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

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. АДМИНИСТРИРОВАНИЕ ПОДСИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) подготовки
№ 3 Комплексная защита объектов информатизации
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва *2017*

Информационные технологии. Администрирование подсистем защиты информации
Рабочая программа дисциплины
Составитель(и):
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 методами формирования комплексной системы информационной безопасности; овладение методами проектирования и поддержки жизненного цикла систем информационной безопасности, формирование практических навыков по управлению и администрированию как отдельными компонентами, так и подсистемой защиты информации в целом, а также по разработке и внедрению предложений по оптимизации комплекса средств защиты информации.

Задачи дисциплины:

- рассмотрение базовых понятий в области жизненного цикла подсистемы защиты информации;
- рассмотрение элементов проектирования подсистемы защиты информации, вопросов разработки модели угроз и модели нарушителя, построения и последующей эксплуатации подсистемы защиты информации с учётом этих моделей;
- определение принципов администрирования подсистемы защиты информации, зоны ответственности и обязанностей администратора информационной безопасности;
- формирование понимания сложности задачи интеграции подсистемы защиты информации в информационную систему и администрирования её без ущерба для целевой функции системы.

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

Коды компетенции	**Содержание компетенций**	**Перечень планируемых результатов обучения по дисциплине**
ОПК-4	способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Знать: состав подсистем защиты информации и принципы их функционирования. Уметь: осуществлять выбор и настройку подсистем защиты информации в соответствии с решаемыми задачами. Владеть навыками установки, настройки и администрирования подсистем защиты информации.
ПСК-3.2	способность формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта с целью обеспечения его информационной безопасности и осуществлять технико-экономическое обоснование предлагаемых мер защиты.	Знать: требования, предъявляемые к подсистеме защиты информации в нормативно-методической документации, методы и способы администрирования подсистемы защиты информации; методики оценки надёжности её функционирования. Уметь: выполнять планирование внедрения, внедрение и эксплуатацию средств защиты информации как встроенных в общесистемное и прикладное программное обеспечение, так и специализированных наложенных. Владеть: навыками документального сопровождения действий по эксплуатации и администрированию комплекса средств защиты информации
ПК-3	способность администрировать подсистемы	Знать: методологические и технологические принципы формирования и эксплуатации под-

	информационной безопасности объекта защиты.	системы защиты информации информационной системы. Уметь: участвовать в разработке моделей угроз и нарушителей, учитывать положения моделей при администрировании комплекса средств защиты информации. Владеть: навыками настройки и администрирования, а также модернизации комплекса средств защиты информации; управления сопряжением и совместной эксплуатацией разнородных средств защиты информации.
ПК-11	способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Знать: структуру подсистем защиты информации и особенности работы с ними. Уметь: осуществлять выбор и настройку подсистем защиты информации, проводить оценку надёжности их функционирования. Владеть: методами оценки эффективности работы подсистем защиты информации.
ПК-12	способность принимать участие в проведении экспериментальных исследований системы защиты информации	Знать: методы проверки работоспособности подсистем защит информации. Уметь: выполнять проверку функционирования подсистем защиты информации. Владеть: навыками тестирования подсистем защиты информации.

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационные технологии. Администрирование подсистем защиты информации» 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 технологии», «Сети и системы передачи информации».
В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Гуманитарные аспекты информационной безопасности», «Комплексное обеспечение безопасности объекта информатизации», «Проектирование систем защиты объектов информатизации».

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет _3_ з.е., _108_ ч., в том числе контактная работа обучающихся с преподавателем _42_ ч., промежуточная аттестация _18_ ч., самостоятельная работа обучающихся _48_ ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		

1	*Место и роль подсистемы защиты информации в современных информационных системах*	**6**	**2**					**4**	Опрос.
2	*Угрозы безопасности информационной системы*	**6**	**2**					**5**	Опрос.
3	*Модель угроз и модель нарушителя*	**6**	**2**					**5**	Опрос.
4	*Сущность администрирования*	**6**	**4**					**5**	Опрос.
5	*Основы технологии виртуальных защищённых сетей VPN*	**6**	**2**					**5**	Опрос.
6	*Защита на канальном, сеансовом и сетевом уровнях. Аспекты защиты вебпорталов*	**6**	**4**					**5**	Опрос.
7	*Администрирование межсетевых экранов*	**6**	**2**					**5**	Опрос.
8	*Оценка эффективности и надёжности функционирования подсистемы защиты информации*	**6**	**2**					**5**	Опрос.
9	*Практические занятия 1. Разработка модели угроз и нарушителя*	**6**				**6**			Отчёт о практическом занятии
10	*Практическое занятие 2. Администрирование встроенных систем защиты ОС Windows и Windows Server*	**6**				**6**			Отчёт о практическом занятии
11	*Практическое занятие 3. Настройка межсетевых экранов*	**6**				**4**			Отчёт о практическом занятии
12	*Практическое занятие 4. Создание VPN-канала.*	**6**				**6**		**9**	Отчёт о практическом занятии
	экзамен	**6**					**18**		*экзамен по билетам*
	итого:		**20**			**22**	**18**	**48**	

3. Содержание дисциплины

Тема 1. Место и роль подсистемы защиты информации в современных информационных системах

Структура автоматизированной информационной системы (АИС). Назначение и задачи, решаемые ПЗИ. Структура ПЗИ. Этапы разработки ПЗИ. Комплексный подход к разработке ПЗИ. Понятие жизненного цикла системы. Жизненный цикл ПЗИ. Модели жизненного цикла. Требования к ПЗИ в нормативно-методической документации.

Тема 2. Угрозы безопасности информационной системы

Угрозы безопасности информации. Утечка информации. Несанкционированный доступ к информации. Классификация угроз. Уязвимости информационных систем. Подсистемы системы ЗИ.

Тема 3. Модель угроз и модель нарушителя

Разработка модели угроз и модели нарушителя. Руководящие нормативные документы по разработке моделей и определения актуальных угроз. Этапы планирования и внедрения средств защиты информации.

Тема 4. Сущность администрирования

Правила, регламенты и стратегия администрирования в АИС. Функции и задачи администрирования. Политика безопасности. Обязанности администратора информационной безопасности. Программы безопасности административного и процедурного уровня. Защита АС как процесс управления рисками. Анализ рисков. Основные подходы к анализу рисков. Этапы анализа рисков и управления ими. Администрирование в ОС семейства Windows. Администрирование в ОС семейства Windows Server.

Тема 5. Основы технологии виртуальных защищённых сетей VPN

Концепция построения виртуальных частных сетей – VPN. Основные понятия и функции сети VPN. Защита информации в процессе её передачи по туннелю VPN. VPN-клиент, VPN-сервер и шлюз безопасности VPN. Реализация механизма VPN. Варианты построения виртуальных защищённых каналов. Средства обеспечения безопасности VPN. Критерии безопасности данных применительно к задачам VPN. VPN-решения для построения защищённых сетей. Классификация сетей VPN. Критерии классификации. Основные варианты архитектуры VPN. Достоинства применения технологий VPN.

Тема 6. Защита на канальном, сеансовом и сетевом уровнях. Аспекты защиты веб-порталов

Протоколы формирования защищённых каналов на канальном уровне. Протокол PPTP. Структура пакета. Протокол L2TP, его преимущества. Формирование защищённого виртуального канала в протоколе L2TP. Протоколы формирования защищённых каналов на сеансовом уровне. Процедура установления *SSL*-сессии. Недостатки протоколов *SSL* и *TLS*. Протокол *SOCKS*, его особенности. Схема установления соединения по протоколу *SOCKS* v5. Защита беспроводных сетей. Протоколы WEP, TKIP, WPA и WPA2.

Защита на канальном, сеансовом и сетевом уровнях. Архитектура средств безопасности IPSec. Компоненты реализаций протокола IPSec имеют следующие. Архитектура стека протоколов IPSec. Защита передаваемых данных с помощью протоколов AH и ESP. Протокол аутентифицирующего заголовка. Применение протокола AH в транспортном и туннельном режимах. Протокол инкапсулирующей защиты, применение протокола ESP в транспортном и туннельном режимах. Алгоритмы аутентификации и шифрования в IPSec. Структура алгоритма HMAC. Протокол управления криптоключами IKE. Задачи, решаемые протоколами IKE. Установление безопасной ассоциации. Базы данных SAD и SPD. Основные схемы применения IPSec. Практические аспекты защиты веб-порталов от информационных атак. Типовая архитектура веб-портала. подсистемы антивирусной защи-

ты, контроля целостности, разграничения доступа, обнаружения вторжений, анализа защищённости, криптографической защиты информации, подсистему управления защитой веб-порталов.

Тема 7. Администрирование межсетевых экранов. Системы обнаружения атак
Угрозы, связанные с периметром корпоративной сети. Составляющие защиты периметра. Межсетевые экраны их виды. Администрирование межсетевых экранов. Демилитаризованная зона. Системы управления уязвимостями. Анализ содержимого почтового и веб-трафика. Системы обнаружения атак. Классификация систем обнаружения атак.

Тема 8. Оценка эффективности и надёжности функционирования подсистемы защиты информации
Понятие эффективности. Показатель и критерий эффективности. Методы оценки эффективности. Модели оценки эффективности. Надёжность подсистемы защиты информации. Понятие аудита информационной безопасности. Типы аудита. Инструментальные проверки.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1	*Место и роль подсистемы защиты информации в современных информационных системах*	*Лекция 1.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Изучение материалов лекций*
2	*Угрозы безопасности информационной системы*	*Лекция 2.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Изучение материалов лекций*
3	*Модель угроз и модель нарушителя*	*Лекция 3.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Изучение материалов лекций*
4	*Сущность администрирования*	*Лекция 4.1* *Лекция 4.2* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Изучение материалов лекций*
5	*Основы технологии виртуальных защищённых сетей VPN*	*Лекция 5.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Изучение материалов лекций*
6	*Защита на канальном, сеансовом и сетевом уровнях. Аспекты защиты веб-порталов*	*Лекция 6.1* *Лекция 6.2* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Изучение материалов лекций*
7	*Администрирование межсетевых экранов*	*Лекция 7* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Изучение материалов лекций*
8	*Оценка эффективно-*	*Лекция 8*	*Традиционная лекция с исполь-*

	сти и надёжности функционирования подсистемы защиты информации	*Самостоятельная работа*	*зованием презентаций* *Изучение материалов лекций*
9	*Практические занятия 1. Разработка модели угроз и нарушителя*	*Лабораторное занятие 1.* *Самостоятельная работа*	*Выполнение практического задания*
10	*Практическое занятие 2. Администрирование встроенных систем защиты ОС Windows и Windows Server*	*Лабораторное занятие 2.* *Самостоятельная работа*	*Выполнение практического задания*
11	*Практическое занятие 3. Настройка межсетевых экрана*	*Лабораторное занятие 3.* *Самостоятельная работа*	*Выполнение практического задания*
12	*Практическое занятие 4. Создание VPN-канала.*	*Практическое занятие 4.* *Самостоятельная работа*	*Выполнение практического задания*

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *– опрос* *– практическое занятие (темы 1,2.4)* *– практическое занятие (тема 3)*	 *3 баллов* *10 баллов* *6 балов*	 *24 баллов* *30 баллов* *6 баллов*
Промежуточная аттестация *экзамен*		*40 баллов*
Итого за дисциплину *экзамен*		*100 баллов*

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

№ п/п	***Контролируемые разделы (темы) дисциплины***	***Код контролируемой компетенции***	***Наименование оценочного средства***
1.	*Тема 1*	ОПК-4	Опрос
2.	*Тема 2*	ОПК-4	Опрос
3.	*Тема 3*	ОПК-4, ПСК-3.2	Опрос
4.	*Тема 4*	ПК-3	Опрос
5.	*Тема 5*	ПК-11, ПСК-3.2	Опрос
6.	*Тема 6*	ПК-11, ПК-12	Опрос
7.	*Тема 7*	ПК-11, ПК-12	Опрос

8.	*Тема 8*	ПК-11, ПК-12, ПСК-3.2	Опрос
9.	*Практические занятия 1.*	ОПК-4, ПСК-3.2	План практического занятия
10.	*Практическое занятие 2.*	ПК-11, ПК-12	План практического занятия
11.	*Практическое занятие 3.*	ПК-11, ПК-12	План практического занятия
12.	*Практическое занятие 4.*	ПК-11, ПК-12	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	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».

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
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. 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.

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

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний, обучающегося по определённому разделу, теме, проблеме и т.п.

Перечень устных вопросов для проверки знаний

№	Вопрос	Реализуемая компетенция
1.	Назначение и задачи, решаемые подсистемой защиты информации (ПЗИ).	ОПК-4
2.	Структура ПЗИ.	ОПК-4
3.	Этапы разработки ПЗИ.	ОПК-4
4.	Угрозы безопасности информации. Классификация угроз.	ОПК-4
5.	Утечка информации. Несанкционированный доступ к информации.	ОПК-4
6.	Уязвимости информационных систем. Подсистемы системы ЗИ	ОПК-4
7.	Разработка модели угроз.	ОПК-4, ПСК-3.2
8.	Разработка модели нарушителя.	ОПК-4, ПСК-3.2
9.	Руководящие нормативные документы по разработке моделей и определения актуальных угроз.	ОПК-4, ПСК-3.2
10.	Политика безопасности.	ПК-3
11.	Программы безопасности административного и процедурного уровня.	ПК-3
12.	Этапы анализа рисков и управления ими.	ПК-3
13.	Реализация механизма VPN	ПК-11, ПСК-3.2
14.	VPN-клиент, VPN-сервер и шлюз безопасности VPN.	ПК-11, ПСК-3.2
15.	Классификация сетей VPN.	ПК-11, ПСК-3.2
16.	Протокол PPTP. Структура пакета.	ПК-11, ПК-12
17.	Процедура установления SSL-сессии.	ПК-11, ПК-12
18.	Защита беспроводных сетей.	ПК-11, ПК-12
19.	Составляющие защиты периметра.	ПК-11, ПК-12
20.	Межсетевые экраны их виды. Администрирование межсетевых экранов.	ПК-11, ПК-12
21.	Демилитаризованная зона, её понятие и структура	ПК-11, ПК-12
22.	Показатель и критерий эффективности функционирования ПЗИ.	ПК-11, ПК-12, ПСК-3.2
23.	Надёжность подсистемы защиты информации. Понятие аудита информационной безопасности.	ПК-11, ПК-12, ПСК-3.2
24.	Модели оценки эффективности.	ПК-11, ПК-12, ПСК-3.2

Примерные вопросы к экзамену – проверка сформированности компетенций – ОПК-4, ПК-3, ПК-11, ПК-12, ПСК-3.2

1. Структура автоматизированной информационной системы (АИС). Назначение и задачи, решаемые ПЗИ. Структура ПЗИ.
2. Этапы разработки ПЗИ. Комплексный подход к разработке ПЗИ. Понятие жизненного цикла системы.
3. Жизненный цикл ПЗИ. Модели жизненного цикла.
4. Требования к ПЗИ в нормативно-методической документации.

5. Угрозы безопасности информации. Классификация угроз.
6. Утечка информации. Каналы утечки.
7. Несанкционированный доступ к информации. Виды НСД.
8. Уязвимости информационных систем.
9. Подсистемы системы защиты информации. Классы защищённости СВТ, АИС, межсетевых экранов.
10. Этапы разработка модели угроз и модели нарушителя. Руководящие нормативные документы по разработке моделей и определения актуальных угроз.
11. Этапы планирования и внедрения средств защиты информации.
12. Правила, регламенты и стратегия администрирования в АИС. Функции и задачи администрирования.
13. Политика безопасности. Обязанности администратора информационной безопасности. Программы безопасности верхнего и процедурного уровня.
14. Защита АИС как процесс управления рисками. Анализ рисков. Основные подходы к анализу рисков. Этапы анализа рисков и управления ими.
15. Администрирование в ОС семейства Windows.
16. Администрирование в ОС семейства Windows Server.
17. Концепция построения виртуальных частных сетей VPN. Защита информации в процессе её передачи по туннелю VPN.
18. VPN-клиент, VPN-сервер и шлюз безопасности VPN. Реализация механизма VPN. Варианты построения виртуальных защищённых каналов.
19. Средства обеспечения безопасности VPN. Критерии безопасности данных применительно к задачам VPN. VPN-решения для построения защищённых сетей.
20. Классификация сетей VPN. Критерии классификации. Основные варианты архитектуры VPN. Достоинства применения технологий VPN.
21. Протокол PPTP. Структура пакета.
22. Протокол L2TP, его преимущества. Формирование защищённого виртуального канала в протоколе L2TP.
23. Процедура установления *SSL*-сессии. Недостатки протоколов *SSL* и *TLS*.
24. Протокол *SOCKS*, его особенности. Схема установления соединения по протоколу *SOCKS* v5.
25. Защита беспроводных сетей. Протоколы WEP, TKIP, WPA и WPA2.
26. Архитектура средств безопасности IPSec. Компоненты реализаций протокола IPSec имеют следующие. Архитектура стека протоколов IPSec.
27. Защита передаваемых данных с помощью протоколов AH и ESP. Применение протокола AH в транспортном и туннельном режимах.
28. Применение протокола ESP в транспортном и туннельном режимах.
29. Алгоритмы аутентификации и шифрования в IPSec. Структура алгоритма HMAC.
30. Протокол управления криптоключами IKE. Задачи, решаемые протоколами IKE. Установление безопасной ассоциации. Базы данных SAD и SPD.
31. Практические аспекты защиты веб-порталов от информационных атак.
32. Угрозы, связанные с периметром корпоративной сети. Составляющие защиты периметра. Межсетевые экраны их виды.
33. Демилитаризованная зона. Анализ содержимого почтового и веб-трафика.
34. Системы обнаружения атак. Классификация систем обнаружения атак.
35. Понятие эффективности. Показатель и критерий эффективности. Методы оценки эффективности. Модели оценки эффективности.
36. Надёжность подсистемы защиты информации.
37. Понятие аудита информационной безопасности. Типы аудита.
38. Инструментальные проверки.

Примерные тестовые задания – проверка сформированности компетенций – ОПК-4, ПК-3, ПК-11, ПК-12, ПСК-3.2

1. Виртуальная защищённая сеть VPN – это

а) объединение компьютеров в сеть через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть для обеспечения безопасности циркулирующих данных.

б) объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных.

в) объединение локальных сетей и отдельных компьютеров через глобальную сеть Интернет в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных.

г) объединение отдельных компьютеров и мобильных устройств через глобальную сеть Интернет в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных.

2. По признаку «рабочего» уровня модели OSI различают следующие группы VPN:

а) VPN канального уровня;

б) VPN прикладного уровня;

в) VPN сеансового уровня.

г) VPN сетевого уровня;

д) VPN транспортного уровня;

е) VPN представительсого уровня.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники

Основные

1. *Базовая модель угроз безопасности* персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г. [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://fstec.ru/component/attachments/download/289, свободный. – Загл. с экрана.
2. *ГОСТ Р 50922-2006*. Защита информации. Основные термины и определения. [Электронный ресурс] / Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=25219#022100440472959426, свободный. – Загл. с экрана
3. *Методика определения актуальных угроз безопасности* персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г. [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380, свободный. – Загл. с экрана.
4. *Методические рекомендации по разработке* нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности. Утверждены руководством 8 Центра ФСБ России от 31 марта 2015 года № 149/7/2/6-432 [Электронный ресурс] / ФСТЭК России. – Режим доступа: по нерабочим дням, в любое время текст документа можно получить на эл. почту http://www.consultant.ru/document/cons_doc_LAW_185051/, свободный. – Загл. с экрана.
5. *Руководящий документ*. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной техни-

ческой 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.

6. *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.
7. *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.

Дополнительные

8. *Приказ ФСТЭК России* от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электронный ресурс] : Режим доступа : https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702, свободный. – Загл. с экрана.
9. *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.
10. *Руководящий документ*. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114. [Электронный ресурс] : Режим доступа : https://fstec.ru/component/attachments/download/294 свободный. – Загл. с экрана
11. *Федеральный закон* «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. от 19.07.2018). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.

Литература

Основная

1.Гвоздева В.А., Информатика, автоматизированные информационные технологии и системы: Учебник / М.:ИД ФОРУМ, НИЦ ИНФРА-М, 2015. - 544 с.
2.Федотова Е.Л. Информационные технологии и системы: Учебное пособие / М.: ИД ФОРУМ: НИЦ Инфра-М, 2013. - 352 с.
3.Затонский А.В. Информационные технологии: разработка информационных моделей и систем: Учеб. пос. / М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014 - 344с.
4.Гвоздева В.А. Информатика, автоматизированные информационные технологии и системы: Учебник / М.:ИД ФОРУМ, НИЦ ИНФРА-М, 2015. - 544 с.

Дополнительная

1. *Гришина Н. В*. Организация комплексной системы защиты информации / Н. В. Гришина. - М. : Гелиос АРВ, 2007. - 254 с. : рис., табл. ; 20 см. - Экз. № 541-08 с автогр. авт. - Библиогр.: с. 248-252 (45 назв.). - ISBN 978-5-85438-172-7 : 150.00.

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.
2. *Банк данных угроз безопасности информации*. [Электронный ресурс] / ФСТЭК России, ФАУ «ГНИИИ ПТЗИ ФСТЭК России» – Режим доступа : http://sec.ru/, свободный. – Загл. с экрана. *Оценка эффективности* систем защиты информации // [Электронный ресурс]: Режим доступа: http://infoprotect.net/note/ocenka_yeffektivnosti_sistem_zasccityi_informacii, свободный
3. *Видео уроки* Cisco Packet Tracer. Курс молодого бойца. [Электронный ресурс] : Режим доступа : https://www.youtube.com/playlist?list=PLcDkQ2Au8aVNYsqGsxRQxYyQijILa94T9, свободный. – Загл. с экрана.

7. Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины необходимо:
1) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должно быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

2) для практических занятий – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Microsoft Office 2010	Microsoft	лицензионное
2		Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное
4	Cisco Packet Tracer v.7.2	Cisco Systems	условно свободное (необходима регистрация в сетевой академии Cisco)
5	VMware Workstation 15 Player и выше	VMware, Inc	свободное
6	или VirtualBox 6.0	Oracle	свободное

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

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-4, ПК-11, ПК-12, ПСК-3.2

Темы учебной дисциплины предусматривают проведение практических занятий, которые служат как целям текущего и промежуточного контроля подготовки 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 практических занятий, выдаваемые преподавателем на каждом занятии.

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

Тематика лабораторных занятий соответствует программе дисциплины.

Лабораторное занятие 1 (6 ч) – проверка сформированности компетенций – ОПК-4, ПСК-3.2

Задания:

1. Проанализировать угрозы безопасности АС организации.
2. Разработать модель угроз по предложенной форме с учётом нормативных документов ФСТЭК.
3. Разработать модель нарушителя

Указания по выполнению заданий:

1. Изучить теоретический материал по теме, нормативные документы ФСТЭК России.
2. Преподавателем выдаётся структура автоматизированной системы организации
3. Ответить на теоретические вопросы в конце практического занятия

Список литературы:

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г. [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://fstec.ru/component/attachments/download/289, свободный. – Загл. с экрана.
2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместите-

лем директора ФСТЭК России 14 февраля 2008 г. [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380, свободный. – Загл. с экрана.

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС Windows 10 Pro и Microsoft Office 2010.

Лабораторное занятие 2 (6 ч.) – проверка сформированности компетенций – ПК-11, ПК-12

Задания:

1. Разработка политики безопасности компании.
2. Администрирование в ОС Windows.
3. Администрирование в ОС Windows Server.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Развернуть на виртуальной машине операционные системы Windows и Windows Server.
3. Преподаватель выдаёт каждому студенту организационно-штатную структуру фирмы и пространство IP-адресов для работы.
4. Ответить на теоретические вопросы в конце практического занятия

Список литературы:

1. *Щеглов А.Ю.* Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. – М. : Издательство Юрайт, 2019. – 309 с. – (Серия : Бакалавр и магистр. Академический курс). – ISBN 978-5-534-04732-5. [Электронный ресурс] : Режим доступа : https://www.biblio-online.ru/book/zaschita-informacii-osnovy-teorii-433715, свободный
2. *Шаньгин В.Ф.* 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

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, виртуальной машиной VMPlayer.

Лабораторное занятие 3 (4 ч.) – проверка сформированности компетенций – ПК-11, ПК-12

Задания:

1. Работа с межсетевым экраном Cisco ASA.
2. Администрирование межсетевых экранов в программе Cisco Packet Tracer.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Выполнить задания.
3. Ответить на теоретические вопросы в конце практического занятия

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, Cisco Packet Tracer.

Лабораторное занятие 4 (6 ч.) – проверка сформированности компетенций – ПК-11, ПК-12

Задания:

1. Создать VPN-канал между филиалами и центральным офисом.
2. Настроить центр авторизации AAA.

Указания по выполнению заданий:

1. Преподаватель выдаёт каждому студенту адресное пространство частных сетей и адресов «провайдера».

2. Ответить на теоретические вопросы в конце практического занятия

Список литературы:

1. *Видео уроки* Cisco Packet Tracer. Курс молодого бойца. [Электронный ресурс] : Режим доступа : https://www.youtube.com/playlist?list=PLcDkQ2Au8aVNYsqGsxRQxYyQijILa94T9, свободный. – Загл. с экрана.

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ndows 10 Pro и Microsoft Office 2010, Cisco Packet Tracer.

По результатам лабораторного занятия обучающиеся составляют отчёт, структура которого представлена ниже. Отчёт составляется в электронной форме с использованием MS Office 2007 и выше и передаётся преподавателю посредством оговорённой формы связи

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Информационные технологии. Администрирование подсистем защиты информации» реализуется на факультете Информационных систем и безопасности для студентов 3-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профиль подготовки – № 3 Комплексная защита объектов информатизации) кафедрой комплексной защиты информации.

Цель дисциплины: ознакомление студентов с методами формирования комплексной системы информационной безопасности; овладение методами проектирования и поддержки жизненного цикла систем информационной безопасности, формирование практических навыков по управлению и администрированию как отдельными компонентами, так и подсистемой защиты информации в целом, а также по разработке и внедрению предложений по оптимизации комплекса средств защиты информации.
Задачи: рассмотрение базовых понятий в области жизненного цикла подсистемы защиты информации; элементы проектирования подсистемы защиты информации, разработка модели угроз и модели нарушителя, построение и последующая эксплуатация подсистемы защиты информации с учётом этих моделей; определения принципов администрирования подсистемы защиты информации, зоны ответственности и обязанностей администратора информационной безопасности; формирование понимания сложности задачи интеграции подсистемы защиты информационной безопасности в информационную систему и администрирования её без ущерба для целевой функции системы.

Дисциплина направлена на формирование следующих компетенций:

- ОПК-4 – способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации
- ПСК-3.2 – способность формировать предложения по оптимизации комплекса технических средств, применяемых в функциональном процессе защищаемого объекта с целью обеспечения его информационной безопасности и осуществлять технико-экономическое обоснование предлагаемых мер защиты.
- ПК-3 – способность администрировать подсистемы информационной безопасности объекта защиты.
- ПК-11 – способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов
- ПК-12 – способность принимать участие в проведении экспериментальных исследований системы защиты информации

В результате освоения дисциплины обучающийся должен:
Знать состав подсистем защиты информации, принципы их функционирования и особенности работы с ними; методологические и технологические принципы формирования и эксплуатации подсистемы защиты информации информационной системы; требования, предъявляемые к подсистеме защиты информации в нормативно-методической документации, методы и способы администрирования подсистемы защиты информации; методики оценки надёжности её функционирования; методы проверки работоспособности подсистем защит информации.
Уметь осуществлять выбор и настройку подсистем защиты информации в соответствии с решаемыми задачами, проводить оценку надёжности их функционирования; выполнять планирование внедрения, внедрение и эксплуатацию средств защиты информации как встроенных в общесистемное и прикладное программное обеспечение, так и специализи-

рованных наложенных; участвовать в разработке моделей угроз и нарушителей, учитывать положения моделей при администрировании комплекса средств защиты информации; выполнять планирование внедрения, внедрение и эксплуатацию средств защиты информации как встроенных в общесистемное и прикладное программное обеспечение, так и специализированных наложенных; выполнять проверку функционирования подсистем защиты информации.

Владеть навыками установки, настройки и администрирования подсистем защиты информации, а также модернизации комплекса средств защиты информации; управления сопряжением и совместной эксплуатацией разнородных средств защиты информации; навыками тестирования и оценки эффективности работы подсистем защиты информации документального сопровождения действий по эксплуатации и администрированию комплекса средств защиты информации.

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.

Общая трудоёмкость освоения дисциплины составляет 3 зачётных 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	*Обновлена структура дисциплины (модуля) для очной формы обучения (2018 г.)*	*26.06.2018 г.*	*11*
3	*Обновлена основная и дополнительная литература*	*26.06.2018 г.*	*11*
4	*Обновление раздела 9. Методические материалы*	*26.06.2018 г.*	*11*
5	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*26.06.2018 г.*	*11*
6	*Обновлена основная и дополнительная литература*	*29.08.2019 г.*	*1*
7	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*29.08.2019 г.*	*1*
8	*Обновлена структура дисциплины (модуля) для очной формы обучения (2020 г.)*	*23.06.2020*	***14***
9	*Обновлена основная и дополнительная литература*	*23.06.2020*	***14***
10	*Обновлен раздел п.4 Образовательные технологии*	*23.06.2020*	***14***
11	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*23.06.2020*	***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
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press
3	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель:
к.т.н. Д.А. Митюшин

Приложение 2
к листу изменений

2. Обновление структуры дисциплины (модуля) для очной формы обучения (2018 г.)

Структура дисциплины (модуля) для очной формы обучения

Общая трудоёмкость дисциплины составляет _3_ з.е., _108_ ч., в том числе контактная работа обучающихся с преподавателем _42_ ч., промежуточная аттестация _18_ ч., самостоятельная работа обучающихся _48_ ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	*Место и роль подсистемы защиты информации в современных информационных системах*	**6**	**2**					**4**	Опрос.
2	*Угрозы безопасности информационной системы*	**6**	**2**					**5**	Опрос.
3	*Модель угроз и модель нарушителя*	**6**	**2**					**5**	Опрос.
4	*Сущность администрирования*	**6**	**4**					**5**	Опрос.
5	*Основы технологии виртуальных защищённых сетей VPN*	**6**	**2**					**5**	Опрос.
6	*Защита на канальном, сеансовом и сетевом уровнях. Аспекты защиты вебпорталов*	**6**	**4**					**5**	Опрос.
7	*Администрирование межсетевых экранов*	**6**	**2**					**5**	Опрос.
8	*Оценка эффективности и надёжности функционирования подсистемы защиты информации*	**6**	**2**					**5**	Опрос.
9	*Практические занятия 1. Разработка модели угроз и нарушителя*	**6**			**6**				Отчёт о практическом занятии
10	*Практическое занятие 2. Администри-*	**6**			**6**				Отчёт о практическом занятии

	рование встроенных систем защиты ОС Windows и Windows Server								
11	*Практическое занятие 3. Настройка межсетевых экранов*	**6**			**4**				Отчёт о практическом занятии
12	*Практическое занятие 4. Создание VPN-канала.*	**6**			**6**			**9**	Отчёт о практическом занятии
	экзамен	**6**					**18**		*экзамен по билетам*
	итого:		**20**		**22**		**18**	**48**	

3.Обновление основной и дополнительной литературы (2018 г.)

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

Дополнить раздел *Основная литература*

Защита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – 2-е изд. – Москва : РИОР : ИНФРА-М, 2018. – 392 с. – (Высшее образование: Бакалавриат; Магистратура). – https://doi.org/10.12737/4868. -- Текст : электронный. – URL: https://new.znanium.com/catalog/product/937469

4.Обновление раздела 9. Методические материалы

В раздел 9 внести следующие изменения.

Заменить производные слова от слова «лабораторный» на соответствующие производные слова от слова «практический».

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

1. 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

2. 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. ЖурналыCambridge 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. Д.А. Митюшин

Приложение 3
к листу изменений

6.Обновление основной и дополнительной литературы (2019 г.)

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

Дополнить раздел *Основная литература*

Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. – Москва : Издательство Юрайт, 2019. – 309 с. – (Бакалавр и магистр. Академический курс). – ISBN 978-5-534-04732-5. – Текст : электронный // ЭБС Юрайт [сайт]. – URL: https://www.biblio-online.ru/bcode/433715 (дата обращения: 23.08.2019).
Шаньгин В.Ф. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. – Москва : ИД «ФОРУМ» : ИНФРА-М, 2019. – 592 с. – (Высшее образование: Бакалавриат). – Текст : электронный. – URL: https://new.znanium.com/catalog/product/996789

7.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	свободнораспространяемое
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 наци-

	ональной подписки в 2019 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2019 г. ЖурналыCambridge 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. Д.А. Митюшин

Приложение 4
к листу изменений

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

Структура дисциплины (модуля) для очной формы обучения

Общая трудоемкость дисциплины составляет 3 з. е., 114 ч., в том числе контактная работа обучающихся с преподавателем 42 ч., самостоятельная работа обучающихся 54 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	*Место и роль подсистемы защиты информации в современных информационных системах*	**6**	**2**					**2**	Опрос.
2	*Угрозы безопасности информационной системы*	**6**	**2**					**3**	Опрос.
3	*Модель угроз и модель нарушителя*	**6**	**2**					**3**	Опрос.
4	*Сущность администрирования*	**6**	**4**					**3**	Опрос.
5	*Основы технологии виртуальных защищённых сетей VPN*	**6**	**2**					**3**	Опрос.
6	*Защита на канальном, сеансовом и сетевом уровнях. Аспекты защиты вебпорталов*	**6**	**4**					**3**	Опрос.
7	*Администрирование межсетевых экранов*	**6**	**2**					**3**	Опрос.
8	*Оценка эффективности и надёжности функционирования подсистемы защиты информации*	**6**	**2**					**3**	Опрос.
9	*Практические занятия 1. Разработка модели угроз и нарушителя*	**6**			**6**			**5**	Отчёт о практическом занятии
10	*Практическое занятие 2. Администри-*	**6**			**6**			**5**	Отчёт о практическом занятии

	рование встроенных систем защиты ОС Windows и Windows Server								
11	*Практическое занятие 3. Настройка межсетевых экранов*	**6**			**4**			**5**	Отчёт о практическом занятии
12	*Практическое занятие 4. Создание VPN-канала.*	**6**			**6**			**7**	Отчёт о практическом занятии
	экзамен	**6**					**18**	**9**	*экзамен по билетам*
	итого:		**20**		**22**		**18**	**54**	

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

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

1. Дополнить раздел **Основная 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 (дата обращения: 11.09.2020).

2. Дополнить раздел **Дополнительная литература**

Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами : монография / А. И. Белоус, В. А. Солодуха. – Москва ; Вологда : Инфра-Инженерия, 2020. – 692 с. – ISBN 978-5-9729-0486-0. – Текст : электронный. – URL: https://znanium.com/catalog/product/1167736 (дата обращения: 11.09.2020). – Режим доступа: по подписке..

10. 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.

11. 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

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 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
17	Zoom	Zoom	лицензионное

Составитель:
к.т.н. Д.А. Митюшин