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

Безопасность сетевых протоколов высокого уровня

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль) / специализация: **Защита информации в системах связи и управления**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **БИС, Кафедра безопасности информационных систем**
Курс: **5**
Семестр: **10**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	10 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Практические занятия	28	28	часов
3	Всего аудиторных занятий	46	46	часов
4	Самостоятельная работа	26	26	часов
5	Всего (без экзамена)	72	72	часов
6	Общая трудоемкость	72	72	часов
		2.0	2.0	З.Е.

Зачёт: 10 семестр

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сенченко П.В.
Должность: Проректор по УР
Дата подписания: 18.12.2019
Уникальный программный ключ:
a1119608-cdff-4455-b54e-5235117c185c

Томск

Согласована на портале № 51106

Рассмотрена и одобрена на заседании кафедры
протокол № 12 от «26» 11 2019 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.02 Информационная безопасность телекоммуникационных систем, утвержденного 16.11.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчики:

доцент кафедра КИБЭВС _____ А. К. Новохрестов

старший преподаватель кафедра ТОР _____ Д. С. Брагин

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Е. М. Давыдова

Заведующий выпускающей каф. БИС _____ Е. Ю. Костюченко

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 № 51106

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Обучить студентов принципам работы и обеспечения безопасности сетевых протоколов высокого уровня.

1.2. Задачи дисциплины

- - принципы работы основных протоколов прикладного уровня;
- - обеспечение безопасности основных протоколов прикладного уровня;
- - принципы работы протоколов транспортного уровня;
- - обеспечение безопасности протоколов транспортного уровня;
- - принципы работы протоколов сетевого уровня;
- - обеспечение безопасности протоколов сетевого уровня;
-
-

2. Место дисциплины в структуре ОПОП

Дисциплина «Безопасность сетевых протоколов высокого уровня» (Б1.Б.08.06) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Защита информации в компьютерных сетях.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПСК-10.5 способностью проводить оценку уровня защищенности и обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи;
- ПСК-10.1 способностью применять теорию сигналов и систем для анализа телекоммуникационных систем и оценки их помехоустойчивости;

В результате изучения дисциплины обучающийся должен:

- **знать** основные протоколы прикладного, транспортного и сетевого уровней модели OSI; знать принципы работы протоколов высокого уровня; уязвимости протоколов высокого уровня; атаки на протоколы высокого уровня; способы обеспечения безопасности на верхних уровнях модели OSI;
- **уметь** определять наличие уязвимостей протоколов высокого уровня; использовать средства защиты протоколов высокого уровня.
- **владеть** навыками обеспечения безопасности протоколов высокого уровня.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		10 семестр
Аудиторные занятия (всего)	46	46
Лекции	18	18
Практические занятия	28	28
Самостоятельная работа (всего)	26	26
Проработка лекционного материала	12	12
Подготовка к практическим занятиям, семинарам	14	14
Всего (без экзамена)	72	72
Общая трудоемкость, ч	72	72

Согласована на портале № 51106

Зачетные Единицы	2.0	2.0

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	Прак. зан., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
10 семестр					
1 Протоколы сетевого уровня	4	4	5	13	ПСК-10.1, ПСК-10.5
2 Протоколы транспортного уровня	4	4	5	13	ПСК-10.1, ПСК-10.5
3 Протоколы прикладного уровня	10	20	16	46	ПСК-10.1, ПСК-10.5
Итого за семестр	18	28	26	72	
Итого	18	28	26	72	

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
10 семестр			
1 Протоколы сетевого уровня	Протоколы маршрутизации. RIP. OSPF. IS-IS. Уязвимости и атаки на протоколы маршрутизации. Обеспечение безопасности протоколов маршрутизации.	2	ПСК-10.1, ПСК-10.5
	Протоколы IPv4 и IPv6. Уязвимости и атаки на протокол IP. Обеспечение безопасности протокола IP.	2	
	Итого	4	
2 Протоколы транспортного уровня	Протокол UDP. Уязвимости и атаки на UDP. Обеспечение безопасности приложений на UDP.	2	ПСК-10.1, ПСК-10.5
	Протокол TCP. Уязвимости и атаки на TCP. Обеспечение безопасности приложений на TCP.	2	
	Итого	4	
3 Протоколы прикладного уровня	Веб-служба. Протоколы HTTP, HTTPS, FTP. Уязвимости и атаки на веб-серверы. Обеспечение безопасности веб-серверов.	2	ПСК-10.1, ПСК-10.5
	Электронная почта. Протоколы SMTP, POP3, IMAP. Уязвимости и атаки на почтовые серверы. Обеспечение безопасно-	2	

Согласована на портале № 51106

	сти почтовых серверов.		
	Система доменных имен. Уязвимости и атаки на DNS. Обеспечение безопасности DNS.	2	
	Протоколы передачи мгновенных сообщений. Уязвимости и атаки на IM-протоколы. Обеспечение безопасности при передаче сообщений. IP-телефония.	2	
	Протоколы удаленного управления. Telnet, SSH, RDP, VNC. Уязвимости и атаки на gротоколы удаленного управления. Обеспечение безопасности удаленного управления.	2	
	Итого	10	
Итого за семестр		18	

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	3
Предшествующие дисциплины			
1 Защита информации в компьютерных сетях	+	+	+

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.	Прак. зан.	Сам. раб.	
ПСК-10.5	+	+	+	Опрос на занятиях, Тест, Отчет по практическому занятию
ПСК-10.1	+	+	+	Опрос на занятиях, Тест, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Не предусмотрено РУП.

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Согласована на портале № 51106

Таблица 8.1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
10 семестр			
1 Протоколы сетевого уровня	Безопасность протоколов маршрутизации и протокола IP.	4	ПСК-10.1, ПСК-10.5
	Итого	4	
2 Протоколы транспортного уровня	Безопасность протоколов UDP и TCP.	4	ПСК-10.1, ПСК-10.5
	Итого	4	
3 Протоколы прикладного уровня	Безопасность веб-серверов.	4	ПСК-10.1, ПСК-10.5
	Безопасность электронной почты	4	
	Безопасность мессенджеров и IP-телефонии.	4	
	Безопасность DNS	4	
	Безопасность удаленного управления.	4	
	Итого	20	
Итого за семестр		28	

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
10 семестр				
1 Протоколы сетевого уровня	Подготовка к практическим занятиям, семинарам	2	ПСК-10.1, ПСК-10.5	Опрос на занятиях, Отчет по практическому занятию, Тест
	Проработка лекционного материала	3		
	Итого	5		
2 Протоколы транспортного уровня	Подготовка к практическим занятиям, семинарам	2	ПСК-10.1, ПСК-10.5	Опрос на занятиях, Отчет по практическому занятию, Тест
	Проработка лекционного материала	3		
	Итого	5		
3 Протоколы прикладного уровня	Подготовка к практическим занятиям, семинарам	10	ПСК-10.1, ПСК-10.5	Опрос на занятиях, Отчет по практическому занятию, Тест
	Проработка лекционного материала	6		
	Итого	16		
Итого за семестр		26		

Согласована на портале № 51106

Итого	26		

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
10 семестр				
Опрос на занятиях	10	10	10	30
Отчет по практическому занятию	10	15	15	40
Тест			30	30
Итого максимум за период	20	25	55	100
Нарастающим итогом	20	45	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	
	60 - 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

Согласована на портале № 51106

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Построение защищенных корпоративных сетей [Электронный ресурс] [Электронный ресурс]: учебное пособие / Р.Н. Ачилов. — Электрон. дан. — Москва : ДМК Пресс, 2013. — 250 с. — Режим доступа: https://e.lanbook.com/book/66472 (дата обращения: 01.06.2021).

12.2. Дополнительная литература

1. Компьютерные сети и службы удаленного доступа [Электронный ресурс] [Электронный ресурс]: справочник / О. Ибе. — Электрон. дан. — Москва : ДМК Пресс, 2007. — 336 с. — Режим доступа: https://e.lanbook.com/book/1169 (дата обращения: 01.06.2021).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Безопасность сетей ЭВМ [Электронный ресурс]: Методические указания для лабораторных и практических работ / Новохрестов А. К., Праскурин Г.А., 2014. – 99 с. [Электронный ресурс] — Режим доступа: https://disk.fb.tusur.ru/bsevm/practice.pdf (дата обращения: 01.06.2021).
2. Безопасность сетей ЭВМ [Электронный ресурс]: Методические указания для самостоятельной работы студента / Новохрестов А.К., Праскурин Г.А., 2014. – 4 с. [Электронный ресурс] — Режим доступа: https://disk.fb.tusur.ru/bsevm/independent_work.pdf (дата обращения: 01.06.2021).

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. http://www.elibrary.ru - научная электронная библиотека;
2. http://www.edu.ru - веб-сайт системы федеральных образовательных порталов;
3. http://edu.fb.tusur.ru/ - образовательный портал факультета безопасности;
4. https://fstec.ru/ - Федеральная служба по техническому и экспортному контролю.

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.

13.1.2. Материально-техническое и программное обеспечение для практических занятий

Лаборатория безопасности сетей ЭВМ / Лаборатория криптографии в банковском деле

учебная аудитория для проведения занятий практического типа, учебная аудитория для про-

Согласована на портале № 51106

ведения 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:

- Cisco Packet Tracer
- Система мониторинга Zabbix
- Microsoft Windows 10
- Анализатор трафика Wireshark
- Дистрибутив Kali Linux
- Межсетевой экран ИКС Lite
- МежсетевойэкранPositive Technologies Application Firewall Education
- Система анализа защищенности сети MaxPatrol Education
- Система обнаружения вторжений Snort
- Система обнаружения вторжений Suricata
- Средство построения виртуальных частных сетей OpenVPN

Согласована на портале № 51106

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.;
- 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

Согласована на портале № 51106

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

Согласована на портале № 51106

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

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

Согласована на портале № 51106

d) серверы и рабочие станции

21. Защита ресурсов сети от несанкционированного использования - это

a) охрана оборудования сети

b) защита ядра безопасности

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

Согласована на портале № 51106

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 и показателями безопасности – это …

a) выявление аномальной деятельности

b) анализ защищённости

c) аудит информационной безопасности

d) установка системы защиты

14.1.2. Вопросы для подготовки к практическим занятиям, семинарам

Безопасность протоколов маршрутизации и протокола IP.

Безопасность протоколов UDP и TCP.

Безопасность веб-серверов.

Безопасность электронной почты

Безопасность мессенджеров и IP-телефонии.

Безопасность DNS

Безопасность удаленного управления.

14.1.3. Темы опросов на занятиях

Протоколы маршрутизации. RIP. OSPF. IS-IS. Уязвимости и атаки на протоколы маршрутизации. Обеспечение безопасности протоколов маршрутизации.

Протоколы IPv4 и IPv6. Уязвимости и атаки на протокол IP. Обеспечение безопасности протокола IP.

Протокол UDP. Уязвимости и атаки на UDP. Обеспечение безопасности приложений на UDP.

Протокол TCP. Уязвимости и атаки на TCP. Обеспечение безопасности приложений на TCP.

Веб-служба. Протоколы HTTP, HTTPS, FTP. Уязвимости и атаки на веб-серверы. Обеспечение безопасности веб-серверов.

Электронная почта. Протоколы SMTP, POP3, IMAP. Уязвимости и атаки на почтовые серверы. Обеспечение безопасности почтовых серверов.

Протоколы передачи мгновенных сообщений. Уязвимости и атаки на IM-протоколы. Обеспечение безопасности при передаче сообщений. IP-телефония.

Протоколы удаленного управления. Telnet, SSH, RDP, VNC. Уязвимости и атаки на gротоколы удаленного управления. Обеспечение безопасности удаленного управления.

14.1.4. Зачёт

1. Протоколы маршрутизации. RIP. OSPF. IS-IS.
2. Уязвимости и атаки на протоколы маршрутизации.
3. Обеспечение безопасности протоколов маршрутизации.
4. Протоколы IPv4 и IPv6.
5. Уязвимости и атаки на протокол IP.
6. Обеспечение безопасности протокола IP.
7. Протокол UDP.
8. Уязвимости и атаки на UDP.
9. Обеспечение безопасности приложений на UDP.
10. Протокол TCP.
11. Уязвимости и атаки на TCP.
12. Обеспечение безопасности приложений на TCP.
13. Веб-служба.
14. Протоколы HTTP, HTTPS, FTP.
15. Уязвимости и атаки на веб-серверы.
16. Обеспечение безопасности веб-серверов.
17. Электронная почта. Протоколы SMTP, POP3, IMAP.
18. Уязвимости и атаки на почтовые серверы.
19. Обеспечение безопасности почтовых серверов.

Согласована на портале № 51106

20. Протоколы передачи мгновенных сообщений.
21. Уязвимости и атаки на IM-протоколы.
22. Обеспечение безопасности при передаче сообщений. IP-телефония.
23. Протоколы удаленного управления. Telnet, SSH, RDP, VNC.
24. Уязвимости и атаки на gротоколы удаленного управления.
25. Обеспечение безопасности удаленного управления.

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;
- 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;

Согласована на портале № 51106

– 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 № 51106