МИНОБРНАУКИ РОССИИ

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

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

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профили) подготовки:
Организация и технология защиты информации
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

Защита от несанкционированного доступа к информации в автоматизированных системах
Рабочая программа дисциплины
Составитель:
Кандидат военных наук, доцент. кафедры КЗИ Д.Н. Баранников

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

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№_10_ от__20.05.2021 г._____

ОГЛАВЛЕНИЕ

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:
– формирование знаний в области основных аспектов по защите информации от НСД, в том числе технических средств защиты информации;
– уяснение основных методов, законов и нормативных актов в области защиты информации от несанкционированного доступа и формирование навыков работы с современными средствами защиты информации от НСД;
– рассмотрение современных тенденций развития.

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-15 *Способен 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*	*ПК-15.1* *Знает технологический процесс защиты информации и процедуру разработки технических заданий, планов и графиков проведения работ по защите информации в соответствии с действующим нормативными и методическими документами*	*Знать:* • *технологический процесс защиты информации;* • *процедуру разработки технических заданий, планов и графиков проведения работ по защите информации в соответствии с действующим нормативными и методическими документами;*
	ПК-15.2 *Умеет применять национальные, межгосударственные и международные стандарты в области защиты информации, применять действующую законодательную базу в области обеспечения защиты информации, читать и понимать нормативные и методические документы по информационной безопасности на английском языке*	*Уметь:* • *применять национальные, межгосударственные и международные стандарты в области защиты информации;* • *применять действующую законодательную базу в области обеспечения защиты информации;* • *читать и понимать нормативные и методические документы по информационной безопасности на английском языке*
	ПК-15.3 *Владеет навыками по контролю над соблюдением установленного порядка выполнения работ, а также действующего законода-*	*Владеть:* • *навыками по контролю над соблюдением установленного порядка выполнения работ, а также действующего законода-*

	тельства Российской Федерации при решении вопросов, касающихся защиты информации	*тельства РФ*

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации от несанкционированного доступа» относится к дисциплинам по выбору части, формируемой участниками образовательных отношений, блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Защита и обработка конфиденциальных документов», «Физические основы защиты информации», «Программно-аппаратные средства защиты информации», «Математические основы защиты информации».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Безопасность операционных систем и программного обеспечения», «Комплексное обеспечение безопасности объекта информатизации», эксплуатационная практика.

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоёмкость дисциплины составляет _2_ з.е., _76__ ч., в том числе контактная работа обучающихся с преподавателем _40_ ч., промежуточная аттестация __ ч., самостоятельная работа обучающихся _36_ ч.

№ п/п	Темы дисциплины/	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	*Введение в защиту информации от несанкционированного доступа*	**5**	**2**					**4**	Опрос, выполнение лабораторного задания
2	*Требования к защите информации от несанкционированного доступа*	**5**	**2**					**4**	Опрос, выполнение лабораторного задания
3	*Авторизация. Методы идентификации и аутентификации пользователя*	**5**	**2**					**4**	Опрос, выполнение лабораторного задания
4	*Управление доступом к ресурсам*	**5**	**2**					**4**	Опрос, выполнение лабораторного задания
5	*Разработка политики безопасности информационной системы*	**5**	**2**					**4**	Опрос, выполнение лабораторного задания
6	*Методика анализа защищённости ИС. Методы и средства выявления угроз её информационной безопасности*	**5**	**2**					**4**	Опрос, выполнение лабораторного задания
7	*Применение средств аппаратной защиты*	**5**	**4**					**4**	Опрос, выполнение лабораторного задания
8	*Лабораторная работа № 1*	**5**				**12**		**4**	Опрос, выполнение лабораторного задания
9	*Лабораторная работа № 2*					**12**		**4**	
	зачет	**5**							*зачет по билетам*

	итого:		**16**			**24**		**36**	

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* *Подготовка к занятиям с использованием ЭБС*
2	*Требования к защите информации от несанкционированного доступа*	*Лекция 2.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
3	*Авторизация. Методы идентификации и аутентификации пользователя*	*Лекция 3.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
4	*Управление доступом к ресурсам*	*Лекция 4.* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
5	*Разработка политики безопасности информационной системы*	*Лекция 5* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
6	*Методика анализа защищённости ИС. Методы и средства*	*Лекция 6*	*Традиционная лекция с использованием презентаций*

	выявления угроз её информационной безопасности	*Самостоятельная работа*	*Подготовка к занятиям с использованием ЭБС*
7	*Применение средств аппаратной защиты*	*Лекция 7* *Самостоятельная работа*	*Традиционная лекция с использованием презентаций* *Подготовка к занятиям с использованием ЭБС*
8	*Лабораторная работа 1*	*Лабораторное занятие 1* *Самостоятельная работа*	*Отчет о лабораторной работе* *Подготовка к занятиям с использованием ЭБС*
9	*Лабораторная работа 2*	*Лабораторное занятие 2* *Самостоятельная работа*	*Отчет о лабораторной работе* *Подготовка к занятиям с использованием ЭБС*

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *– опрос (темы 1-3)* *– опрос (темы 4-7)* *– Лабораторные работы 1-2*	 *6 балла* *5 балла* *12 баллов*	 *18 баллов* *20 баллов* *24 баллов*
Промежуточная аттестация *зачет*		*38 баллов*
Итого за дисциплину *зачет*		*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-15.1; ПК-15.2; ПК-15.3	Опрос
2.	Лабораторные занятия 1 – 2	ПК-15.1; ПК-15.2; ПК-15.3	План лабораторного 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».
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
		Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

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-15.1; ПК-15.2; ПК-15.3
2.	Первая группа требований (необходимые требования) к системе защиты	ПК-15.1; ПК-15.2; ПК-15.3
3.	Вторая группа требований (дополнительные требования) к системе защиты	ПК-15.1; ПК-15.2; ПК-15.3
4.	Виды угроз автоматизированным системам	ПК-15.1; ПК-15.2; ПК-15.3
5.	Классы защищённости АС и СВТ от НСД	ПК-15.1; ПК-15.2; ПК-15.3
6.	Состав первой группы защиты АС	ПК-15.1; ПК-15.2; ПК-15.3
7.	Подсистемы механизма ЗИ от НСД.	ПК-15.1; ПК-15.2; ПК-15.3
8.	Требования к защите информации АС групп 1Г и 1В..	ПК-15.1; ПК-15.2; ПК-15.3
9.	Понятие идентификации и аутентификации.	ПК-15.1; ПК-15.2; ПК-15.3

10.	Процедура авторизации.	ПК-15.1; ПК-15.2; ПК-15.3
11.	Классификация задач, решаемых механизмами идентификации и аутентификации.	ПК-15.1; ПК-15.2; ПК-15.3
12.	Механизмы парольной защиты.	ПК-15.1; ПК-15.2; ПК-15.3
13.	Угрозы преодоления парольной защиты. Явные и скрытые угрозы.	ПК-15.1; ПК-15.2; ПК-15.3
14.	Основные механизмы ввода пароля. Биометрический и комбинированный способ ввода пароля.	ПК-15.1; ПК-15.2; ПК-15.3
15.	Способы усиления парольной защиты. Добавочные механизмы усиления парольной защиты и требования к ним.	ПК-15.1; ПК-15.2; ПК-15.3
16.	Основные способы разделения доступа субъектов к совместно используемым объектам.	ПК-15.1; ПК-15.2; ПК-15.3
17.	Дискреционная (матричная) модель разделения доступа.	ПК-15.1; ПК-15.2; ПК-15.3
18.	Многоуровневые (мандатные) модели разделения доступа.	ПК-15.1; ПК-15.2; ПК-15.3
19.	Список прав доступа ACL.	ПК-15.1; ПК-15.2; ПК-15.3
20.	Ролевая модель разграничения доступа.	ПК-15.1; ПК-15.2; ПК-15.3
21.	Управления доступом на основе атрибутов. Выбор модели разграничения доступа.	ПК-15.1; ПК-15.2; ПК-15.3
22.	Классификация субъектов и объектов доступа.	ПК-15.1; ПК-15.2; ПК-15.3
23.	Централизованное и децентрализованное управление доступом.	ПК-15.1; ПК-15.2; ПК-15.3
24.	Протоколы аутентификации (AAA). RADIUS, TACACS.	ПК-15.1; ПК-15.2; ПК-15.3
25.	Нормативные документы по разработке политики безопасности.	ПК-15.1; ПК-15.2; ПК-15.3
26.	Средства защиты информации для государственных и коммерческих структур.	ПК-15.1; ПК-15.2; ПК-15.3
27.	Примерный состав группы по разработке политик безопасности.	ПК-15.1; ПК-15.2; ПК-15.3
28.	Архитектура корпоративной системы защиты информации.	ПК-15.1; ПК-15.2; ПК-15.3
29.	Анализ защищённости внешнего периметра корпоративной сети.	ПК-15.1; ПК-15.2; ПК-15.3
30.	Анализ защищённости внутренней инфраструктуры сети.	ПК-15.1; ПК-15.2; ПК-15.3
31.	Методы предотвращения сетевых атак на периметр сети.	ПК-15.1; ПК-15.2; ПК-15.3
32.	Угрозы перевода системы защиты в пассивное состояние, их реализация.	ПК-15.1; ПК-15.2; ПК-15.3
33.	Метод контроля вскрытия аппаратуры, общий подход.	ПК-15.1; ПК-15.2; ПК-15.3
34.	Принципы комплексирования средств защиты информации	ПК-15.1; ПК-15.2; ПК-15.3

Промежуточная аттестация (примерные вопросы к зачету)

№	Вопрос	Реализуемая компетенция
1.	Документы Гостехкомиссии (ФСТЭК) России по защите от НСД. Система государственных нормативных актов по ЗИ от НСД.	ПК-15.1; ПК-15.2; ПК-15.3
2.	Виды угроз современным АС.	ПК-15.1; ПК-15.2; ПК-15.3
3.	Классы защищённости СВТ и АС. Показатели защищённости межсетевых экранов и их увязка с классами защищённости АС.	ПК-15.1; ПК-15.2; ПК-15.3
4.	Подсистемы механизма ЗИ от НСД. Требования к защите информации АС групп 1Г и 1В.	ПК-15.1; ПК-15.2; ПК-15.3
5.	Понятие идентификации и аутентификации. Процедура авторизации.	ПК-15.1; ПК-15.2; ПК-15.3
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.	ПК-15.1; ПК-15.2; ПК-15.3
7.	Механизмы парольной защиты. Функциональное назначение и реализация механизмов парольной защиты.	ПК-15.1; ПК-15.2; ПК-15.3
8.	Угрозы преодоления парольной защиты.	ПК-15.1; ПК-15.2; ПК-15.3
9.	Основные механизмы ввода пароля.	ПК-15.1; ПК-15.2; ПК-15.3
10.	Двухуровневая авторизация на уровне ОС и BIOS. Сетевая авторизация.	ПК-15.1; ПК-15.2; ПК-15.3
11.	Протоколы аутентификации.	ПК-15.1; ПК-15.2; ПК-15.3
12.	Абстрактные модели доступа. Понятия «владелец» и «собственник» информации.	ПК-15.1; ПК-15.2; ПК-15.3
13.	Дискреционное разграничение доступа.	ПК-15.1; ПК-15.2; ПК-15.3
14.	Мандатное разграничение доступа.	ПК-15.1; ПК-15.2; ПК-15.3
15.	Ролевая модель разграничения доступа.	ПК-15.1; ПК-15.2; ПК-15.3
16.	Управления доступом на основе атрибутов. Выбор модели разграничения доступа.	ПК-15.1; ПК-15.2; ПК-15.3
17.	Корректность и полнота реализации разграничительной политики доступа. Классификация субъектов и объектов доступа. Требования к механизмам управления доступом.	ПК-15.1; ПК-15.2; ПК-15.3
18.	Централизованное и децентрализованное управление доступом.	ПК-15.1; ПК-15.2; ПК-15.3
19.	Общие положения разработки политики безопасности. Нормативные документы по разработке политики безопасности.	ПК-15.1; ПК-15.2; ПК-15.3
20.	Процесс разработки политики безопасности. Требования к политикам безопасности.	ПК-15.1; ПК-15.2; ПК-15.3
21.	Реализация политик безопасности. Архитектура корпоративной системы защиты информации. Настройки основных компонент системы защиты компании.	ПК-15.1; ПК-15.2; ПК-15.3

22.	Типовая методика анализа защищённости ИС	ПК-15.1; ПК-15.2; ПК-15.3
23.	Методы количественной оценки систем информационной безопасности.	ПК-15.1; ПК-15.2; ПК-15.3
24.	Анализ защищённости внешнего периметра и внутренней инфраструктуры корпоративной сети.	ПК-15.1; ПК-15.2; ПК-15.3
25.	Инструментальные средства анализа защищённости. Методы предотвращения сетевых атак на периметр сети.	ПК-15.1; ПК-15.2; ПК-15.3
26.	Угрозы перевода системы защиты в пассивное состояние, их реализация. Методы противодействия угрозам перевода системы защиты в пассивное состояние.	ПК-15.1; ПК-15.2; ПК-15.3
27.	Реализация программно-аппаратного контроля (мониторинга) активности системы защиты.	ПК-15.1; ПК-15.2; ПК-15.3
28.	Метод контроля целостности и активности программных компонент системы защиты программно-аппаратными средствами.	ПК-15.1; ПК-15.2; ПК-15.3
29.	Механизм удалённого мониторинга активности системы защиты, как альтернатива применению аппаратной компоненты защиты.	ПК-15.1; ПК-15.2; ПК-15.3
30.	Метод контроля вскрытия аппаратуры, общий подход. Реализация системы контроля вскрытия аппаратуры.	ПК-15.1; ПК-15.2; ПК-15.3
31.	Принципы комплексирования средств защиты информации	ПК-15.1; ПК-15.2; ПК-15.3

Промежуточная аттестация –
проверка сформированности компетенций – ПК-15

1.	Исследование компьютерной системы на предмет наличия уязвимых мест и разработка рекомендаций по их устранению.	ПК-15.1; ПК-15.2; ПК-15.3
2.	Исследование угрозы безопасности информации в информационно-вычислительных системах.	ПК-15.1; ПК-15.2; ПК-15.3
3.	Исследование защита от несанкционированного доступа. Средства и методы ограничения доступа к файлам.	ПК-15.1; ПК-15.2; ПК-15.3
4.	Определение механизмов обеспечения безопасности информации	ПК-15.1; ПК-15.2; ПК-15.3

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Литература

Основная

1. *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

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: 11.05.2021)

3. *Руководящий документ*. 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.
4. *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.
5. *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.
6. *Федеральный закон* «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (ред. от 19.07.2018). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.
7. Платонов В.В. Программно-аппаратные средства защиты информации (2-е изд., стер.), М. Академия, 2014, https://academia-library.ru/catalogue/4831/105545/
8. Душкин А.В.,Барсуков О.М.,Кравцов Е.В.,Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2016.- 248 с. https://znanium.com/bookread2.php?book=973806
9. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2016. – 184 с. https://znanium.com/bookread2.php?book=536932
10. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2016. – 172 с. https://znanium.com/bookread2.php?book=536932

Дополнительная

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных».
3. Федеральный закон от 27 декабря 2002 г. No 184-ФЗ «О техническомрегулировании».
4. Федеральный закон от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности».
5 .Федеральный закон от 30 декабря 2001 г. N 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
6 .Указ Президента Российской Федерации от 16 августа 2004 г. N 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
7. Указ Президента Российской Федерации от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера».
8. Указ Президента Российской Федерации от 17 марта 2008 г. N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. N 608.
10. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. N 21.
11. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
12. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. No 83.
13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от12 июля 2012 г. N 84.
14. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. No 282.
15. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. N 17.
16. Требования о защите информации, содержащейся в информационных системахобщего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. No 416/489.
17. Руководящий документ. Геоинформационные системы. Защита информации отнесанкционированного доступа. Требования по защите информации. Утвержден ФСТЭКРоссии, 2008.
18. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
19. Сети нового поколения – NGN: Учебное пособие для вузов / В.И. Битнер, Ц.Ц. Михайлова. – Москва : Гор. линия-Телеком, 2011. – 226 с.: ил.; 60x88 1/16. – (Специальность). (обложка) ISBN 978-5-9912-0149-0, 500 экз. – Текст : электронный. - URL: https://new.znanium.com/catalog/product/308917 (дата обращения: 19.05.2021)
20. Бирюков, А. А. Информационная безопасность: защита и нападение / А.А. Бирюков. – 2-е изд., перераб. и доп. – Москва : ДМК Пресс, 2017. – 434 с. - ISBN 978-5-97060-435-9. – Текст : электронный. – URL: https://new.znanium.com/catalog/product/1028060 (дата обращения: 19.05.2021)

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

1.Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2.Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3.Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4.Справочно-правовая система «Консультант Плюс» www.consultant.ru
5.Справочно-правовая система «Гарант» » www.garant.ru
6.Федеральный портал «Российское образование www.edu.ru
7.Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8.Российский биометрический портал www.biometrics.ru

9.Федеральный портал «Информационно- коммуникационные технологии вобразовании» htpp\\:www.ict.edu.ru
10.Сайт Научной электронной библиотеки www.elibrary.ru

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
4	Cisco Packet Tracer v.7.2	Cisco Systems	свободное
5	Apache 2.0	Apache Software Foundation	свободное
6	Nginx	NGINX, Inc	свободное
7	WireShark	Wireshark Foundation	свободное

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

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

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.
  – акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
  – передвижными, регулируемыми эргономическими партами СИ-1;
  – компьютерной техникой со специальным программным обеспечением.

7. Методические материалы

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 (12 ч.) Определение уязвимостей сети – проверка сформированности компетенций – 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 (12 ч.) Разграничение доступа – проверка сформированности компетенций – 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 электронной виде с использованием ПКП MS Office 2007 и выше и передаётся преподавателю посредством оговорённого способа связи.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Защита информации от несанкционированного 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 (профили подготовки – Организация и технология защиты информации) кафедрой комплексной защиты информации.

Цель дисциплины: теоретическое изучение и практическое освоение принципов защиты информации от несанкционированного доступа в автоматизированных системах.

Задачи:
- формирование знаний в области выбора, анализа и применения защиты информации от несанкционированного доступа;
- уяснение основных понятий и определений в области защиты информации от несанкционированного доступа в автоматизированных системах;
- рассмотрение современных тенденций развития сетей связи.

Дисциплина направлена на формирование следующих компетенций:
- ПК-15 - способен 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
  - ПК-15.1 - Знает технологический процесс защиты информации и процедуру разработки технических заданий, планов и графиков проведения работ по защите информации в соответствии с действующим нормативными и методическими документами
  - ПК-15.2 - Умеет применять национальные, межгосударственные и международные стандарты в области защиты информации, применять действующую законодательную базу в области обеспечения за-щиты информации, читать и понимать нормативные и методические документы по информационной безопасности на английском языке.
  - ПК-15.3 - Владеет навыками по контролю над соблюдением установленного порядка выполнения работ, а также действующего законодательства Российской Федерации при решении вопросов, касающихся защиты информации.

В результате освоения дисциплины обучающийся должен:
Знать: технологический процесс защиты информации и процедуру разработки технических заданий, планов и графиков проведения работ по защите информации в соответствии с действующим нормативными и методическими документами.
Уметь: применять национальные, межгосударственные и международные стандарты в области защиты информации, применять действующую законодательную базу в области обеспечения защиты информации, читать и понимать нормативные и методические документы по информационной безопасности на английском языке.
Владеть: навыками по контролю над соблюдением установленного порядка выполнения работ, а также действующего законодательства Российской Федерации при решении вопросов, касающихся защиты информации.

По дисциплине предусмотрена промежуточная аттестация в форме зачета.

Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы.

Приложение 2

УТВЕРЖДЕНО
Протокол заседания кафедры
№_____ от_____

ЛИСТ ИЗМЕНЕНИЙ

в рабочей программе дисциплины Защита информации от несанкционированного доступа

по направлению подготовки 10.03.01 Информационная безопасность

на 20__/20__ учебный год

1. В _____ вносятся следующие изменения:
(элемент рабочей программы)
1.1. ……..;
1.2. ……...;
…
1.9. …… .

2. В _____ вносятся следующие изменения:
(элемент рабочей программы)
2.1. ……..;
2.2. ……...;
…
2.9. …… .

3. В _____ вносятся следующие изменения:
(элемент рабочей программы)
3.1. ……..;
3.2. ……...;
…
3.9. …… .

Составитель подпись расшифровка подписи
дата