) файлов (Log Files Monitors)
?) Системы контроля аномальной деятельности (Anomaly Activity Control Systems)
?) Обманные системы (Deception Systems)
?) Системы обнаружения атак на сетевом уровне (Network IDS)

7. Какие 2 из перечисленных протоколов НЕВОЗМОЖНО использовать для получения цифрового сертификата?
?) SNMP
?) ARP
?) FTP
?) HTTP
?) LDAP

8. Для защиты сетей от несанкционированного доступа используются межсетевые экраны (брандмауэры).

Какими 3 из перечисленных характеристик должен обладать любой брандмауэр?
?) Единственная точка входа во внутреннюю сеть
?) Протоколирование входящего и исходящего трафика
?) Проверка на вирусы
?) Аутентификация пользователей
?) Реализация правил безопасности

9. Для обеспечения безопасной работы мобильных пользователей решено использовать VPN подключения, для аутентификации пользователей - систему сертификатов.

Какой из перечисленных протоколов позволит решить поставленную задачу?
?) PPP
?) L2TP
?) EAP
?) HTTPS
?) PPTP

10. Политика безопасности компании требует разрешения только следующих сетевых сервисов: DNS, электронная почта, WWW.

Какой из перечисленных типов брандмауэров позволит реализовать данную политику безопасности?
?) Брандмауэр пакетной фильтрации
?) Брандмауэр уровня приложений
?) Proxy сервер
?) Брандмауэр не требуется
?) NAT

11. При использовании инфраструктуры открытых ключей, создается иерархия центров сертификации (ЦС).Какой из перечисленных ЦС расположен во главе (наверху) иерархии?
?) Control (Контролирующий ЦС)
?) Self signed (Самоподписанный ЦС)
?) Main (Главный ЦС)
?) Root (Корневой ЦС)
?) Enterprise (ЦС Предприятия)

12. Необходимо защитить все коммуникации с серверами, работающими под управлением ОС Linux. Какой стандартный протокол следует использовать для удаленного администрирования сервера с соблюдением требования конфиденциальности?
?) TLS
?) RDP
?) VNC
?) SSL
?) SSH

13. Для обеспечения безопасного обмена информацией и подтверждения подлинности используются цифровые сертификаты.

Какой из перечисленных форматов цифровых сертификатов является наиболее распространенным?
?) X.509
?) 802.1a
?) CA
?) 802.1x
?) IDEA

14. Какой из перечисленных протоколов обеспечения безопасности является частью протокола IPSec и выполняет функцию шифрования данных (обеспечение конфиденциальности)?
?) DSA
?) ESP
?) AH
?) 3DES
?) RSA

15. Для обеспечения возможности подключения мобильных пользователей в компании планируется использовать несколько серверов удаленного доступа. Были разработаны следующие требования безопасности:

1. Централизованное хранение базы данных пользователей;
2. Обеспечение конфиденциальной передачи данных;
3. Защита данных от подмены;
4. Обеспечение целостности данных;
5. Централизованное использование политик удаленного доступа.

Решено использовать RADIUS сервер.
Каким требованиям политики безопасности соответствует данное решение?
?) 1, 2
?) 1, 5
?) 2, 5
?) 2, 3, 4
?) 1, 2, 5

Экзаменатор _____Таныгин М.О.