МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. В. Сенченко
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Технологии построения защищенных каналов передачи данных

Уровень образования: **высшее образование - магистратура**
Направление подготовки / специальность: **10.04.01 Информационная безопасность**
Направленность (профиль) / специализация: **Информационная безопасность объектов критической информационной инфраструктуры**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **1**
Семестр: **2**
Учебный план набора 2021 года

Распределение рабочего времени

№	Виды учебной деятельности	2 семестр	Всего	Единицы
1	Лекции	16	16	часов
2	Лабораторные работы	32	32	часов
3	Всего аудиторных занятий	48	48	часов
4	Самостоятельная работа	60	60	часов
5	Всего (без экзамена)	108	108	часов
6	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е.

Зачёт: 2 семестр

Томск

Согласована на портале № 48824

Рассмотрена и одобрена на заседании кафедры
протокол № 13 от «24» 12 2019 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.04.01 Информационная безопасность, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:

Доцент Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ А. К. Новохрестов

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Д. В. Кручинин

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперты:

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ А. А. Конев

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ К. С. Сарин

Согласована на портале № 48824

1. Цели и задачи дисциплины

1.1. Цели дисциплины

подготовить выпускника к деятельности, связанной с выработкой предложений по вопросам построения защищенных каналов передачи данных, разработке предложений по совершенствованию и повышению эффективности комплекса мер защиты каналов передачи данных.

1.2. Задачи дисциплины

– изучить принципы построения защищенных каналов передачи данных и и управления ими;

– обучиться использованию программных и аппаратных средств защиты каналов передачи данных;

– познакомиться с методами проектирования, развертывания и сопровождения защищенных каналов передачи данных;

– познакомиться с методами обследования и анализа защищенности каналов передачи данных.

–

2. Место дисциплины в структуре ОПОП

Дисциплина «Технологии построения защищенных каналов передачи данных» (Б1.В.5) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Технологии обеспечения информационной безопасности.

Последующими дисциплинами являются: Защищенные информационные системы, Управление информационной безопасностью.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-14 способностью организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;

– ПК-15 способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности;

В результате изучения дисциплины обучающийся должен:

– **знать** принципы функционирования сетевых протоколов, включающих криптографические алгоритмы; принципы функционирования средств защиты каналов связи.

– **уметь** оценивать угрозы безопасности каналам связи и передаваемой по ним информации; обосновывать выбор используемых программно-аппаратных средств защиты каналов связи; конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты каналов связи.

– **владеть** навыками конфигурирования программно-аппаратных средств защиты информации в каналах связи; навыками контроля корректности функционирования программно-аппаратных средств защиты информации в каналах связи.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		2 семестр
Аудиторные занятия (всего)	48	48
Лекции	16	16
Лабораторные работы	32	32

Согласована на портале № 48824

Самостоятельная работа (всего)	60	60
Оформление отчетов по лабораторным работам	16	16
Подготовка к лабораторным работам	16	16
Проработка лекционного материала	16	16
Подготовка к тесту	12	12
Всего (без экзамена)	108	108
Общая трудоемкость, ч	108	108
Зачетные Единицы	3.0	3.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
2 семестр					
1 Основы построения защищенных каналов передачи данных	6	0	10	16	ПК-14
2 Технологии обеспечения безопасности в каналах передачи данных	10	32	50	92	ПК-15
Итого за семестр	16	32	60	108	
Итого	16	32	60	108	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины (по лекциям)	Трудоемкость, ч	Формируемые компетенции
2 семестр			
1 Основы построения защищенных каналов передачи данных	Определения. Построение каналов передачи данных. сетевые протоколы. Классификация способов построения защищенных каналов передачи информации. Нормативно-правовые основы построения защищенных каналов.	2	ПК-14
	Угрозы каналам связи и передаваемой по ним информации. Уязвимости каналов связи. Классификация атак на каналы связи. Подходы к построению модели угроз и анализу рисков.	2	
	Алгоритмы аутентификации и шифрования. Алгоритмы обмена ключами.	2	
	Итого	6	
2 Технологии	Виртуальные сети ViPNet. Компоненты	4	ПК-15

Согласована на портале № 48824

обеспечения безопасности в каналах передачи данных	виртуальной сети ViPNet. Функции координатора. Принципы взаимодействия узлов ViPNet в виртуальной сети. Первоначальные настройки защищенной сети. Механизмы соединений в сети ViPNet. Варианты подключения координаторов к внешней сети. Туннелирование IP-трафика открытых ресурсов. Виртуальные адреса в сети ViPNet. Маршрутизация трафика координаторов с несколькими сетевыми интерфейсами. Туннелирование трафика открытых ресурсов на канальном уровне.		
	Построение защищенных каналов на канальном уровне. Протокол PPTP. Протокол L2TP.	2	
	Построение защищенных каналов на сетевом уровне. IPSec. Архитектура IPSec. Заголовок AH. Заголовок ESP. Транспортный режим. Туннельный режим. IKE.	2	
	Построение защищенных каналов на прикладном уровне. Протокол SSL. Протокол TLS. Протокол SSH.	2	
	Итого	10	
Итого за семестр		16	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин	
	1	2
Предшествующие дисциплины		
1 Технологии обеспечения информационной безопасности	+	
Последующие дисциплины		
1 Защищенные информационные системы		+
2 Управление информационной безопасностью		+

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4.

Таблица 5.4 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий			Формы контроля
	Лек.	Лаб. раб.	Сам. раб.	

Согласована на портале № 48824

ПК-14	+		+	Опрос на занятиях, Зачёт, Тест
ПК-15	+	+	+	Отчет по лабораторной работе, Опрос на занятиях, Зачёт, Тест

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7.1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
2 семестр			
2 Технологии обеспечения безопасности в каналах передачи данных	Развертывание защищенной сети ViPNET	4	ПК-15
	Модификация защищенной сети и настройка политик безопасности на узлах	4	
	Межсетевое взаимодействие	4	
	Работа с ViPNet Coordinator 4 for Windows	4	
	Защита АРМ пользователя на основе технологии ViPNet	4	
	Построение защищенных каналов на канальном уровне	4	
	Построение защищенных каналов на сетевом уровне	4	
	Построение защищенных каналов на прикладном уровне	4	
	Итого	32	
Итого за семестр		32	

8. Практические занятия (семинары)

Не предусмотрено РУП.

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
2 семестр				
1 Основы построения защищенных каналов передачи данных	Подготовка к тесту	4	ПК-14	Зачёт, Опрос на занятиях, Тест
	Проработка лекционного материала	6		
	Итого	10		
2 Технологии обеспечения безопасности в каналах передачи данных	Подготовка к тесту	8	ПК-15	Зачёт, Опрос на занятиях, Отчет по лабораторной работе, Тест
	Проработка лекционного материала	10		
	Подготовка к лабораторным работам	16		

Согласована на портале № 48824

	Оформление отчетов по лабораторным работам	16		
	Итого	50		
Итого за семестр		60		
Итого		60		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
2 семестр				
Зачёт			30	30
Опрос на занятиях	4	6	4	14
Отчет по лабораторной работе	10	15	15	40
Тест			16	16
Итого максимум за период	14	21	65	100
Нарастающим итогом	14	35	100	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11.2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 - 69	

Согласована на портале № 48824

	60 - 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Корячко, В. П. Корпоративные сети [Электронный ресурс]: технологии, протоколы, алгоритмы : монография / В. П. Корячко, Д. А. Перепелкин. — Москва : Горячая линия-Телеком, 2015. — 216 с. — ISBN 978-5-9912-0202-2. — Режим доступа: https://e.lanbook.com/book/111068 (дата обращения: 25.03.2020).

12.2. Дополнительная литература

1. Основы построения инфокоммуникационных систем и сетей [Электронный ресурс]: Учебное пособие / А. В. Пуговкин - 2014. 156 с. — Режим доступа: https://edu.tusur.ru/publications/6061 (дата обращения: 25.03.2020).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Безопасность сетей ЭВМ. Часть 1 [Электронный ресурс]: Лабораторный практикум / А. К. Новохрестов, А. И. Гуляев - 2017. 92 с. — Режим доступа: https://edu.tusur.ru/publications/7225 (дата обращения: 25.03.2020).
2. Основы построения компьютерных сетей [Электронный ресурс]: Учебно-методическое пособие по практическим и самостоятельным занятиям / С. П. Куксенко - 2016. 128 с. — Режим доступа: https://edu.tusur.ru/publications/6523 (дата обращения: 25.03.2020).

12.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. https://fstec.ru/ - Федеральная служба по техническому и экспортному контролю
2. Дополнительно рекомендуется использовать информационные, справочные и нормативные базы данных https://lib.tusur.ru/ru/resursy/bazy-dannyh

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

Согласована на портале № 48824

13.1.2. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория безопасности сетей ЭВМ / Лаборатория криптографии в банковском деле

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 804 ауд.

Описание имеющегося оборудования:

- Компьютер: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор (14 шт.);
- Обучающий стенд локальные компьютерные сети Microtik routerboard (2 шт.);
- ViPNET УМК «Безопасность сетей»;
- Коммутатор Mikrotik CRS125-24G-1S-IN (6 шт.);
- Компьютер класса не ниже i5-7400/8DDR4/SSD120G;
- Анализатор кабельных сетей MI 2016 Multi LAN 350 (3 шт.);
- Анализатор Wi-Fi сетей NETSCOUT AirCheck G2 (2 шт.);
- Сервер класса не ниже 4xE7-4809v4/512GBRE16/L9300-8i/5T6000G7;
- Маршрутизатор Cisco 891-K9 (2 шт.);
- Маршрутизатор Cisco C881-V-K9 (2 шт.);
- Маршрутизатор Check Point CPAP-SG1200R-NGFW (2 шт.);

Стенды для изучения проводных и беспроводных компьютерных сетей, включающие:

- абоненские устройства: компьютеры SuperMicro;
- коммутаторы: Mikrotik CRS125-24G-1S-IN; Mikrotik RouterBoard 1100;
- маршрутизаторы: Cisco 891-K9, Cisco C881-V-K9, Check Point CPAP-SG1200R-NGFW;
- средства анализа сетевого трафика и углубленной проверки сетевых пакетов: анализатор трафика Wireshark, дистрибутив Kali Linux;
- межсетевые экраны: ИКС Lite, Positive Technologies Application Firewall Education, CISCO ASA 5505, МЭ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- системы обнаружения компьютерных атак: Snort, Suricata, СОВ в составе маршрутизатора Check Point CPAP-SG1200R-NGFW;
- точки доступа: D-link dwl3600ap;
- системы защиты от утечки данных: Контур информационной безопасности SearchInform;
- средства мониторинга состояния автоматизированных систем: система мониторинга Zabbix;
- средства сканирования защищенности компьютерных сетей: сканер безопасности Xspider Education, система анализа защищенности сети MaxPatrol Education.

Стенды для изучения средств криптографической защиты информации в банковском деле, включающие:

- абоненские устройства: компьютеры SuperMicro;
- коммутаторы: Mikrotik CRS125-24G-1S-IN; Mikrotik RouterBoard 1100;
- маршрутизаторы: Cisco 891-K9, Cisco C881-V-K9, Check Point CPAP-SG1200R-NGFW;
- средства криптографической защиты информации: программно-аппаратный комплекс шифрования «ФПСУ-IP», программно-аппаратный комплекс шифрования «ФПСУ-IP/Клиент»;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Microsoft Windows 10
– Анализатор трафика Wireshark
– Средство построения виртуальных частных сетей OpenVPN

13.1.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;

Согласована на портале № 48824

- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:
- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:
- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

14.1.1. Тестовые задания

1. По масштабу компьютерные сети подразделяются на
a) звездообразные, кольцевые, шинные
b) одноранговые и сети "клиент-сервер"
c) проводные и беспроводные
d) локальные и глобальные

2. Задачей какого уровня модели OSI является управление доступом к среде в сетях, построенных на основе разделяемой среды?
a) прикладного
b) сетевого
c) канального
d) физического

3. Какое минимальное количество уровней протоколов (в терминах модели OSI) должны поддерживать маршрутизаторы сетей с коммутацией пакетов?

Согласована на портале № 48824

a) 1
b) 2
c) 3
d) 4

4. К транспортному уровню модели OSI относятся протоколы:
a) IP, RIP, OSPF
b) SSL, TLS
c) SMTP, IMAP, POP3
d) UDP, TCP

5. По какой причине в протоколе RIP расстояние в 16 хопов между сетями полагается недостижимым?
a) поле, отведенное для хранения значения расстояния, имеет длину 4 двоичных разряда
b) для получения приемлемого времени сходимости алгоритма
c) сети, в которых работает RIP, редко бывают большими
d) таблицы маршрутизации не могут хранить больше 16 записей

6. Что нужно сделать на DHCP сервере чтобы исключить выдачу определенного IP адреса из существующего диапазона?
a) создать диапазон IP адресов
b) создать параметр DHCP
c) создать область DHCP
d) создать исключение для IP адреса

7. Как называется объект Active Directory, который хранит информацию об учетных записях, общих ресурсах, подразделениях?
a) сетевой доступ
b) каталог
c) папка
d) домен

8. Какой протокол используется для доступа к службе каталогов AD?
a) LDAP
b) ShareDiscovery
c) ADSL
d) UDP

9. Компьютер, занимающийся обслуживанием сети, управлением передачей сообщений, и предоставляющий удаленный доступ к своим ресурсам, называется
a) хабом
b) сервером
c) рабочей станцией
d) хостом

10. Метод передачи данных, при котором данные пересылаются в двух направлениях одновременно, называется …
a) симплексным
b) дуплексным
c) синхронным
d) полудуплексным

11. Анализ защищенности - это …
a) выбор обоснованного набора контрмер, позволяющих снизить уровень рисков до приемлемой величины
b) независимая экспертиза отдельных областей функционирования предприятия
c) процедура учета действий, выполняемых пользователем на протяжении сеанса доступа
d) поиск уязвимых мест информационной системы

12. Воздействие на систему с целью создания условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднен.
a) DoS-атака

Согласована на портале № 48824

b) несанкционированный доступ

c) незаконное использование привилегий

d) программная закладка

13. Программное средство для удаленной или локальной диагностики различных элементов сети на предмет выявления в них различных уязвимостей.

a) агент безопасности

b) политика безопасности

c) средство делегирования административных полномочий

d) сканер безопасности

14. … - процесс блокировки выявленных вторжений.

a) анализ защищенности

b) обнаружение атак

c) предотвращение атак

d) аудит безопасности

15. В журнале аутентификации обнаружено несколько записей неуспешных попыток войти в систему под учетными записями пользователей. Возможно была попытка подбора паролей. Какое стандартное средство следует использовать для уменьшения риска такого рода атак?

a) использовать систему обнаружения вторжений

b) переименовать учетную запись администратора

c) использовать мультифакторную аутентификацию

d) включить блокировку учетных записей при определенном количестве неуспешных попыток регистрации

16. Политика безопасности требует сокрытия схемы IP-адресации, используемой во внутренней сети. Какая из перечисленных технологий позволит решить поставленную задачу?

a) система обнаружения вторжений

b) персональный межсетевой экран

c) NAT

d) антивирусное программное обеспечение

17. Технология, которая для обнаружения атак использует, например, образец IP-пакета, характерного для какой-нибудь определенной атаки.

a) монитор регистрационных файлов

b) контроль целостности

c) выявление аномальной деятельности

d) анализ сигнатур

18. Согласно классификации ФСТЭК России, межсетевой экран применяемый на логической границе ИС или между логическими границами сегментов ИС, это МЭ …

a) типа А

b) типа Б

c) типа В

d) типа Г

19. Согласно классификации ФСТЭК России системы обнаружения вторжений делятся на

a) уровня узла и уровня сети

b) внешние и внутренние

c) симметричные и асимметричные

d) коммутируемые и некоммутируемые

20. Согласно профилю защиты средства антивирусной защиты типа «Б» устанавливаются на … информационной системы, функционирующей на базе вычислительной сети.

a) рабочие станции пользователей

b) серверы

c) рабочую станцию администратора

d) серверы и рабочие станции

21. Защита ресурсов сети от несанкционированного использования - это

a) охрана оборудования сети

b) защита ядра безопасности

Согласована на портале № 48824

c) контроль доступа

d) защита периметра безопасности

22. Средство защиты, обеспечивающее защищенность информации от угроз нелегитимной передачи данных из защищенного сегмента системы путем анализа и блокирования исходящего трафика

a) межсетевой экран

b) средство антивирусной защиты

c) DLP-система

d) сканер безопасности

23. Средство, решающее задачи консолидации и хранения журналов событий от различных источников, а также имеющее инструменты для анализа событий и разбора инцидентов на основе их корреляции и обработки по правилам – это …

a) DLP-система

b) система обнаружения вторжений

c) SIEM-система

d) сканер безопасности

24. Способ перехвата информации, при котором на машину устанавливается программное средство, собирающее и передающее информацию – это …

a) перехват в разрыв

b) сетевой перехват

c) агентский перехват

d) перехват путем интеграции со сторонними продуктами

25. Программное или аппаратное средство, которое осуществляет мониторинг сети в реальном времени с целью выявления, предотвращения и блокировки вредоносной активности.

a) межсетевой экран

b) система обнаружения вторжений

c) система предотвращения вторжений

d) средство антивирусной защиты

26. К каким методам сбора данных, использующихся при аудите информационной безопасности, относится MaxPatrol?

a) анализ документации

b) предоставление опросных листов

c) использование специализированных программных средств

d) интервьюирование

27. Какой из методов проверки направлен на определение наличия уязвимости по косвенным признакам?

a) активные зондирующие проверки

b) проверка заголовков и активные зондирующие проверки

c) проверка заголовков

d) имитация атак

28. В каком режиме сканирования системы анализа защищенности MaxPatrol можно произвести подбор паролей?

a) Audit

b) Compliance

c) PenTest

d) Pentest и Compliance

29. В каком режиме функционирования IPsec шифруется весь исходный IP-пакет, а затем он вставляется в поле данных нового пакета?

a) транспортном

b) туннельном

c) в обоих режимах

d) IPsec не использует шифрование

30. Процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности организации в соответствии с определёнными критериями

Согласована на портале № 48824

и показателями безопасности – это …

a) выявление аномальной деятельности

b) анализ защищённости

c) аудит информационной безопасности

d) установка системы защиты

14.1.2. Темы опросов на занятиях

Определения. Построение каналов передачи данных. сетевые протоколы. Классификация способов построения защищенных каналов передачи информации. Нормативно-правовые основы построения защищенных каналов.

Угрозы каналам связи и передаваемой по ним информации. Уязвимости каналов связи. Классификация атак на каналы связи. Подходы к построению модели угроз и анализу рисков.

Алгоритмы аутентификации и шифрования. Алгоритмы обмена ключами.

Виртуальные сети ViPNet. Компоненты виртуальной сети ViPNet. Функции координатора. Принципы взаимодействия узлов ViPNet в виртуальной сети. Первоначальные настройки защищенной сети. Механизмы соединений в сети ViPNet. Варианты подключения координаторов к внешней сети. Туннелирование IP-трафика открытых ресурсов. Виртуальные адреса в сети ViPNet. Маршрутизация трафика координаторов с несколькими сетевыми интерфейсами. Туннелирование трафика открытых ресурсов на канальном уровне.

Построение защищенных каналов на канальном уровне. Протокол PPTP. Протокол L2TP.

Построение защищенных каналов на сетевом уровне. IPSec. Архитектура IPSec. Заголовок AH. Заголовок ESP. Транспортный режим. Туннельный режим. IKE.

Построение защищенных каналов на прикладном уровне. Протокол SSL. Протокол TLS. Протокол SSH.

14.1.3. Зачёт

1. Типовые конфигурации информационных систем. Влияние конфигурации информационной системы на безопасность хранимых, обрабатываемых и передаваемых по сети данных.

2. Угроза. Уязвимость. Атака. Взаимосвязь между этими понятиями.

3. Классификация угроз информационной безопасности вычислительных сетей.

4. Классификация уязвимостей.

5. Классификация атак.

6. Перехват информации в сети. Инструменты. Способы противодействия перехвату.

7. Spoofing. Способы подделки идентификаторов. Способы противодействия spoofing`у.

8. DOS-атаки. Особенности реализации. Способы противодействия DOS-атакам.

9. Универсальные методы обеспечения информационной безопасности компьютеров и компьютерных сетей.

10. Специализированные методы обеспечения информационной безопасности компьютерных сетей.

11. Идентификация и аутентификация. Особенности аутентификации пользователей в компьютерных сетях.

12. Протокол Kerberos. Назначение. Особенности функционирования.

13. Разграничение доступа к информационным ресурсам компьютерных сетей.

14. Криптографическая защита информации в компьютерных сетях. Достоинства и недостатки. Способы преодоления криптографической защиты информации.

15. Электронная подпись. Назначение. Применение для защиты сетевого взаимодействия. Примеры.

16. Сканеры безопасности. Способы выявления уязвимостей в информационных системах.

17. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.

18. Системы обнаружения вторжений. Системы предотвращения вторжений. Методики выявления сетевых атак.

19. Сетевые и хостовые системы обнаружения и предотвращения вторжений. Достоинства и недостатки.

20. Межсетевые экраны. Классификация. Варианты размещения межсетевого экрана. Достоинства и недостатки.

Согласована на портале № 48824

21. Демилитаризованная зоны. Назначение. Способы выделения.

22. Классификация межсетевых экранов по уровням защищенности. Показатель защищенности, применяемые для классификации. Применение межсетевых экранов различных классов.

23. Технология VPN (Виртуальные частные сети). Назначение. Достоинства и недостатки.

24. Основные компоненты технологии виртуальных частных сетей (VLAN).

25. Вредоносные программы. Классификация. Каналы распространения. Влияние на информационные системы.

26. Антивирусные средства. Классификация. Методики выявления вредоносного кода.

27. Средства обеспечения информационной безопасности в ОС Windows'2003. Разграничение доступа к данным. Групповая политика. Область действия групповых политик.

28. Основные этапы разработки защищенной компьютерной сети.

29. Проблемы обеспечения безопасности прикладных сервисов (Веб, почта, FTP) и их решения.

30. Физические средства обеспечения информационной безопасности.

14.1.4. Темы лабораторных работ

Развертывание защищенной сети ViPNET

Модификация защищенной сети и настройка политик безопасности на узлах

Межсетевое взаимодействие

Работа с ViPNet Coordinator 4 for Windows

Защита АРМ пользователя на основе технологии ViPNet

Построение защищенных каналов на канальном уровне

Построение защищенных каналов на сетевом уровне

Построение защищенных каналов на прикладном уровне

14.2. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14.

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами исходя из состояния обучающегося на момент проверки

14.3. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;

Согласована на портале № 48824

– предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

– письменно на бумаге;
– набор ответов на компьютере;
– набор ответов с использованием услуг ассистента;
– представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в форме электронного документа;
– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;
– в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 48824