

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ
Декан ФИиВТ

УТВЕРЖДАЮ /А.А. Кречетов/
(Ф.И.О. декана (директора института))

02.02.2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

С.1.1.48 Системы обнаружения и предотвращения компьютерных атак

(код и наименование дисциплины по учебному плану)

Направление подготовки (специальность)	10.05.03 Информационная безопасность автоматизированных систем
Квалификация выпускника	Специалист (бакалавр/магистр/специалист)
Специализация	Безопасность автоматизированных систем критически важных объектов

Курс	5
Семестр	10

Распределение учебного времени

Трудоемкость по учебному плану	144 / 4	часов/зачетных единиц
Лекции	32	часов
Лабораторные работы	-	часов
Практические занятия	48	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	80	часов
Контактная работа по экзамену	-	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	64	часов
Самостоятельная работа по подготовке к экзамену	-	часов
Экзамен	-	семестр
Зачет	-	семестр
БРК, ДЗ	10	семестр

(год)

Программа составлена в соответствии с требованиями ФГОС ВО направления подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем

Программу составили:

доцент с ученой степенью кандидата наук	ИБ	СОГЛАСОВАНО	А.А. Кречетов
(должность)	(кафедра)		(И.О. Фамилия)

РАССМОТРЕНА и ОДОБРЕНА на заседании кафедры, за которой закреплена дисциплина
Кафедра информационной безопасности

	(наименование кафедры)	
31.01.2022	протокол №	5
(дата)		
Заведующий кафедрой	СОГЛАСОВАНО	И.Г. Сидоркина
		(И.О. Фамилия)

Рабочая программа СОГЛАСОВАНА с факультетом (институтом), выпускающей(ими)
кафедрой(ами).
СООТВЕТСТВУЕТ действующей ОП.

Заведующий кафедрой	СОГЛАСОВАНО	И.Г. Сидоркина
		(И.О. Фамилия)

Председатель методической комиссии факультета (института), в который входит
выпускающая кафедра

	СОГЛАСОВАНО	А.А. Кречетов
		(И.О. Фамилия)

Эксперт(ы): Зверева Екатерина Васильевна, Начальник отдела ПД ИТР ОАО ММЗ

Рабочая программа проверена и зарегистрирована в УМЦ 07.02.2022 г.
Специалист учебно-методического центра СОГЛАСОВАНО /Т.А. Смирнова/

Раздел 1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является достижение планируемых результатов обучения, соответствующих установленным в ОПОП индикаторам достижения компетенций:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
1. ОПК-19 Способен разрабатывать системы защиты информации, функционирующие на критически важных объектах и в автоматизированных системах критически важных объектов	ОПК-19.1 знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	знания: принципы построения современных систем обеспечения информационной безопасности; - принципы статистического анализа; - способы описания поведения системы умения: навыки:
	ОПК-19.2 умеет оценивать информационные риски в автоматизированных системах	знания: умения: - формализовать задачу контроля параметров безопасности информационными системами навыки:
	ОПК-19.3 Владеть методами анализа структурных и функциональных схем защищенных автоматизированных информационных систем	знания: умения: навыки: - средствами фиксации параметров безопасности информационных систем; - методами оценки рисков информационной безопасности

Раздел 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к обязательной части ОПОП.

Дисциплина является обязательной

Для продолжения формирования заявленных компетенций необходимы знания предшествующих дисциплин: Интеллектуальные системы информационной безопасности (ОПК-19)

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих государственной итоговой аттестации в форме: Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-19)

Раздел 3. ОПИСАНИЕ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

Для формирования заявленных компетенций используются методологические технологии, реализующие деятельностный, личностно-ориентированный, практико-ориентированный подходы.

Основными стратегическими технологиями являются: лекционные занятия, практические и лабораторные занятия

На достижение конкретных целей обучения направлены применяемые тактические технологии: задания, классическая лекция

Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

10 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
Системы обнаружения и предотвращения компьютерных атак	144	ОПК-19

Лекция. Системы обнаружения вторжений	16
Лекция. Система обнаружения вторжений Snort	16
Практическое занятие. Настройка интерфейсов виртуальных машин	8
Практическое занятие. Fail2Ban	10
Практическое занятие. Конфигурация правила для SOV	10
Практическое занятие. Развертывание открытых списков правил	10
Практическое занятие. Подключение средства мониторинга Barnyard2	10
Задания для самостоятельной работы, в том числе выполнение Проработка лекций	
Подготовка к практическим занятиям	64
Иная контактная работа: дифференцированный зачет (БРК)	0

Раздел 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины (**модуля**) рекомендуется начать с ознакомления с рабочей программой, ее структурой и содержанием разделов. Учебный материал структурирован, изучение дисциплины осуществляется в тематической последовательности. **Занятия лекционного типа** дают систематизированные знания по дисциплине (**модулю**), концентрируют внимание на наиболее сложных и важных вопросах. Во время лекционных занятий рекомендуется вести конспектирование учебного материала; обращать внимание на формулировки и категории, раскрывающие суть проблемы, явления или процесса; зафиксировать выводы и практические рекомендации. (**при наличии**) Содержание **самостоятельной работы** определяется рабочей программой дисциплины (**модуля**), оценочными и методическими материалами, заданиями и указаниями преподавателя. Самостоятельная работа может осуществляться в аудиторной и внеаудиторной формах. Эффективным средством осуществления самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к образовательной программе, рабочей программе дисциплины (**модуля**), к электронным библиотечным системам, профессиональным базам данных и информационным справочным системам. Изучение дисциплины (**модуля**) включает выполнение **лабораторной работы**. Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплин представлены в рабочей программе. Формой промежуточной аттестации по дисциплине (**модулю**) является **балльно-рейтинговый контроль**.

Раздел 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-методическое обеспечение

№№ п/п	Список используемой литературы	Количество экземпляров печатных изданий, имеющих в библиотеке, или электронный адрес издания (ресурса) в сети Интернет
УЧЕБНЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И НАУЧНЫЕ ИЗДАНИЯ		
1.	Кречетов, Александр Александрович. Методы анализа используемых средств защиты информации от	20 / https://portal.volgatech.net/b

	несанкционированного доступа [Текст] : учебное пособие / А. А. Кречетов. Йошкар-Ола: МарГТУ, 2007. - 142 с. Экземпляры: всего 20.	ooks/krechetov_metody.pdf
2.	Мельников, Виталий Викторович. Безопасность информации в автоматизированных системах [Текст] / В. В. Мельников. М.: Финансы и статистика, 2003. - 367 с. ISBN 5-279-02560-7. Экземпляры: всего 20.	20
3.	Кияев, В. И. Безопасность информационных систем [Электронный ресурс] / Кияев В. И., Граничин О. Н. 2-е изд. Москва: ИНТУИТ, 2016. - 191 с.	https://e.lanbook.com/book/100580
4.	Зима, Владимир М. Безопасность глобальных сетевых технологий [Текст] / Зима Владимир М., Молдовян Александр А., Молдовян Николай А. 2-е изд. СПб.: БХВ-Петербург, 2003. - 362 с. ISBN 5-94157-213-1. Экземпляры: всего 5.	5
ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ		
1.	Справочно-правовая система Консультант+	http://www.consultant.ru
2.	Информационно-правовой портал Гарант	http://www.garant.ru
3.	Профессиональные справочные системы Техэксперт	http://www.cntd.ru

6.2. Материально-техническая база и программное обеспечение

№№ п/п	Аудитории для проведения учебных занятий, самостоятельной работы и проведения государственной итоговой аттестации	Перечень основного оборудования	Программное обеспечение
1.	107 (III)	Анализатор линейных коммуникаций УЛАН-2 (1), Генератор шума Соната -P2 (1), Доска маркерная 100*200см (1), ИБП UPS 1100VA (7), Коммутатор D-Link DES-3200-28 (8), Коммутатор D-Link DES-3810-28 (2), Комплекс защиты информации Secret Disk 4.0 (1), Комплекс защиты информации Secret Net 5.0 (2), Компьютер RAMEC STORM Custom i7-3770K/8ГБ/ монитор LCD 21.5", клавиат.,мышь (15), Нелинейный локатор SEL SP-61/M "Катран" (1), ПК Intel Core i7/GA-Z77-D3H/DDRIII 8Gb/500Gb SATA II/INWIN ATX-450, Монитор BenQ G2450HM,клав,мышь (3), ПК Intel Core i7/GA-Z77-D3H/DDRIII 8Gb/500Gb SATAIII/INWIN EAR003, Монитор 24" BenQ G2450HM,клав,мышь (2), Проектор мультимедийный Hitachi CP-X1250+разветвитель видеосигнала	Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ПО для решения основных пользовательских задач

	(1), Система виброакустической защиты "Соната-АВ" (1), Система виброакустической защиты "Соната-РС2" (1), Средства ограничения доступа к компьютеру АПМДЗ "КРИПТОН-ЗАМОК/Е" (2), Экран настенный 200*200см Braun Roll Vision (1), Комплект учебной мебели (1)	
--	---	--

Раздел 7. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ/ ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Критерии оценивания индикаторов достижения компетенций направлены на:

- усвоение теоретического материала (объем знаний, глубина усвоения), предусмотренного рабочей программой;
- умение излагать материал (четкость, грамотность изложения материала, точность и полнота воспроизведения учебного материала);
- умение применять теоретические знания при решении практических заданий.

Шкала оценивания представлена ниже.

Уровень сформированности элементов компетенции	Критерии оценивания	Шкала оценивания
Пороговый уровень	Обучающийся имеет знания основного материала, проявляет умение логично его излагать, но может допускать неточности в изложении материала, недостаточно правильные формулировки, испытывает затруднения в выполнении практических заданий.	удовлетворительно
Продвинутый уровень	Обучающийся твердо знает программный материал, излагает его грамотно и по существу, не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения	хорошо
Высокий уровень	Обучающийся глубоко и прочно усвоил программный материал, грамотно и логически стройно его излагает, дает исчерпывающие ответы на поставленные вопросы. В ответе тесно увязывается теория с практикой, при этом обучающийся не затрудняется с ответом при видоизменении задания, свободно справляется с задачами, вопросами и другими видами применения знаний, показывает знакомство с монографической литературой, периодическими изданиями, правильно обосновывает принятые решения, свободно владеет разносторонними навыками, приемами выполнения практических работ	отлично

7.1. Текущий контроль успеваемости

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины (модуля) и производится с применением технологии рейтингового контроля в соответствии с технологической картой дисциплины. Порядок составления технологической карты и

алгоритм проведения процедуры оценивания видов деятельности обучающихся, направленных на освоение знаний, умений, навыков и/или опыта деятельности, по накопительной системе в баллах устанавливается положением о системе РИТМ в ФГБОУ ВО «ПГТУ»

7.2. Промежуточная аттестация обучающихся

Промежуточная аттестация обучающихся направлена на оценивание результатов обучения по дисциплине (модулю) и проводится с использованием фондов оценочных средств.

Примеры типовых контрольных заданий из базы фонда оценочных средств по образовательной программе.

1. Из каких составляющих складывается многоуровневая защита интрасетей?
2. Что такое политика безопасности интрасети? Каковы ее основные компоненты? Кто ее вырабатывает и каким образом? Какие к ней предъявляются требования?
3. Какие два вида категорий политик безопасности Вам известны?
4. Рассмотрите трастовые модели для интрасетей.
5. Из чего состоит содержание документа, описывающего политику безопасности интрасети организации?
6. Расскажите о четырех основных и некоторых специализированных политиках безопасности.
7. Рассмотрите некоторые меры защиты, связанные с обнаружением вторжений в интрасети.
8. Что такое сетевой аудит? Из чего он состоит?
9. Каково место систем обнаружения вторжений в многоуровневой защите интрасети?
10. Как эти системы взаимодействуют с сетевыми экранами?
11. Каков порядок развертывания в интрасети систем обнаружения вторжений?
12. Какую информацию для принятия решений используют системы обнаружения вторжений?
13. Как можно оценить эффективность работы системы обнаружения вторжений?
14. По каким критериям можно классифицировать системы обнаружения вторжений?
15. В каких случаях рекомендуется применять статические, а в каких динамические системы обнаружения вторжений?
16. Какие четыре типа систем обнаружения вторжений можно выделить?
17. Какие задачи решают системы контроля целостности файлов?
18. На основе какой информации и как работают мониторы регистрационных файлов?
19. Что Вам известно об эволюции систем обнаружения вторжений?
20. Что такое системное обнаружение вторжений? Каковы его достоинства и недостатки?

Какие системы этого типа Вам известны?

21. Что такое сетевое обнаружение вторжений? Каковы его достоинства и недостатки? Какие системы этого типа Вам известны?
22. В чем особенности систем обнаружения аномалий? Каковы их слабые и сильные стороны?
23. В чем особенности систем обнаружения злоупотреблений? Каковы их слабые и сильные стороны?
24. Что Вам известно о системах комплексного обнаружения вторжений?
25. Как можно охарактеризовать преимущества систем обнаружения вторжений?
26. Каковы проблемы, которые еще не решены в современных системах обнаружения вторжений?
27. Какие атаки предпринимаются злоумышленниками против самих систем обнаружения вторжений?
28. В чем проявляется ограниченность современных систем обнаружения вторжений?
29. Где в интрасети чаще всего размещаются сетевые системы обнаружения вторжений? В каких случаях какое размещение предпочтительно и почему?
30. Расскажите о двух специальных видах систем обнаружения вторжений - network grep и honeypot.
31. Какова роль хоста-бастиона при обнаружении вторжений в интрасети?
32. Каким образом система обнаружения вторжений реагирует на обнаруженные аномальные события в интрасети?
33. Какие способы повышения эффективности обнаружения вторжений в различных операционных системах (Windows, Unix, Macintosh) наиболее действенны?
34. Какова ситуация в области стандартов, регламентирующих обнаружение вторжений и реализующих его систем?
35. Перечислите основные характеристики перспективных систем обнаружения вторжений.
36. Расскажите о возможностях системы обнаружения злоупотреблений CMDS, подробнее останавливаясь на функциях, присущие именно этому типу COB.

Перечень вопросов для проведения промежуточной аттестации

37. Из каких составляющих складывается многоуровневая защита интрасетей?
38. Что такое политика безопасности интрасети? Каковы ее основные компоненты? Кто ее вырабатывает и каким образом? Какие к ней предъявляются требования?
39. Какие два вида категорий политик безопасности Вам известны?
40. Рассмотрите трастовые модели для интрасетей.
41. Из чего состоит содержание документа, описывающего политику безопасности интрасети организации?

42. Расскажите о четырех основных и некоторых специализированных политиках безопасности.
43. Рассмотрите некоторые меры защиты, связанные с обнаружением вторжений в интрасети.
44. Что такое сетевой аудит? Из чего он состоит?
45. Каково место систем обнаружения вторжений в многоуровневой защите интрасети?
46. Как эти системы взаимодействуют с сетевыми экранами?
47. Каков порядок развертывания в интрасети систем обнаружения вторжений?
48. Какую информацию для принятия решений используют системы обнаружения вторжений?
49. Как можно оценить эффективность работы системы обнаружения вторжений?
50. По каким критериям можно классифицировать системы обнаружения вторжений?
51. В каких случаях рекомендуется применять статические, а в каких динамические системы обнаружения вторжений?
52. Какие четыре типа систем обнаружения вторжений можно выделить?
53. Какие задачи решают системы контроля целостности файлов?
54. На основе какой информации и как работают мониторы регистрационных файлов?
55. Что Вам известно об эволюции систем обнаружения вторжений?
56. Что такое системное обнаружение вторжений? Каковы его достоинства и недостатки? Какие системы этого типа Вам известны?
57. Что такое сетевое обнаружение вторжений? Каковы его достоинства и недостатки? Какие системы этого типа Вам известны?
58. В чем особенности систем обнаружения аномалий? Каковы их слабые и сильные стороны?
59. В чем особенности систем обнаружения злоупотреблений? Каковы их слабые и сильные стороны?
60. Что Вам известно о системах комплексного обнаружения вторжений?
61. Как можно охарактеризовать преимущества систем обнаружения вторжений?
62. Каковы проблемы, которые еще не решены в современных системах обнаружения вторжений?
63. Какие атаки предпринимаются злоумышленниками против самих систем обнаружения вторжений?
64. В чем проявляется ограниченность современных систем обнаружения вторжений?
65. Где в интрасети чаще всего размещаются сетевые системы обнаружения вторжений? В каких случаях какое размещение предпочтительно и почему?
66. Расскажите о двух специальных видах систем обнаружения вторжений - network grep и honeypot.

67. Какова роль хоста-бастиона при обнаружении вторжений в интрасети?
68. Каким образом система обнаружения вторжений реагирует на обнаруженные аномальные события в интрасети?
69. Какие способы повышения эффективности обнаружения вторжений в различных операционных системах (Windows, Unix, Macintosh) наиболее действенны?
70. Какова ситуация в области стандартов, регламентирующих обнаружение вторжений и реализующих его систем?
71. Перечислите основные характеристики перспективных систем обнаружения вторжений.
72. Расскажите о возможностях системы обнаружения злоупотреблений CMDS, подробнее останавливаясь на функциях, присущие именно этому типу COB.