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

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

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ. МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ, ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профили) подготовки:
№ 2 Организация и технология защиты информации
№ 3 Комплексная защита объектов информатизации
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2017

Программно-аппаратные средства защиты информации. Межсетевое экранирование, обнаружение вторжений
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
№_6_ от__24.01.2017 г._____

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – ознакомление студентов с основными понятиями в области межсетевого экранирования и систем обнаружения вторжения; осознание понимания места данных механизмов в общей архитектуре подсистемы защиты информации информационной системы; формирование навыков установки, настройки и реконфигурирования этих средств защиты информации; знакомство с нормативно-методической базой в части их применения.
Задачи дисциплины: изучение принципов фильтрации информационных потоков на границе сетей, идентификационных признаков потенциально опасных информационных потоков, сигнатур сетевых атак (вторжений), систем пакетной фильтрации, критериев фильтрации пакетов, управления информационными потоками посредством фильтрации, сопряжения и совместной эксплуатации систем межсетевого экранирования и систем обнаружения вторжений.

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

Коды компетенции	**Содержание компетенций**	**Перечень планируемых результатов обучения по дисциплине**
ОПК-3	должен обладать способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач	Знать: требования, предъявляемые к системам межсетевого экранирования и обнаружения вторжения отечественной нормативно-методической базой; базовые функции и место в общей системе информационной безопасности; Уметь: осуществлять установку и настройку типовых систем межсетевого экранирования и обнаружения вторжений как уровня узла, так и уровня сети. Владеть: навыками оценки сетевого трафика с целью выделения потенциально опасных информационных потоков.
ОПК-7	должен обладать способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Знать: архитектуру и принципы функционирования межсетевых экранов и систем обнаружения вторжений. Уметь: выполнять настройку систем пакетной фильтрации, встроенных в коммуникационное оборудование. Владеть: навыками определения признаков потенциально опасных потоков и формирования правил межсетевого экранирования, такие потоки исключающих.

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Программно-аппаратные средства защиты информации. Межсетевое экранирование, обнаружение вторжений» относится к базовой части блока дисциплин учебного плана.
Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Информационные техно-

логии», «Информационные процессы и системы. Вычислительные сети», «Программно-аппаратные средства защиты информации. Основная часть».
В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Комплексное обеспечение безопасности объекта информатизации», «Проектирование систем защиты объектов информатизации».

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет _2_ з.е., _72_ ч., в том числе контактная работа обучающихся с преподавателем _28_ ч., самостоятельная работа обучающихся _44_ ч.

№ п/п	Темы дисциплины/	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	*Предмет и задачи программно-аппаратной защиты информации*	**6**	**2**					**8**	Опрос
2	*Удалённые сетевые атаки*	**6**	**2**			**2**		**10**	Опрос, отчёт по лабораторной работе
3	*Межсетевые экраны и аппаратные криптографические шлюзы*	**6**	**4**			**6**		**8**	Опрос, отчёт по лабораторной работе
4	*Виртуализация и облачные технологии. Виртуальные частные сети*	**6**	**2**			**4**		**8**	Опрос, отчёт по лабораторной работе
5	*Системы обнаружения и предотвращения вторжений*	**6**	**2**			**4**		**8**	Опрос, отчёт по лабораторной работе
	зачет	**6**							*зачет по билетам*
	итого:		**12**			**16**		**44**	

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	**Предмет и задачи программно-аппаратной защиты информации**	Предмет защиты. Свойства информации и её ценность. Объект защиты информации. Виды информации. Утечка информации и её виды. Сетевое и межсетевое взаимодействие. Политика безопасности.
2	**Вредоносные программы и удалённые сетевые атаки**	Вредоносные программы. Компьютерные вирусы. Троянские кони. Сетевые черви. Потайные ходы и руткиты. вредоносные программы для мобильных устройств. Прочие вредоносные программы. Наименование вирусов. Элементы защиты от вредоносного программного обеспечения. Технология Black и Whitelisting. Удалённые сетевые атаки. Сетевые атаки. Обобщённый сценарий атаки. Атаки «отказ в обслуживании». Атаки на протоколы IP, ICMP, UDP, TCP. Генераторы атак. Атака К. Митника. Классификации удалённых атак.
3	**Межсетевые экраны**	Развитие технологий межсетевого экранирования. Фильтрация пакетов. Межсетевые экраны уровня соединения. Межсетевые экраны прикладного уровня. Межсетевые экраны с динамической фильтрацией пакетов. Межсетевые экраны инспекции состояний. Межсетевые экраны уровня ядра. Персональные межсетевые экраны. Распределённые межсетевые экраны. Межсетевые экраны Web-приложений. Новое поколение межсетевых экранов. Обход межсетевых экранов. Постепенный подход. Туннелирование. Требования и показатели защищённости межсетевых экранов. Тестирование межсетевых экранов. Примеры межсетевых экранов.
4	**Виртуальные частные сети**	Виртуализация и облачные технологии. Туннелирование. Протоколы VPN канального уровня. Протокол IPSec. Ассоциация обеспечения безопасности. Туннельный и транспортный режимы протокола IPSec. Протокол обмена интернет-ключами. Протокол аутентификации заголовка. Протокол безопасной инкапсуляции содержимого пакета. Пример применения протокола IKE. Совместное использование протоколов ESP и AH. Основные типы защищённых связей. Протоколы VPN транспортного уровня. Цифровые сертификаты. Примеры отечественного построения VPN. Криптошлюзы. Инфраструктура PKI

5	**Системы обнаружения и предотвращения вторжений**	Модели систем обнаружения вторжений. Модель Д. Деннинг. Модель CIDF. Классификация систем обнаружения вторжений. Обнаружение сигнатур. Система обнаружения вторжений Snort. Декодер пакетов. Препроцессоры. Препроцессоры сборки пакетов. Препроцессоры нормализации протоколов. Препроцессоры обнаружения аномалий. Процессор обнаружения. Модули вывода. Правила Snort. Примеры правил. Обнаружение аномалий. Методы Data Mining. Методы технологии мобильных агентов. Методы построения иммунных систем. Применение генетических алгоритмов. Применение нейронных сетей. Языки описания атак. Другие методы обнаружения вторжений. Системы анализа защищённости. Системы анализа целостности. Вспомогательные средства обнаружения. Методы обхода систем обнаружения вторжений. Методы обхода сетевых систем обнаружения вторжений. Методы обхода хостовых систем обнаружения вторжений. Динамические методы обхода. Тестирование систем обнаружения вторжений. Тестирование коммерческих систем. Тестирование исследовательских прототипов. Методы формирования тестовых наборов. Матрица несоответствий. Системы предупреждения вторжений

4. Образовательные технологии

№ п/п	**Наименование раздела**	**Виды учебных занятий**	**Образовательные технологии**
1	**2**	**3**	**4**
1.	*Предмет и задачи программно-аппаратной защиты информации*	*Лекция 1.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям*
2	*Удалённые сетевые атаки*	*Лекция 2.* *Лабораторная работа 2.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Занятия с использованием специализированного ПО* *Подготовка к занятиям*
3	*Межсетевые экраны и аппаратные криптографические шлюзы*	*Лекция 3.1.* *Лекция 3.2.* *Лабораторная работа 3.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Занятия с использованием специализированного ПО и оборудования* *Подготовка к занятиям*

4	*Виртуализация и облачные технологии. Виртуальные частные сети*	*Лекция 4.* *Лабораторная работа 4.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Занятия с использованием специализированного ПО и оборудования* *Подготовка к занятиям*
5	*Системы обнаружения и предотвращения вторжений*	*Лекция 5.1.* *Лекция 5.2.* *Лабораторная работа 5.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Занятия с использованием специализированного ПО и оборудования* *Подготовка к занятиям с использованием ЭБС*

5. Оценка планируемых результатов обучения. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *– опрос (темы 1-5)* *– лабораторные работы (темы 2-5)*	 *4 балла* *10 баллов*	 *20 баллов* *40 баллов*
Промежуточная аттестация *экзамен*		*40 баллов*
Итого за дисциплину *экзамен*		*100 баллов*

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	зачтено	A
83 – 94			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»/ «зачтено (отлично)»/ «зачтено»	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»/ «зачтено (хорошо)»/ «зачтено»	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	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	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.

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
		Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»/ не зачтено	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.

Виртуализация и облачные технологии. Туннелирование. Протоколы VPN канального уровня. Протокол IPSec. Ассоциация обеспечения безопасности. Туннельный и транспортный режимы протокола IPSec. Протокол обмена интернет-ключами. Протокол аутентификации заголовка. Протокол безопасной инкапсуляции содержимого пакета. Пример применения протокола IKE. Совместное использование протоколов ESP и AH. Основные типы защищённых связей. Протоколы VPN транспортного уровня. Цифровые сертификаты. Примеры отечественного построения VPN. Криптошлюзы. Инфраструктура PKI

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

Примерные вопросы к экзамену - *проверка сформированности компетенций ОПК-3, ОПК-7)*

1. Предмет и объект защиты программно-аппаратной защиты. Свойства, виды информации и её ценность.
2. Утечка информации и её виды. Каналы утечки.
3. Сетевое и межсетевое взаимодействие.
4. Политика безопасности.
5. Вредоносные программы. Компьютерные вирусы.
6. Троянские кони и сетевые черви.
7. Вредоносные программы. Потайные ходы и руткиты.
8. вредоносные программы для мобильных устройств. Прочие вредоносные программы.
9. Наименование вирусов. Элементы защиты от вредоносного программного обеспечения.
10. Технология Black и Whitelisting.
11. Сетевые атаки. Обобщённый сценарий атаки.
12. Атаки «отказ в обслуживании».
13. Атаки на протоколы IP, ICMP, UDP, TCP. Генераторы атак. Атака К. Митника.

14. Классификации удалённых атак.
15. Технологии межсетевого экранирования.
16. Методы обхода межсетевых экранов.
17. Требования и показатели защищённости межсетевых экранов.
18. Тестирование межсетевых экранов.
19. Сущность виртуализации и облачных технологий.
20. Туннелирование. Протоколы VPN канального уровня.
21. Протокол IPSec.
22. Протокол обмена интернет-ключами. Пример применения протокола IKE.
23. Протокол аутентификации заголовка. Протокол безопасной инкапсуляции содержимого пакета. Совместное использование протоколов ESP и AH.
24. Основные типы защищённых связей. Протоколы VPN транспортного уровня.
25. Криптошлюзы.
26. Инфраструктура PKI
27. Модели систем обнаружения вторжений.
28. Классификация систем обнаружения вторжений.
29. Обнаружение сигнатур и обнаружение аномалий.
30. Система обнаружения вторжений Snort.
31. Методы Data Mining. Методы технологии мобильных агентов и построения иммунных систем.
32. Методы Data Mining. Применение генетических алгоритмов и нейронных сетей.
33. Методы обнаружения вторжений на основе анализа защищённости, анализа целостности. Вспомогательные средства обнаружения.
34. Методы обхода систем обнаружения вторжений.
35. Тестирование систем обнаружения вторжений.
36. Системы предупреждения вторжений

Примерные задания для тестирования- проверка сформированности компетенций ОПК-3, ОПК-7

1. Протокол IPSec работает на коком уровне модели OSI:
а) на сетевом уровне.
б) на канальном уровне.
в) на физическом уровне.

2. Руткит — это:
а) компьютерный вирус.
б) набор программных средств (например, исполняемых файлов, скриптов, конфигурационных файлов), обеспечивающих: маскировку объектов (процессов, файлов, каталогов, драйверов);управление (событиями, происходящими в системе);сбор данных (параметров системы).
в) рекламное программное обеспечение.

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. *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

2. *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

3. 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. Варновский Н.П. Курс лекций по математической криптографии [Электронный ресурс]. – Режим доступа: http://cryptography.ru/wp-content/uploads/2014/11/varn_lectures_long.pdf

2. Goldreich O. Foundations of cryptography. [Электронный ресурс]. – Режим доступа: http://www.twirpx.com/file/493751/

6.3.Перечень БД и ИСС

№п/п	Наименование

1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
2	Компьютерные справочные правовые системы Консультант Плюс, Гарант

7 Материально-техническое обеспечение дисциплины

Для проведения занятий необходимо следующее материально-техническое обеспечение:
1) лекционный класс с видеопроектором и компьютером, на котором должны быть установлены:
– лицензионное ПО MS Windows 7 и старше;
– лицензионное ПО MS Office 2010 (с обязательным наличием MS PowerPoint) и старше
2) компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлены:
– лицензионное ПО MS Windows 7 и старше;
– лицензионное ПО MS Office 2010 и старше;
– система управления виртуальными машинами (ВМ) VMPlayer или VirtualBox (свободное ПО) с установленными ВМ MS Windows 7 и MS Windows Server 2008.
– средство обнаружения вторжений Snort;
– OpenVPN (с установленными параметрами конфигурации и сертификатом);
– набор межсетевых экранов (МЭ)

Перечень ПО

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 7 Pro	Microsoft	лицензионное
3	Microsoft Share Point 2010	Microsoft	лицензионное
4	Microsoft Office 2013	Microsoft	лицензионное
5	Windows 10 Pro	Microsoft	лицензионное
6	Kaspersky Endpoint Security	Kaspersky	Лицензионное
7	Vmware Player 15.5 + Гостевая ОС CentOS 7	VMWare	Свободное ПО, Режим доступа: https://www.vmware.com/products/ Демо-версия Открытое ПО Режим доступа: https://www.centos.org/download/ Инсталляционный дистрибутив Linux
8	Snort	Snort	Свободное ПО, Режим доступа: https://www.snort.org/downloads

9	Набор МЭ: Avast firewall Avira firewall Comodo firewall DrWeb Security suite Zone Alarm firewall OutPost firewall McAffe Total Security Avg-internet-security	 Avast Avira Comodo DrWeb Zone Alarm Agnitum OutPost McAfee AVG	Свободное ПО, Режим доступа: https://www.avast.ru/f-firewall https://www.avira.com/ru/downloads https://www.comodo.com/home/internet-security/firewall.php https://products.drweb.ru/enterprise_security_suite/ https://www.zonealarm.com/software/free-firewall http://www.agnitum.ru/products/outpost/index.php http://download.mcafee.com/ https://www.avg.com/ru-ru/ Демо-версии
10	Open VPN	OpenVPN	Свободное ПО, Режим доступа: https://openvpn.net/
11	Wireshark 3.0	Wireshark	Свободное ПО, Режим доступа: https://www.wireshark.org/

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

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 лабораторных занятий - *проверка сформированности компетенций ОПК-3, ОПК-7*

Темы учебной дисциплины предусматривают проведение лабораторных работ, которые служат как целям текущего и промежуточного контроля за подготовкой студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания для лабораторных работ, выдаваемые преподавателем на каждом занятии.

Целью лабораторных работ является закрепление теоретического материала и приобретение практических навыков работы с соответствующим оборудованием, программным обеспечением и нормативными правовыми документами.

Тематика лабораторных работ соответствует программе дисциплины.

Лабораторная работа 1 (2 ч.). Исследование траффика с помощью сниффера - проверка сформированности компетенций ОПК-3

Задания:

1. Проанализировать возможные угрозы и атаки на АИС организации.
2. Изучение траффика с помощью WireShark.

Указания по выполнению заданий:

1. Изучить теоритический материал по теме.
2. Ответить на теоритические вопросы в конце лабораторной работы

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, сниффер WireShark, виртуальная машина CentOS 7, ППП MS Office v.2007 и выше. Занятия проходят в специально оборудованном компьютерном классе.

Лабораторная работа 2 (6 ч.). Исследование методов сетевой фильтрации на примере набора межсетевых экранов ОС Windows - проверка сформированности компетенций ОПК-7

Задания:

1. Настройка и конфигурирование межсетевого экрана для ОС Windows.
2. Создание демилитаризованной зоны.
3. Тестирование функциональности.

Указания по выполнению заданий:

1. Изучить теоритический материал по теме.
2. Ответить на теоритические вопросы в конце лабораторной работы
3. Оформить отчёт по лабораторной работе.

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной, ППП MS Office v.2007 и выше, набор МЭ по указанию преподавателя. Занятия проходят в специально оборудованном компьютерном классе.

Лабораторная работа 3 (4 ч.). Исследование защищенности ОС Linux на примере iptables - проверка сформированности компетенций ОПК-3, ОПК-7

Задания:

1. Настроить безопасное взаимодействие двух IP-сетей между собой через сеть общего пользования (Интернет), средствами программного продукта OpenVPN.
2. Создать ключи и сертификаты безопасности.
3. Настроить конфигурационный файл VPN-клиента.

4. Настроить iptables.Проверить применение правил фильтрации.

Указания по выполнению заданий:

1. Изучить теоритический материал по теме.
2. Ответить на теоритические вопросы в конце лабораторной работы
3. Оформить отчёт по лабораторной работе.

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной, ППП MS Office v.2007 и выше, OpenVPN,виртуальной машиной CentOS 7 . Занятия проходят в специально оборудованном компьютерном классе.

Лабораторная работа 4 (4 ч.). Средство обнаружения вторжения Snort - проверка сформированности компетенций ОПК-7

Задания:

1. Установить систему обнаружения вторжений Snort
2. Настроить Snort под задачи организации.

Указания по выполнению заданий:

1. Изучить теоритический материал по теме.
2. Ответить на теоритические вопросы в конце лабораторной работы
3. Оформить отчёт по лабораторной работе.

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной, ППП MS Office v.2007 и выше, Snort, виртуальная машина CentOS 7. Занятия проходят в специально оборудованном компьютерном классе.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Программно-аппаратные средства защиты информации. Межсетевое экранирование, обнаружение вторжений» реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – № 2 Организация и технология защиты информации и № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.

Дисциплина реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации

Цель дисциплины: ознакомление студентов с основными понятиями в области межсетевого экранирования и систем обнаружения вторжения; осознание понимания места данных механизмов в общей архитектуре подсистемы защиты информации информационной системы; формирование навыков установки, настройки и реконфигурирования этих средств защиты информации; знакомство с нормативно-методической базой в части их применения.

Задачи:

– изучение принципов фильтрации информационных потоков на границе сетей, идентификационных признаков потенциально опасных информационных потоков, сигнатур сетевых атак (вторжений), систем пакетной фильтрации, критериев фильтрации пакетов, управления информационными потоками посредством фильтрации, сопряжения и совместной эксплуатации систем межсетевого экранирования и систем обнаружения вторжений.

Дисциплина направлена на формирование следующих компетенций:

- ОПК-3 – способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач.
- ОПК-7 – способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

В результате освоения дисциплины обучающийся должен:

Знать: требования, предъявляемые к системам межсетевого экранирования и обнаружения вторжения отечественной нормативно-методической базой; базовые функции и место в общей системе информационной безопасности; архитектуру и принципы функционирования межсетевых экранов и систем обнаружения вторжений; назначение и сущность контрольных проверок систем фильтрации пакетов и систем обнаружения вторжений

Уметь: осуществлять установку и настройку типовых систем межсетевого экранирования и обнаружения вторжений как уровня узла, так и уровня сети; выполнять настройку систем пакетной фильтрации, встроенных в коммуникационное оборудование.

Владеть: навыками оценки сетевого трафика с целью выделения потенциально опасных информационных потоков; навыками определения признаков потенциально

опасных потоков и формирования правил межсетевого экранирования, такие потоки исключающих.

По дисциплине предусмотрена промежуточная аттестация в форме зачета.

Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы.

Приложение 2

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*29.06.2017 г.*	***10***
2	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*26.06.2018 г.*	***11***
3	*Обновлена структура дисциплины (модуля) для очной формы обучения (2019 г.)*	*29.08.2019 г.*	***1***
4	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*29.08.2019 г.*	***1***
5	*Обновлена структура дисциплины (модуля) для очной формы обучения (2020 г.)*	*23.06.2020 г*	***14***
6	*Обновлена основная и дополнительная литература*	*23.06.2020 г*	***14***
7	*Обновлен раздел п.4 Образовательные технологии*	*23.06.2020 г*	***14***
8	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*23.06.2020 г*	***14***

Приложение 1
к листу изменений

1. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2017 г.)

Перечень ПО

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	MicrosoftOffice 2013	Microsoft	лицензионное
2	Windows XP	Microsoft	лицензионное
3	KasperskyEndpointSecurity	Kaspersky	лицензионное
4	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное

Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель: К.т.н, доцент, А.С. Моляков

Приложение 2
к листу изменений

2. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2018 г.)

Перечень ПО

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statisctics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statisctics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное

Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2018 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2018 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis Электронные издания издательства Springer
	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель: К.т.н, доцент, А.С. Моляков

Приложение 3
к листу изменений

3. Обновление структуры дисциплины (модуля) для очной формы обучения (2019 г.)

Структура дисциплины (модуля) для очной формы обучения

Общая трудоёмкость дисциплины составляет 2 з.е., 72 ч., в том числе контактная работа обучающихся с преподавателем 28 ч., промежуточная аттестация 18 ч., самостоятельная работа обучающихся 26 ч.

№ п/п	Темы дисциплины/	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	*Предмет и задачи программно-аппаратной защиты информации*	**6**	**2**					**5**	Опрос
2	*Удалённые сетевые атаки*	**6**	**2**			**2**		**5**	Опрос, отчёт по лабораторной работе
3	*Межсетевые экраны и аппаратные криптографические шлюзы*	**6**	**4**			**6**		**6**	Опрос, отчёт по лабораторной работе
4	*Виртуализация и облачные технологии. Виртуальные частные сети*	**6**	**2**			**4**		**5**	Опрос, отчёт по лабораторной работе
5	*Системы обнаружения и предотвращения вторжений*	**6**	**2**			**4**		**5**	Опрос, отчёт по лабораторной работе
	экзамен	**6**					**18**		*экзамен по билетам*
	итого:		**12**			**16**	**18**	**26**	

4.Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2019 г.)

Перечень ПО

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое

5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statisctics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statisctics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2019 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2019 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель: К.т.н, доцент, А.С. Моляков

Приложение 4
к листу изменений

5. Обновление структуры дисциплины (модуля) для очной формы обучения (2020 г.)

Структура дисциплины (модуля) для очной формы обучения

Общая трудоемкость дисциплины составляет 2 з. е., 76 ч., в том числе контактная работа обучающихся с преподавателем 28 ч., самостоятельная работа обучающихся 30 ч.

№ п/п	Темы дисциплины/	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Предмет и задачи программно-аппаратной защиты информации	**6**	**2**					**6**	Опрос
2	Удалённые сетевые атаки	**6**	**2**			**2**		**6**	Опрос, отчёт по лабораторной работе
3	Межсетевые экраны и аппаратные криптографические шлюзы	**6**	**4**			**6**		**6**	Опрос, отчёт по лабораторной работе
4	Виртуализация и облачные технологии. Виртуальные частные сети	**6**	**2**			**4**		**6**	Опрос, отчёт по лабораторной работе
5	Системы обнаружения и предотвращения вторжений	**6**	**4**			**4**		**6**	Опрос, отчёт по лабораторной работе
	экзамен	**6**					**18**		экзамен по билетам
	итого:		**12**			**16**	**18**	**30**	

6. Обновление основной и дополнительной литературы (2020 г.)

В раздел **6. Учебно-методическое и информационное обеспечение дисциплины** вносятся следующие изменения:

Дополнить раздел Основная литература

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

Дополнить раздел **Дополнительная литература**

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

7. В элемент рабочей программы **п.4 Образовательные технологии** вносятся следующие изменения:

В период временного приостановления посещения обучающимися помещений и территории РГГУ. для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции;

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

8. В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

Состав программного обеспечения (ПО)

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распростра-

			няемое
5	Archicad 21 Rus Student	Graphisoft	свободно распростра-няемое
6	SPSS Statisctics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statisctics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное
17	Zoom	Zoom	лицензионное

Составитель:

К.т.н. доцент, А.С. Моляков