

УТВЕРЖДАЮ
Декан факультета

_____ Матвеев П.В.

« ____ » _____ 20__

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление/специальность подготовки	09.03.02 Информационные системы и технологии
Специализация/профиль/программа подготовки	Информационная безопасность
Уровень высшего образования	Бакалавриат
Форма обучения	Очная
Факультет	О Естественнонаучный
Выпускающая кафедра	О7 Информационные системы и программная инженерия
Кафедра-разработчик рабочей программы	О7 Информационные системы и программная инженерия

КУРС	СЕМЕСТР	ОБЩАЯ ТРУДОЁМКОСТЬ (ЗАЧЕТНЫХ ЕДИНИЦ)	ЧАСЫ (по наличию видов занятий)									ВИД ПРОМЕЖУТОЧНОГО КОНТРОЛЯ
			ОБЩАЯ ТРУДОЁМКОСТЬ	АУДИТОРНЫЕ ЗАНЯТИЯ				САМОСТОЯТЕЛЬНАЯ РАБОТА				
				ВСЕГО	ЛЕКЦИИ	ЛАБОРАТОРНЫЙ ПРАКТИКУМ	ПРАКТИЧЕСКИЕ ЗАНЯТИЯ	ВСЕГО	КУРСОВОЙ ПРОЕКТ	КУРСОВАЯ РАБОТА	ДРУГИЕ ВИДЫ САМОСТ. РАБОТЫ	
4	7	4	144	68	34	0	34	76	0	18	58	ЭКЗ.

ЛИСТ СОГЛАСОВАНИЯ

РАБОЧАЯ ПРОГРАММА СОСТАВЛЕНА В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ФЕДЕРАЛЬНОГО
ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ (ФГОС ВО)

09.03.02 Информационные системы и технологии

год набора группы: 2025

Программу составил:

Кафедра О7 Информационные системы и программная инженерия
Белов Александр Владимирович, к.т.н., доцент

Программа рассмотрена
на заседании кафедры-разработчика
рабочей программы **О7 Информационные системы и программная инженерия**

Заведующий кафедрой Семенова Е.Г., д.т.н., проф.

Программа рассмотрена
на заседании выпускающей кафедры

О7 Информационные системы и программная инженерия

Заведующий кафедрой Семенова Е.Г., д.т.н., проф.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Разделы рабочей программы

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО
3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ
5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ
6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приложения к рабочей программе дисциплины

- Приложение 1. Аннотация рабочей программы
- Приложение 2. Технологии и формы обучения
- Приложение 3. Фонды оценочных средств

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование следующих компетенций:

ПК-2.1 — Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности, принимать участие в проведении экспериментальных исследований системы защиты информации

Формированию компетенций служит достижение следующих результатов образования:

ПК-2.1

знания:

методы анализа и оценки защищённости автоматизированных систем;

национальные и международные стандарты в области аудита и оценки информационной безопасности;

методы сбора и оценки соответствия свидетельств аудита информационной безопасности защищённых автоматизированных систем управления нормативным требованиям по защите информации;;

умения:

разрабатывать методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем;

применять национальные и международные стандарты в области защиты информации для оценки защищённости автоматизированной системы;;

навыки:

способы контроля эффективности реализации политики информационной безопасности организации;

сбор и оценка соответствия свидетельств аудита информационной безопасности защищённых автоматизированных систем управления нормативным требованиям по защите информации;.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*.

Содержание дисциплины является логическим продолжением дисциплин: **ВВЕДЕНИЕ В ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**.

Содержание дисциплины является основой для освоения дисциплин: **ВЫПОЛНЕНИЕ И ЗАЩИТА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**.

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- ОПК-3 — Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
- ПК-2.1 — Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности, принимать участие в проведении экспериментальных исследований системы защиты информации
- ПК-2.2 — Способен определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
- ПК-94 — Способен к управлению информацией и данными, поиску источников информации и данных, восприятию, анализу, запоминанию и передаче информации с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч.

3.1. Содержание (дидактика) дисциплины

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %
				ВСЕГО	Лекции	Практические занятия		ПК-2.1
4	7	Раздел 1. Общая модель процесса аудита информационной безопасности объекта. 1.1 Термины: аудит информационной безопасности объекта (организации, автоматизированной системы), свидетельство аудита информационной безопасности. 1.2 Назначение, цель аудита информационной безопасности (ИБ) объекта. Необходимость аудита ИБ. 1.3 Виды аудита ИБ. Критерии аудита ИБ. Принципы аудита ИБ. Роли при проведении аудита ИБ.	25	9	5	4	16	20
4	7	Раздел 2. Этапы, процедуры аудита информационной безопасности защищенных автоматизированных систем и организаций. 2.1 Взаимодействие аудиторской организации с проверяемой организацией. Ответственность аудиторской организации и проверяемой организации. 2.2 Определение области аудита ИБ, критериев аудита ИБ. 2.3 Сбор свидетельств аудита ИБ. Анализ свидетельств аудита ИБ. 2.4 Завершение аудита ИБ. Отчёт и заключение по результатам аудита ИБ.	32	16	8	8	16	20
4	7	Раздел 3. Методы оценки информационной безопасности защищенных автоматизированных систем и организаций. 3.1 Модель оценки ИБ. 3.2 Методы измерения атрибутов оценки. Способы формирования показателей оценки. Критерии принятия решения для формирования результатов оценки. Интерпретация результатов оценки. 3.3 Оценка соответствия ИБ автоматизированных систем, организаций требованиям нормативных документов по ИБ. 3.4 Процессно-ориентированная оценка ИБ объекта. 3.5 Риск-ориентированная оценка ИБ объекта.	28	15	7	8	13	20
4	7	Раздел 4. Управление аудитом информационной безопасности. 4.1 Планирование программы аудита ИБ. 4.2 Реализация и поддержка программы аудита ИБ. 4.3 Контроль и совершенствование программы аудита ИБ.	27	14	6	8	13	20
4	7	Раздел 5. Международные, национальные и корпоративные стандарты и руководства в области аудита и оценки информационной безопасности. 5.1 Международные стандарты в области аудита и оценки ИБ ISO/IEC 27007, ISO/IEC 27008. 5.2 Национальные стандарты и руководства в области аудита и оценки ИБ GAO/AIMD-12.19.6, NIST 800-26. 5.3 Российские стандарты в области аудита и оценки ИБ ГОСТ Р ИСО/МЭК 27004, ГОСТ Р ИСО 19011. 5.4 Корпоративные стандарты и руководства в области аудита и оценки ИБ. Стандарты Банка России СТО БР ИББС-1.1, СТО БР ИББС-1.2.	32	14	8	6	18	20
Всего за 7 семестр			144	68	34	34	76	100
Всего по дисциплине			144	68	34	34	76	100

3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 1. Общая модель процесса аудита информационной безопасности объекта.	Практическая работа №1 – «Измерение и оценивание атрибутов на основе модели измерения и оценивания ИБ»	4
2	Раздел 2. Этапы, процедуры аудита информационной безопасности защищенных автоматизированных систем и организаций.	Практическая работа №2 – «Построение методики оценки соответствия ИБ требованиям нормативных документов с использованием анкет для измерения атрибутов объекта оценки (для выбранной области обеспечения ИБ)»	8
3	Раздел 3. Методы оценки информационной безопасности защищенных автоматизированных систем и организаций.	Практическая работа №3 – «Построение методики оценки соответствия ИБ требованиям нормативных документов с использованием метрик для измерения атрибутов объекта оценки (для выбранной области обеспечения ИБ).»	8
4	Раздел 4. Управление аудитом информационной безопасности.	Практическая работа №4 – «Построение методики процессно-ориентированной оценки ИБ (для различных уровней возможности процессов)»	8
5	Раздел 5. Международные, национальные и корпоративные стандарты и руководства в области аудита и оценки информационной безопасности.	Практическая работа №5 – «Формирование программы аудита ИБ для различных объектов, для различных областей обеспечения ИБ объекта.»	6

3.3. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов
1	Раздел 1. Общая модель процесса аудита информационной безопасности объекта.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	10
2		Подготовка к практическому занятию 1, оформление отчета.	4
3		Выполнение 1-го этапа курсовой работы	2
4	Раздел 2. Этапы, процедуры аудита информационной безопасности защищенных автоматизированных систем и организаций.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	6
5		Подготовка к практическому занятию 2, оформление отчета.	6
6		Выполнение 2-го этапа курсовой работы	4
7	Раздел 3. Методы оценки информационной безопасности защищенных автоматизированных систем и организаций.	Подготовка к практическому занятию 3, оформление отчета.	4
8		Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	9
9	Раздел 4. Управление аудитом информационной безопасности.	Подготовка к практическому занятию 4, оформление отчета.	4
10		Выполнение 3-го этапа курсовой работы	4
11		Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	5
12	Раздел 5. Международные, национальные и корпоративные стандарты и руководства в области аудита и оценки информационной безопасности.	Подготовка к практическому занятию 5, оформление отчета.	2
13		Оформление курсовой работы	2
14		Подготовка к защите курсовой работы	2
15		Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	12
Всего за 7 семестр			76

3.4. Курсовая работа

СОДЕРЖАНИЕ ЭТАПА	ПЕРИОД ИСПОЛНЕНИЯ (недели семестра)	ПЛАНИРУЕМОЕ ВРЕМЯ (час)
Этап 1. Выбор темы, обоснование актуальности темы	4 - 5	2
Этап 2. Выбор объекта ИБ и разработка программы аудита	6 - 10	4
Этап 3. Обоснование решений, принятых при создании программы аудита	11 - 14	4
Этап 4. Оформление курсовой работы	15 - 16	4
Этап 5. Подготовка к защите курсовой работы	16 - 17	4
Всего за 7 семестр		18

4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

СЕМЕСТР	НЕДЕЛИ СЕМЕСТРА																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
7	Отч. по ПЗ		Отч. по ПЗ		ДР		КР	Отч. по ПЗ		ДР		Отч. по ПЗ		КР			ДР	КР

Условные обозначения:

- ДР – диагностическая работа;
- Отч. по ПЗ – отчет по практическому заданию;
- КР – курсовая работа.

Текущий контроль успеваемости студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- отчет по практическому заданию;
- курсовая работа.

Промежуточная аттестация проводится в формах:

- экзамен.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература по дисциплине:

1. . Аудит. Москва: Юрайт, 2020, эл. рес.
2. . Аудит. Москва: Юрайт, 2021, эл. рес.
3. А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации. М.: КноРус, 2018, 70 экз.
4. А. Голдсмит. . Беспроводные коммуникации. М.: Техносфера, 2011, 5 экз.
5. А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. . Вычислительные системы, сети и телекоммуникации. М.: КноРус, 2017, 60 экз.
6. В. И. Ярочкин. . Информационная безопасность. М.: Академический Проект, 2006, 48 экз.
7. В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации. СПб.: Питер, 2011, 27 экз.
8. В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации. СПб.: Питер, 2007, эл. рес.
9. В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность. М.: РУСАЙНС, 2017, 70 экз.
10. С. А. Жданов, Н. Ю. Иванова, В. Г. Маняхина. . Операционные системы, сети и интернет-технологии. М.: Академия, 2014, 15 экз.
11. С. А. Нестеров. . Информационная безопасность. Москва: Юрайт, 2019, эл. рес.
12. Э. Таненбаум, Х. Бос. . Современные операционные системы. СПб.: Питер, 2019, эл. рес.
13. Ю. А. Родичев. . Информационная безопасность. Национальные стандарты Российской Федерации. Санкт-Петербург: Питер, 2019, эл. рес.

5.2. Дополнительная литература по дисциплине:

1. Ю. Г. Одегов, Т. В. Никонова. . Аудит и контроллинг персонала. М.: Альфа-Пресс, 2006, 1 экз.

5.3. Периодические издания:

не требуются.

5.4. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины, электронные библиотечные системы:

1. <http://www.intuit.ru/department/security/secbasics/> — НОУ ИНТУИТ | Основы информационной безопасности | Информация;
2. <http://www.intuit.ru/department/security/secst/> — НОУ ИНТУИТ | Стандарты информационной безопасности | Информация;
3. <http://e.lanbook.com/> — ЭБС Лань;;
4. <https://urait.ru/> — Образовательная платформа «Юрайт». Для вузов и ссузов.;;
5. <http://library.voenmeh.ru/jirbis2/> — Р«Р»Р°РІРSP°СЦ; — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова;
6. <https://scholar.google.com/> — Академия Google.

Современные профессиональные базы данных:

1. <https://rusneb.ru> – Национальная электронная библиотека (НЭБ);
2. <https://cyberleninka.ru/> - Научная электронная библиотека «Киберленинка»;
<http://www.rfbr.ru/rffi/ru/library> - Полнотекстовая электронная библиотека Российского фонда фундаментальных исследований.

Информационные справочные системы:

1. Техэксперт – Информационный портал технического регулирования: Нормы, правила, стандарты РФ;
2. http://library.voenmeh.ru/jirbis2/index.php?option=com_irbis&view=irbis&Itemid=457 - БД ГОСТов собственной генерации БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова;
3. <http://www.consultant.ru/>- КонсультантПлюс- информационный портал правовой информации.

5.5. Программное обеспечение:

1. LibreOffice;
2. Linux;
3. Notepad++.

5.6. Информационные технологии:

взаимодействие с обучающимися посредством ЭИОС Moodle БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Лекционные занятия:

специализированные требования по оборудованию отсутствуют; аудитория с посадочными местами по количеству студентов; доска.

6.2. Практические занятия:

1. Проектор;
2. LibreOffice;
3. Linux;
4. Notepad++.

6.3. Прочее:

1. рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
2. рабочие места студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде.

Аннотация рабочей программы

Дисциплина **АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*. Дисциплина реализуется на факультете *О Естественнoнаучный БГТУ "ВОЕНМЕХ"* им. Д.Ф. Устинова кафедрой *О7 Информационные системы и программная инженерия*.

Дисциплина нацелена на формирование *компетенций*:

ПК-2.1 Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности, принимать участие в проведении экспериментальных исследований системы защиты информации.

Содержание дисциплины охватывает круг вопросов, связанных с процедурами аудита информационной безопасности защищённых автоматизированных систем и организаций, со сбором и анализом свидетельств аудита информационной безопасности и их оценке. Также рассматриваются вопросы разработки и применения методик информационной безопасности автоматизированных систем.

Программой дисциплины предусмотрены следующие **виды контроля**:

Текущий контроль успеваемости студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- отчет по практическому заданию;
- курсовая работа.

Промежуточная аттестация проводится в формах:

- экзамен.

Общая трудоемкость освоения дисциплины составляет **4 з.е., 144 ч.** Программой дисциплины предусмотрены лекционные занятия (**34 ч.**), практические занятия (**34 ч.**), самостоятельная работа студента (**76 ч.**).

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 144 ч., из них 68 ч. аудиторных занятий, и 76 ч., отведенных на самостоятельную работу студента.

Рекомендации по распределению учебного времени по видам самостоятельной работы и разделам дисциплины приведены в таблице.

Контроль освоения дисциплины производится в соответствии с Положением о текущем, рубежном контроле успеваемости и промежуточной аттестации обучающихся.

Формы контроля и критерии оценивания приведены в приложении 3 к Рабочей программе.

Наименование работы	Рекомендуемая литература	Трудоемкость, час.
Раздел 1. Общая модель процесса аудита информационной безопасности объекта.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	Э. Таненбаум. . Современные операционные системы: СПб.: Питер, 2012 (7) Э. Таненбаум, Х. Бос. . Современные операционные системы: СПб.: Питер, 2019 (7) В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (5-7) А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. .	10
Подготовка к практическому занятию 1, оформление отчета.	Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (3-5) В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2011 (4) В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (4)	4
Выполнение 1-го этапа курсовой работы	А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (3-5) В. И. Ярочкин. . Информационная безопасность: М.: Академический Проект, 2006 (4-6)	2
Итого по разделу 1		16
Раздел 2. Этапы, процедуры аудита информационной безопасности защищенных автоматизированных систем и организаций.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (5)	6
Подготовка к практическому занятию 2, оформление отчета.	В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (5)	6
Выполнение 2-го этапа курсовой работы	В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (5-7) Э. Таненбаум, Х. Бос. . Современные операционные системы: СПб.: Питер, 2019 (8) Э. Таненбаум. . Современные операционные системы: СПб.: Питер, 2012 (8) В. И. Ярочкин. . Информационная безопасность: М.: Академический Проект, 2006 (4-6) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (3-	4

	4) А. Голдсмит. . Беспроводные коммуникации: М.: Техносфера, 2011 (6) А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. . Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (3-5)	
Итого по разделу 2		16
Раздел 3. Методы оценки информационной безопасности защищенных автоматизированных систем и организаций.		
Подготовка к практическому занятию 3, оформление отчета.	А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. . Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (5-7) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (2)	4
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	С. А. Жданов, Н. Ю. Иванова, В. Г. Маняхина. . Операционные системы, сети и интернет-технологии: М.: Академия, 2014 (7-9) В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (5) В. И. Ярочкин. . Информационная безопасность: М.: Академический Проект, 2006 (6)	9
Итого по разделу 3		13
Раздел 4. Управление аудитом информационной безопасности.		
Подготовка к практическому занятию 4, оформление отчета.	Э. Таненбаум, Х. Бос. . Современные операционные системы: СПб.: Питер, 2019 (7-9) Э. Таненбаум. . Современные операционные системы: СПб.: Питер, 2012 (7-9)	4
Выполнение 3-го этапа курсовой работы	С. А. Нестеров. . Информационная безопасность: Москва: Юрайт, 2019 (5-7) Ю. Г. Одегов, Т. В. Никонова. . Аудит и контроллинг персонала: М.: Альфа-Пресс, 2006 (1-3)	4
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. . Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (5-7) . Аудит: Москва: Юрайт, 2020 (1-5)	5
Итого по разделу 4		13
Раздел 5. Международные, национальные и корпоративные стандарты и руководства в области аудита и оценки информационной безопасности.		
Подготовка к практическому занятию 5, оформление отчета.	. Аудит: Москва: Юрайт, 2021 (5) Ю. А. Родичев. . Информационная безопасность. Национальные стандарты Российской Федерации: Санкт-Петербург: Питер, 2019 (1-4)	2
Оформление курсовой работы		2
Подготовка к защите курсовой работы		2
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе		12
Итого по разделу 5		18

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств, позволяющие оценить результаты обучения по данной дисциплине, включают в себя:

- диагностическая работа
- отчет по практическому заданию;
- курсовая работа;
- экзамен.

Критерии оценивания

Диагностическая работа

Диагностическая работа проводится в форме теста в ЭИОС Moodle:

- при правильном ответе менее чем на 60% вопросов - не аттестация;
- при правильном ответе на 60% вопросов и более - аттестация.

Отчет по практическому заданию

При подготовке к выполнению практических заданий рекомендуется повторить теоретические сведения по теме данной работы в соответствии с указаниями в таблице Приложения 3 к настоящей рабочей программе. При подготовке к защите рекомендуется подготовить ответы на контрольные вопросы по теме данной работы. В случаях затруднений обращаться к преподавателю на очередном практическом занятии или на консультации.

К каждому ПЗ необходимо подготовить отчет в электронном виде. После выполнения отчета его необходимо предоставить на проверку преподавателю (либо лично, либо посредством электронной почты). При выполнении отчета руководствоваться ГОСТ 7.32-2017. Состав отчета описывается в постановке задачи каждого ПЗ.

ПЗ считается выполненным и защищенным успешно при условии:

- наличия корректного решения поставленной задачи;
- наличия отчета;
- защиты ПЗ по комплекту тестовых вопросов для защиты ПЗ, размещенного в УМК дисциплины.

Критерии оценивания:

- соответствие решения указанным требованиям, его работоспособность и эффективность – 7 баллов;
- отчет оформлен полностью в соответствии с ГОСТ 7.32-2017 – 3 балла;
- правильность ответов на вопросы – 7 баллов;
- своевременность выполнения и защиты индивидуального задания – 3 балла.

Основанием для снижения количества баллов являются:

- несоответствие решения указанным требованиям, его неэффективность или некорректная работа;
- оформление отчета не соответствует ГОСТ 7.32-2017 в 3 и более пунктах;
- неверные ответы на вопросы или отсутствие ответов;
- несвоевременность выполнения и защиты индивидуального задания.

В случае, если ПЗ и отчет к нему выполнены своевременно в соответствии с указанными требованиями, а также получены правильные ответы на вопросы при его защите студент получает максимальное количество баллов – 20.

Для того, чтобы ПЗ было сдано, требуется набрать 12 баллов.

Курсовая работа

Список примерных тем курсовых работ содержится в УМК дисциплины.

Выполненные курсовые работы представляются в электронной форме в виде пояснительной записки, оформленной в соответствии с

Положением по содержанию, оформлению, организации выполнения и защиты курсовых проектов и курсовых работ БГТУ. СМК-П-4.2-12 – электронный ресурс – http://voenmeh.ru/files/0/Polozhenie_KRKP_2.0.pdf.

Критерии оценивания:

Курсовая работа допускается к защите при следующих условиях:

- предъявляемая программа аудита выполняет поставленную задачу;

- электронная и печатная версии пояснительной записки соответствуют установленным требованиям.

Оценка написанной КР:

- Работа выполнена, но не соответствует теме либо не использованы требуемые технологии, либо не реализованы все заявленные требования – 3 балла
- Работа выполнена в соответствии с темой, отвечает поставленным требованиям, но анализ ряда направлений аудита привел к некорректному выбору используемой методики - 6 баллов
- Работа выполнена в соответствии с темой, отвечает поставленным требованиям, но программа аудита не полностью использует возможности выбранной методики - 9 баллов
- Работа выполнена в соответствии с темой, отвечает поставленным требованиям, огрехов не найдено - 10 баллов

Оценка содержания пояснительной записки к курсовой работе:

- Содержание пояснительной записки имеет признаки чрезмерного заимствования, слабо описан анализ направления аудита и не раскрыты этапы аудита – 2 балла
- Содержание пояснительной записки имеет незначительные признаки заимствования, недостаточно обоснован выбор методики проведения аудита – 3 балла
- Пояснительная записка имеет четкую структуру в виде выделенных разделов и подразделов, обоснован выбор методики проведения аудита, в описании допущены неточности, которые сильно не влияют на применимость программы – 4 балла
- Пояснительная записка имеет четкую структуру в виде выделенных разделов и подразделов, обоснован выбор методики проведения аудита, огрехов не найдено - 5 баллов

Оценка оформления, стиля пояснительной записки

- Пояснительная записка оформлена с нарушениями, язык работы не соответствует научному стилю, некорректно оформленные заимствования, некорректно оформлен список источников – 2 балла
- Пояснительная записка оформлена с нарушениями, язык работы не соответствует научному стилю, есть замечания к оформлению списка источников – 3 балла
- Есть отдельные замечания к оформлению и стилю изложения, оформлению списка источников – 4 балла
- Нет замечаний к оформлению и стилю изложения, оформлению списка источников – 5 баллов

Максимальное количество баллов – 20

Оценка «отлично» - 17-20 баллов

Оценка «хорошо» - 13-16 баллов

Оценка «удовлетворительно» - 10-12 баллов

Оценка «не защитил» - меньше 10 или работа не была предъявлена

Экзамен

Перечень теоретических вопросов к экзамену, представленный в УМК дисциплины, предоставляется преподавателем. Вопросы соответствуют программе практических занятий. При подготовке ответов на теоретические вопросы рекомендуется помимо текстов лекций использовать источники основной и дополнительной литературы. Особое внимание следует уделить подготовке практических примеров к теоретическим экзаменационным вопросам.

На экзамене студенту предлагается два теоретических вопроса. При успешном ответе на оба вопроса выставляется оценка «отлично». При ответе на один из двух предложенных вопросов преподавателем может быть выставлена оценка «хорошо» при успешном выполнении всех практических заданий. При отсутствии успешных ответов зачет может быть оформлен с оценкой «удовлетворительно» на основании успешного выполнения предусмотренных рабочей программой практических заданий. При несвоевременном или неполном выполнении практических заданий и при неуспешной сдаче экзамена выставляется оценка «не сдано».

Паспорт фонда оценочных средств

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %	НАИМЕНОВАНИЕ ОЦЕНОЧНОГО СРЕДСТВА
				ВСЕГО	Лекции	Практические занятия		ПК-2.1	
4	7	Раздел 1. Общая модель процесса аудита информационной безопасности объекта.	25	9	5	4	16	20	Отчет по практическому заданию, Курсовая работа
4	7	Раздел 2. Этапы, процедуры аудита информационной безопасности защищенных автоматизированных систем и организаций.	32	16	8	8	16	20	Курсовая работа, Отчет по практическому заданию
4	7	Раздел 3. Методы оценки информационной безопасности защищенных автоматизированных систем и организаций.	28	15	7	8	13	20	Отчет по практическому заданию, Курсовая работа
4	7	Раздел 4. Управление аудитом информационной безопасности.	27	14	6	8	13	20	Отчет по практическому заданию, Курсовая работа
4	7	Раздел 5. Международные, национальные и корпоративные стандарты и руководства в области аудита и оценки информационной безопасности.	32	14	8	6	18	20	Отчет по практическому заданию, Курсовая работа
Всего за 7 семестр			144	68	34	34	76	100	
Всего по дисциплине			144	68	34	34	76	100	

ПК-2.1 - Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности, принимать участие в проведении экспериментальных исследований системы защиты информации

№ 1 Прочитайте текст и установите соответствие

Установите соответствие между типами аудита и их основными характеристиками:

Тип аудита	Характеристика
А. Внутренний аудит	1. Осуществляется независимыми внешними экспертами, не связанными с организацией
В. Внешний аудит	2. Выполняется собственным подразделением организации с целью самооценки
С. Аудит на соответствие	3. Проверяет соблюдение установленных стандартов и нормативных требований
	4. Такого типа не существует

№ 2 Прочитайте текст и запишите развернутый обоснованный ответ

Опишите общую модель процесса аудита информационной безопасности и её основные этапы. Назовите международные стандарты в области аудита информационной безопасности.

№ 3 Прочитайте текст и установите соответствие

Установите соответствие между основными объектами аудита и типами проверяемой информации:

Объект	Проверяемая информация
А. Политика безопасности	1. Содержание нормативных документов, ответственность, актуальность
В. Информационная система	2. Наличие технических и программных мер защиты, конфигурация
С. Пользовательские действия	3. Журналы активности, инциденты, соблюдение инструкций
	4. Комплект годовой бухгалтерской отчётности с пояснениями

№ 4 Прочитайте текст и установите последовательность

Расположите этапы подготовки к внешнему аудиту:

А. Ознакомление аудиторов с объектом

В. Определение области аудита

С. Назначение ответственных лиц

Д. Согласование временных рамок

№ 5 Прочитайте текст и установите последовательность

Определите правильную последовательность действий при оценке соответствия системы стандарту ISO/IEC 27001:

А. Сопоставление политики ИБ с требованиями

В. Проверка реализации технических мер

С. Анализ рисков

Д. Формирование отчета с рекомендациями

№ 6 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Какой метод используется для проверки устойчивости системы к внешним атакам?

- A. Анализ документации
- B. Интервью с пользователями
- C. Тестирование на проникновение
- D. Сканирование антивирусами

№ 7 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Какой тип аудита проводится организацией самостоятельно?

- A. Внешний аудит
- B. Сертификационный аудит
- C. Обязательный аудит
- D. Внутренний аудит

№ 8 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Какое из утверждений наилучшим образом характеризует функцию аудитора?

- A. Сбор, анализ и интерпретация доказательств
- B. Проведение расследований инцидентов
- C. Управление отделом информационной безопасности
- D. Разработка защитного программного обеспечения

№ 9 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Какие методы сбора информации применяются в аудите информационной безопасности?

- A. Наблюдение
- B. Взлом системы
- C. Интервью
- D. Анализ документации

№ 10 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Какие из перечисленных угроз относятся к физической безопасности?

- A. Пожар
- B. Несанкционированный вход в серверную
- C. Вирусы
- D. Повреждение оборудования от воды

№ 11 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Какие действия относятся к заключительному этапу аудита ИБ?

- A. Формирование отчета
- B. Предоставление рекомендаций
- C. Мониторинг реализации мер
- D. Оценка затрат на защиту

№ 12 Прочитайте текст и запишите развернутый обоснованный ответ

В чём заключается управление аудитом информационной безопасности и какие функции оно выполняет? Опишите основные методы оценки информационной безопасности автоматизированных систем.