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
«Аудит информационной безопасности автоматизированных систем»
(деловая игра)

Направление подготовки – 10.04.01 «Информационная безопасность»
Направленность (профиль) – «Аудит информационной безопасности»

2021 г.

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций**:**

Компетенция ПК-3 «Способен проводить аудит информационной безопасности» сформулирована на основе проекта новой редакции профессионального стандарта 064.033 «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный № 43857).

Обобщенная трудовая функция D/7. Аудит информационной безопасности автоматизированной системы.

Трудовая функция D/01.7. Подготовка к проведению аудита информационной безопасности автоматизированной системы.

Трудовая функция D/02.7. Проведение аудита информационной безопасности автоматизированной системы.

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
ПК-3. Способен проводить аудит информационной безопасности	ПК-3.АИБАСДИ. Способен проводить аудит информационной безопасности -	**Знания** порядок разработки и содержание технического задания на проведение аудита информационной безопасности автоматизированной системы (АС); структуру и порядок подготовки конкурсной документации на проведение аудита информационной безопасности АС; требования к содержанию программы и методики аудита информационной безопасности АС. порядок и методики проведения аудита информационной безопасности АС; состав и требования к содержанию документов, оформляемых по результатам аудита информационной безопасности АС. **Умения:** проводить предварительное обследование объекта информатизации; разрабатывать техническое задание на проведение аудита ин-

Компетенции	Подкомпетенции, формируемые в дисциплине	Индикаторы достижения подкомпетенций
		формационной безопасности АС; разрабатывать конкурсную документацию на проведение аудита информационной безопасности АС; разрабатывать программу и методики аудита информационной безопасности АС. проводить аудит информационной безопасности АС в соответствие с разработанными методиками; состав и требования к содержанию документов, оформляемых по результатам аудита информационной безопасности АС. **Опыт практической деятельности:** проведения аудита информационной безопасности АС.

В результате изучения дисциплины студент должен:

Знать:

- порядок разработки и содержание технического задания на проведение аудита информационной безопасности автоматизированной системы (АС);
- структуру и порядок подготовки конкурсной документации на проведение аудита информационной безопасности АС;
- требование к содержанию программы и методики аудита информационной безопасности АС.
- порядок и методики проведения аудита информационной безопасности АС:
- состав и требования к содержанию документов, оформляемых по результатам аудита информационной безопасности АС.

Уметь:

- проводить предварительное обследование объекта информатизации;
- разрабатывать техническое задание на проведение аудита информационной безопасности АС;
- разрабатывать конкурсную документацию на проведение аудита информационной безопасности АС;
- разрабатывать программу и методики аудита информационной безопасности АС.
- проводить аудит информационной безопасности АС в соответствие с разработанными методиками;
- состав и требования к содержанию документов, оформляемых по результатам аудита

информационной безопасности АС.

Иметь практический опыт:

– проведения аудита информационной безопасности АС.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Аудит информационной безопасности автоматизированных систем» (деловая игра) входит в часть, формируемую участниками образовательных отношений, Блока 1 «Дисциплины (модули)» образовательной программы и изучается на 2-м курсе в 4-м семестре.

Изучение дисциплины базируется на знаниях и умениях, полученных при изучении дисциплин «Технологии защиты информации от несанкционированного доступа», «Технологии защиты информации от утечки по техническим каналам», «Правовые основы аудита информационной безопасности», «Организация аудита информационной безопасности» изучаемых 1 – 3 семестрах магистратуры.

Знания и умения, полученные в результате изучения дисциплины, используются в производственной практике 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	Лабораторные работы	Практическая подготовка при проведении практических занятий	Групповые консультации		
2	4	3	108	68	-	-	48	20	40	ЗаО

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Номер и наименование модуля	Контактная работа, часы					Самостоятельная работа, часы	Вид промежуточной аттестации
	ВСЕГО	Лекции	Лабораторные работы	Практическая подготовка при проведении практических занятий	Групповые консультации		
Аудит информационной безопасности автоматизированной информационной системы обработки конфиденциальной информации на соответствие требованиям нормативных документов ФСТЭК России	68	-	-	48	20	40	Зачет по ПЗ 1 - 6

4.1. Лекционные занятия

[Не предусмотрены]

4.2. Практические занятия
(практическая подготовка при проведении практических занятий)

Номер модуля дисциплины	**Номер практического занятия**	**Объем занятий, часы**	**Краткое содержание**
1.	1.	8	**Практическое занятие (групповое упражнение) №1.** Предварительное специальное обследование объекта информатизации. Разработка технического задания (ТЗ) на проведение аудита информационной безопасности автоматизированной системы (АС).
	2.	8	**Практическое занятие (групповое упражнение) № 2.** Разработка конкурсной документации на проведение аудита информационной безопасности АС. Организация и сопровождение закупки услуги по аудиту информационной безопасности АС.
	3.	8	**Практическое занятие (групповое упражнение) № 3.** Разработка программы и методики аудита информационной безопасности АС.

Номер модуля дисциплины	Номер практического занятия	Объем занятий, часы	Краткое содержание
	4.	8	**Практическое занятие (групповое упражнение) № 4. Проведение аудита информационной безопасности АС:** Анализ полноты исходных данных, проверка их соответствия реальным условиям размещения, монтажа и эксплуатации технических средств АС. Исследование технологического процесса обработки и хранения информации, анализ информационных потоков, определение состава использованных для обработки и передачи информации ОТСС. Проверка состояния организации работ и выполнения организационных и технических требований по защите информации. Оценка правильности категорирования и классификации (уровня защищенности). Оценка полноты разработки организационно-распорядительной, проектной и эксплуатационной документации. Оценка уровня подготовки кадров, обеспечивающих защиту информации в АС и распределения ответственности пользователей АС за выполнение требований безопасности информации. Проверка помещения, в котором производится обработка информации, на соответствие требованиям по защите информации. Проверка АС на соответствие требованиям по защите информации от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН). Проверка выполнения требований по защите информации АС от утечки за счет возможно внедренных электронных закладочных устройств в ОТСС иностранного производства. Проверку АС на соответствие требованиям по защите информации от несанкционированного доступа (НСД). Проверка АС на соответствие требованиям по защите информации от специальных программных воздействий на нее и ее носители.
	5.	8	**Практическое занятие (групповое упражнение) № 5. Проведение аудита информационной безопасности АС:** Проведение испытаний АС на соответствие требованиям по защите информации от утечки по техническим каналам. Проведение испытаний АС на соответствие требованиям по защите информации от НСД.
	6.	8	**Практическое занятие (групповое упражнение) № 6. Оформление результатов аудита информационной безопасности АС.**

4.3. Лабораторные работы
(практическая подготовка при проведении лабораторных работ)

[Не предусмотрены]

4.4. Самостоятельная работа студентов

Номер модуля дисциплины	Объем занятий, часы	Вид СРС
1	6	**Подготовка к практическому занятию (групповому упражнению) №1:** Изучение методических рекомендаций по проведению группового упражнения № 1 и рекомендованной литературы.
	6	**Подготовка к практическому занятию (групповому упражнению) №2:** Изучение методических рекомендаций по проведению группового упражнения № 2 и рекомендованной литературы.
	6	**Подготовка к практическому занятию (групповому упражнению) №3:** Изучение методических рекомендаций по проведению группового упражнения № 3 и рекомендованной литературы.
	6	**Подготовка к практическому занятию (групповому упражнению) № 4:** Изучение методических рекомендаций по проведению группового упражнения № 4 и рекомендованной литературы.
	6	**Подготовка к практическому занятию (групповому упражнению) № 5:** Изучение методических рекомендаций по проведению группового упражнения № 5 и рекомендованной литературы.
	6	**Подготовка к практическому занятию (групповому упражнению) № 6:** Изучение методических рекомендаций по проведению группового упражнения № 6 и рекомендованной литературы.
	4	**Подготовка к компьютерному тесту КТ-1** Изучение материалов лекций и рекомендованной литературы.

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 «Аудит информационной безопасности автоматизированной информационной системы обработки конфиденциальной информации на соответствие требованиям нормативных документов ФСТЭК России»:

Руководства по проведению групповых упражнений № 1 – 6. ОРИОКС// URL: http://orioks.miet.ru/

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ

Литература

1. Воеводин, В. А. Аудит информационной безопасности автоматизированных систем учебное пособие / В. А. Воеводин, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 208 с. - ISBN 978-5-7256-0974-5 : - Текст : непосредственный.
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. Организационное и правовое обеспечение информационной безопасности : Учебник и практикум для бакалавриата и магистратуры / Т.А. Полякова, А.А. Стрельцов, С.Г. Чубукова, В.А. Ниесов; Под ред. Т. А. Поляковой, А. А. Стрельцова. - М. : Юрайт, 2018. - 325 с. - (Бакалавр и магистр. Академический курс). - URL: https://urait.ru/bcode/413158 (дата обращения: 15.03.2021). - ISBN 978-5-534-03600-8. - Текст : электронный.
4. Воеводин, В. А. Правовые основы аудита информационной безопасности: учебное пособие / В. А. Воеводин, П. Л. Пилюгин; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ". - Москва : МИЭТ, 2021. - 180 с. - ISBN 978-5-7256-0961-5 - Текст : непосредственный.
5. 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 : Текст : непосредственный.
6. Программно-аппаратные средства защиты информации : учебно-методическое пособие / А. В. Душкин, О. Р. Лукманова, А. Н. Петухов, А. А. Хорев; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.А. Хорева. - Москва : МИЭТ, 2021. - 216 с. - ISBN 978-5-7256-0958-5 : Текст : непосредственный.
7. Зайцев А.П. Технические средства и методы защиты информации : Учеб. пособие / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков. - 7-е изд. - М. : Горячая линия-Телеком, 2012. - 442 с. - URL: https://e.lanbook.com/book/5155 (дата обращения: 16.03.2021). - ISBN 978-5-9912-0233-6.
8. 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.
9. Хорев А.А. Техническая защита информации : Учеб. пособие: В 3-х т. Т. 1 : Технические каналы утечки информации / А.А. Хорев; М-во образования и науки РФ, Федеральное агентство по образованию, МИЭТ(ТУ). - М. : НПЦ Аналитика, 2008. - 436 с. - ISBN 978-59901488-1-9 .

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

1. 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 : [сайт]. – URL: https://docs.cntd.ru/document/901990051. - (дата обращения 15.03.2021).
2. Федеральный закон от 27 июля 2006 г. N 152-ФЗ: (ред. от 02.07.2021) «О персональных данных»; Текст: электронный // Техэксперт : [сайт]. https://docs.cntd.ru/document/573249803?marker=64U0IK - (дата обращения 15.03.2021).
3. Методический документ. Методика оценки угроз безопасности информации. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2021 г. (утверждена ФСТЭК России 5 февраля 2021 г.)
4. Методический документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 г.
5. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 г.
6. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 25 июля 1997 г.
7. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.
8. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.
9. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Решение председателя Гостехкомиссии России от 30 марта 1992 г.
10. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 30 марта 1992 г.
11. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования: Общие положения; Национальный стандарт РФ : Введ. 09.02.1995: М.: Издательство стандартов (Переиздание) Стандартинформ, август 2006.-8 л. -Текст: непосредственный.
12. 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).- Текст: электронный.
13. ГОСТ Р 51275-2006 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) -Текст: электронный.
14. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Information protection. Sequence of protected operational system formation. General provisions; Национальный стандарт РФ: Введ. 01.09.2014.- М.: Стандартинформ, (Переиздание) октябрь 2018. -URL: https://docs.cntd.ru/document/1200108858 (дата обращения: 10.03.2021)- Текст: электронный.
15. Рекомендации по стандартизации Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации Information technologies. Basic terms and definitions in scope of technical protection of information, Национальный стандарт РФ: Введ. 01.01.2006.- М.: Стандартинформ, 2018.
16. Рекомендации по стандартизации Р 50.1.056-2005 Техническая защита информации. Основные термины и определения: Technical information protection. Terms and definitions Национальный стандарт РФ: Введ. 01.06.2006.- М.: Стандартинформ, 2006.

Периодические издания

1. 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). - Текст : электронный.
2. Вестник УрФО. Безопасность в информационной сфере: научный журнал/ Южно-Уральский государственный университет (национальный исследовательский университет). – Челябинск: УРГУ, 2011 -2018. - URL: http://info-secur.ru/index.php/ojs/issue/archive (дата обращения: 10.03.2021). - Режим доступа: свободный. - ISSN 2225-5435 (Print). - Текст: электронный.
3. Information Security / Информационная безопасность».–URL: http://www.itsec.ru/articles2/allpubliks (дата обращения: 15.03.2021). – Режим доступа: свободный.
4. «Вопросы кибербезопасности». – URL: http://cyberrus.com/ (дата обращения: 15.03.2021). – Режим доступа: свободный.
5. Защита информации. Inside : информационно-методический журнал / Издательский дом "Афина". - Санкт-Петербург : ИД Афина, 2004 - . - URL: http://elibrary.ru/contents.asp?titleid=25917 (дата обращения: 10.03.2021). - Режим доступа: по подписке (2017-2021). - ISSN 2413-3582. - Текст : электронный
6. Jet Info./ Инфосистемы Джет. – URL: http://www.jetinfo.ru (дата обращения: 15.03.2021). – Режим доступа: свободный.
7. 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: 09.03.2021). -

Режим доступа: для зарегистрированных пользователей. - ISSN 1682-7813. - Текст : электронный.

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). – Текст: электронный.
2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург,2010 -. - URL: https://e.lanbook.com (дата обращения: 10.03.2021). - Текст: электронный.
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). - Текст: электронный.
4. ФСТЭК России: Банк данных угроз безопасности информации. – Москва, 2014. - . - URL: https://bdu.fstec.ru/ (дата обращения: 10.03.2021). - Текст: электронный.
5. Бюро научно-технической информации «Техника для спецслужб». – URL: http://www.bnti.ru/about.asp (дата обращения: 15.03.2021). – Режим доступа: свободный.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе 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).

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 (микрофон, звуковые колонки), вебкамера с микрофоном). Учебная доска.	Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Firefox/Google Chrome/Explorer).
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. Корпоративная информационно - технологическая платформа ОРИОКС (Из реестра МИЭТ п.88) – 28 шт.

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность учебных аудиторий и помещений для самостоятельной работы	Перечень программного обеспечения
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 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. 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

10. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ/ПОДКОМПЕТЕНЦИЙ

ФОС по подкомпетенции ПК-3.АИБАСДИ. «Способен проводить аудит информационной безопасности».

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

11.1. Методические указания студентам по подготовке к практическим занятиям (групповым упражнениям)

Выполнение студентами групповых упражнений (ГУ) 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 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 исследовательские умения (наблюдать, сравнивать, анализировать, устанавливать зависимости, делать выводы и обобщения, оформлять результаты).

Групповое упражнение, как вид учебного занятия проводиться в мультимедийных аудиториях. Продолжительность - не менее двух академических часов.

По каждому ГУ разработаны и утверждены методические указания по их проведению.

Групповые упражнения носят репродуктивный характер и отличаются тем, что при их проведении студенты пользуются подробными инструкциями, в которых указаны: цель работы, пояснения (теория), порядок выполнения работы, контрольные вопросы, учебная и специальная литература.

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

Методические рекомендации по выполнению ГУ работ включают в себя:

- пояснительную записку;
- наименование раздела (темы);

- объем учебного времени, отведенный на ГУ;
- наименование темы ГУ;
- цель 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 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 ГУ студенту необходимо:

- уяснить вопросы и задания, рекомендуемые для подготовки к ГУ;
- ознакомиться с методическими рекомендации по выполнению 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 ГУ;
- подготовить отчеты для заполнения.

Групповые упражнения проводятся в форме деловой игры. Для выполнения практических занятий учебная группа разбивается на 4 подгруппы.

На ГУ каждый студент в соответствие с отведенной ему ролью должен выполнить задание в соответствии с методическими указаниями и оформить отчет.

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

11.2. Система контроля и оценивания

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.

Выполнение контрольных мероприятий текущего контроля (защита отчетов по практическим заданиям), результаты итогового контроля (зачет с оценкой) оцениваются баллами, общая сумма которых составляет 100 баллов (максимальное значение нормативного рейтинга учебной дисциплины – $R_{нор}$).

Примерная структура и график контрольных мероприятий приведены в таблице 11.1.

Таблица 11.1

Структура и график контрольных мероприятий дисциплины

Неделя	Название контрольного мероприятия	Баллы	
		максимальный балл	минимальный положительный
1– 2	Практическое занятие (групповое упражнение) № 1	14	7
3– 4	Практическое занятие (групповое упражнение) № 2	14	7
5– 6	Практическое занятие (групповое упражнение) № 3	14	7
7– 8	Практическое занятие (групповое упражнение) № 4	14	7
9– 10	Практическое занятие (групповое упражнение) № 5	14	7
11– 12	Практическое занятие (групповое упражнение) № 6	14	7
	Итого за текущий контроль	***84***	***42***
	Итоговый контроль	***16***	***8***
	Накопленный рейтинг	**100**	**50**

В зачетную ведомость и зачетную книжку вносится ***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 семестрового и итогового контроля. При выставлении итоговой оценки используется шкала, приведенная в таблице:

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

РАЗРАБОТЧИК

Доцент кафедры «Информационная безопасность»
Кандидат технических наук _____ В.А. Воеводин

Рабочая программа дисциплины «Аудит информационной безопасности автоматизированных систем» (деловая игра) по направлению подготовки 10.04.01 «Информационная безопасность», направленности (профилю) «Аудит информационной безопасности» 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 /