МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

ЗАЩИТА ИНФОРМАЦИИ ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) Безопасность автоматизированных систем
(по отрасли или в сфере профессиональной деятельности)

Уровень высшего образования: бакалавриат
Форма обучения: очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва *2022*

Защита информации от вредоносного программного обеспечения
Рабочая программа дисциплины

Составитель:
Кандидат технических наук, доцент кафедры КЗИ А.С. Моляков

Ответственный редактор
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 8 от 31.03.2022

Оглавление

1. Пояснительная записка 4
1.1. Цель и задачи дисциплины 4
1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине: 4
1.3. Место дисциплины в структуре образовательной программы 5
2. Структура дисциплины 5
3. Содержание дисциплины 6
4. Образовательные технологии 7
5. Оценка планируемых результатов обучения 8
5.1. Система оценивания 8
5.2. Критерии выставления оценки по дисциплине 9
5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине 10
6. Учебно-методическое и информационное обеспечение дисциплины 11
6.1. Список источников и литературы 11
6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет». ..13
6.3. Профессиональные базы данных и информационно-справочные системы 13
7. Материально-техническое обеспечение дисциплины 13
8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья 14
9. Методические материалы 15
9.1. Планы практических занятий 15
Приложение 1. Аннотация рабочей программы дисциплины 20

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – формирование систематизированных знаний о процессах разработки защищенных объектов информатизации и систем защиты информации на примере мобильных систем и промышленных сетей, применяемых при этом подходах, методиках и механизмах защиты информации от вредоносного ПО, а также формирование у обучающихся умений и навыков, необходимых при непосредственном участии в указанных процессах.

Задачи дисциплины:

– сформировать знания о моделях и этапах жизненного цикла защищенных объектов информатизации и систем защиты информации, применяемых подходах и методах по обеспечению безопасности на каждом из этапов;

– сформировать представления об уязвимостях, присущих объектов информатизации, связанных с ними угрозами, а также навыки формирования моделей угроз безопасности и моделей потенциальных нарушителей;

– сформировать и развить компетенции, знания и практические навыки обеспечения технологической и эксплуатационной безопасности объектов информатизации.

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине:

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-2 Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	ПК-2.1 Знать архитектуру и принципы построения операционных систем, подсистем защиты информации, состав типовых конфигураций программно-аппаратных средств защиты информации, языки и системы программирования	Знать: архитектуру и принципы построения операционных систем, подсистем защиты информации, состав типовых конфигураций программно-аппаратных средств защиты защищенных объектов информатизации и систем защиты информации на примере мобильных систем и промышленных сетей
	ПК-2.2 Умеет противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации	Уметь: противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации на примере мобильных систем и промышленных сетей
	ПК-2.3 Владеет контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах	Владеть: контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах примере IoT и Industrial Ethernet

ПК-8 Способен осуществлять мониторинг и аудит защищенности информации в автоматизированных системах	ПК-8.1 Знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах, организационные меры по защите информации	Знать: - угрозы безопасности информации и возможные пути их реализации Уметь: - определять информационные ресурсы, подлежащие защите; - определять угрозы безопасности информации.
	ПК-8.2 Умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах; вести протоколы и журналы учета при осуществлении аудита систем защиты информации автоматизированных систем	Уметь: - определять информационные ресурсы, подлежащие защите; - анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем; - определять угрозы безопасности информации при проведении аудита.
	ПК-8.3 Владеет навыками выработки рекомендаций для принятия решения о модернизации системы защиты информации автоматизированной системы	Владеть: - навыками по определению угроз безопасности информации - навыками по выработке рекомендаций в рамках модернизации системы защиты автоматизированных систем.

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации от вредоносного программного обеспечения» относится к части, формируемой участниками образовательных отношений блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Аппаратные средства вычислительной техники», «Безопасность операционных систем», «Сети и системы передачи информации», «Программно-аппаратные средства защиты информации».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Оценка безопасности программного обеспечения автоматизированных систем», «Преддипломная практика».

2. Структура дисциплины

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 академических часа

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
7	Лекции	**16**
7	Практические работы	**24**
	Всего:	**40**

Объем дисциплины в форме самостоятельной работы обучающихся составляет _32_ академических часа.

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	**Понятие мобильные системы. Базовые знания по защите объектов информатизации**	Понятие, структура и состав мобильных систем. Классификация объектов информатизации с точки зрения безопасности. Принципы обеспечения информационной безопасности. Понятие и виды вредоносного ПО.
2	**Понятие промышленные сети. Базовые знания по защите объектов информатизации**	Понятие, структура и состав промышленных сетей. Классификация объектов информатизации с точки зрения безопасности. Принципы обеспечения информационной безопасности.Понятие и виды вредоносного ПО
3	**Проектирование системы защиты конфиденциальной информации на примере мобильных систем и промышленных сетей**	Формирование требований к объекту информатизации. Моделирование угроз безопасности. Методы обеспечения защищенности объектов информатизации на этапе внедрения и эксплуатации.
4	**Архитектура мобильных систем**	Структура и назначение системы защиты информации. Этапы построения системы защиты информации. Порядок разработки системы защиты конфиденциальной информации.
5	**Архитектура промышленных сетей**	Структура и назначение системы защиты информации. Этапы построения системы защиты информации. Порядок разработки системы защиты конфиденциальной информации.
6	**Нормативно-правовые требования по сертификации мобильных систем**	Противоречия между необходимостью применения программно—технических средств защиты информации и требований по осуществлению контрольных мероприятий на основе подобных средств. В данном случае процедуры контрольных мероприятий могут осуществляться с ис-

		пользованием персональных данных работника, подвергающегося проверке. Комплекс нормативно — правовых документов, определяющих как категории и виды конфиденциальной информации, требования по обеспечения информационной безопасности подобных информационных ресурсов, так и перечень рекомендуемых для использования способов и средств защиты информации
7	**Анализ, классификация и методы внедрения вредоносных программ**	Боевые вредоносные программы. Классификации вредоносных программ. Методы внедрения вредоносных программ. Вредоносная программа Stuxnet. Вредоносная программа Wiper.Вредоносная программа Flame. Вредоносная программа Duqu. Вредоносная программа Icefog. Анализ средств доставки вредоносных программ до объектов их атаки

4. Образовательные технологии

Образовательные технологии

№ п/п	**Наименование раздела**	**Виды учебных занятий**	**Образовательные технологии**
1	**2**	**3**	**4**
1	Понятие мобильные системы. Базовые знания по защите объектов информатизации	Лекция 1 Практическое занятие 1	Традиционная лекция с использованием презентаций Выполнение заданий Работа с литературой
2	Понятие промышленные сети. Базовые знания по защите объектов информатизации	Лекция 2 Практическое занятие 2	Традиционная лекция с использованием презентаций Выполнение заданий Работа с литературой
3	Проектирование системы защиты конфиденциальной информации на примере мобильных систем и промышленных сетей	Лекция 3 Практическое занятие 2	Традиционная лекция с использованием презентаций Выполнение заданий Работа с литературой
4	Архитектура мобильных систем	Лекция 4 Практическое занятие 3	Традиционная лекция с использованием презентаций Выполнение заданий Работа с литературой
5	Архитектура промышленных сетей	Лекция 5	Традиционная лекция с использованием презентаций

		Практическое занятие 5	Выполнение заданий Работа с литературой
6	Нормативно-правовые требования по сертификации мобильных систем	Лекция 6 Практическое занятие 6	Традиционная лекция с использованием презентаций Выполнение заданий Работа с литературой
7	Анализ, классификация и методы внедрения вредоносных программ	Лекция 7.1 Лекция 7.2 Практическое занятие 7	Традиционная лекция с использованием презентаций Выполнение заданий Работа с литературой

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: - *практическое занятие № 1* - *практическое занятие № 2* - *практическое занятие № 3* - *практическое занятие № 4 -7*	 *9 баллов* *17 баллов* *17 баллов* *17 баллов*	 *9 баллов* *17 баллов* *17 баллов* *17 баллов*
Промежуточная аттестация - зачёт с оценкой (ответы на вопросы)		*40 баллов*
Итого за семестр		*100 баллов*

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

№ п/п	***Контролируемые разделы дисциплины***	***Код контролируемой компетенции***	***Наименование оценочного средства***
1.	Темы 1 – 7	ПК-2.1, ПК-2.2, ПК-2.3, ПК-8.1, ПК-8.2, ПК-8.3	Опрос
2.	Практические занятия 1 – 7	ПК-2.1, ПК-2.2, ПК-2.3, ПК-8.1, ПК-8.2, ПК-8.3	План практического занятия

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично		A

83 – 94		зачтено	B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	отлично	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	хорошо	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	удовлетво-рительно	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	неудовлет-ворительно	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Вопросы к зачету - проверка сформированности компетенций ПК-2, ПК-8

Контрольные вопросы	**Реализуемые компетенции**
1. Понятие, структура и состав мобильных систем.	ПК-2.1, ПК-2.2, ПК-8.1, ПК-8.2
2. Классификация систем систем.	ПК-2.1, ПК-2.2, ПК-8.1, ПК-8.2
3. Принципы обеспечения информационной безопасности.	ПК-2.1, ПК-2.2, ПК-8.1, ПК-8.2
4. Жизненный цикл мобильных систем.	ПК-2.1, ПК-2.2, ПК-8.1, ПК-8.2
5. Моделирование угроз безопасности объекта информатизации.	ПК-2.1, ПК-2.2, ПК-8.1, ПК-8.2
6. Управление проектированием защищенных объектов информатизации.	ПК-2.1, ПК-2.2, ПК-2.3, ПК-8.1, ПК-8.2, ПК-8.3
7. Структура и назначение системы защиты информации на примере мобильных систем.	ПК-2.1, ПК-2.2, ПК-8.1, ПК-8.2
8. Этапы построения системы защиты информации.	ПК-2.1, ПК-2.2, ПК-8.1, ПК-8.2
9. Архитектура мобильных систем.	ПК-2.1, ПК-2.2, ПК-8.1, ПК-8.2
10. Оценка соответствия системы защиты.	ПК-2.1, ПК-2.3, ПК-8.1, ПК-8.3
11. Методики анализа рисков информационной безопасности.	ПК-2.1, ПК-2.3, ПК-8.1, ПК-8.3
12. Аттестация объектов информатизации по безопасности.	ПК-2.1, ПК-2.2, ПК-8.1, ПК-8.2
13. Противоречия между необходимостью применения программно—технических средств защиты информации и требований по осуществлению контрольных мероприятий на основе подобных средств.	ПК-2.1, ПК-2.2, ПК-8.1, ПК-8.2
14. Факторы риска при использовании мобильных устройств для передачи корпоративной информации.	ПК-2.1, ПК-2.3, ПК-8.1, ПК-8.3
15. Ответственность пользователей при обработке корпоративных данных на мобильном устройстве.	ПК-2.1, ПК-2.3, ПК-8.1, ПК-8.3
16. Возможности перехвата мобильных сообщений, звонков и передаваемых файлов по незащищенным каналам связи (подключение к публичным точкам Wi-Fi, использование незащищенных приложений для звонков, сообщений и хранения файлов и др.)	ПК-2.1, ПК-2.3, ПК-8.1, ПК-8.3
17. Программы-вымогатели для мобильных устройств.Ботнеты.	ПК-2.1, ПК-2.3, ПК-8.1, ПК-8.3
18. Защищенность мобильных ОС.	ПК-2.1, ПК-2.3, ПК-8.1, ПК-8.3
19. MDM-решения для защиты мобильных устройств.	ПК-2.1, ПК-2.2,ПК-2.3, ПК-8.1, ПК-8.2, ПК-8.3

20. Capsule Workspace как изолированная от остальной операционной среды мобильного устройства защищенная и зашифрованная область, внутри которой уже развернуты почта, календарь, хранилище файлов, браузер и др.	ПК-2.1, ПК-2.2,ПК-2.3, ПК-8.1, ПК-8.2, ПК-8.3
21. Интеллектуальные системы предупреждения вторжений.	ПК-2.1, ПК-2.2,ПК-2.3, ПК-8.1, ПК-8.2, ПК-8.3
22. Антивирусы как средство защиты от вредоносного ПО.	ПК-2.1, ПК-2.2,ПК-2.3, ПК-8.1, ПК-8.2, ПК-8.3
23. Средства обнаружения атак на примере Snort и Surricata.	ПК-2.1, ПК-2.2,ПК-2.3, ПК-8.1, ПК-8.2, ПК-8.3
24. Система Enstein. Ее функционал и назначение.	ПК-2.1, ПК-2.2,ПК-2.3, ПК-8.1, ПК-8.2, ПК-8.3
25. Методы перехвата информации и технология противодействия ССИВ.	ПК-2.1, ПК-2.2,ПК-2.3, ПК-8.1, ПК-8.2, ПК-8.3
26. Перспективные направления развития высокоскоростных сетей и их защиты.	ПК-2.1, ПК-2.2,ПК-2.3, ПК-8.1, ПК-8.2, ПК-8.3
27. Этичный хакинг.	ПК-2.1, ПК-2.2,ПК-2.3, ПК-8.1, ПК-8.2, ПК-8.3
28. Технология ноубтов.	ПК-2.1, ПК-2.2,ПК-2.3, ПК-8.1, ПК-8.2, ПК-8.3

Примерные задания для тестирования- проверка сформированности компетенций ПК-2, ПК-8

1. **Позволяет получать доступ к информации, перехваченной другими программными закладками, модель воздействия программных закладок типа**

a) перехват
b) уборка мусора
c) наблюдение
d) компрометация

2. **Первым этапом разработки системы защиты ИС является:**

a) анализ потенциально возможных угроз информации
b) изучение информационных потоков
c) стандартизация программного обеспечения
d) оценка возможных потерь

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники
основные

1. *Руководящий докумен*т. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3, свободный. – Загл. с экрана.

2. *Руководящий документ*. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g, свободный. – Загл. с экрана.
3. *Руководящий документ*. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2, свободный. – Загл. с экрана.
4. *Руководящий документ*. Средства вычислительной техники. Межсетевые экраны Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g, свободный. – Загл. с экрана.

Литература
Основная

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452368
2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/454453
3. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва: Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449285
4. Гостев, И. М. Операционные системы : учебник и практикум для вузов / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 164 с. — (Высшее образование). — ISBN 978-5-534-04520-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451231
5. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва: ИНФРА-М, 2020. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464.

- ISBN 978-5-16-015149-6. - Текст: электронный. - URL: https://znanium.com/catalog/product/1018665

6. *Комплексная защита* информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/546679
7. *Шаньгин В.Ф.* Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В. Ф. Шаньгин. - М.: ДМК Пресс, 2010. - 544 с.: ил. - ISBN 978-5-94074-518-1. - Режим доступа: http://znanium.com/catalog/product/408107
8. Методы и средства защиты программного обеспечения [Электронный ресурс] : учеб.-метод. комплекс : для бакалавриата по направлению подготовки 090900 Информационная безопасность : по профилям: Организация и технология защиты информации, Комплексная защита объектов информатизации / Минобрнауки России, Федер. гос. бюджетное образоват. учреждение высш. проф. образования "Рос. гос. гуманитарный ун-т" (РГГУ), Ин-т информац. наук и технологий безопасности, Фак. информац. систем и безопасности, Каф. компьютерной безопасности ; [сост.: Казарин О. В. ; отв. ред. А. А. Тарасов]. - Электрон. дан. - Москва: РГГУ, 2013. - 30 с. - Режим доступа: http://elib.lib.rsuh.ru/elib/000009341. - Загл. с экрана. - ISBN 978-5-7281-1789-6.

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. OXPAHA.ru. Российское СМИ о безопасности. [Электронный ресурс] : Режим доступа : https://oxpaha.ru/, свободный. – Загл. с экрана.
2. Sec.ru. Портал по безопасности. [Электронный ресурс] : Режим доступа : http://sec.ru/, необходима регистрация. – Загл. с экрана.
3. *Банк данных угроз безопасности информации*. [Электронный ресурс] / ФСТЭК России, ФАУ «ГНИИИ ПТЗИ ФСТЭК России» – Режим доступа : http://sec.ru/, свободный. – Загл. с экрана.

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ru www.grebennikon.ru
Cambridge University Press
ProQuest Dissertation & Theses Global
SAGE Journals
Taylor and Francis
JSTOR

6.3. Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения:

для лекционных занятий - учебная аудитория, доска, компьютер или ноутбук, проектор (стационарный или переносной) для демонстрации учебных материалов.

Состав программного обеспечения:
1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

2) для практических занятий – компьютерный класс или лаборатория, доска, проектор (стационарный или переносной), компьютер или ноутбук для преподавателя, компьютеры для обучающихся.

Состав программного обеспечения:
1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security
4. Mozilla Firefox
5. Vmware Player 15.5
6. Microsoft Share Point 2010

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

– лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

– письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;

– обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

– для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;

– письменные задания оформляются увеличенным шрифтом;

– экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

– лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;

– письменные задания выполняются на компьютере в письменной форме;

– экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

– лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

– письменные задания выполняются на компьютере со специализированным программным обеспечением;

– экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

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

- для глухих и слабослышащих:

– в печатной форме;
– в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

– в печатной форме;
– в форме электронного документа;
– в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:

– устройством для сканирования и чтения с камерой SARA CE;
– дисплеем Брайля PAC Mate 20;
– принтером Брайля EmBraille ViewPlus;

- для глухих и слабослышащих:

– автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
– акустический усилитель и колонки;

- для обучающихся с нарушениями опорно-двигательного аппарата:

– передвижными, регулируемыми эргономическими партами СИ-1;
– компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий

- проверка сформированности компетенций ПК-2, ПК-8

Практическое занятие 1 (2 ч.) «Общая архитектура мобильных систем» - проверка сформированности компетенций ПК-2, ПК-8

Задания:

1. Обсудить понятие, структуру и состав мобильных систем. Дать классификацию объектов информатизации по заданию преподавателя.

Практическое занятие 2(2 ч.). Тенденции в развитии современных средств защиты информации (проверка сформированности компетенций ПК-2, ПК-8)
Задание*:* Изучить

- Современные тенденции защиты информации в распределенных мобильных системах Российской Федерации
- Совершенствование государственной системы обнаружения, предупреждения и ликвидации последствий кибератак на российские сети Повышение защищенности информационных систем и сетей связи госорганов Развитие ГОССОПКА Киберзащита органов власти Международное сотрудничество ООН, БРИКС, АТЭС, ОДКБ, СНГ Объективное использование иностранных ПАК Безопасный интернет.
- Указ Президента Указ Президента Российской Федерации от г. 646 Об утверждении Доктрины информационной безопасности Российской Федерации ФЗ ПП РФ ПП РФ Федеральный Закон Российской Федерации «О безопасности критической информационной инфраструктуры Российской Федерации» Постановление Правительства РФ от "О внесении изменений в требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации" Постановление Правительства РФ от 6 мая 2016 г. 399 «Об организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях ОПК»
- Изменения в профильных направлениях защиты информации ФСТЭК России Модель иностранных технических разведок до 2025 года (приказ) Требования к межсетевым экранам (приказ 9дсп) Требования по технической защите информации, содержащие сведения, составляющие ГТ (приказ) Требования безопасности информации к операционным системам (приказ 119) Требования к средствам уничтожения информации на машинных магнитных носителях информации способом магнитно-силового воздействия (приказ 18) Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (приказ 17) О внесении изменений в состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (приказ 49)
- О мерах по защите информации, направленных на нейтрализацию угроз безопасности информации, связанных с проникновением и распространением вредоносного программного обеспечения WannaCry, Petya, Misha и их модификаций
- Поиск уязвимостей в информационно-телекоммуникационных инфраструктурах предприятий и органов власти.Устаревшее ПО Отказы в обслуживании (DNS, DTLS для OpenSSL) Выработка рекомендаций Замена SSL-сертификата сервера на новый, использующий алгоритм SHA-256 Использование защищенного протокола HTTPS Доработка исходных кодов приложения с целью обеспечения фильтрации данных поступающих от пользователей

Вопросы для обсуждения:
1.Перечень основных нормативно-правовых документов.
2. Современные средства обнаружения вторжений.
3. Понятие многоагентной системы.

Практическое занятие 3 (4 ч.) «Анализ угроз конфиденциальной информации» - проверка сформированности компетенций ПК-2, ПК-8

Задания:

1. Формирование требований по уровню защищенности.
2. Моделирование угроз безопасности.

Список литературы:
Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной, ППП MS Office v.2007 и выше

Практическое занятие 4 (4 ч.) «Проектирование мобильных систем» - проверка сформированности компетенций ПК-2, ПК-8

Задания:

1. Порядок разработки системы защиты мобильных систем.
2. Оценка соответствия системы защиты.

Практическое занятие 5(4 ч.). Использование «облачных» технологий при реализации механизмов безопасности и многоагентные системы - проверка сформированности компетенций ПК-2, ПК-8
Задания:

1. Познакомиться с Облачными технологиями: основные понятия, задачи и тенденции развития. Современные облачные технологии не только используются в готовом сетевом и серверном оборудовании, но и постепенно проникают на рынок встраиваемых систем (embedded cloud) и становятся причиной масштабной реструктуризации рынка.
2. Исследовать современные многоагентные системы ИБ включает набор зондов, которые отвечают за обнаружение и оценку вторжений в тех подсетях, в которых они функционируют. Каждый зонд обеспечен фильтром данных с перестраиваемой конфигурацией, блоком вывода и решателем. Зонды могут действовать автономно. Если обнаружены компоненты вторжения, то информация о событии может быть отправлена другим заинтересованным зондам, которые подпишутся на информацию о подобных событиях, это позволит получать более полное понимание схемы вторжения. Этим способом могут быть идентифицированы разные подсети, которые участвуют в осуществлении вторжения. Зонды связаны с анализаторами

3. Изучить *Интернет вещей* (*Internet of Things, IoT*) — концепция физических предметов вычислительной сети (*«вещей»*), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека.

4. Разработать Модель безопасного функционирования IoT

Результатом выполнение практического задания является Отчет.
Правила оформления отчета:
Отчет о выполнении должен содержать:
- название и цель работы;
- комментарии и пояснения по каждому пункту выполняемого задания
- вывод.

В выводах должны быть обобщены результаты работы.

Вопросы для обсуждения:
1.Понятие мобильный агент.
2.Примеры алгоритмов шифрования.
3. Понятие криптостойкости алгоритмов шифрования.

Практическое занятие 6(4 ч.) «Нормативно-правовые требования в области создания мобильных систем» - проверка сформированности компетенций ПК-2, ПК-8

Задания:
3. Порядок сертификации и процедура ввода в эксплуатацию
4. Умение поддерживать непрерывный цикл анализа защищенности

Практическое занятие 7 (4 ч.). Интегрированные решения по защите информации - проверка сформированности компетенций ПК-2, ПК-8
Студенты изучают современные интегрированные решения с использованием мобильных агентов.
Результатом выполнение практического задания является Отчет.
Правила оформления отчета:
Отчет о выполнении должен содержать:
- название и цель работы;
- Схему разделов и статей Закона Российской Федерации, регламентирующих разработку и сертификацию интегрированных решений по защите информации;
- ответы на тестовое задание
- вывод.

В выводах должны быть обобщены результаты работы.

Вопросы для обсуждения:
1.Модель OSI
2. Snort. Функциональность системы.
3. Использование Barnyard для визуализации информации.

Приложение 1. Аннотация
рабочей программы дисциплины

Дисциплина «Защита информации от вредоносного программного обеспечения» реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации.

Цель дисциплины – формирование систематизированных знаний о процессах разработки защищенных объектов информатизации и систем защиты информации на примере мобильных систем, применяемых при этом подходах, методиках и механизмах защиты информации, а также формирование у обучающихся умений и навыков, необходимых при непосредственном участии в указанных процессах.
Задачи дисциплины:
– сформировать знания о моделях и этапах жизненного цикла защищенных объектов информатизации и систем защиты информации, применяемых подходах и методах по обеспечению безопасности на каждом из этапов;
– сформировать представления об уязвимостях, присущих объектов информатизации, связанных с ними угрозами, а также навыки формирования моделей угроз безопасности и моделей потенциальных нарушителей;
– сформировать и развить компетенции, знания и практические навыки обеспечения технологической и эксплуатационной безопасности объектов информатизации.

Дисциплина направлена на формирование следующих компетенций:

- ПК-2 - Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
- ПК-8 - Способен осуществлять мониторинг и аудит защищенности информации в автоматизированных системах

В результате освоения дисциплины обучающийся должен:
Знать:
архитектуру и принципы построения операционных систем, подсистем защиты информации, состав типовых конфигураций программно-аппаратных средств защиты защищенных объектов информатизации и систем защиты информации на примере мобильных систем и промышленных сетей;угрозы безопасности информации и возможные пути их реализации

Уметь: противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации на примере мобильных систем и промышленных сетей;определять информационные ресурсы, подлежащие защите; определять угрозы безопасности информации.

Владеть:
контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах примере IoT и Industrial Ethernet;
навыками по определению угроз безопасности информации; навыками по выработке рекомендаций в рамках модернизации системы защиты автоматизированных систем

По дисциплине предусмотрена промежуточная аттестация в форме зачета с оценкой.
Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы.