МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

22.03.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ Б1.В.ДВ.03.02 Организация защищенных вычислительных сетей

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

"Безопасность компьютерных систем и сетей" (по отрасли или в сфере профессиональной деятельности)

3. Квалификация (степень) выпускника: Специалист

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

кибербезопасности информационных систем

6. Составители программы:

Сафронов Виталий Владимирович, к.т.н., доцент кафедры кибербезопасности информационных систем

7. Рекомендована:
НМС факультета ПММ, протокол № 7 от 26.05.2023г.
Внесены изменения: протокол УС факультета ПММ, протокол № 8 от 27.02.2024г.
Рекомендована с изменениями: протокол НМС факультета ПМ, протокол № 5 от 22.03.2024г.

8. Учебный год: 2026/2027 **Семестр(ы):** 8

9. Цели и задачи учебной дисциплины

Даются общие принципы организации и функционирования современных открытых и закрытых сетей, современных средств анализа и обнаружения информационных атак и методов защиты информации в сетях. А также рассматриваются основные технологий, применяемые для обеспечения безопасности сетей.

В рамках дисциплины изучаются принципы и методы обеспечения безопасности и анализа современных сетевых технологий с построением виртуальных каналов и туннелей их научных основ. Современные технологии построения безопасных сетей с использованием межсетевых экранов, передача данных через интернет с использованием шифрования, обеспечение конфиденциальности передаваемых данных через открытый канал.

10. Место учебной дисциплины в структуре ОПОП: дисциплина относится к вариативной части блока Б1 дисциплин учебного плана.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения

Код	Название компетенции	Код(ы)	Индикаторы(ы)	Планируемые результаты обучения
ПК-1	Способен проводить анализ требований и выполнять работы по проектированию программных и аппаратных компонент системы безопасности компьютерных систем и сетей, в том числе с использованием современных методов и средств защиты информации	ПК-1.4	проводит оценку соответствия механизмов безопасности компьютерной системы требованиям нормативных документов, а также их корректности существующим рискам;	Знает: требования нормативных документов оценки соответствия механизмов безопасности компьютерной системы. Умеет: проводить оценку соответствия механизмов безопасности компьютерной системы требованиям нормативных документов, а также их корректности существующим рискам.
ПК-2	Способен принимать участие в экспертизе и анализе уязвимостей, угроз и инцидентов информационной безопасности в компьютерных системах и сетях	ПК-2.4	разрабатывает модели угроз безопасности информации и нарушителей	Знает: модели угроз безопасности информации и нарушителей. Умеет: разрабатывать модели угроз безопасности информации и нарушителей.
ПК-3	Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных ,	ПК-3.2	знает методы администрирования систем управления событиями информационной безопасности, систем обнаружения и предотвращения вторжений, мониторинга событий и инцидентов	Знает: методы администрирования систем управления событиями информационной безопасности, систем обнаружения и предотвращения вторжений, мониторинга событий и инцидентов. Умеет: проводить анализ и формализацию

	исследовательских и прикладных задач	ПК-3.4	способен проводить анализ и формализацию поставленных задач в области безопасности компьютерных систем и сетей	поставленных задач в области безопасности компьютерных систем и сетей.	

12. Объем дисциплины в зачетных единицах/час - 3/108.
Форма промежуточной аттестации - зачет с оценкой.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			8			
Аудиторные занятия	48		48			
в том числе: лекции	16		28			
Практические	0		16			
Лабораторные	32		32			
Самостоятельная работа	60		60			
Контроль	0		0			
Итого:	108		108			
Форма промежуточной аттестации	зачет с оценкой		зачет с оценкой			

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Типовые угрозы сетевой безопасности	Сетевые атаки. Механизмы реализации атак в сетях TCP/IP. Методы перехвата сетевых соединений в сетях TCP/IP. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак.	Б1.В.ДВ.03.02 Организация защищенных вычислительных сетей (10.05.01)
1.2	Криптографические методы защиты информации в компьютерных сетях	Криптографические протоколы обеспечения безопасности. Защита виртуальных частных сетей (VPN). Разработка защищенных сетевых приложений.	
1.3	Программно-аппаратные средства обеспечения безопасности в компьютерных сетях	Средства защиты локальных сетей при подключении к Интернет. Защита серверов и рабочих станций. Средства и методы предотвращения и обнаружения вторжений.	
2. Лабораторные работы			
2.1	Строение сетей.	Изучение базовых механизмов получения информации о конфигурации сети. Получение навыков работы с различными программами, позволяющими определить конфигурацию сети или конфигурацию отдельного устройства в сети. Требуется для выполнения всех последующих лабораторных работ.	Б1.В.ДВ.03.02 Организация защищенных вычислительных сетей (10.05.01)
2.2	Удалённый доступ по протоколу SSH	Изучение возможностей протокола SSH для получения удалённого доступа к серверу. Применение функцию шифрования каналов связи при использовании протокола SSH.	

2.3	Использование VPN	Изучение возможностей программного обеспечения VPN для создания защищенных компьютерных сетей. Получение навыков работы со стандартным программным обеспечением для создания защищенных каналов связи.	
2.4	Работа с сертификатами SSL	Изучение возможностей центров сертификации (Certificate Authorities). Получение навыков работы с криптографическими ключами. Применение встроенных систем шифрования информации в стандартных приложениях операционных систем.	
2.5	Моделирование виртуальной сети	Ознакомление с методами моделирования сетей. Знакомство с телекоммуникационным оборудованием компании CISCO. Решение практических задач.	
2.6	Обнаружение вторжений	Изучение возможностей современного программного обеспечения для обнаружения вторжений. Управление правилами безопасности, анализ журналов событий.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)					
		Лекции	Практ.	Лаб. раб.	Самостоятельная работа	Контроль	Всего
1.1	Типовые угрозы сетевой безопасности	4	0	4	20	0	28
1.2	Криптографические методы защиты информации в компьютерных сетях	4	0	12	20	0	36
1.3	Программно-аппаратные средства обеспечения безопасности в компьютерных сетях	8	0	16	20	0	44
	Итого:	16	0	32	60	0	108

14. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины включает в себя лекционные занятия, лабораторные занятия и самостоятельную работу обучающихся. На первом занятии студент получает информацию для доступа к комплексу учебно-методических материалов.

Лекционные занятия посвящены рассмотрению теоретических основ дисциплины. Лабораторные занятия предназначены для формирования умений и навыков, закрепленных компетенциями по ОПОП. Самостоятельная работа студентов включает в себя проработку учебного материала лекций, разбор лабораторных заданий, подготовку к экзамену.

Для успешного освоения дисциплины рекомендуется подробно конспектировать лекционный материал, просматривать презентации (при наличии) по соответствующей теме, изучать основную и дополнительную литературу рекомендуемой библиографии,

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) : учебное пособие / О. И. Шелухин, Д. Ж. Сакалема, А. С. Филинова ; под редакцией О. И. Шелухина. – Москва : Горячая линия-Телеком, 2018. – 220 с. – ISBN 978-5-9912-0323-4. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/111119. – Режим доступа: для авториз. пользователей.
2	Костин, В. Н. Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей : учебное пособие / В. Н. Костин. – Москва : МИСИС, 2018. – 31 с. – ISBN 978-5-906953-53-7. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/116743. – Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
3	Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях : учебное пособие / М. А. Иванов, И. В. Чугунков. – Москва : НИЯУ МИФИ, 2012. – 400 с. – ISBN 978-5-7262-1676-8. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/75810. – Режим доступа: для авториз. пользователей.
4	Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. – 2-е изд. – Москва : ИНТУИТ, 2016. – 368 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/100522. – Режим доступа: для авториз. пользователей.

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
5	Электронно-библиотечная система «Лань» - Режим доступа: https://e.lanbook.com
6	Электронный каталог Научной библиотеки Воронежского государственного университета. - Режим доступа: http//:www.lib.vsu.ru.
7	Криптографические протоколы (10.05.01)/Степанец Ю.А. - Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа

студентов: изучение теоретического материала; подготовка к лекциям, работа с учебно-методической литературой, подготовка отчётов по лабораторным работам, подготовка к экзамену.

Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебно-методический комплекс, который включает в себя: программу курса, учебные пособия и справочные материалы, методические указания по выполнению заданий лабораторных работ. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение)

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий. Для организации занятий рекомендован онлайн-курс «Б1.В.ДВ.03.02 Организация защищенных вычислительных сетей (10.05.01)», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15в.5.

18. Материально-техническое обеспечение дисциплины

Учебная аудитория для лекций: специализированная мебель, компьютер преподавателя, мультимедийный проектор, экран.

Учебная аудитория для лабораторных занятий: специализированная мебель, персональные компьютеры, мультимедийный проектор, экран, лабораторное оборудование программно-аппаратных средств обеспечения информационной безопасности.

Аудитория для самостоятельной работы: учебная мебель, компьютер с возможностью подключения к сети «Интернет» и электронной платформе Электронного университета ВГУ.

Программное обеспечение (см.файл МТО): ОС Windows v.7, 8, 10, набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Типовые угрозы сетевой безопасности	ПК-1	ПК-1.4	устный опрос, тест, лабораторная работа
		ПК-2	ПК-2.4	
2	Криптографические методы защиты информации в компьютерных сетях	ПК-1	ПК-1.4	устный опрос, тест, лабораторная работа
		ПК-2	ПК-2.4	
3	Программно-аппаратные средства обеспечения безопасности в компьютерных сетях	ПК-3	ПК-3.2	устный опрос, тест, лабораторная работа
			ПК-3.4	
Промежуточная аттестация, форма контроля - зачет с оценкой				Перечень вопросов (КИМ№1)

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

- лабораторные работы.

Перечень лабораторных работ

1	Строение сетей.	Изучение базовых механизмов получения информации о конфигурации сети. Получение навыков работы с различными программами, позволяющими определить конфигурацию сети или конфигурацию отдельного устройства в сети. Требуется для выполнения всех последующих лабораторных работ.
2	Удалённый доступ по протоколу SSH	Изучение возможностей протокола SSH для получения удалённого доступа к серверу. Применение функцию шифрования каналов связи при использовании протокола SSH.
3	Использование VPN	Изучение возможностей программного обеспечения VPN для создания защищенных компьютерных сетей. Получение навыков работы со стандартным программным обеспечением для создания защищенных каналов связи.
4	Работа с сертификатами SSL	Изучение возможностей центров сертификации (Certificate Authorities). Получение навыков работы с криптографическими ключами. Применение встроенных систем шифрования информации в стандартных приложениях операционных систем.
5	Моделирование виртуальной сети	Ознакомление с методами моделирования сетей. Знакомство с телекоммуникационным оборудованием компании CISCO. Решение практических задач.
6	Обнаружение вторжений	Изучение возможностей современного программного обеспечения для обнаружения вторжений. Управление правилами безопасности, анализ журналов событий.

Технология проведения

Все лабораторные работы обязательны для выполнение. Задание является общим для всех, выполняется индивидуально под наблюдением преподавателя.

Критерии оценивания

- оценивается «зачтено», если работа выполнена в полном объеме (приведены все задания, и они правильные, даны пояснения);

оценивается «не зачтено», работа выполнена не полностью или в представленной части много ошибок

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: вопросы к зачету с оценкой.

Перечень вопросов к зачету с оценкой (КИМ №1)

1. Стадии проведения сетевой атаки.
2. Классификация сетевых угроз, уязвимостей и атак.
3. Атаки на реализации сетевых протоколов, отдельные узлы и службы.
4. Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI.
5. Проблемы обеспечения конфиденциальности, целостности и доступности информации на различных уровнях модели ISO/OSI.
6. Удалённое определение версии ОС с использованием особенностей реализации стека протоколов TCP/IP.

7. Методы сканирования портов.
8. Методы обнаружения пакетных сниферов. Методы обхода МЭ.
9. Имперсонация вслепую. Десинхронизация TCP-соединений.
10.Атаки, направленные на сетевую инфраструктуру.
11.Принуждение к ускоренной передаче. Атаки, направленные на отказ в обслуживании.
12.Изменение конфигурации и состояния хостов. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации.
13.Технические меры защиты от сетевых атак.
14.Протоколы аутентификации на прикладном уровне.
15.Протокол Kerberos. Протоколы аутентификации на транспортном уровне. Протокол SSL/TLS.
16.Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI.
17. Назначение, основные возможности, принципы функционирования и варианты реализации VPN.
18.Организация туннелирования на различных уровнях модели ISO/OSI. Достоинства и недостатки применения VPN.
19.Протокол IPSEC. Протоколы AH и ESP. Особенности работы протокола IP SEC в туннельном и
транспортном режимах.
20. Протокол управления ключами ISAKMP/Oakley. Использование протокола L2TP для организации виртуальных частных сетей.
21.Аутентификация, шифрование, обеспечение целостности с использованием программного
интерфейса SSPI. Программный интерфейс OpenSSL.
22.Межсетевые экраны (МЭ). Место и роль МЭ в обеспечении сетевой безопасности.
23.Классификация МЭ. Требования к МЭ. Основные возможности и схемы развертывания МЭ.
24.Достоинства и недостатки МЭ. Построение правил фильтрации.
25.Методы сетевой трансляции адресов (NAT). Шлюзы уровня приложений.
26.Реализация сетевой политики безопасности с использованием МЭ. Методы обхода межсетевых экранов.
27.Системы обнаружения вторжений (СОВ).
28.Назначение и возможности средств обнаружения вторжений на хосты, протоколы и сетевые службы.
29.Место и роль средств обнаружения вторжений в общей системе обеспечения сетевой безопасности.
30.Классификация СОВ. Выявление атак на основе сигнатур атак и выявления аномалий.
31.Аудит прикладных служб. Средства обнаружения уязвимостей сетевых служб.
32.Способы противодействия вторжениям.
33.Системы виртуальных ловушек (Honey Pot и Padded Cell).

Критерии оценки ответов на вопросы зачета с оценкой

Для оценивания результатов обучения на зачете с оценкой используется - 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», критериоценивания приведены ниже.

Оценка «отлично» - студент демонстрирует глубокое понимание темы, умеет распространять вытекающие из теории выводы.

Оценка «хорошо» - студент демонстрирует понимание теоретических положений темы и базовых понятий, но допускает неточности в ответах, испытывает затруднения в применении знаний к анализу состояния проекта.

Оценка «удовлетворительно» - студент отвечает не на все предложенные вопросы, но не менее, чем на половину из них; не демонстрирует способности применения теоретических знаний для анализа ситуаций.

Оценка «неудовлетворительно» - студент демонстрирует непонимание теоретических основ и базовых понятий курса.

Оценка промежуточной аттестации формируется как интегральная оценка по следующей формуле (При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». При этом, все лабораторные работы должны быть выполнены и защищены

$$Q_{пром\_ат} = 0{,}2Q_{КР1} + 0{,}2Q_{КР2} + 0{,}6Q_{экз}$$

При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». При этом, все лабораторные работы должны быть выполнены и защищены.

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

закрытые задания (тестовые, средний уровень сложности):

ПК-1. Способен проводить анализ требований и выполнять работы по проектированию программных и аппаратных компонент системы безопасности компьютерных систем и сетей, в том числе с использованием современных методов и средств защиты информации;

1. Наименее помехоустойчивыми являются линии связи….
неэкранированная
витая пара;
беспроводные
(радиолинии);
экранированная
витая пара.
2. Для сети с маской 255.255.255.0 соответствующий блок адресного пространства конечных хостов составит…
255;
600;
4.
3. Узлы, между которыми устанавливается защищённый канал, называются…
точками
доступа
контрольными
точками
шлюзами
безопасности.
4. Канальный уровень модели OSI отвечает за...
логическую
доставку данных по наиболее оптимальному пути;
коммутацию;
IPадресацию;
MACадресацию.
5. По какому типу оптического волокна можно передавать несколько разных сигналов одновременно?
одномодовое;
многомодовое;
мультимодовое.
6. Какой термин описывает состояние сети, когда спрос на сетевые ресурсы превышает доступную мощность?
синхронизация;
конвергенция;
перегрузка;
оптимизация.
7. Какой интерфейс позволяет удаленно управлять коммутатором уровня
первый
интерфейс порта Ethernet;
интерфейс

консольного порта;
виртуальный
интерфейс коммутатора;
интерфейс
AUX.
8. Конфигурация (топология) локальной компьютерной сети, в которой
все рабочие станции последовательно соединены друг с другом, называется:
сетевой;
кольцевой;
шинной.

ПК-2. Способен принимать участие в экспертизе и анализе уязвимостей, угроз и инцидентов информационной безопасности в компьютерных системах и сетях

Вопрос 1. Укажите, верно ли утверждение, что вопросы безопасности физической инфраструктуры вычислительных сетей могут быть решены при помощи инженерно-технических мер защиты:
а. верно, поскольку инженерно-технические меры защиты обеспечивают безопасность объекта информатизации, что означает безопасность и располагающихся на нем элементов вычислительных сетей.
б. не верно, поскольку инженерно-технические меры защит обеспечивают только безопасность объекта информатизации и носителей информации
ОТВЕТ: а.
Вопрос 2. Для чего необходим контроль доступа к кабельным конструкциям и физическим линиям связи, входящим в состав вычислительных сетей?
а. предотвращение намеренных и непреднамеренных повреждений линий связи, исключение контактного и бесконтактного съема передаваемых сигналов нарушителем
б. обеспечение качественной работы кабельных конструкций и линий связи за счет круглосуточного наблюдения и контроля в. контроль не нужен, а любые действия по контролю никак не влияют на безопасность вычислительных сетей
ОТВЕТ: а.
Вопрос 3. Укажите общие причины, приводящие к проблемам безопасности вычислительных сетей, связанные с активными компонентами сетевой инфраструктуры:
а. невыявленные недостатки программного обеспечения активных компонент
б. способы связи активных компонент между собой
в. ошибки в настройках и конфигурационных файлах активных компонент
г. аппаратная составляющая активных компонент
д. бренд, производитель активных компонент и политическая обстановка в мире
ОТВЕТ: а, б, г.
Вопрос 4. Укажите общие причины, приводящие к проблемам безопасности вычислительных сетей, связанные с применяемыми сетевыми протоколами обмена данными:
а. открытые спецификации, позволяющие злоумышленникам хорошо разбираться в принципах работы и организации обмена данными
б. устаревшие спецификации, не предусматривающие никаких подходов к решению проблем информационной безопасности сетевого обмена данными в. возможности перехода к «нештатным» режимам и алгоритмам осуществления сетевого обмена, не противоречащим основным принципам спецификаций
г. все перечисленное выше
ОТВЕТ: г.
Вопрос 5. Необходимо ли специалисту по защите информации досконально знать особенности взаимосвязи и работы множества компонентов распределенной многокомпонентной ИС, функционирующей с использованием вычислительных сетей?:
а. необходимо, поскольку могут использоваться сторонние компоненты с независимым режимом обновления, либо компоненты распределенной ИС могут использоваться сторонними приложениями
б. это не нужно, поскольку специалист по защите информации обеспечивает общую защиту вычислительных сетей
ОТВЕТ: а.
Вопрос 6. Влияет ли безопасная и правильная работа вспомогательных систем электропитания и кондиционирования/вентиляции на предприятии на безопасную работу вычислительных сетей:
а. не влияет, поскольку эти системы никак не связаны с работой активных и пассивных компонентов вычислительных сетей и используемых протоколов обмена данными
б. влияет, поскольку указанные вспомогательные системы обеспечивают штатный режим работы компонентов вычислительных сетей, и их выход из строя или нарушение работы приведет к сбоям или отказу компонентов вычислительных сетей
ОТВЕТ: б.
Вопрос 7. Предусматривает ли базовый стандарт Ethernet (IEEE 802.3) какие-либо меры или механизмы, обеспечивающие безопасность сетевого обмена с точки зрения конфиденциальности, целостности или доступности?:
а. не предусматривают, вычисление CRC (контр. суммы) не является решением задачи обеспечения целостности
б. предусматривают, в стандарте есть подходы к аутентификации сторон обмена друг перед другом, обеспечение целостности и решение вопросов доступности в. предусматривают частично, решены вопросы аутентификации сторон и обеспечения целостности обмена г. предусматривают частично, решены вопросы обеспечения только целостности за счет вычисления контрольной суммы (CRC) для проверки правильности каждого отправления

ОТВЕТ: а.
Вопрос 8. Верно ли утверждение, что использование самых простых сетевых коммутаторов Ethernet позволяет решить вопросы безопасности сетевого обмена на канальном уровне:
а. не верно, принципы и алгоритмы работы коммутаторов никаких вопросов безопасности не решают
б. не верно, несмотря на то, что принцип коммутации сетевых отправлений от одной стороны к другой и применение технологии VLAN позволяет изолировать двусторонний обмен от остальных участников сети в. верно, поскольку принцип коммутации сетевых отправлений от одной стороны к другой и применение технологии VLAN позволяет изолировать двусторонний обмен от остальных участников сети г. верно, поскольку работа самых простых сетевых коммутаторов учитывает необходимость решать вопросы обеспечения конфиденциальности, целостности и доступности сетевого обмена
ОТВЕТ: а.
Вопрос 9. Является ли проблема неконтролируемого подключения к сети Ethernet одной из проблем сетевой безопасности?:
а. является, поскольку алгоритм работы сетевых коммутаторов и стандарт Ethernet позволяют включиться в сетевой обмен любым устройствам
б. не является, поскольку стандартный алгоритм работы сетевых коммутаторов учитывает вопросы контроля и ограничений в момент включения новых устройств в сеть Ethernet в. не является, поскольку сетевой администратор решает подобные вопросы на организационном уровне в виде регламента работы пользователей «под роспись» и постоянно контролирует исполнение регламента работы
ОТВЕТ: а.
Вопрос 10. Укажите причины, по которой неконтролируемое подключение к сети Ethernet является проблемой сетевой безопасности:
а. особенность алгоритма штатной работы коммутаторов Ethernet по автоматическому изучению поступающих на порты коммутаторов кадров и заполнению таблицы коммутации
б. физическая удаленность точек подключения рабочих станций и иных устройств от сетевых портов коммутатора Ethernet при помощи СКС
в. автоматическое подключение сетевых устройств к коммутаторам Ethernet в момент их нахождения рядом друг с другом
г. простота проводного подключения стороннего устройства к порту СКС организации и далее – к сетевому коммутатору Ethernet
ОТВЕТ: а, б, г.

ПК-3. Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и прикладных задач

Вопрос 1. Принцип сетевой атаки MAC-Flooding (переполнение таблицы коммутации) заключается в:
а. отправке большого количества кадров Ethernet со случайным заполнением поля MAC-адреса отправителя на порт коммутатора Ethernet для переполнения заполняемой автоматически таблицы коммутации
б. отправке большого количества кадров Ethernet со случайным заполнением поля MAC-адреса получателя на порт коммутатора Ethernet для переполнения заполняемой автоматически таблицы коммутации в. отправке большого количества кадров Ethernet с заполнением поля MAC-адреса получателя широковещательным адресом на порт коммутатора Ethernet для переполнения заполняемой автоматически таблицы коммутации
ОТВЕТ: а.
Вопрос 2. Каковы последствия успешной сетевой атаки MAC-Flooding (переполнение таблицы коммутации)?:
а. переполнение таблицы коммутации приводит к затиранию существующих «правильных» записей и переводит коммутатор в режим «хаба» с ретранслированием всего сетевого обмена на все доступные порты
б. переполнение таблицы коммутации приводит к переходу в режим ретранслирования всего сетевого обмена на единственный порт нарушителя в. переполнение таблицы коммутации приводит к отказу и выходу из строя коммутатора Ethernet
ОТВЕТ: а.
Вопрос 3. Применение технологии VLAN 802.1Q на коммутаторе Ethernet позволяет предотвратить сетевую атаку MAC-Flooding (переполнение таблицы коммутации)?:
а. позволяет, поскольку технология VLAN 802.1Q создавалась специально для решения этой проблемы
б. не позволяет, применение технологии VLAN 802.1Q в ходе атаки всего лишь ограничивает работу коммутатора в режиме «хаба» с ретранслированием всего сетевого обмена группой включенных в определенный VLAN портов коммутатора в. позволяет, поскольку применение технологии VLAN 802.1Q полностью изменяет алгоритм автоматического заполнения таблицы коммутации
ОТВЕТ: б.
Вопрос 4. Каким встроенным средством интеллектуальных коммутаторов Ethernet можно попробовать частично решить проблему неконтролируемого подключения к сети Ethernet:
а. применением статических записей в таблице коммутации
б. включением уведомлений о подключении сетевых устройств к портам коммутатора в. включением веб-ориентированного интерфейса управления интеллектуальным коммутатором
ОТВЕТ: а.
Вопрос 5. Применение ограничителей и списков доступа (ACL) на порту коммутатора Ethernet позволяет:
а. ограничить поступающие на порт Ethernet-кадры только определенными кадрами с MAC-адресами отправителей, включенными в список доступа
б. ограничить количество разных MAC-адресов отправителя, которые могут быть изучены на конкретном порту коммутатора и добавлены в качестве записи в таблицу коммутации в. ограничить подключающиеся на порт коммутатора

сетевые устройства в зависимости от типа операционной системы (управляющей системы) сетевых устройств г. ограничить подключающиеся на порт коммутатора сетевые устройства в зависимости от имени работающего с сетевым устройством пользователя
ОТВЕТ: а, б.

1) открытые задания (тестовые, средний уровень сложности):

ПК-1. Способен проводить анализ требований и выполнять работы по проектированию программных и аппаратных компонент системы безопасности компьютерных систем и сетей, в том числе с использованием современных методов и средств защиты информации;

Вопрос 1. Поясните базовые меры обеспечения безопасности физической инфраструктуры локальных вычислительных сетей?
ОТВЕТ: Защита кабельных линий и каналов, серверных помещений и точек коммутации инженерно-техническими методами от повреждения и непосредственных физических воздействий и включений; хранение проектной документации для согласования иных работ в местах прохождения кабельных линий; ведение эксплуатационной документации в точках коммутации и обеспечение на них общего порядка. Дополнительно – разрешение вопросов гарантированного электропитания и работы систем климат-контроля серверных помещений и промежуточных узлов размещения активного оборудования.
Вопрос 2. Раскройте причину основных проблем обеспечения безопасности работы активного сетевого оборудования?
ОТВЕТ: Недостатки программного обеспечения активного сетевого оборудования, которыми может воспользоваться злоумышленник для перевода в нештатный режим работы; ошибки настройки сетевого оборудования, влияющие на информационный обмен в локальной сети; аппаратные дефекты и сбои.
Вопрос 3. Чем опасна некорректная настройка активного сетевого оборудования с точки зрения безопасности ?
ОТВЕТ: Неправильная конфигурация приводит к изменению корректных режимов коммутации и маршрутизации, а также к блокированию или неправильному разрешению сессий и сеансов информационного обмена.
Вопрос 4. Влияет ли сбой в работе вспомогательных систем климат-контроля, электропитания и наблюдения на работу вычислительных сетей и наоборот ?
ОТВЕТ: Вспомогательные системы могут использовать возможности корпоративных вычислительных сетей для обеспечения своей работы. В этом случае сбой в работе сети может вызвать сбой в работе вспомогательных систем. И наоборот, сбой в работе систем климат-контроля, например, может приводить к перегреву и выходу из строя активного сетевого оборудования.
Вопрос 5. Опишите с позиции безопасности недостатки технологии Ethernet ?
ОТВЕТ: Отсутствует понятие аутентификации сторон при установлении обмена. Отсутствует механизм обеспечения конфиденциальности обмена. Отсутствует механизм обеспечения целостности обмена. Отсутствует механизм исключения петель (looping) (ETH-кадры – вечноживущие!).
Вопрос 6. Почему технологию VLAN 802.1Q нельзя в полной мере считать хорошим решением для организации безопасного сетевого обмена в корпоративной сети ?
ОТВЕТ: Разделение кадров Ethernet на независимые VLAN происходит «виртуально» исключительно благодаря алгоритму работы сетевого оборудования с небольшой модификацией исходного заголовка кадра Ethernet, весь обмен на самом деле происходит по прежнему в единой среде.
Вопрос 7. Поясните суть проблемы неконтролируемого подключения к корпоративной сети стандарта Ethernet?
ОТВЕТ: С использованием СКС реальные места подключения оконечного оборудования удаляются на десятки метров от портов сетевых коммутаторов. В самих коммутаторах штатный алгоритм обеспечивает автоматическое вовлечение в сетевой обмен любого подключенного активного оборудования.
Вопрос 8. Опишите суть атаки MAC-Flooding (переполнение таблицы коммутации FDB)?
ОТВЕТ: Суть атаки – отправка на порт коммутатора большого числа Eth-фреймов, содержащих фальшивые сетевые идентификаторы (MAC-адреса отправителя). Постоянное обновление FDB приводит к затиранию старых записей и поддержанию FDB в заполненном состоянии. Отсутствие возможности внести «легитимную» запись о реальных участниках обмена в FDB превращает коммутатор в «неинтеллектуальный хаб» – с ретранслированием всего обмена на все доступные порты.
Вопрос 9. Какой самый простой механизм противодействия неконтролируемому подключению к сети Ethernet можно найти на интеллектуальных коммутаторах?
ОТВЕТ: Создание статических записей в таблице коммутации.
Вопрос 10. Поясните суть работы статических записей для противодействия неконтролируемому подключению к сети Ethernet ?
ОТВЕТ: Появление статическкой записи делает связь MAC-адреса получателя с определенным портом постоянной. В этом случае, появление дублирующей записи будет исключаться, а оборудование всегда будет коммутировать адресуемые кадры в строго определенный порт.

ПК-2. Способен принимать участие в экспертизе и анализе уязвимостей, угроз и инцидентов информационной безопасности в компьютерных системах и сетях

Вопрос 1. Решает ли полностью использование статических записей проблему неконтролируемого подключения к сети Ethernet ?
ОТВЕТ: Не решает. Подключение на «занятый» порт абсолютно нового устройства будет выполнено согласно штатному алгоритму работы коммутаторов с возможностью последующего обмена кадрами.
Вопрос 2. Поясните суть работы списков доступа (ACL), применяемых на портах коммутаторов Ethernet?

ОТВЕТ: Механизм фильтрации поступающих на порт коммутатора кадров Ethernet сверяет адреса отправителя со списком ACL и пропускает или отбрасывает кадры согласно разрешениям списка.
Вопрос 3. Решает ли полностью использование списков доступа (ACL) проблему неконтролируемого подключения к сети Ethernet?
ОТВЕТ: Решает почти полностью, поскольку механизм фильтрации может обеспечивать поступление и дальнейшую коммутацию только кадров от определенного устройства (с определенным MAC-адресом). Единственная проблема – подделка или дублирование разрешенного MAC-адреса устройства на другом устройстве нарушителя.
Вопрос 4. Какие популярные технологии применяются в корпоративных сетях Ethernet для исключения потенциальных «петель» и зацикливания кадров ?
ОТВЕТ: Применяются технологии STP/RSTP/MSTP, а также метод исключения петель с использованием кадров ECTP
Вопрос 5. Поясните задачу технологии 802.1X в корпоративных сетях Ethernet ?
ОТВЕТ: Технология 802.1X обеспечивает идентификацию и аутентификацию подключаемых к корпоративной сети устройств.
Вопрос 6. Возможен ли произвольный обмен кадрами Ethernet между оконечным устройством и коммутатором, работающим с поддержкой технологии 802.1X ?
ОТВЕТ: Если порт коммутатора настроен на работу с поддержкой технологии 802.1X, то произвольный обмен кадрами невозможен до полного прохождения процедуры идентификации и аутентификации подключенного устройства.

ПК-3. Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и прикладных задач

Вопрос 1. Чем выгодно использование единого сервера аутентификации (сервера безопасности) для корпоративной сети с поддержкой технологии 802.1X ?
ОТВЕТ: Использование единого сервера аутентификации (сервера безопасности) позволяет образовать единую точку хранения идентификационной и аутентификационной информации, а также дает возможность жестко контролировать порт и идентификатор оборудования, к которому подключается оконечное устройство.
Вопрос 2. Какой протокол используется для обмена данными между оконечным устройством и сетевым коммутатором в случае поддержки технологии 802.1X?
ОТВЕТ: Поддерживается протокол EAP (Extensible Athentication Protocol) в варианте EAP over LAN (EAPoL).
Вопрос 3. Какой протокол используется для обмена данными между сетевым коммутатором и сервером аутентификации в случае поддержки технологии 802.1X?
ОТВЕТ: Поддерживается протокол RADIUS.
Вопрос 4. Какие существуют решения, позволяющие плавно интегрировать в работу сети с технологией 802.1X оконечные устройства, не поддерживающие эту технологию по умолчанию?
ОТВЕТ: Возможность перевода порта коммутатора в т.н. «гостевой» VLAN при отсутствии обмена кадрами EAPoL.

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).