

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ
Декан ФИиВТ

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

30.06.2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

С.1.1.36 Мониторинг безопасности информационных систем

(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	4
Семестр	8

Распределение учебного времени

Трудоемкость по учебному плану	216 / 6	часов/зачетных единиц
Лекции	48	часов
Лабораторные работы	64	часов
Практические занятия	-	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	112	часов
Контактная работа по экзамену	-	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	104	часов
Самостоятельная работа по подготовке к экзамену	-	часов
Экзамен	-	семестр
Зачет	-	семестр
БРК, ДЗ	8	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)	
30.04.2021	протокол №	17
(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 01.07.2021 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-16 Способен анализировать основные этапы и закономерности исторического развития России, её место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма	ОПК-16.1 Организационные меры по защите информации	знания: меры по защите информации умения: меры по защите информации навыки: меры по защите информации
	ОПК-16.2 Анализировать цели создания автоматизированных систем и задачи, решаемые автоматизированными системами	знания: проводить анализ защищенности информационных систем умения: проводить анализ защищенности информационных систем навыки: проводить анализ защищенности информационных систем
	ОПК-16.3 Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите	знания: классифицировать информацию и выделять защищаемую умения: классифицировать информацию и выделять защищаемую навыки: классифицировать информацию и выделять защищаемую
2. ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	ОПК-13.1 знает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации	знания: - принципы построения современных систем обеспечения информационной безопасности; - принципы статистического анализа; - способы описания поведения системы умения: навыки:
	ОПК-13.2 умеет осуществлять контроль обеспечения уровня защищенности в автоматизированных системах	знания: умения: - формализовать задачу контроля параметров безопасности информационными системами навыки:
	ОПК-13.3 владеет методами выявления уязвимости информационно-технологических ресурсов автоматизированных 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

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-13), Подготовка к

процедуре защиты и защита выпускной квалификационной работы (ОПК-16)

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

8 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
Мониторинг безопасности информационных систем	216	ОПК-13, ОПК-16
Лекция. Обзор наиболее важных стандартов и спецификаций в области информационной безопасности	4	
Лекция. «Общие критерии»	8	
Лекция. Профили защиты, разработанные на основе «Общих критериев».	8	
Лекция. Рекомендации семейства X.500	2	
Лабораторная работа. Расчет рисков невыполнения требований стандарта ISO 17799	10	
Лабораторная работа. Расчет риска невыполнения требований стандарта ISO 17799 с помощью системы КОНДОР	12	
Лабораторная работа. Расчет рисков информационной системы на основе модели информационных потоков	14	
Лабораторная работа. Расчет и управление информационными рисками на основе модели информационных потоков	14	
Лабораторная работа. Расчет рисков информационной системы на основе модели угроз и уязвимостей	14	
Лекция. Спецификация Internet-сообщества IPsec	4	
Лекция. Спецификация Internet-сообщества T L S	4	
Лекция. Спецификация Internet-сообщества «Обобщенный прикладной программный интерфейс службы безопасности»	4	
Лекция. Спецификация Internet-сообщества «Руководство по информационной безопасности предприятия»	4	
Лекция. Спецификация Internet-сообщества «Как реагировать на нарушения информационной безопасности»	4	
Лекция. Спецификация Internet-сообщества «Как выбирать поставщика Интернет-услуг»	2	
Лекция. Британский стандарт BS 7799	2	
Лекция. Федеральный стандарт С III А FIPS 140-2 «Требования безопасности для криптографических модулей»	2	

Задания для самостоятельной работы, в том числе выполнение	
Проработка лекций	
Подготовка к лабораторным работам	104
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 несанкционированного доступа [Текст] : учебное пособие / А. А. Кречетов. Йошкар-Ола: МарГТУ, 2007. - 142 с. Экземпляры: всего 20.	20 / https://portal.volgatech.net/books/krechetov_metody.pdf
2.	Галатенко, В. А. Стандарты информационной безопасности [Электронный ресурс] / Галатенко В. А. 2-е изд. Москва: ИНТУИТ, 2016. - 307 с. ISBN 5-9556-0053-1.	https://e.lanbook.com/book/100511
3.	Основы информационной безопасности [Текст] : учебное пособие : [по направлению подготовки "Информационные системы и технологии"] / [Ю. Ю. Громов и др.]. Старый Оскол: ТНТ, 2017. - 381 с. ISBN 978-5-94178-216-1. Экземпляры: всего 10.	10

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/М "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 (1), Система виброакустической защиты "Соната-AB" (1), Система виброакустической.защиты "Соната-PC2" (1), Средства ограничения доступа к компьютеру АПМДЗ "КРИПТОН-ЗАМОК/Е" (2), Экран настенный 200*200см Braun Roll Vision (1), Комплект учебной мебели (1)	Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ПО для решения основных пользовательских задач

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. История создания и текущий статус «Общих критериев»
2. Основные понятия и идеи «Общих критериев»
3. Основные понятия и идеи «Общей методологии оценки безопасности информационных

технологий»

4. Классификация функциональных требований безопасности
5. Классы функциональных требований, описывающие элементарные сервисы безопасности
6. Классы функциональных требований, описывающие производные сервисы безопасности
7. Защита данных пользователя
8. Защита функций безопасности объекта оценки
9. Классы функциональных требований, играющие инфраструктурную роль
10. Основные понятия и классификация требований доверия безопасности
11. Оценка профилей защиты и заданий по безопасности
12. Требования доверия к этапу разработки
13. Требования к этапу получения, представления и анализа результатов разработки
14. Требования к поставке и эксплуатации, поддержка доверия
15. Оценочные уровни доверия безопасности
16. Общие предположения безопасности
17. Общие угрозы безопасности
18. Общие элементы политики и цели безопасности
19. Общие функциональные требования
20. Общие требования доверия безопасности
21. Биометрическая идентификация и аутентификация
22. Требования к произвольному (дискреционному) управлению доступом
23. Требования к принудительному (мандатному) управлению доступом
24. Ролевое управление доступом
25. Межсетевое экранирование
26. Системы активного аудита
27. Анонимизаторы
28. Выпуск и управление сертификатами
29. Анализ защищенности
30. Операционные системы
31. Системы управления базами данных
32. Виртуальные частные сети
33. Виртуальные локальные сети
34. Смарт-карты
35. Основные понятия и идеи рекомендаций семейства X.500

36. Каркас сертификатов открытых ключей
37. Каркас сертификатов атрибутов
38. Простая и сильная аутентификация
39. Архитектура средств безопасности IP-уровня
40. Контексты безопасности и управление ключами
41. Протокольные контексты и политика безопасности
42. Обеспечение аутентичности IP-пакетов
43. Обеспечение конфиденциальности сетевого трафика
44. Основные идеи и понятия протокола TLS
45. Протокол передачи записей
46. Протокол установления соединений и ассоциированные
47. протоколы
48. Применение протокола HTTP над TLS
49. Функции для работы с удостоверениями
50. Создание и уничтожение контекстов безопасности
51. Защита сообщений
52. Логика работы пользователей интерфейса безопасности
53. Представление некоторых объектов интерфейса безопасности в среде языка C
54. Общие принципы выработки официальной политики предприятия в области информационной безопасности
55. Анализ рисков, идентификация активов и угроз
56. Регламентация использования ресурсов
57. Реагирование на нарушения политики безопасности (административный уровень)
58. Подход к выработке процедур для предупреждения нарушений безопасности

Перечень вопросов для проведения промежуточной аттестации

59. История создания и текущий статус «Общих критериев»
60. Основные понятия и идеи «Общих критериев»
61. Основные понятия и идеи «Общей методологии оценки безопасности информационных технологий»
62. Классификация функциональных требований безопасности
63. Классы функциональных требований, описывающие элементарные сервисы безопасности
64. Классы функциональных требований, описывающие производные сервисы безопасности
65. Защита данных пользователя
66. Защита функций безопасности объекта оценки
67. Классы функциональных требований, играющие инфраструктурную роль
68. Основные понятия и классификация требований доверия безопасности
69. Оценка профилей защиты и заданий по безопасности
70. Требования доверия к этапу разработки
71. Требования к этапу получения, представления и анализа результатов разработки
72. Требования к поставке и эксплуатации, поддержка доверия
73. Оценочные уровни доверия безопасности
74. Общие предположения безопасности
75. Общие угрозы безопасности
76. Общие элементы политики и цели безопасности
77. Общие функциональные требования
78. Общие требования доверия безопасности
79. Биометрическая идентификация и аутентификация
80. Требования к произвольному (дискреционному) управлению доступом
81. Требования к принудительному (мандатному) управлению доступом
82. Ролевое управление доступом
83. Межсетевое экранирование
84. Системы активного аудита
85. Анонимизаторы
86. Выпуск и управление сертификатами
87. Анализ защищенности
88. Операционные системы
89. Системы управления базами данных
90. Виртуальные частные сети

91. Виртуальные локальные сети
92. Смарт-карты
93. Основные понятия и идеи рекомендаций семейства X.500
94. Каркас сертификатов открытых ключей
95. Каркас сертификатов атрибутов
96. Простая и сильная аутентификация
97. Архитектура средств безопасности IP-уровня
98. Контексты безопасности и управление ключами
99. Протокольные контексты и политика безопасности
100. Обеспечение аутентичности IP-пакетов
101. Обеспечение конфиденциальности сетевого трафика
102. Основные идеи и понятия протокола TLS
103. Протокол передачи записей
104. Протокол установления соединений и ассоциированные
105. протоколы
106. Применение протокола HTTP над TLS
107. Функции для работы с удостоверениями
108. Создание и уничтожение контекстов безопасности
109. Защита сообщений
110. Логика работы пользователей интерфейса безопасности
111. Представление некоторых объектов интерфейса безопасности в среде языка C
112. Общие принципы выработки официальной политики предприятия в области информационной безопасности
113. Анализ рисков, идентификация активов и угроз
114. Регламентация использования ресурсов
115. Реагирование на нарушения политики безопасности (административный уровень)
116. Подход к выработке процедур для предупреждения нарушений безопасности