МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет
«Московский институт электронной техники»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ И.Г.Игнатова
«23» марта 2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
«Защита информации от несанкционированного доступа»

Направление подготовки – 10.03.01 «Информационная безопасность»
Направленность (профиль) – «Техническая защита информации»

2021 г.

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций**:**

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9. ЗИНСД. Способен применять технологии защиты информации от несанкционированного доступа для решения задач профессиональной деятельности	**Знания:** классификация и общая характеристика уязвимостей и угроз несанкционированного доступа к информации в автоматизированной системе (АС); модели нарушителя; технологии аутентификации и идентификация; модели управления доступом: дискреционные (матричные) модели управления доступом, мандатные модели управления доступом, тематические модели управления доступом, ролевые модели управления доступом; технологии обеспечения целостности и доступность данных; угрозы безопасности вычислительных сетей, виды сетевых атак; технологии защиты вычислительных сетей от несанкционированного доступа к информации; скрытые каналы утечки информации; методы моделирования систем защиты; методы оценки эффективности защиты информации. **Умения:** применять современные технологии аутентификации и идентификация для обеспечения безопасности АС и вычислительных сетей; применять современные технологии управления доступом для

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		обеспечения безопасности АС и вычислительных сетей; применять современные технологии обеспечения целостности и доступность данных для обеспечения безопасности АС и вычислительных сетей. **Опыт практической деятельности:** применения современные технологии защиты информации от несанкционированного доступа для обеспечения безопасности АС и вычислительных сетей.

В результате изучения дисциплины студент должен:

Знать:

- классификацию и общую характеристику уязвимостей и угроз несанкционированного доступа к информации в автоматизированной системе (АС);
- модели нарушителя;
- технологии аутентификации и идентификация;
- модели управления доступом: дискреционные (матричные) модели управления доступом, мандатные модели управления доступом, тематические модели управления доступом, ролевые модели управления доступом;
- технологии обеспечения целостности и доступность данных;
- угрозы безопасности вычислительных сетей, виды сетевых атак;
- технологии защиты вычислительных сетей от несанкционированного доступа к информации;
- скрытые каналы утечки информации;
- методы моделирования систем защиты;
- методы оценки эффективности защиты информации.

Уметь:

- применять современные технологии аутентификации и идентификация для обеспечения безопасности АС и вычислительных сетей;
- применять современные технологии управления доступом для обеспечения безопасности АС и вычислительных сетей;
- применять современные технологии обеспечения целостности и доступность данных для обеспечения безопасности АС и вычислительных сетей.

Иметь опыт практической деятельности:

- применения современные технологии защиты информации от несанкционированного доступа для обеспечения безопасности АС и вычислительных сетей.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Защита информации от несанкционированного доступа» входит в обязательную часть Блока 1 «Дисциплины (модули)» образовательной программы и читается на 3-м курсе в 6-м семестре.

Изучение дисциплины базируется на дисциплинах образовательной подготовки (ОП) бакалавриата по направлению подготовки 10.03.01 «Информационная безопасность» и профилю подготовки «Техническая защита информации»: «Информатика», «Программирование на языке высокого уровня», «Технологии и методы программирования», «Объектно-ориентированное программирование», «Аппаратные средства вычислительной техники», «Информационные технологии 1. Операционные системы», «Информационные технологии 2. Базы данных», «Информационные технологии 3. Вычислительные сети», «Теория вероятностей и математическая статистика», «Дискретная математика», «Основы информационной безопасности».

Знания и практические навыки, полученные в результате изучения дисциплины используются в дисциплинах: «Программно-аппаратные средства защиты информации», «Безопасность телекоммуникационных систем», «Основы управления информационной безопасностью», в учебной и производственной практиках и при подготовке ВКР.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Курс	Семестр	Общая трудоёмкость (ЗЕ)	Общая трудоёмкость (часы)	Контактная работа, часы					Самостоятельная работа, часы	Вид промежуточной аттестации
				ВСЕГО	Лекции	Практическая подготовка при проведении лабораторных работ	Практические занятия	Групповые консультации		
3	6	5	180	80	32	16	16	16	64	Экз. (36)

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Номер и наименование модуля	Контактная работа, часы				Самостоятельная работа, часы	Формы текущего контроля
	Лекции	Лабораторные работы	Практические занятия	Групповые консультации		
1. Теоретические основы безопасности операционных систем и баз данных.	22	8	16	12	48	Отчет по ПЗ (ГУ) № 2. Отчет по Лр № 1-3 . Компьютерный тест КТ-1.
2. Основы безопасности вычислительных сетей.	6	8	-	4	12	Отчет по Лр № 4 Компьютерный тест КТ-2.
3. Проблемные вопросы обеспечения информационной безопасности автоматизированных систем	4	-	-	-	4	Компьютерный тест КТ-3

4.1. Лекционные занятия

Номер модуля дисциплины	**Номер лекции**	**Объем занятий, часы**	**Краткое содержание**
1	1.	2	**Вводная лекция. Классификация угроз безопасности информации при ее обработке в автоматизированных системах (АС).** Классификация угроз несанкционированного доступа к информации в АС. Общая характеристика источников угроз несанкционированного доступа в АС. Общая характеристика уязвимостей АС. Угрозы программно-математических воздействий. Модели нарушителя. Модель системы защиты «с полным перекрытием». Основные функции систем защиты информации.
			Тема 1 «Основные функции и модели систем защиты от НСД»
	2.	4	**Аутентификация и идентификация**: процедура проверки подлинности субъектов и объектов, параметры парольной идентификации, особенности аутентификации в вычислительных сетях.

Номер модуля дисциплины	Номер лекции	Объем занятий, часы	Краткое содержание
	3.	2	**Модели управления доступом**: модель системы защиты с полным перекрытием, субъектно-объектная модель системы защиты, понятие изолированной системы, особенности моделирования механизмов безопасности операционных систем и баз данных, основные виды моделей политик управления доступом — ограниченность моделей и проблемы изменения прав доступа.
			Тема 2 «Основные модели управления доступом систем защиты от НСД»
	4.	4	**Дискреционные (матричные) модели управления доступом:** матрица доступа, пятимерное пространства безопасности Хартсона, модели HRU и Take-Grant, основные результаты, их достоинства и недостатки, основные направления развития.
	5.	4	**Мандатные модели управления доступом:** MLS модель «военной безопасности», модель Белла-ЛаПадулы, решетки безопасности
	6.	2	**Тематические модели управления доступом:** тематические классификаторы и решетки мультирубрик.
	7.	2	**Ролевые модели управления доступом:** использование функциональной структуры организации для управления доступом, индивидуально групповая модель управления доступом
	8.	2	**Целостность и доступность данных:** модель Биба, ЭЦП, целостность и доступность информации в СУБД.
2			**Тема 3 «Основы безопасности вычислительных сетей»**
	9.	4	**Угрозы и проблемы защиты информации в сетях:** субъекты и объекты компьютерных атак в сетях, виды сетевых атак; методы защиты вычислительных сетей: задачи аутентификации, авторизации и акаунтинга (ААА). Проблемные вопросы обеспечения безопасности информации в распределенных вычислительных средах (виртуальные вычисления в центрах обработки данных, «облачные вычисления»).
	10.	2	**Скрытые каналы утечки информации:** понятие, виды (по памяти, по времени, статистические), обнаружение и методы противодействия; утечки информации в статистических БД;
3			**Тема 3 «Проблемные вопросы обеспечения информационной безопасности автоматизированных систем»**
	11.	2	**Вероятностные методы моделирования систем защиты:** теоретико-вероятностная модель «невыводимости» и «невлияния», методы оптимизации и методы теории игр при моделировании систем защиты.
	12.	2	**Оценка эффективности защиты информации.** Измерение качества систем защиты в качественных и количественных шкалах. Классификации и упорядоченные классы требований безопасности.

4.2. Практические занятия

№ модуля дисциплины	№ практического занятия	Объем занятий (часы)	Краткое содержание
1	1.	4	**Практическое занятие (семинар). Модели управления доступом** Математический аппарат дискретной математики используемого при моделировании управления доступом: Машина Тьюринга, сложность вычислений, проблема останова.
	2.	4	**Практическое занятие (групповое упражнение). Основные свойства дискреционных моделей** Сравнение полученных результатов моделирования; решение задач по распространению прав доступа в моделях HRU и Take-Grant; решение задач по распространению прав доступа в мандатных моделях управления доступом.
	3.	4	**Практическое занятие (групповое упражнение). Технологии обеспечения безопасности операционных систем и баз данных** Технологии обеспечения безопасности операционных систем Linux.
	4.	4	**Практическое занятие (групповое упражнение). Технологии обеспечения безопасности операционных систем и баз данных** Технологии обеспечения безопасности операционных систем Windows.

4.3. Лабораторные работы

№ модуля дисциплины	№ лабораторной работы	Объем занятий (часы)	Краткое содержание
1	1.	4	**Реализации матрицы доступа и проверка введенных ограничений по доступу в среде операционной системы Windows** Реализации матрицы доступа и проверка введенных ограничений по доступу в среде операционной системы Windows: Создание с использованием командной строки и системы меню объектов (файлы, каталоги). Создание с использованием командной строки и системы меню субъектов (пользователи, группы). Введение ограничений с использованием командной строки и системы меню по доступу субъектов к объектам.
	2.	4	**Реализации матрицы доступа и проверка введенных ограничений по доступу в среде операционной системы Linux** Реализации матрицы доступа и проверка введенных ограничений по

№ модуля дисциплины	№ лабораторной работы	Объем занятий (часы)	Краткое содержание
			доступу в среде операционной системы Linux: Создание с использованием командной строки и системы меню объектов (файлы, каталоги). Создание с использованием командной строки и системы меню субъектов (пользователи, группы). Введение ограничений с использованием командной строки и системы меню по доступу субъектов к объектам.
	3.	4	**Исследование возможностей расширения технологий защиты от несанкционированного доступа к информации с использованием мандатной и ролевой моделей доступа в SELinux.** Исследование технологий разграничения доступа к данным, реализуемых SELinux. Использование технологий управления потоками информации, реализуемых программными средствами защиты информации для повышения класса систем защиты.
2	4.	4	**Исследование сетевых атак** Разведка как первый этап организации сетевой атаки. Использование программных средств и утилит командной строки для сбора информации о компьютерной сети.

4.4. Самостоятельная работа студентов

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
1	6	Подготовка к практическому занятию (семинару) № 1: Изучение материалов лекции № 1 и рекомендованной литературы. Изучение плана проведения семинара № 1. Подготовка доклада и презентации по одному из вопросов семинара
	6	Подготовка к практическому занятию (групповому упражнению) № 2: Изучение материалов лекции № 2 - 8 и рекомендованной литературы. Изучение методических рекомендаций по проведению группового упражнения № 1.
	6	Подготовка к практическому занятию (групповому упражнению) № 3. Изучение материалов лекции № 2 - 8 и рекомендованной литературы. Изучение методических рекомендаций по проведению группового упражнения № 2.

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
	6	Подготовка к практическому занятию (групповому упражнению) №43. Изучение материалов лекции № 2 - 8 и рекомендованной литературы. Изучение методических рекомендаций по проведению группового упражнения № 3.
	6	Подготовка к лабораторной работе № 1: Изучение материалов лекции № 2 - 7 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 1
	6	Подготовка к лабораторной работе № 2: Изучение материалов лекции №№ 2 - 8 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 2
	6	Подготовка к лабораторной работе № 3: Изучение материалов лекции №№ 2 - 8 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 3
	6	Подготовка к рубежному контролю КТ 1: Изучение материалов лекции №№ 1 – 8 и рекомендованной литературы.
2	6	Подготовка к лабораторной работе № 4: Изучение материалов лекции № 9 - 10 и рекомендованной литературы. Изучение методических рекомендаций по проведению лабораторной работы № 4
	6	Подготовка к рубежному контролю КТ 2: Изучение материалов лекции №№ 9 - 10 и рекомендованной литературы.
3	4	Подготовка к рубежному контролю КТ 3: Изучение материалов лекции №№ 11 - 12 и рекомендованной литературы.

4.5. Примерная тематика курсовых работ (проектов)

Не предусмотрены

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Учебно-методическое обеспечение для самостоятельной работы студентов в составе УМК дисциплины (ОРИОКС, http://orioks.miet.ru/):

Модуль 1. Теоретические основы безопасности операционных систем и баз данных:

Тексты лекций № 1 – 8. ОРИОКС// URL: http://orioks.miet.ru/

Планы проведения семинарских занятий № 1 - 3. ОРИОКС// URL: http://orioks.miet.ru/

Руководство по выполнению группового упражнения № 1. ОРИОКС// URL: http://orioks.miet.ru/

Руководства по проведению лабораторных работ № 1 – 3. ОРИОКС// URL: http://orioks.miet.ru/

Модуль 2. Основы безопасности вычислительных сетей:

Тексты лекций № 9-10. ОРИОКС// URL: http://orioks.miet.ru/

Руководство по проведению лабораторной работы № 4. ОРИОКС// URL: http://orioks.miet.ru/

Модуль 3. Проблемные вопросы обеспечения информационной безопасности автоматизированных систем:

Тексты лекций № 11 – 12. ОРИОКС// URL: http://orioks.miet.ru/

1. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : Учеб. пособие / П.Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с. - URL: https://e.lanbook.com/book/5150 (дата обращения: 10.03.2021). - ISBN 978-5-9912-0147-6.
2. Мельников, Д. А. Информационная безопасность открытых систем : учебник / Д. А. Мельников. - Москва: Флинта: Наука, 2014. - 448 с. - URL: https://e.lanbook.com/book/48368 (дата обращения: 16.03.2021). - ISBN 978-5-9765-1613-7; ISBN 978-5-02-037923-7.
3. Программно-аппаратные средства защиты информации : учебное пособие / В. А. Воеводин, А. В. Душкин, А. Н. Петухов, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 280 с. - ISBN 978-5-7256-0972-1.
4. Управление безопасностью критических информационных инфраструктур : учебное пособие / А. Н. Петухов, П. Л. Пилюгин, А. В. Душкин, Ю. А. Губсков; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.В. Душкина. - Москва : МИЭТ, 2021. - 208 с. - ISBN 978-5-7256-0973-8.
5. Хорев П.Б. Программно-аппаратная защита информации : Учеб. пособие / П.Б. Хорев. - М. : Форум, 2013. - 352 с. - (Высшее образование). - ISBN 978-5-91134-353-8 .

Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы

1. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения Protection of information. Object of informatisation. Factors influencing the information. General: Национальный стандарт РФ: Введ. 01.02.2008.- М.: Стандартинформ, (Переиздание) 2018. -URL: https://docs.cntd.ru/document/1200057516 (дата обращения: 16.03.2021)
2. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования; Computers technique. Information protection against unauthorised access to information. General technical requirements:

Национальный стандарт РФ: Введ. 01.01.1996: М.: Издательство стандартов, 1995 Стандартинформ, 2006.- URL: https://docs.cntd.ru/document/9039120 (дата обращения 16.03.2021).

3. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения; Protection of information. Basic terms and definitions: Национальный стандарт РФ: Введ. 01.02.2008: М.: Стандартинформ, 2008. URL: https://docs.cntd.ru/document/1200058320 (дата обращения 16.03.2021)

4. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения: Национальный стандарт РФ: Введ. 01.10.2009: М.: Стандартинформ, 2008.- 20 л. -URL: https://docs.cntd.ru/document/1200075565 (дата обращения: 16.03.2021)

5. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель; Information technology. Security techniques. Evaluation criteria for IT security. Part 1. Introduction and general model Национальный стандарт РФ: Введ. 01.12.2013: М.: Стандартинформ, 2014. –URL: https://docs.cntd.ru/document/1200101777 (дата обращения: 15.03.2021)

6. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности; Information technology. Security techniques. Evaluation criteria for IT security. Part 2. Security functional components: Национальный стандарт РФ: Введ. 01.09.2014: М.: Стандартинформ, 2014.–URL: https://docs.cntd.ru/document/1200105710 (дата обращения: 16.03.2021)

7. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности; Information technology. Security techniques. Evaluation criteria for IT security. Part 3. Security assurance requirements: Национальный стандарт РФ: Введ. 01.09.2014: М.: Стандартинформ, 2014.- URL: https://docs.cntd.ru/document/1200105711 (дата обращения: 15.03.2021) -Текст: электронный.

8. Федеральный закон от 27 июля 2006 г. N 149-ФЗ: с изм. на 02 июля 2021 г.- «Об информации, информационных технологиях и о защите информации»; Текст: электронный // Техэксперт : – URL: https://docs.cntd.ru/document/901990051 - (дата обращения 15.03.2021)

Периодические издания

1. ЗАЩИТА ИНФОРМАЦИИ. INSIDE : информационно-методический журнал / Издательский дом "Афина". - Санкт-Петербург : ИД Афина, 2004 - . - URL: http://elibrary.ru/contents.asp?titleid=25917 (дата обращения: 15.03.2021). - Режим доступа: по подписке (2017-2021). - ISSN 2413-3582.

2. Безопасность информационных технологий : научный журнал / ФГАОУ ВО "Национальный исследовательский ядерный университет "МИФИ". - Москва : НИЯУ МИФИ, 1994 - . - URL: https://bit.mephi.ru/index.php/bit/index (дата обращения: 10.03.2021). - Режим доступа: свободный. - ISSN 2074-7128 (Print); 2074-7136 (Online).

3. Информация и безопасность: научный журнал / ФГБОУ ВО "Воронежский государственный технический университет" (ВГТУ). - Воронеж : ВГТУ, 1998 - . - URL:

https://www.elibrary.ru/title_about_new.asp?id=8748 (дата обращения:16.03.2021). - Режим доступа: для зарегистрированных пользователей. - ISSN 1682-7813.

7. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: https://www.elibrary.ru (дата обращения: 16.03.2021).
2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург,2010 -. - URL: https://e.lanbook.com (дата обращения: 10.03.2021).
3. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. - . - URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 10.03.2021).
4. ФСТЭК России: Банк данных угроз безопасности информации. – Москва, 2014. - . - URL: https://bdu.fstec.ru/ (дата обращения: 10.03.2021).

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе реализации обучения используется смешанное обучение, которое основано на интеграции технологий традиционного и электронного обучения, замещении части традиционных учебных форм занятий формами и видами взаимодействия в электронной образовательной среде.

Освоение образовательной программы обеспечивается ресурсами электронной информационно-образовательной среды ОРИОКС http://orioks.miet.ru.

Для взаимодействия студентов с преподавателем используются сервисы обратной связи: ОРИОКС «Домашние задания», электронная почта преподавателя.

В процессе обучения при проведении занятий и для самостоятельной работы используются внутренние электронные ресурсы (http://orioks.miet.ru).

Тестирование проводится в ОРИОКС (MOODLe) и с использованием сервиса https://www.academtest.ru/.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Наименование учебных аудиторий и помещений для самостоятельной работы	**Оснащенность учебных аудиторий и помещений для самостоятельной работы**	**Перечень программного обеспечения**
Учебная аудитория	Мультимедийное оборудование: компьютер с программным обеспечением, возможностью подключения к сети Интернет и обеспечением доступа в электронно-образовательную среду МИЭТ; телевизор/проектор; акустическое оборудование	Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Fire-fox/Google Chrome /Explorer).

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	(микрофон, звуковые колонки), вебкамера с микрофоном). Учебная доска.	
Учебная аудитория № 3226: Лаборатория «Технологий и управления информационной безопасностью»	1. Автоматизированное рабочее место преподавателя (АРМ-П): ПЭВМ Flagman-G в составе: Монитор 22" Samsung S22B370H, HDMI (LED); ИБП APC BK650EI; Клавиатура Logitech K120 USB; Манипулятор Logitech B110 – 1 шт. 2. Автоматизированное рабочее место студента (АРМ-С): ПЭВМ Flagman-G в составе: корпус InWin S617 450W; Источник бесперебойного питания APC BK650EI; Клавиатура Logitech K120 USB; МанипуляторLogitech B110 – 27 шт.	1. Операционная система Microsoft Win Pro 7 2. Неисключительное право на использование Microsoft Office Std 2013 RUS OLP NL (Из реестра МИЭТ п.18) – 28 шт. 3. Лиц. на ПО Multisim 9 Academic Edituon Single seal (Из реестра МИЭТ п.78) – 28 шт. 4. Корпоративная информационно - технологическая платформа ОРИОКС (Из реестра МИЭТ п.88) – 28 шт.
Помещение для самостоятельной работы обучающихся: Учебная аудитории № 3226	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в ОРИОКС: 1. Автоматизированное рабочее место преподавателя (АРМ-П): ПЭВМ Flagman-G в составе: Монитор 22" Samsung S22B370H, HDMI (LED); ИБП APC BK650EI; Клавиатура Logitech K120 USB; Манипулятор Logitech B110	1. Неисключительное право на использование операционной системы Microsoft Win Pro 7 2. Неисключительное право на использование Microsoft Office Std 2013 RUS OLP NL 3. Лиц. на ПО Multisim 9 Academic Edituon Single seal 4. Корпоративная информационно - технологическая платформа ОРИОКС

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
	– 1 шт. 2. Автоматизированное рабочее место студента (АРМ-С): ПЭВМ Flagman-G в составе: корпус InWin S617 450W; Источник бесперебойного питания APC BK650EI; Клавиатура Logitech K120 USB; МанипуляторLogitech B110 – 27 шт.	

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции ОПК-9. ЗИНСД. Способен применять технологии защиты информации от несанкционированного доступа для решения задач профессиональной деятельности

Фонды оценочных средств представлены отдельными документами и размещены в составе УМК дисциплины электронной информационной образовательной среды ОРИОКС// URL: http://orioks.miet.ru/.

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

В целях практической подготовки в дисциплине предусмотрены лабораторные работы и практические занятия (семинары и групповые упражнения).

Каждая лабораторная работа и каждое практическое занятие направлены на формирование отдельных умений, необходимых для формирования общепрофессиональных и профессиональных компетенции.

11.1. Методические указания студентам по подготовке к семинарам

Семинар - развернутая беседа с обсуждением доклада. Проводится на основе заранее разработанного плана, по вопросам которого готовится вся учебная группа. Основными компонентами такого занятия являются: вступительное слово преподавателя, доклады обучаемых, вопросы докладчикам, выступления студентов по докладу и обсуждаемым вопросам, заключение преподавателя.

Развернутая беседа позволяет вовлечь в обсуждение проблем наибольшее число обу-

чаемых. Главная задача преподавателя при проведении такого семинарского занятия состоит в использовании всех средств активизации: постановки хорошо продуманных, четко сформулированных дополнительных вопросов, умелой концентрации внимания на наиболее важных проблемах, умения обобщать и систематизировать высказываемые в выступлениях идеи, сопоставлять различные точки зрения, создавать обстановку свободного обмена мнениями. Данная форма семинара способствует выработке у обучаемых коммуникативных навыков.

Как правило, темы докладов разрабатываются преподавателем заранее и включаются в планы семинаров. Доклад носит характер краткого (10-15 мин.) аргументированного изложения одной из центральных проблем семинарского занятия с использованием презентации.

11.2. Методические указания студентам по подготовке к лабораторным работам и групповым упражнениям

Выполнение студентами к лабораторных работ и групповых упражнений направлено на:

- обобщение, систематизацию, углубление, закрепление полученных теоретических знаний по конкретным темам дисциплины;
- формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности;
- развитие интеллектуальных умений у будущих специалистов: аналитических, проектировочных, конструктивных и др.;
- выработку при решении поставленных задач таких профессионально значимых качеств, как самостоятельность, ответственность, точность, творческая инициатива.

Ведущей дидактической целью ЛР (ГУ) является формирование практических умений выполнять определенные действия, операции, необходимые в последующем в профессиональной деятельности.

Наряду с ведущей дидактической целью в ходе выполнения заданий у студентов формируются практические умения и навыки обращения с различными приборами, установками, лабораторным оборудованием, аппаратурой, которые могут составлять часть профессиональной практической подготовки, а также исследовательские умения (наблюдать, сравнивать, анализировать, устанавливать зависимости, делать выводы и обобщения, самостоятельно вести исследование, оформлять результаты).

Лабораторные работы и групповые упражнения, как виды учебных занятий проводиться в специально оборудованных учебных лабораториях. Продолжительность - не менее двух академических часов. Необходимыми структурными элементами ЛР (ГУ), помимо самостоятельной деятельности студентов, являются инструктаж, проводимый преподавателем, а также организация обсуждения итогов выполнения лабораторной работы.

По каждой ЛР (ГУ) разработаны и утверждены методические указания по их проведению.

Лабораторные работы и групповые упражнения носят репродуктивный характер и отличаются тем, что при их проведении студенты пользуются подробными инструкциями, в которых указаны: цель работы, пояснения (теория, основные характеристики), оборудование, аппаратура, материалы и их характеристики, порядок выполнения работы, таблицы, выводы (без формулировки), контрольные вопросы, учебная и специальная литература.

Формы организации студентов на ЛР (ГУ): индивидуальная, при которой каждый студент выполняет индивидуальное задание.

Для проведения ЛР (ГУ) преподавателями разрабатываются методические рекомендации по их выполнению, которые рассматриваются и утверждаются на заседании кафедры. Методические рекомендации разрабатываются по каждой ЛР (ГУ), предусмотренными рабочей программой учебной дисциплины: в соответствии с количеством часов, требованиями к знаниям и умениям, темой практических занятий и лабораторных работ, установленными рабочей программой учебной дисциплины по соответствующим разделам (темам).

Методические рекомендации по выполнению ЛР (ГУ) включают в себя:

- пояснительную записку;
- наименование раздела (темы);
- объем учебного времени, отведенный на ЛР (ГУ);
- наименование темы ЛР (ГУ);
- цель ЛР (ГУ) (в т.ч. требования к знаниям и умениям студентов, которые должны быть реализованы);
- перечень необходимых средств обучения (оборудование, материалы и др.);
- требования по теоретической готовности студентов к выполнению ЛР (ГУ) (требования к знаниям, перечень дидактических единиц);
- содержание заданий;
- рекомендации (инструкции) по выполнению заданий;
- требования к результатам работы, в т.ч. к оформлению;
- критерии оценки и формы контроля;
- список рекомендуемой литературы;
- приложения.

При подготовке к ЛР (ГУ) студенту необходимо:

- уяснить вопросы и задания, рекомендуемые для подготовки к ЛР (ГУ);
- ознакомиться с методическими рекомендации по выполнению ЛР (ГУ);
- прочитать конспект лекций и соответствующие главы учебника (учебного пособия), дополнить запись лекций выписками из него;
- прочитать дополнительную литературу, рекомендованную преподавателем. Наиболее интересные мысли следует выписать;
- сформулировать и записать развернутые ответы на вопросы для подготовки к ЛР (ГУ);
- изучить схемы лабораторных установок (стендов), порядок работы на аппаратуре и технике, правила и меры безопасности;
- подготовить отчеты для заполнения.

На ЛР (ГУ) студент должен выполнить задание в соответствии с методическими указаниями.

Отчет о ЛР (ГУ) должен быть оформлен в соответствии методическими указаниями и ГОСТами.

При защите отчета о ЛР (ГУ) убедительно четко и аргументировано изложить содержание проведенных исследований и выводы по полученным результатам.

По завершению занятия студент должен уяснить недостатки, указанные преподавателем при необходимости записать их содержание.

Студенты, по каким-либо причинам, отсутствовавшие на занятии, в свободное время должны самостоятельно изучить учебный материал и провести исследования, после чего отчитаться в проделанной работе перед преподавателем.

Студенты на ЛР (ГУ) обязаны соблюдать меры безопасности при работе на аппаратуре (оборудовании). Перед началом занятий, каждый студент должен пройти инструктаж по соблюдению мер безопасности на рабочем месте и уяснить места расположения средств пожаротушения и обесточивания аппаратуры (оборудования).

11.3. Система контроля и оценивания

Для оценки успеваемости студентов по дисциплине используется накопительно-бальная система.

Под накопительно-бальной системой понимается система количественной, балльно - рейтинговой оценки качества освоения учебной дисциплины студентом $R_{нак}$ по суммарному результату текущего $R_{тек}$ и итогового контроля $R_{итог}$, с учетом посещаемости студентом занятий, его активности на занятиях и качества выполнения им текущих заданий $R_{пр}$.

Выполнение контрольных мероприятий текущего контроля (сдача компьютерных тестов, защита отчетов по лабораторным работам, защита отчетов по выполнению практических заданий), посещаемость занятий и активность на занятиях, результаты итогового контроля (сдача экзамена) оцениваются баллами, общая сумма которых составляет 100 баллов (максимальное значение нормативного рейтинга учебной дисциплины – $R_{нор}$).

Примерные структура и график контрольных мероприятий приведены в таблице 11.1.

Таблица11.1

Структура и график контрольных мероприятий

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
2	Практическое занятие (семинар) № 1	4	2
6	Практическое занятие (групповое упражнение) № 2	4	2
7	Практическое занятие (семинар) № 3	4	2
8	Практическое занятие (семинар) № 4	4	2
9	Лабораторная работа № 1	8	4
10	Лабораторная работа № 2	8	4
11	Лабораторная работа № 3	8	4
11	Компьютерный тест КТ-1	6	3
14	Лабораторная работа № 4	8	4
14	Компьютерный тест КТ-2	4	2
16	Компьютерный тест КТ-3	4	2
16	Активность, посещаемость	8	4
	Итого за текущий контроль	***70***	***35***
	Итоговый контроль	***30***	***15***
	Накопленный рейтинг	**100**	**50**

В экзаменационную ведомость и зачетную книжку вносится не экзаменационная оценка по дисциплине, а ***итоговая 5-балльная оценка*** за семестр, рассчитанная на основе накопленных рейтинговых баллов по результатам семестрового и итогового контроля учебной дисциплины. Итоговая оценка студенту по дисциплине за семестр по 5-ти балльной шкале выставляется на основе накопленной им общей суммы баллов $R_{нак}$ по итогам семест-

рового и итогового контроля с учетом бонусных баллов системы ОРИОКС. При выставлении итоговой оценки используется шкала, приведенная в таблице:

Сумма баллов	**Оценка**
Менее 50	2
50 – 69	3
70 – 85	4
86 – 100	5

Положительная оценка («отлично», «хорошо», «удовлетворительно») заносится в экзаменационную ведомость и зачетную книжку студента. Оценка «неудовлетворительно» проставляется только в экзаменационную ведомость.

РАЗРАБОТЧИК

Доцент кафедры «Информационная безопасность»
кандидат технических наук _____ П.Л.Пилюгин

Рабочая программа дисциплины «Защита информации от несанкционированного доступа» по направлению подготовки 10.03.01 «Информационная безопасность», направленности (профилю) «Техническая защита информации» разработана на кафедре «Информационная безопасность» и утверждена на заседании кафедры 17 марта 2021 года, протокол № 3.

Заведующий кафедрой «Информационная безопасность»
доктор технических наук, профессор _____ А.А.Хорев

Лист согласования

Рабочая программа согласована с Центром подготовки к аккредитации и независимой оценки качества
Начальник АНОК _____/ И.М.Никулина /

Рабочая программа согласована с библиотекой МИЭТ
Директор библиотеки _____/ Т.П.Филиппова /