

УТВЕРЖДАЮ
Декан факультета

_____ Матвеев П.В.

« ____ » _____ 20__

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

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	0	76	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 ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

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-2.2 — 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

Формированию компетенций служит достижение следующих результатов образования:

ПК-2.2

знания:

особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;;

умения:

применять программные и программно-аппаратные средства для защиты информации в базах данных;

проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;;

навыки:

обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ** 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, СТРУКТУРЫ И ОРГАНИЗАЦИЯ ДАННЫХ, 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
- ОПК-6 — Способен разрабатывать алгоритмы и программы, пригодные для практического применения в области информационных систем и технологий
- 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-2.2
4	7	Раздел 1. Предмет и задачи программно-аппаратной защиты информации. 1.1. Место программно-аппаратной защиты информации в системе информационной безопасности 1.2. Объект и предмет программно-аппаратной защиты информации 1.3. Назначение и состав системы программно-аппаратной защиты информации 1.4. Эшелонированная оборона.	5	2	2	0	3	10
4	7	Раздел 2. Основные угрозы, каналы утечки и уязвимости объектов программно-аппаратной защиты информации. 2.1. Угрозы информации и источники угроз 2.2. Уязвимые компоненты компьютеров, компьютерных систем и сетей 2.3. Виды и статистика нарушений информационной безопасности компьютерных систем и сетей.	16	6	2	4	10	10
4	7	Раздел 3. Формализованные требования к программно-аппаратной защите информации. 3.1. Политика и показатели безопасности средств вычислительной техники и автоматизированных систем 3.2. Формализованные требования к защите объектов программно-аппаратной защиты информации 3.3. Новое поколение нормативно-технических документов по безопасности информации.	15	8	4	4	7	10
4	7	Раздел 4. Задачи и классификация программно-аппаратных средств защиты информации. 4.1. Задачи программно-аппаратной защиты информации 4.2. Классификация программно-аппаратных средств защиты информации 4.3. Средства защиты, встроенные в аппаратуру 4.4. Средства защиты информации, встроенные в операционную систему компьютера 4.5. Автономные средства защиты информации 4.6. Специализированные системы защиты компьютерной информации 4.7. Сетевая защита в компьютерных системах и сетях.	34	17	4	13	17	10
4	7	Раздел 5. Разграничение доступа к информации. 5.1. Базовые функции подсистемы управления доступом 5.2. Идентификация, аутентификация и авторизация 5.3. Управление доступом пользователей к защищаемым ресурсам 5.4. Модели доступа 5.5. Корректность и полнота реализации политики разграничения доступа 5.6. Создание замкнутой рабочей среды для пользователей.	11	4	4	0	7	10
4	7	Раздел 6. Защита информации в сетях. 6.1. Принципы адресации и передачи информации в сети «Интернет» 6.2. Межсетевые экраны 6.3. Системы обнаружения вторжений 6.4. Виртуальные частные сети.	32	17	4	13	15	10
4	7	Раздел 7. Защита от вредоносного программного обеспечения. 7.1. Разрушающие программные воздействия и защита от них 7.2. Принципы и методы защиты от разрушающих программных воздействий.	8	4	4	0	4	10
4	7	Раздел 8. Добавочные средства защиты информации. 8.1. Общие сведения о системе защиты компьютерной информации Dallas Lock 8.2. Установка и администрирование СЗКИ Dallas Lock.	6	2	2	0	4	10
4	7	Раздел 9. DLP-системы. 9.1. Функциональные требования, основные функции и способы перехвата информации Falcongaze Secure Tower 9.2. Архитектурные решения DLP 9.3. Сертификация и соответствие требованиям регуляторов 9.4. Методика реализации функциональных возможностей.	8	4	4	0	4	10
4	7	Раздел 10. Методология экспертного оценивания программ и данных. 10.1. Общая методология компьютерно-технической экспертизы 10.2. Типичные правовые ошибки при выполнении СКТЭ 10.3. Особенности экспертизы программного обеспечения 10.4. Примеры проявления недокументированных функций программного обеспечения.	9	4	4	0	5	10
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 2. Основные угрозы, каналы утечки и уязвимости объектов программно-аппаратной защиты информации.	Классификация программно-аппаратных средств защиты информации	2
2		Изучение основных программных средств защиты информации	2
3	Раздел 3. Формализованные требования к программно-аппаратной защите информации.	Нормативно-правовая база, регулирующая применение программно-аппаратных средств защиты информации	4
4	Раздел 4. Задачи и классификация программно-аппаратных средств защиты информации.	Программно-аппаратное средство защиты информации от несанкционированного доступа. Защита программ от изменения и контроль целостности	8
5		Защита программ от разрушающих программных воздействий и защита автоматизированной	5

		системы от вредоносного программного обеспечения	
6	Раздел 6. Защита информации в сетях.	Изучение механизмов защиты СУБД MS Access	4
7		Изучение штатных средств защиты СУБД MySQL Server	4
8		Изучение штатных средств защиты СУБД Postgre SQL	4
9		Обобщение полученных знаний и умений по механизмам защиты	1
Всего за 7 семестр			34

3.3. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов
1	Раздел 1. Предмет и задачи программно-аппаратной защиты информации.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	3
2	Раздел 2. Основные угрозы, каналы утечки и уязвимости объектов программно-аппаратной защиты информации.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	3
3		Подготовка к практической работе №1, оформление отчета.	7
4	Раздел 3. Формализованные требования к программно-аппаратной защите информации.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	3
5		Подготовка к практической работе №2, оформление отчета.	4
6	Раздел 4. Задачи и классификация программно-аппаратных средств защиты информации.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	7
7		Подготовка к практической работе №3, оформление отчета.	10
8	Раздел 5. Разграничение доступа к информации.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	7
9	Раздел 6. Защита информации в сетях.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	3
10		Подготовка к практической работе №4, оформление отчета.	12
11	Раздел 7. Защита от вредоносного программного обеспечения.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	4
12	Раздел 8. Добавочные средства защиты информации.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	4
13	Раздел 9. DLP-системы.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	4
14	Раздел 10. Методология экспертного оценивания программ и данных.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	5
Всего за 7 семестр			76

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	ДР			Отч. по ПЗ	ДР			Отч. по ПЗ		Отч. по ПЗ	ДР	Вопр. Экз

Условные обозначения:

- ДР – диагностическая работа;
- Отч. по ПЗ – отчет по практическому заданию;
- Вопр. Экз – вопросы к экзамену.

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

- диагностическая работа;
- отчет по практическому заданию;
- вопросы к экзамену.

Промежуточная аттестация проводится в формах:

- экзамен.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература по дисциплине:

1. А. А. Внуков. . Защита информации. Москва: Юрайт, 2021, эл. рес.
2. А. В. Васильков, И. А. Васильков. . Безопасность и управление доступом в информационных системах. Москва: Форум, 2020, эл. рес.
3. Б. А. Фороузан. . Криптография и безопасность сетей. М.: Интернет-Ун-т Информ. Технол., 2010, 12 экз.
4. Б. А. Фороузан. . Криптография и безопасность сетей. М.: Национальный Открытый Университет ИНТУИТ, 2016, эл. рес.
5. В. Ф. Шаньгин. . Комплексная защита информации в корпоративных системах. М.: Форум, 2010, 5 экз.
6. Д. А. Мельников. . Информационная безопасность открытых систем. Москва: Флинта, 2014, эл. рес.
7. Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019, эл. рес.
8. Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019, 42 экз.
9. М. В. Рыбальченко. . Архитектура информационных систем. Москва: Юрайт, 2020, эл. рес.
10. П. Б. Хорев. . Программно-аппаратная защита информации. Москва: Форум, 2019, эл. рес.
11. С. Д. Поляков. . Сертификация программной продукции. Старый Оскол: ТНТ, 2020, эл. рес.
12. Ю. И. Коваленко. . Защита информационных технологий. М.: РУСАЙНС, 2016, 30 экз.
13. Ю. Ю. Громов, В. О. Драчёв, О. Г. Иванова. . Информационная безопасность и защита информации. Старый Оскол: ТНТ, 2010, 22 экз.

5.2. Дополнительная литература по дисциплине:

1. В. Я. Ищейнов, М. В. Мецатунян. . Защита конфиденциальной информации. М.: Форум, 2009, 2 экз.
2. Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. . Защита информации в персональном компьютере. М.: Форум, 2009, 2 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°СІ; — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

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. Microsoft SQL Server 2005 Express Edition.

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. LibreOffice;
2. Linux;
3. Microsoft SQL Server 2005 Express Edition.

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 **ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*. Дисциплина реализуется на факультете О Естественнотехнический БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрой О7 Информационные системы и программная инженерия.

Дисциплина нацелена на формирование *компетенций*:

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.

Содержание дисциплины охватывает круг вопросов, связанных с изучением основных угроз безопасности информации в автоматизированных системах и освоением методов защиты от данных угроз; с изучением методов, алгоритмов, программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем, основных мер по защите информации и программных продуктов от несанкционированного доступа, модификации и изучения в автоматизированных системах.

Программой дисциплины предусмотрены следующие **виды контроля**:

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

- диагностическая работа;
- отчет по практическому заданию;
- вопросы к экзамену.

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. Предмет и задачи программно-аппаратной защиты информации.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	А. А. Внуков. . Защита информации: Москва: Юрайт, 2021 (2) Д. А. Мельников. . Информационная безопасность открытых систем: Москва: Флинта, 2014 (3) Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. . Защита информации в персональном компьютере: М.: Форум, 2009 (1) Ю. Ю. Громов, В. О. Драчёв, О. Г. Иванова. . Информационная безопасность и защита информации: Старый Оскол: ТНТ, 2010 (1) А. А. Малюк, С. В. Пазизин, Н. С. Погожин. . Введение в защиту информации в автоматизированных системах: М.: Горячая линия-Телеком, 2004 (1-2)	3
Итого по разделу 1		3
Раздел 2. Основные угрозы, каналы утечки и уязвимости объектов программно-аппаратной защиты информации.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. . Защита информации в персональном компьютере: М.: Форум, 2009 (2) Ю. И. Коваленко. . Защита информационных технологий: М.: РУСАЙНС, 2016 (3) А. А. Малюк, С. В. Пазизин, Н. С. Погожин. . Введение в защиту информации в автоматизированных системах: М.: Горячая линия-Телеком, 2004 (2-4)	3
Подготовка к практической работе №1, оформление отчета.	Б. А. Фороузан. . Криптография и безопасность сетей: М.: Национальный Открытый Университет ИНТУИТ, 2016 (1-3)	7
Итого по разделу 2		10
Раздел 3. Формализованные требования к программно-аппаратной защите информации.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. Я. Ищейнов, М. В. Мецатунян. . Защита конфиденциальной информации: М.: Форум, 2009 (3-5) Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (2)	3
Подготовка к практической работе №2, оформление отчета.	В. Ф. Шаньгин. . Комплексная защита информации в корпоративных системах: М.: Форум, 2010 (5) Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. .	4

	Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (2)	
Итого по разделу 3		7
Раздел 4. Задачи и классификация программно-аппаратных средств защиты информации.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	Ю. И. Коваленко. . Защита информационных технологий: М.: РУСАЙНС, 2016 (5) Б. А. Фороузан. . Криптография и безопасность сетей: М.: Национальный Открытый Университет ИНТУИТ, 2016 (1-3, 5) В. Я. Ищейнов, М. В. Мецатунян. . Защита конфиденциальной информации: М.: Форум, 2009 (4) Б. А. Фороузан. . Криптография и безопасность сетей: М.: Интернет-Ун-т Информ. Технол., 2010 (1-3, 5) Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. . Защита информации в персональном компьютере: М.: Форум, 2009 (1-4)	7
Подготовка к практической работе №3, оформление отчета.	В. Ф. Шаньгин. . Комплексная защита информации в корпоративных системах: М.: Форум, 2010 (3-4) А. А. Малюк, С. В. Пазизин, Н. С. Погожин. . Введение в защиту информации в автоматизированных системах: М.: Горячая линия-Телеком, 2004 (3-5)	10
Итого по разделу 4		17
Раздел 5. Разграничение доступа к информации.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	А. В. Васильков, И. А. Васильков. . Безопасность и управление доступом в информационных системах: Москва: Форум, 2020 (2)	7
Итого по разделу 5		7
Раздел 6. Защита информации в сетях.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	Б. А. Фороузан. . Криптография и безопасность сетей: М.: Национальный Открытый Университет ИНТУИТ, 2016 (2) Б. А. Фороузан. . Криптография и безопасность сетей: М.: Интернет-Ун-т Информ. Технол., 2010 (2)	3
Подготовка к практической работе №4, оформление отчета.	Ю. Ю. Громов, В. О. Драчёв, О. Г. Иванова. . Информационная безопасность и защита информации: Старый Оскол: ТНТ, 2010 (3)	12
Итого по разделу 6		15
Раздел 7. Защита от вредоносного программного обеспечения.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	А. А. Внуков. . Защита информации: Москва: Юрайт, 2021 (1) В. Ф. Шаньгин. . Комплексная защита информации в корпоративных системах: М.: Форум, 2010 (3) Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (1) Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (1)	4
Итого по разделу 7		4
Раздел 8. Добавочные средства защиты информации.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	А. А. Внуков. . Защита информации: Москва: Юрайт, 2021 (1)	4
Итого по разделу 8		4
Раздел 9. DLP-системы.		
Изучение предусмотренных	С. Д. Поляков. . Сертификация программной	4

программой дидактических единиц по рекомендуемой литературе	продукции: Старый Оскол: ТНТ, 2020 (1) М. В. Рыбальченко. . Архитектура информационных систем: Москва: Юрайт, 2020 (2)	
Итого по разделу 9		4
Раздел 10. Методология экспертного оценивания программ и данных.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	П. Б. Хорев. . Программно-аппаратная защита информации: Москва: Форум, 2019 (2)	5
Итого по разделу 10		5

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

- диагностическая работа
- вопросы к экзамену;
- отчет по практическому заданию;
- 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.

Вопросы к экзамену

Перечень теоретических вопросов к экзамену предоставляется преподавателем. Перечень вопросов представлен в УМК дисциплины. При подготовке ответов на теоретические вопросы рекомендуется помимо конспектов лекций использовать источники основной и дополнительной литературы.

Отчет по практическому заданию

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 каждой ПЗ.

ПЗ считается выполненным и защищенным успешно при условии:

- наличия приложения, реализующего поставленную задачу;
- наличия отчета;
- защиты ПЗ по комплекту тестовых вопросов для защиты ПЗ, размещенного в УМК дисциплины.

Критерии оценивания:

- соответствие приложения 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 программного приложения 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.

Экзамен

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 зачета выставляется оценка «не сдано».

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-2.2	
4	7	Раздел 1. Предмет и задачи программно-аппаратной защиты информации.	5	2	2	0	3	10	Вопросы к экзамену
4	7	Раздел 2. Основные угрозы, каналы утечки и уязвимости объектов программно-аппаратной защиты информации.	16	6	2	4	10	10	Отчет по практическому заданию, Вопросы к экзамену
4	7	Раздел 3. Формализованные требования к программно-аппаратной защите информации.	15	8	4	4	7	10	Отчет по практическому заданию, Вопросы к экзамену
4	7	Раздел 4. Задачи и классификация программно-аппаратных средств защиты информации.	34	17	4	13	17	10	Вопросы к экзамену, Отчет по практическому заданию
4	7	Раздел 5. Разграничение доступа к информации.	11	4	4	0	7	10	Вопросы к экзамену
4	7	Раздел 6. Защита информации в сетях.	32	17	4	13	15	10	Вопросы к экзамену, Отчет по практическому заданию
4	7	Раздел 7. Защита от вредоносного программного обеспечения.	8	4	4	0	4	10	Вопросы к экзамену
4	7	Раздел 8. Добавочные средства защиты информации.	6	2	2	0	4	10	Вопросы к экзамену
4	7	Раздел 9. DLP-системы.	8	4	4	0	4	10	Вопросы к экзамену
4	7	Раздел 10. Методология экспертного оценивания программ и данных.	9	4	4	0	5	10	Вопросы к экзамену
Всего за 7 семестр			144	68	34	34	76	100	
Всего по дисциплине			144	68	34	34	76	100	

Оценочные материалы по дисциплине ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА 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

- № 1 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов
Какие технологии применяют для защиты от атак на DMA-каналы?
- A. IOMMU
 - B. Аудит драйверов
 - C. Аппаратные ограждения памяти
 - D. DLP-модуль
- № 2 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа
Какой компонент ПАСЗИ обеспечивает изоляцию процессов пользователя в «замкнутой рабочей среде»?
- A. Виртуальная машина
 - B. Аппаратный криптопроцессор
 - C. Межсетевой экран
 - D. DLP-агент
- № 3 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа
Какой механизм ОС обеспечивает контроль целостности файлов?
- A. MD5-хеширование и сравнение
 - B. DNS-запрос
 - C. DHCP-сервер
 - D. ARP-таблица
- № 4 Прочитайте текст и запишите развернутый обоснованный ответ
Объясните, как реализуется модель «замкнутой рабочей среды» (sandbox) для пользователей.
- № 5 Прочитайте текст и установите соответствие
Установите соответствие между типом сетевого экрана и способом фильтрации трафика:
- | Тип сетевого экрана | Способ фильтрации трафика |
|---------------------------------|---|
| A. Пакетный | 1. По значениям заголовков IP-пакетов |
| B. Сеансовый | 2. Отслеживание состояния соединений |
| C. Приложенческий | 3. Анализ содержимого протоколов приложений |
| 4. Такой фильтр не предусмотрен | |
- № 6 Прочитайте текст и установите последовательность
Установите порядок действий при развертывании агента DLP на конечных узлах:
- A. Настройка политик
 - B. Установка клиента

- С. Тестирование работы
- D. Регистрация в системе
- № 7 Прочитайте текст и установите последовательность
Укажите последовательность стадий тестирования замкнутой рабочей среды:
- A. Настройка изолированной VM
- B. Запуск приложений
- C. Попытки обхода ограничений
- D. Сравнение с исходной средой
- № 8 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа
Какой режим работы криптографического процессора позволяет обновлять ключи без прерывания работы?
- A. ECB-режим
- B. CBC-режим
- C. Горячая замена ключа
- D. SHA-режим
- № 9 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов
Какие каналы утечки контролирует DLP-система?
- A. USB-порты
- B. HTTPS-трафик
- C. SMTP (эл. почта)
- D. Чтение экранных данных камерой
- № 10 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов
Какие функции выполняет межсетевой экран?
- A. NAT (маскарадинг)
- B. VPN-терминация
- C. Аудит вызовов API приложений
- D. Фильтрация пакетов
- № 11 Прочитайте текст и запишите развернутый обоснованный ответ
В чем состоит назначение программно-аппаратных средств защиты информации (ПАСЗИ) в автоматизированных системах?
- № 12 Прочитайте текст и установите соответствие
Соотнесите модель доступа и её характеристику:
- | Модель доступа | Характеристика |
|-------------------------------|---|
| A. Мандатная | 1. Управление владельцем ресурса |
| B. Дискреционная | 2. Решение на основе атрибутов объекта |
| C. Ролевая | 3. Назначение прав ролям и их пользователей |
| D. Такой модели не существует | 4. Такой модели не существует |