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

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

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*

Защита информации от несанкционированного доступа
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
1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине
1.3. Место дисциплины в структуре образовательной программы
2. Структура дисциплины
3. Содержание дисциплины
4. Образовательные технологии
5. Оценка планируемых результатов обучения
5.1. Система оценивания
5.2. Критерии выставления оценок
5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине
5.4 Курсовые работы
6. Учебно-методическое и информационное обеспечение дисциплины
6.1. Список источников и литературы
6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»
7. Материально-техническое обеспечение дисциплины
8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья
9. Методические материалы
9.1. Планы практических (семинарских, лабораторных) занятий
9.2. Методические рекомендации по подготовке письменных работ

Приложения
Приложение 1. Аннотация дисциплины
Приложение 2. Лист изменений

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – получение знаний по существующим угрозам информационной безопасности, применению современных методов и способов защиты информации от несанкционированного доступа (НСД); формирование навыков, необходимых для защиты информации от НСД в современных информационных системах.

Задачи дисциплины:

– овладение методами решения профессиональных задач по защите информации от НСД;
– формирование навыков работы с современными средствами защиты информации от НСД

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

Коды компетенции	**Содержание компетенций**	**Перечень планируемых результатов обучения по дисциплине**
ПК-11	способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Знать: принципы организации информационных систем в соответствии с требованиями по защите информации от НСД. Уметь: формулировать и настраивать политику безопасности в информационной системе; Владеть: методикой анализа защищённости информационной системы
ПК-12	способность принимать участие в проведении экспериментальных исследований системы защиты информации	Знать: принципы организации информационных систем в соответствии с требованиями по защите информации от НСД. Уметь: анализировать и оценивать угрозы безопасности информационной системы. Владеть: методикой анализа защищённости информационной системы
ПК-15	способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	Знать: основные модели доступа (мандатная, дискреционная, ролевая и др.), принципы и методы защиты информации от НСД; принципы организации информационных систем в соответствии с требованиями по защите информации от НСД. Уметь: пользоваться нормативными документами по защите информации от НСД. Владеть: методикой анализа защищённости информационной системы

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации от несанкционированного доступа» относится к дисциплинам по выбору вариативной части блока дисциплин учебного плана.

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

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Безопасность критически важных информационных систем», «Комплексное обеспечение безопасности объекта информатизации».

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет _4_ з.е., _144__ ч., в том числе контактная работа обучающихся с преподавателем _28_ ч., промежуточная аттестация _-_ ч., самостоятельная работа обучающихся – 114 ч, курсовая работа (контроль)- 2_ 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	*Введение в защиту информации от несанкционированного доступа*	**6**	**2**					**4**	Опрос.
2	*Требования к защите информации от несанкционированного доступа*	**6**	**2**					**4**	Опрос
3	*Авторизация. Методы идентификации и аутентификации пользователя*	**6**	**2**					**4**	Опрос.
4	*Управление доступом к ресурсам*	**6**	**2**					**6**	Опрос.
5	*Разработка политики безопасности информационной системы*	**6**	**4**					**6**	Опрос.
6	*Методика анализа защищённости ИС. Методы и средства выявления угроз её информационной безопасности*	**6**	**2**					**6**	Опрос.
7	*Применение средств аппаратной защиты*	**6**	**2**					**6**	Опрос.

8	*Лабораторная работа № 1*					**6**			Отчёт по лабораторной работе
9	*Лабораторная работа № 2*					**6**			Отчёт по лабораторной работе
10	*курсовая работа*						**2**	**70**	*оценка курсовой работы*
	Зачёт с оценкой	**6**							*Зачёт с оценкой по билетам*
	итого:		**16**			**12**	**2**	**114**	

3. Содержание дисциплины

Тема 1. Введение в защиту информации от несанкционированного доступа
Основные термины и определения ЗИ от НСД. Классификация требований к системам защиты от НСД. Ответственность за НСД. Документы Гостехкомиссии (ФСТЭК) России по защите от НСД. Система государственных нормативных актов, стандартов, руководящих документов и требований по ЗИ от НСД. Особенности современных АС. Виды угроз современным АС. Классы защищённости СВТ и АС. Показатели защищённости межсетевых экранов и их увязка с классами защищённости АС.

Тема 2. Требования к защите информации от несанкционированного доступа
Формализованные требования к ЗИ от НСД. Классы защищённости СВТ. Классификация АС по защищённости от НСД. Состав первой группы защиты АС. Подсистемы механизма ЗИ от НСД. Требования к защите информации АС групп 1Г и 1В.

Тема 3. Методы идентификации и аутентификации пользователя
Понятие идентификации и аутентификации. Процедура авторизации. Формализованные и дополнительные требования к идентификации и аутентификации. Авторизация в контексте количества и вида зарегистрированных пользователей. Рекомендации по построению авторизации, исходя из вида и количества зарегистрированных пользователей. Классификация задач, решаемых механизмами идентификации и аутентификации. Критерии классификации. Механизмы парольной защиты. Функциональное назначение и реализация механизмов парольной защиты. Угрозы преодоления парольной защиты. Явные и скрытые угрозы. Основные механизмы ввода пароля. Биометрический и комбинированный способ ввода пароля. Способы усиления парольной защиты. Добавочные механизмы усиления парольной защиты и требования к ним. Двухуровневая авторизация на уровне ОС и BIOS. Сетевая авторизация. Протоколы аутентификации.

Тема 4. Управление доступом к ресурсам
Основные способы разделения доступа субъектов к совместно используемым объектам. Абстрактные модели доступа. Модели Биба, Гогена-Мезигера, Кларка-Вильсона, Сазерлендская модель. Дискреционная (матричная) модель. Многоуровневые (мандатные) модели. Понятия «владелец» и «собственник» информации.
Базовые модели доступа. Дискреционное разграничение доступа. Матрица доступа и домен безопасности. Список прав доступа ACL. Мандатное разграничение доступа. Ролевая модель разграничения доступа. Управления доступом на основе атрибутов. Выбор модели разграничения доступа.
Корректность и полнота реализации разграничительной политики доступа. Классификация субъектов и объектов доступа. Требования к механизмам управления доступом.
Централизованное и децентрализованное управление доступом. Протоколы аутентификации (AAA). RADIUS, TACACS.

Тема 5. Разработка политики безопасности информационной системы
Общие положения разработки политики безопасности. Нормативные документы по разработке политики безопасности. Важные аспекты при разработке политик безопасности. Средства защиты информации для государственных и коммерческих структур. Процесс разработки политики безопасности. Примерный состав группы по разработке политик безопасности. Требования к политикам безопасности. Типовые политики безопасности.
Реализация политик безопасности. Общие правила безопасности. Архитектура корпоративной системы защиты информации. Настройки основных компонент системы защиты компании.

Тема 6. Методика анализа защищённости ИС. Методы и средства выявления угроз её информационной безопасности

Типовая методика анализа защищённости ИС. Методы тестирование систем информационной безопасности. Методы количественной оценки систем информационной безопасности. Методы и средства анализа защищённости автоматизированной системы. Анализ защищённости внешнего периметра корпоративной сети. Анализ защищённости внутренней инфраструктуры сети. Инструментальные средства анализа защищённости. Методы предотвращения сетевых атак на периметр сети.

Тема 7. Применение средств аппаратной защиты

Необходимость и принципы использования аппаратных средств защиты. Угрозы перевода системы защиты в пассивное состояние, их реализация. Методы противодействия угрозам перевода системы защиты в пассивное состояние. Реализация программно-аппаратного контроля (мониторинга) активности системы защиты. Метод контроля целостности и активности программных компонент системы защиты программно-аппаратными средствами. Механизм удалённого мониторинга активности системы защиты, как альтернатива применению аппаратной компоненты защиты. Метод контроля вскрытия аппаратуры, общий подход. Реализация системы контроля вскрытия аппаратуры. Принципы комплексирования средств защиты информации

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1	*Введение в защиту информации от несанкционированного доступа*	*Лекция 1.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Работа с литературой*
2	*Требования к защите информации от несанкционированного доступа*	*Лекция 2.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Работа с литературой*
3	*Авторизация. Методы идентификации и аутентификации пользователя*	*Лекция 3.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Работа с литературой*
4	*Управление доступом к ресурсам*	*Лекция 4.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Работа с литературой*
5	*Разработка политики безопасности информационной системы*	*Лекция 5.1* *Лекция 5.2* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Работа с литературой*
6	*Методика анализа защищённости ИС. Методы и средства выявления угроз её информационной безопасности*	*Лекция 6.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Работа с литературой*
7	*Применение средств аппаратной защиты*	*Лекция 7.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Работа с литературой*
8	*Лабораторная работа 1*	*Лабораторная работа № 1*	*Отчёт о лабораторной*

			работе
9	*Лабораторная работа 2*	*Лабораторная работа № 2*	*Отчёт о лабораторной работе*

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *- опрос (темы 1-7)* *- лабораторная работа № 1* *- лабораторная работа № 2*	 *4 баллов* *6 баллов* *8 баллов*	 *28 баллов* *16 баллов* *16 баллов*
Промежуточная аттестация *зачёт*		*40 баллов*
Итого за дисциплину *зачёт*		*100 баллов*

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

№ п/п	***Контролируемые разделы дисциплины***	***Код контролируемой компетенции***	***Наименование оценочного средства***
1.	Темы 1-7	ПК-11, ПК-15, ПК-12	Результаты опроса
2.	Лабораторная работа № 1, 2	ПК-11, ПК-15, 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)»/	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
	«зачтено»	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. 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 заня-

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		тиях 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.	Понятия «доступ к информации», «правила разграничения доступа» «санкционированный и несанкционированный доступ к информации	ПК-15
2.	Первая группа требований (необходимые требования) к системе защиты	ПК-15
3.	Вторая группа требований (дополнительные требования) к системе защиты	ПК-15
4.	Виды угроз автоматизированным системам	ПК-11, ПК-15, ПК-12
5.	Классы защищённости АС и СВТ от НСД	ПК-11, ПК-15, ПК-12
6.	Состав первой группы защиты АС	ПК-11, ПК-15, ПК-12
7.	Подсистемы механизма ЗИ от НСД.	ПК-11, ПК-15, ПК-12
8.	Требования к защите информации АС групп 1Г и 1В..	ПК-11, ПК-15, ПК-12
9.	Понятие идентификации и аутентификации.	ПК-11, ПК-15, ПК-12
10.	Процедура авторизации.	ПК-11, ПК-15, ПК-12
11.	Классификация задач, решаемых механизмами идентификации и аутентификации.	ПК-11, ПК-15, ПК-12
12.	Механизмы парольной защиты.	ПК-11, ПК-15, ПК-12

13.	Угрозы преодоления парольной защиты. Явные и скрытые угрозы.	ПК-11, ПК-15, ПК-12
14.	Основные механизмы ввода пароля. Биометрический и комбинированный способ ввода пароля.	ПК-11, ПК-12
15.	Способы усиления парольной защиты. Добавочные механизмы усиления парольной защиты и требования к ним.	ПК-11, ПК-12
16.	Основные способы разделения доступа субъектов к совместно используемым объектам.	ПК-11, ПК-12
17.	Дискреционная (матричная) модель разделения доступа.	ПК-11, ПК-12
18.	Многоуровневые (мандатные) модели разделения доступа.	ПК-11, ПК-12
19.	Список прав доступа ACL.	ПК-11, ПК-12
20.	Ролевая модель разграничения доступа.	ПК-11, ПК-12
21.	Управления доступом на основе атрибутов. Выбор модели разграничения доступа.	ПК-11, ПК-12
22.	Классификация субъектов и объектов доступа.	ПК-11, ПК-15, ПК-12
23.	Централизованное и децентрализованное управление доступом.	ПК-11, ПК-15, ПК-12
24.	Протоколы аутентификации (AAA). RADIUS, TACACS.	ПК-11, ПК-15, ПК-12
25.	Нормативные документы по разработке политики безопасности.	ПК-11, ПК-15, ПК-12
26.	Средства защиты информации для государственных и коммерческих структур.	ПК-11, ПК-15, ПК-12
27.	Примерный состав группы по разработке политик безопасности.	ПК-11, ПК-15, ПК-12
28.	Архитектура корпоративной системы защиты информации.	ПК-11, ПК-15, ПК-12
29.	Анализ защищённости внешнего периметра корпоративной сети.	ПК-11, ПК-15, ПК-12
30.	Анализ защищённости внутренней инфраструктуры сети.	ПК-11, ПК-15, ПК-12
31.	Методы предотвращения сетевых атак на периметр сети.	ПК-11, ПК-15, ПК-12
32.	Угрозы перевода системы защиты в пассивное состояние, их реализация.	ПК-11, ПК-15, ПК-12
33.	Метод контроля вскрытия аппаратуры, общий подход.	ПК-11, ПК-15, ПК-12
34.	Принципы комплексирования средств защиты информации	ПК-11, ПК-15, ПК-12

Промежуточная аттестация (примерные вопросы к зачёту) – проверка сформированности компетенций – ПК-11, ПК-12, ПК-15

1. Документы Гостехкомиссии (ФСТЭК) России по защите от НСД. Система государственных нормативных актов по ЗИ от НСД.
2. Виды угроз современным АС.
3. Классы защищённости СВТ и АС. Показатели защищённости межсетевых экранов и их увязка с классами защищённости АС.
4. Подсистемы механизма ЗИ от НСД. Требования к защите информации АС групп 1Г и 1В.
5. Понятие идентификации и аутентификации. Процедура авторизации.

6. Формализованные и дополнительные требования к идентификации и аутентификации. Авторизация в контексте количества и вида зарегистрированных пользователей. Рекомендации по построению авторизации, исходя из вида и количества зарегистрированных пользователей.
7. Механизмы парольной защиты. Функциональное назначение и реализация механизмов парольной защиты.
8. Угрозы преодоления парольной защиты.
9. Основные механизмы ввода пароля.
10. Двухуровневая авторизация на уровне ОС и BIOS. Сетевая авторизация.
11. Протоколы аутентификации.
12. Абстрактные модели доступа. Понятия «владелец» и «собственник» информации.
13. Дискреционное разграничение доступа.
14. Мандатное разграничение доступа.
15. Ролевая модель разграничения доступа.
16. Управления доступом на основе атрибутов. Выбор модели разграничения доступа.
17. Корректность и полнота реализации разграничительной политики доступа. Классификация субъектов и объектов доступа. Требования к механизмам управления доступом.
18. Централизованное и децентрализованное управление доступом.
19. Общие положения разработки политики безопасности. Нормативные документы по разработке политики безопасности.
20. Процесс разработки политики безопасности. Требования к политикам безопасности.
21. Реализация политик безопасности. Архитектура корпоративной системы защиты информации. Настройки основных компонент системы защиты компании.
22. Типовая методика анализа защищённости ИС
23. Методы количественной оценки систем информационной безопасности.
24. Анализ защищённости внешнего периметра и внутренней инфраструктуры корпоративной сети.
25. Инструментальные средства анализа защищённости. Методы предотвращения сетевых атак на периметр сети.
26. Угрозы перевода системы защиты в пассивное состояние, их реализация. Методы противодействия угрозам перевода системы защиты в пассивное состояние.
27. Реализация программно-аппаратного контроля (мониторинга) активности системы защиты.
28. Метод контроля целостности и активности программных компонент системы защиты программно-аппаратными средствами.
29. Механизм удалённого мониторинга активности системы защиты, как альтернатива применению аппаратной компоненты защиты.
30. Метод контроля вскрытия аппаратуры, общий подход. Реализация системы контроля вскрытия аппаратуры.
31. Принципы комплексирования средств защиты информации

Примерные тестовые задания – проверка сформированности компетенций – ПК-15

1. Процедура, призванная каждому пользователю (группе пользователей) сопоставить соответствующую ему разграничительную политику доступа на защищаемом объекте называется

а) аутентификация

б) идентификация

в) авторизация

2. Мандатной защитой характеризуется:

а) вторая группа защищённости СВТ от НСД

б) первая группа защищённости СВТ от НСД
в) третья группа защищённости СВТ от НСД
г) пятая группа защищённости СВТ от НСД

Примерные темы курсовых работ – проверка сформированности компетенций – ПК-11, ПК-12, ПК-15

Учебным планом по дисциплине «Защита информации от несанкционированного доступа» предусмотрено выполнение курсовых работ.

1. Система нормативных актов РФ в области защиты от НСД (ПК-15)
2. Угрозы и уязвимости современных автоматизированных систем (ПК-12)
3. Классы защищённости современных автоматизированных систем и программно-аппаратных средств (ПК-11, ПК-12)
4. Авторизация как процесс доступа (ПК-11, ПК-12)
5. Реализация механизмов парольной защиты для организации банковского сектора (ПК-11, ПК-12)
6. Межсетевые экраны как средство защиты информации от несанкционированного доступа (ПК-11, ПК-12)
7. Анализ рынка средств усиления парольной защиты (ПК-11, ПК-12)
8. Реализация добавочных механизмов усиления парольной защиты (ПК-11, ПК-12)
9. Разработка политики информационной безопасности для государственной организации (ПК-11, ПК-12, ПК-15)
10. Разработка политики информационной безопасности для организации оборонно-промышленного комплекса (ПК-12, ПК-15)
11. Архитектура корпоративной системы защиты информации машиностроительного предприятия (ПК-12, ПК-15)
12. Анализ современных способов разграничения доступа (ПК-11, ПК-12)
13. Анализ защищённости внутренней инфраструктуры сети государственной организации (ПК-11, ПК-12)
14. Анализ защищённости внутренней инфраструктуры сети коммерческой организации (ПК-11, ПК-12)
15. Применения инструментальных средств анализа защищённости внутренней инфраструктуры сети (ПК-11, ПК-12)
16. Анализ рынка программно-аппаратных средств защиты информации от несанкционированного доступа (ПК-11, ПК-12)
17. Технико-экономическая оценка комплексирования средств защиты информации на примере коммерческой организации (ПК-11, ПК-12)
18. Разработка модели угроз безопасности информации коммерческой фирмы (ПК-12, ПК-15)
19. Разработка модели угроз безопасности информации государственной организации (ПК-12, ПК-15)
20. Анализ рынка биометрических средств ввода пароля (ПК-12, ПК-15)

Курсовые работы являются составной частью самостоятельной учебно-исследовательской работы студента и предназначены для углубленного изучения дисциплин учебного плана, развития индивидуальных творческих способностей студента.

Цель курсовой работы – подготовка к самостоятельному решению задач, связанных с процессом защиты информации от несанкционированного доступа..

Достижение цели курсового проектирования осуществляется за счёт решения задач по разработке построения системы защиты информации от НСД на объекте информатизации, выполняемых во взаимосвязанной последовательности из ряда тем.
Задачами преподавателя по проверке курсовой работы:

– оценить уровень овладения студентом профессиональными компетенциями;
– проверить подготовленность студента к выполнению выпускной квалификационной работы.
Задачами работы студента над курсовыми работами являются:
– углубленное изучение выбранной темы;
– приобретение умения вести поиск необходимого фактического материала, его анализа и систематизации, формулирования научных целей и выводов;
– развития навыков грамотного и логически доказательного изложения текста;
– получение опыта правильного оформления научной работы.

Курсовая работа представляет собой исследование по одной из научных проблем или отдельной теме учебной дисциплины.
Курсовая работа может быть написана как одна из глав будущей дипломной работы студента. По содержанию курсовая работа может иметь как теоретический, так и прикладной характер. Научный материал, который студент должен использовать при написании курсовой работы, отбирается индивидуально по каждой теме.
Тема курсовой работы может развивать и углублять тему ранее написанного студентом реферата.

Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1	Курсовая работа	Самостоятельная работа	Работа с литературой

Система оценивания

Форма контроля	Количество баллов
Содержание работы соответствует выбранной теме, раскрывает ее полно и всесторонне, демонстрирует свободное владение материалом	30
Использована обязательная и дополнительная литература, соответствующие информационные ресурсы	10
Работа написана грамотным литературным языком с соблюдением стилистических норм и корректным использованием профессиональной терминологии.	10
Структура работы соответствует плану, обнаруживает стройную логическую последовательность разделов.	10
Оформление соответствует актуальным требованиям к оформлению курсовой работы.	20
Защита курсовой работы	20
Итого оценка за курсовую работу	100

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:

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.
5. *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. N 114
6. *Базовая модель угроз* безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). (утв. ФСТЭК РФ 15.02.2008) [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379, свободный. – Загл. с экрана.
7. *Федеральный закон* «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ. [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.

Дополнительные

8. *Приказ ФСТЭК России* от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». [Электронный ресурс] : Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=214004&dst=0&rnd=92395C5151F01C02B8725B20C4BBFEB5#034991095371992622 по рабочим дням с 20-00 до 24-00 (время московское), в выходные и праздничные дни в любое время. – Загл. с экрана.

9. *Приказ ФСТЭК России* от 18 февраля 2013 г. № 21. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.. [Электронный ресурс] : Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=215976&dst=0&rnd=92395C5151F01C02B8725B20C4BBFEB5#08164959407738432 свободный. – Загл. с экрана.

Литература

Основная

1. Аппаратно-программные средства защиты информации: Практикум / Душкин А.В., Дубровин А.С., Здольник В.В. - Воронеж: Научная книга, 2017. - 198 с.: ISBN 978-5-4446-1043-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/977192. – Режим доступа: по подписке.

Дополнительная

2. *Щеглов, А.Ю.* Математические модели и методы формального проектирования систем защиты информационных систем : учебное пособие / А. Ю. Щеглов, К. А. Щеглов. – Санкт-Петербург : НИУ ИТМО, 2015. – 93 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/70897. - Режим доступа: для авториз. пользователей.
3. *Баранова, Е. К*. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. – Москва : РИОР : ИНФРА-М, 2017. – 322 с. – (Высшее образование). – ww.dx.doi.org/10.12737/11380. - ISBN 978-5-369-01450-9. – Текст : электронный. – URL: https://znanium.com/catalog/product/763644 – Режим доступа: по подписке.
4. Система защиты информации от несанкционированного доступа на основе программно-аппаратного комплекса "Secret Net 5.0" / Помешкин А.А., Коротких И.В. - Новосибирск :НГТУ, 2012. - 47 с.: ISBN 978-5-7782-1990-8 - Текст : электронный. - URL: https://new.znanium.com/catalog/product/556699

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

1. *Банк данных угроз безопасности информации*. [Электронный ресурс] / ФСТЭК России, ФАУ «ГНИИИ ПТЗИ ФСТЭК России» – Режим доступа : http://sec.ru/, свободный. – Загл. с экрана.

6.3. Перечень БД и ИСС

№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 ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

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
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
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное
5	VMware Workstation 15 Player и выше	VMware, Inc	свободное
6	или VirtualBox 6.0	Oracle	свободное
7	Zenmap	nmap.org	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 – ПК-11, ПК-12, ПК-15

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 (4 ч.) Определение уязвимостей сети – проверка сформированности компетенций – ПК-11, ПК-12, ПК-15
Задания:
1. Установить на компьютеры класса сканер портов Zenmap.
2. Провести общее сканирование сети класса.
3. Провести углублённое сканирование двух соседних хостов с использованием различных профилей сканирования.

Указания по выполнению заданий:
1. Изучить теоретические основы защиты сканирования сетей и работу с Zenmap.
2. Составить отчёт о лабораторной работе.

Список литературы:
1. Материалы лекций
2. Программно-аппаратная защита информации : учеб. пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2019. — 352 с. — (Высшее образование). - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1025261 (дата обращения: 11.08.2019)

Материально-техническое обеспечение занятия:
1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows.

Лабораторная работа 2 (6 ч.) Разграничение доступа – проверка сформированности компетенций – ПК-11, ПК-12, ПК-15
Задания:
1. На виртуальную машину установить ОС MS Windows Server, MS Windows и Linux.
2. Запустить виртуальную машину.
3. Запустить гостевых ОС семейства.
4. Зарегистрировать по два пользователя на каждой ОС, один с правами администратора, один – с правами пользователя. Для ОС MS Windows Server – один пользователь с правами администратора
5. Провести разграничение доступа на хосты с хоста администратора (MS Windows Server)

Указания по выполнению заданий:
1. Изучить теоретические основы защиты ОС.
2. Составить отчёт о лабораторной работе.

Список литературы:
1. Материалы лекций
2. Программно-аппаратная защита информации : учеб. пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2019. — 352 с. — (Высшее образование). - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1025261 (дата обращения: 11.08.2019)

Материально-техническое обеспечение занятия:
1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной.

Результаты лабораторных работ обучающиеся составляют по оговорённой преподавателем форме, в электронном виде с использованием ПКП MS Office 2007 и выше и передаётся преподавателю посредством оговорённого способа связи.

9.2. Методические рекомендации по подготовке письменных работ

Требования к оформлению курсовой работы содержатся в Методических рекомендациях «Порядок подготовки, оформления и защиты курсовых и выпускных квалифика-

ционных работ (с различными видами доступа) для направления подготовки 10.03.01 «Информационная безопасность» (квалификация (степень) «бакалавр») профили: «Организация и технология защиты информации» и «Комплексная защита объектов информатизации».

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Защита информации от несакционированного доступа» 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: получение знаний по существующим угрозам информационной безопасности, применению современных методов и способов защиты информации от НСД; формирование навыков, необходимых для защиты информации от НСД в современных информационных системах.

Задачи: овладение методами решения профессиональных задач по защите информации от НСД; формирование навыков работы с современными средствами защиты информации от НСД.

Дисциплина направлена на формирование следующих компетенций:

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
ПК-15	способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

В результате освоения дисциплины обучающийся должен:

Знать основные модели доступа (мандатная, дискреционная, ролевая и др.), принципы и методы защиты информации от НСД; принципы организации информационных систем в соответствии с требованиями по защите информации от НСД.

Уметь формулировать и настраивать политику безопасности в информационной системе; осуществлять меры по защите информации от НСД, пользоваться нормативными документами по защите информации от НСД; анализировать и оценивать угрозы безопасности информационной системы.

Владеть методикой анализа защищённости информационной системы; методами и средствами выявления угроз её информационной безопасности.

По дисциплине предусмотрена промежуточная аттестация в форме зачёта с оценкой и защиты курсовой работы.

Общая трудоёмкость освоения дисциплины составляет 4 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)*	*29.06.2017г.*	***10***
2	*Обновлена структура дисциплины (модуля) для очной формы обучения (2018 г.)*	*26.06.2018 г.*	***11***
3	*Внести изменения в подраздел 9.1. Планы лабораторных занятий*	*26.06.2018 г.*	***11***
4	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*26.06.2018 г.*	***11***
5	*Обновлена основная и дополнительная литература*	*29.08.2019 г*	***1***
6	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*29.08.2019 г*	***1***
7	*Обновлена структура дисциплины (модуля) для очной формы обучения (2020 г.)*	*23.06.2020*	***14***
8	*Обновлена основная и дополнительная литература*	*23.06.2020*	***14***
9	*Обновлен раздел п.4 Образовательные технологии*	*23.06.2020*	***14***
10	*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 для очной формы обучения

Общая трудоёмкость дисциплины составляет _4_ з.е., _144__ ч., в том числе контактная работа обучающихся с преподавателем _28_ ч., промежуточная аттестация _-_ ч., самостоятельная работа обучающихся – 114 ч, курсовая работа (контроль) - 2_ 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	*Введение в защиту информации от несанкционированного доступа*	**6**	**2**					**4**	Опрос.
2	*Требования к защите информации от несанкционированного доступа*	**6**	**2**					**4**	Опрос
3	*Авторизация. Методы идентификации и аутентификации пользователя*	**6**	**2**					**4**	Опрос.
4	*Управление доступом к ресурсам*	**6**	**2**					**6**	Опрос.
5	*Разработка политики безопасности информационной системы*	**6**	**4**					**6**	Опрос.
6	*Методика анализа защищённости ИС. Методы и средства выявления угроз её информационной безопасности*	**6**	**2**					**6**	Опрос.
7	*Применение средств аппаратной защиты*	**6**	**2**					**6**	Опрос.
8	*Лабораторная работа № 1*					**6**			Отчёт по лабораторной работе
9	*Лабораторная работа № 2*					**6**			Отчёт по лабораторной работе
10	*курсовая работа*						**2**	**70**	*оценка курсовой работы*
	зачёт	**6**							*Зачёт по билетам*
	итого:		**16**			**12**	**2**	**114**	

3. Внести изменения в подраздел 9.1. Планы лабораторных занятий - проверка сформированности компетенций – ПК-15

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 (4 ч.) Определение уязвимостей сети – проверка сформированности компетенций – ПК-15

Задания:

4. Установить на компьютеры класса сканер портов Zenmap.

5. Провести общее сканирование сети класса.

6. Провести углублённое сканирование двух соседних хостов с использованием различных профилей сканирования.

Указания по выполнению заданий:

3. Изучить теоретические основы защиты сканирования сетей и работу с Zenmap.

4. Составить отчёт о лабораторной работе.

Материально-техническое обеспечение занятия:

2. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows.

Лабораторная работа 2 (6 ч.) Разграничение доступа – проверка сформированности компетенций – ПК-15

Задания:

6. На виртуальную машину установить ОС MS Windows Server, MS Windows и Linux.

7. Запустить виртуальную машину.

8. Запустить гостевых ОС семейства.

9. Зарегистрировать по два пользователя на каждой ОС, один с правами администратора, один – с правами пользователя. Для ОС MS Windows Server – один пользователь с правами администратора

10. Провести разграничение доступа на хосты с хоста администратора (MS Windows Server)

Указания по выполнению заданий:

3. Изучить теоретические основы защиты ОС.

4. Составить отчёт о лабораторной работе.

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной.

Результаты лабораторных работ обучающиеся составляют по оговорённой преподавателем форме, в электронной виде с использованием ПКП MS Office 2007 и выше и передаётся преподавателю посредством оговорённого способа связи.

4. 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(и):
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

Приложение 3
к листу изменений

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

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

Дополнить раздел Основная литература

Гаврилов, М. В. Информатика и информационные технологии : учебник для прикладного бакалавриата / М. В. Гаврилов, В. А. Климов. – 4-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2019. – 383 с. – (Серия : Бакалавр. Прикладной курс). – ISBN 978-5-534-00814-2. – Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/bcode/431772

Программно-аппаратная защита информации : учеб. пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2019. — 352 с. — (Высшее образование). - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1025261 (дата обращения: 11.08.2019)

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, 2019. – 309 с. – (Серия : Бакалавр и магистр. Академический курс). – ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. – URL: https://www.biblio-online.ru/book/zaschita-informacii-osnovy-teorii-433715.

6.Обновление состава 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(и):
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

Приложение 4
к листу изменений

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

Общая трудоемкость дисциплины составляет 4 з. е., 152 ч., в том числе контактная работа обучающихся с преподавателем 28 ч., самостоятельная работа обучающихся 122 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	*Введение в защиту информации от несанкционированного доступа*	**6**	**2**					**4**	Опрос.
2	*Требования к защите информации от несанкционированного доступа*	**6**	**2**					**4**	Опрос
3	*Авторизация. Методы идентификации и аутентификации пользователя*	**6**	**2**					**4**	Опрос.
4	*Управление доступом к ресурсам*	**6**	**2**					**6**	Опрос.
5	*Разработка политики безопасности информационной системы*	**6**	**4**					**6**	Опрос.
6	*Методика анализа защищённости ИС. Методы и средства выявления угроз её информационной безопасности*	**6**	**2**					**6**	Опрос.
7	*Применение средств аппаратной защиты*	**6**	**2**					**6**	Опрос.
8	*Лабораторная работа № 1*	**6**				**6**		**8**	Отчёт по лабораторной работе
9	*Лабораторная работа № 2*	**6**				**6**		**8**	Отчёт по лабораторной работе
10	*курсовая работа*	**6**					**2**	**70**	*оценка курсовой работы*
	зачёт	**6**							*Зачёт по билетам*
	итого:	**152**	**16**			**12**	**2**	**122**	

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

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

1. Дополнить раздел **Основная литература**

Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П. Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2020. — 327 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1035570 (дата обращения: 11.09.2020). – Режим доступа: по подписке..

2. 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 (дата обращения: 11.09.2020).

9. 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.

10. 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 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