МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова»
(БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова)

УТВЕРЖДАЮ
Декан факультета

_____ Матвеев П.В.
(подпись) ФИО
«31» 05 2022

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.

Санкт-Петербург
2022 г.

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: 2022

Программу составил:

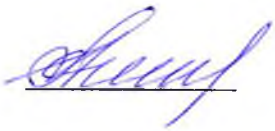
Кафедра О7 Информационные системы и программная инженерия
Бармина Анастасия Александровна, старший преподаватель

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

Приложения к рабочей программе дисциплины

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование следующих компетенций:

ПСК-2.10 — Способность выполнять работы по обслуживанию программно-аппаратными средствами сетей и инфокоммуникаций
ПСК-2.16 — Способностью администрировать подсистемы информационной безопасности объекта защиты
ПСК-2.7 — Владение навыками моделирования, анализа и использования формальных методов конструирования программного обеспечения
ПСК-2.8 — Способность выполнять интеграцию программных модулей и компонент

Формированию компетенций служит достижение следующих результатов образования:

ПСК-2.10

знания:

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

умения:

устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

навыки:

установки, настройки программных средств защиты информации в автоматизированной системе.

ПСК-2.16

знания:

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.

ПСК-2.7

знания:

особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;

умения:

применять средства гарантированного уничтожения информации;

навыки:

решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;

учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности.

ПСК-2.8

знания:

типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного;

умения:

осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак;

навыки:

выявления событий и инцидентов безопасности в автоматизированной системе.

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
- ОПК-7 — Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем
- 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
- ПСК-2.1 — Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности, принимать участие в проведении экспериментальных исследований системы защиты информации.
- ПСК-2.18 — Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации
- ПСК-2.4 — Владение навыками использования различных технологий разработки программного обеспечения
- ПСК-2.5 — Способность оценивать качество программного обеспечения, в том числе с точки зрения информационной безопасности, проведение тестирования и исследование результатов

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		ПСК-2.10	ПСК-2.16	ПСК-2.7	ПСК-2.8
4	7	**Раздел 1. Нормативные документы, регулирующие применение программно-аппаратных средств защиты информации.** 1.1. Роль стандартов информационной безопасности. Документы Государственной технической комиссии России. 1.2. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности. Требования к процессу сертификации продукта информационных технологий 1.3. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности. 1.4. Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем.	27	12	8	4	15	30	10	30	10
4	7	**Раздел 2. Теоретические аспекты применения программно-аппаратных средств обеспечения информационной безопасности.** 2.1. Понятие политики безопасности. Описание типовых политик безопасности. Угрозы безопасности компьютерных систем. Обеспечение гарантий выполнения политики безопасности. 2.2. Модель компьютерной системы. Понятие монитора безопасности. Концепция диспетчера доступа. 2.3. Метод генерации изолированной программной среды при проектировании механизмов гарантированного поддержания политики безопасности. Модели безопасного взаимодействия в КС. 2.4. Процедура идентификации и аутентификации: защита на уровне расширений BIOS, защита на уровне загрузчиков операционной среды.	29	12	8	4	17	25	20	25	20
4	7	**Раздел 3. Программно-аппаратные средства обеспечения информационной безопасности.** 3.1. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности. 3.2. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности. 3.3. Взаимодействие с общесистемными компонентами вычислительных систем. Методы и средства ограничения доступа к компонентам вычислительных систем. 3.4. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. 3.5. Управление криптографическими ключами. Методы и средства хранения ключевой информации. 3.6. Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение. Защита от разрушающих программных воздействий и вредоносного программного обеспечения. Защита программ от изменения и контроль целостности.	40	23	10	13	17	25	25	25	25
4	7	**Раздел 4. Защита информации в базах данных.** 4.1. Основные типы угроз. Модель нарушителя 4.2. Средства идентификации и аутентификации. Управление доступом 4.3. Средства контроля целостности информации в базах данных 4.4. Средства аудита и контроля безопасности. Критерии защищенности баз данных 4.5. Применение криптографических средств защиты информации в базах данных.	48	21	8	13	27	20	45	20	45
Всего за 7 семестр			144	68	34	34	76	100	100	100	100
Всего по дисциплине			144	68	34	34	76	100	100	100	100

3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 1. Нормативные документы, регулирующие применение программно-аппаратных средств защиты информации.	Нормативно-правовая база, регулирующая применение программно-апаратных средств защиты информации	4
2	Раздел 2. Теоретические аспекты применения программно-аппаратных	Классификация программно-аппаратных средств защиты информации	2

3	средств обеспечения информационной безопасности.	Изучение основных программных средств защиты информации	2
4	Раздел 3. Программно-аппаратные средства обеспечения информационной безопасности.	Программно-аппаратное средство защиты информации от несанкционированного доступа. Защита программ от изменения и контроль целостности	8
5		Защита программ от разрушающих программных 4 воздействий и защита автоматизированной системы от вредоносного программного обеспечения	5
6	Раздел 4. Защита информации в базах данных.	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. Нормативные документы, регулирующие применение программно-аппаратных средств защиты информации.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	15
2	Раздел 2. Теоретические аспекты применения программно-аппаратных средств обеспечения информационной безопасности.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	8
3		Подготовка к практической работе №1, оформление отчета.	9
4	Раздел 3. Программно-аппаратные средства обеспечения информационной безопасности.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	8
5		Подготовка к практической работе №2, оформление отчета.	9
6	Раздел 4. Защита информации в базах данных.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	17
7		Подготовка к практической работе №3, оформление отчета.	10
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						ДР				ДР			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. Б. А. Фороузан. . Криптография и безопасность сетей. М.: Национальный Открытый Университет ИНТУИТ, 2016, эл. рес.
3. Б. А. Фороузан. . Криптография и безопасность сетей. М.: Интернет-Ун-т Информ. Технол., 2010, 12 экз.
4. В. Ф. Шаньгин. . Комплексная защита информации в корпоративных системах. М.: Форум, 2010, 5 экз.
5. Д. А. Мельников. . Информационная безопасность открытых систем. Москва: Флинта, 2014, эл. рес.
6. Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019, 42 экз.
7. Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации. СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019, эл. рес.
8. Ю. И. Коваленко. . Защита информационных технологий. М.: РУСАЙНС, 2016, 30 экз.
9. 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°РІРЅР°СЦ; — 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* Естественнонаучный БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрой О7 Информационные системы и программная инженерия.

Дисциплина нацелена на формирование *компетенций*:
ПСК-2.10 Способность выполнять работы по обслуживанию программно-аппаратными средствами сетей и инфокоммуникаций;
ПСК-2.16 Способностью администрировать подсистемы информационной безопасности объекта защиты;
ПСК-2.7 Владение навыками моделирования, анализа и использования формальных методов конструирования программного обеспечения;
ПСК-2.8 Способность выполнять интеграцию программных модулей и компонент.

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. Нормативные документы, регулирующие применение программно-аппаратных средств защиты информации.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	А. А. Внуков. . Защита информации: Москва: Юрайт, 2021 (2) Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. . Защита информации в персональном компьютере: М.: Форум, 2009 (1) Д. А. Мельников. . Информационная безопасность открытых систем: Москва: Флинта, 2014 (3) 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)	15
Итого по разделу 1		15
Раздел 2. Теоретические аспекты применения программно-аппаратных средств обеспечения информационной безопасности.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	Б. А. Фороузан. . Криптография и безопасность сетей: М.: Национальный Открытый Университет ИНТУИТ, 2016 (1-3) 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)	8
Подготовка к практической работе №1, оформление отчета.		9
Итого по разделу 2		17
Раздел 3. Программно-аппаратные средства обеспечения информационной безопасности.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. Ф. Шаньгин. . Комплексная защита информации в корпоративных системах: М.: Форум, 2010 (5) Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (2) Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский. . Защита компьютерной информации: СПб.БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова, 2019 (2)	8
Подготовка к практической работе №2, оформление отчета.		9

	В. Я. Ищейнов, М. В. Мецатунян. . Защита конфиденциальной информации: М.: Форум, 2009 (3-5)	
Итого по разделу 3		17
Раздел 4. Защита информации в базах данных.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	А. А. Малюк, С. В. Пазизин, Н. С. Погожин. . Введение в защиту информации в автоматизированных системах: М.: Горячая линия-Телеком, 2004 (3-5) 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) В. Ф. Шаньгин. . Комплексная защита информации в корпоративных системах: М.: Форум, 2010 (3-4)	17
Подготовка к практической работе №3, оформление отчета.		10
Итого по разделу 4		27

ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

Фонды 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

Обучающийся имеет право на получение минимальной положительной оценки при условии успешного прохождения текущего контроля успеваемости в форме диагностической работы в соответствии с графиком раздела 4.
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 сдачи зачета выставляется оценка «не зачтено».

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		ПСК-2.10	ПСК-2.16	ПСК-2.7	ПСК-2.8	
4	7	**Раздел 1. Нормативные документы, регулирующие применение программно-аппаратных средств защиты информации.**	27	12	8	4	15	30	10	30	10	Вопросы к экзамену
4	7	**Раздел 2. Теоретические аспекты применения программно-аппаратных средств обеспечения информационной безопасности.**	29	12	8	4	17	25	20	25	20	Отчет по практическому заданию, Вопросы к экзамену
4	7	**Раздел 3. Программно-аппаратные средства обеспечения информационной безопасности.**	40	23	10	13	17	25	25	25	25	Отчет по практическому заданию, Вопросы к экзамену
4	7	**Раздел 4. Защита информации в базах данных.**	48	21	8	13	27	20	45	20	45	Вопросы к экзамену, Отчет по практическому заданию
Всего за 7 семестр			144	68	34	34	76	100	100	100	100	
Всего по дисциплине			144	68	34	34	76	100	100	100	100	