Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

Новоуральский технологический институт –
филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»

УТВЕРЖДЕНА
Ученым советом НТИ НИЯУ МИФИ
Протокол №1 от 30.01.2024

Рабочая программа учебной дисциплины
"Программно-технические средства обеспечения информационной безопасности"

Направление подготовки *09.03.01 – Информатика и вычислительная техника*

Профиль подготовки *Информационные технологии и бизнес-аналитика*

Квалификация (степень) выпускника *Академический бакалавр*

Форма обучения *очно-заочная*

Новоуральск 2024

	Очная форма обучения
Семестр	**9**
Трудоемкость, ЗЕТ	4 ЗЕТ
Трудоемкость, ч.	144 ч.
Аудиторные занятия, в т.ч.:	50 ч.
- лекции	20 ч.
- лабораторные работы	20 ч.
- практические работы	10 ч.
Самостоятельная работа	58 ч.
Контроль	36 ч.
Форма итогового контроля	зачет

Программу составил
доцент кафедры АУ Степанов П.И.

СОДЕРЖАНИЕ

1 ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина "Программно-технические средства обеспечения информационной безопасности" относится к циклу общепрофессиональных.

Целью изучения дисциплины является: изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

2 МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВПО

Дисциплина «Программно-технические средства обеспечения информационной безопасности» входит в число дисциплин окончательного формирования общекультурных и профессиональных компетенций выпускника и служит опорой для подготовки к его итоговой государственной аттестации.

Данная учебная дисциплина входит в общепрофессиональный модуль (Б1.О.03.15).

Дисциплина знакомит с общими закономерностями информационных процессов, позволяет оценить качество функционирования информационных систем.

Предшествующий уровень образования обучаемого – среднее (полное) общее образование.

3 ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Общепрофессиональные компетенции выпускников и индикаторы их достижения:

Код и наименование общепрофессиональной компетенции	**Код и наименование индикатора достижения общепрофессиональной компетенции**
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	**З-ОПК-3** Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **У-ОПК-3** Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **В-ОПК-3** Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

4 ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Цели и задачи воспитания, воспитательный потенциал дисциплин:

Направления/цели воспитания	**Задачи воспитания (код)**	**Воспитательный потенциал дисциплин**
Интеллектуальное воспитание	**В11** Формирование культуры умственного труда	Использование воспитательного потенциала дисциплин гуманитарного, естественнонаучного, общепрофессионального и профессионального модуля для формирования культуры умственного труда посредством вовлечения студентов в учебные исследовательские задания, курсовые работы и др.

5 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

5.1 Структура курса «Программно-технические средства обеспечения информационной без-опасности»

Общая трудоемкость дисциплины составляет **4 зачетные единицы, 144 часа.**

№ п/п	Название темы/раздела учебной дисциплины	Виды учебной деятельности, включая самостоятельную работу студентов и трудоемкость (в часах)				Текущий контроль (форма*, неделя)	Максимальный балл за раздел	Индикаторы освоения компетенции
		Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа			
1.	Основные понятия и определения. Концептуальные основы ИБ и ЗИ	4	4	2	10	ПР1, ЗЛР1	10	З-ОПК-3 У-ОПК-3 В-ОПК-3
2.	Организационно-правовые аспекты ЗИ. Политика безопасности и управление рисками.	4	4	2	10	ПР2, ЗЛР2	15	
3.	Стандартизация в сфере ИТ-безопасности	4	4	2	10	ПР3, ЗЛР3	15	
4.	Математические методы и модели в задачах защиты информации	4	4	2	10	ПР4, ЗЛР4	15	
5.	Многоуровневая защита информации в компьютерных системах и сетях	4	4	2	18	ПР5, ЗЛР5	15	
Итого:		20	20	10	58	36	70	
Зачет							30	

*Сокращение наименований форм текущего контроля и аттестации разделов:
ЗЛР – Защита лабораторной работы, ПР – практическая работа

5.2 Содержание лекционных занятий (9-й семестр) –20 часов

Неделя	Раздел курса, № занятия	Темы лекционных занятий	Трудоемкость, час.
1-3	Раздел 1 Л1-2	Лекция 1. Основные понятия и определения. Лекция 2. Концептуальные основы ИБ и ЗИ	4
4-6	Раздел 2 Л3-4	Лекция 3. Организационно-правовые аспекты ЗИ. Лекция 4. Политика безопасности и управление рисками.	4
7-9	Раздел 3 Л5-6	Лекция 5. Стандартизация в сфере ИТ-безопасности.	4
10-12	Раздел 4 Л7-8	Лекция 6. Математические методы и модели в задачах защиты информации.	4
14-18	Раздел 5 Л9-10	Лекция 7. Многоуровневая защита информации в компьютерных системах и сетях.	4

5.3 Темы лабораторных занятий (9-й семестр) – 20 часов

Неделя	Раздел курса, № занятия	Темы лабораторных занятий Мероприятие по текущему аудиторному контролю знаний	Трудоемкость, час.
1-3	Раздел 1 ЛР1	Лабораторная работа 1. Парольная защита.	4
4-6	Раздел 2 ЛР2	Лабораторная работа 2. Архивирование с паролем.	4
7-9	Раздел 3 ЛР3	Лабораторная работа 3. Шифр простой замены, таблица Вижинера.	4
10-12	Раздел 4 ЛР4	Лабораторная работа 4. Обмен ключами по Диффи-Хелману.	4
14-18	Раздел 5 ЛР5	Лабораторная работа 5. Шифр RSA.	4

5.4 Темы практических занятий (9-й семестр) – 10 часов

Неделя	Раздел курса, № занятия	Темы лабораторных занятий Мероприятие по текущему аудиторному контролю знаний	Трудоемкость, час.
1-3	Раздел 1 ПР1	Практическое занятие 1. Концептуальные основы ИБ и ЗИ.	2
4-6	Раздел 2 ПР2	Практическое занятие 2. Политика безопасности и управление рисками.	2
7-9	Раздел 3 ПР3	Практическое занятие 3. Стандартизация в сфере ИТ-безопасности.	2
10-12	Раздел 4 ПР4	Практическое занятие 4. Математические модели в задачах защиты информации.	2
14-18	Раздел 5 ПР5	Практическое занятие 5. Многоуровневая защита информации в компьютерных системах.	2

5.5 Самостоятельная работа – 68 часов

Самостоятельная работа студента по учебной дисциплине регламентируется «Положением об организации самостоятельной работы студентов в НТИ НИЯУ МИФИ».

№ п/п	Виды самостоятельной работы / разделы курса	Трудоемкость, час.
1.	Подготовка к практическому занятию 1, лабораторной работе 1.	10
2.	Подготовка к практическому занятию 2, лабораторной работе 2.	10
3.	Подготовка к практическому занятию 3, лабораторной работе 3.	10
4.	Подготовка к практическому занятию 4, лабораторной работе 4.	10
5.	Подготовка к практическому занятию 5, лабораторной работе 5, подготовка к зачету.	18

Перечень учебно-методического обеспечения самостоятельной работы студентов приведен в Приложении 1.

Методические указания для студентов по освоению дисциплины приведены в Приложении 2.

6 ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При реализации программы дисциплины «Программно-технические средства обеспечения информационной безопасности» используются различные образовательные технологии – аудиторные занятия проводятся в форме лекций и лабораторных (практических) занятий.

В процессе изучения дисциплины на лекциях, которые проводятся в специализированной аудитории, используется мультимедийный проектор и заранее подготовленный демонстрационный материал.

В начале каждого семестра все желающие студенты обеспечиваются электронными версиями методических пособий, имеющихся на кафедре, по изучаемому курсу для работы дома.

На сервере кафедры организован каталог со всеми методическими пособиями, разработанными на кафедре, для возможности постоянного студенческого доступа к ним с любого компьютера во время всех видов занятий.

Самостоятельная работа студентов подразумевает проработку лекционного материала с использованием рекомендуемой литературы (методических пособий по курсу) для подготовки к лабораторным и контрольным работам, контрольным тестам и зачету, а также выполнение контрольных домашних заданий и самостоятельное изучение ряда тем.

Для повышения уровня знаний студентов по курсу «Программно-технические средства обеспечения информационной безопасности» в течение семестра организуются консультации преподавателей (согласно графику консультаций кафедры, АУ). Во время консультационных занятий:

- проводится объяснение непонятных для студентов разделов теоретического курса;
- разъясняются алгоритмы решения задач индивидуальных домашних заданий;
- принимаются задолженности по тестовым и контрольным работам и т.д.

Перечень учебно-методического обеспечения самостоятельной работы студентов приведен в Приложении 1.

Методические указания для студентов по освоению дисциплины приведены в Приложении 2.

Реализация компетентностного подхода предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий, предполагающих активную обратную связь между преподавателем и студентами.

В процессе изучения дисциплины «Программно-технические средства обеспечения информационной безопасности» используются интерактивные формы обучения при проведении лабораторных (практических) занятий:

- выступление студентов с докладом по теме для самостоятельного изучения;
- защита домашнего контрольного задания;
- дискуссии;
- презентации.

7 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в таблице:

№ п.п.	Контролируемые модули, разделы (темы) дисциплины	Результаты освоения ООП		Виды аттестации		Наименование оценочного средства
		Код контролируемой компетенции	Индикаторы освоения компетенции	Текущий контроль	Промежуточная аттестация	
1	Основные понятия и определения. Концептуальные основы ИБ и ЗИ	ОПК-3	З-ОПК-3 У-ОПК-3 В-ОПК-3	ПР1, ЗЛР1	По итогам текущего контроля	Практическая работа 1, выполнение и защита Лабораторной работы 1
2	Организационно-правовые аспекты ЗИ. Политика безопасности и управление рисками.			ПР2, ЗЛР2	По итогам текущего контроля	Практическая работа 2, выполнение и защита Лабораторной работы 2
3	Стандартизация в сфере ИТ-безопасности			ПР3, ЗЛР3	По итогам текущего контроля	Практическая работа 3, выполнение и защита Лабораторной работы 3
4	Математические методы и модели в задачах защиты информации			ПР4, ЗЛР4	По итогам текущего контроля	Практическая работа 4, выполнение и защита Лабораторной работы 4
5	Многоуровневая защита информации в компьютерных системах и сетях			ПР5, ЗЛР5	По итогам текущего контроля	Практическая работа 5, выполнение и защита Лабораторной работы 5

В целях повышения эффективности процесса обучения студентов и стимулирования их самостоятельной работы в течение семестра используется система контроля текущей успеваемости и достижения ПР УД, включающая:

- посещение лекций;
- выполнение лабораторных работ;
- выполнение домашних контрольных работ;
- выполнение практических контрольных работ (проверка практических навыков студента);

- выполнение контрольных тестов (программированный экспресс-опрос по теоретическому материалу);
- самостоятельное изучение ряда тем.

Для оценки достижений студента используется балльно-рейтинговая система (Приложение 3).

Для целей промежуточной аттестации используется фонд оценочных средств (ФОС) по дисциплине (хранится на кафедре «Автоматизация управления»).

Результаты каждого тестового задания оцениваются в баллах, на основании которых выставляется оценка.

Задание, по которому проводится тест, считается зачтенным, если по нему набрано не менее половины от максимального количества баллов.

К зачету в конце семестра студент допускается, если он сдал все лабораторные работы, выполнил все тестовые задания на положительные оценки, а также сдал все домашние контрольные задания.

На зачете студенту предлагается выполнить 3 конкретных практических задания на компьютере по различным темам курса.

Итоговая оценка по курсу выводится с учетом балла, полученного на зачете, и баллов, полученных по указанным выше компонентам аттестации текущей работы студента в семестре. Шкала перевода баллов в традиционную систему оценок представлена в следующей таблице:

<table>
<tr><th>Оценка по 5 бальной шкале</th><th>Зачет</th><th>Сумма баллов по дисциплине</th><th>Оценка (ECTS)</th><th>Градация</th></tr>
<tr><td>5 (отлично)</td><td rowspan="6">Зачтено</td><td>90-100</td><td>A</td><td>Отлично</td></tr>
<tr><td rowspan="3">4 (хорошо)</td><td>85-89</td><td>B</td><td>Очень хорошо</td></tr>
<tr><td>75-84</td><td>C</td><td>Хорошо</td></tr>
<tr><td>70-74</td><td rowspan="2">D</td><td rowspan="2">Удовлетворительно</td></tr>
<tr><td rowspan="2">3 (удовлетворительно)</td><td>65-69</td></tr>
<tr><td>60-64</td><td>E</td><td>Посредственно</td></tr>
<tr><td>2 (неудовлетворительно)</td><td>Не зачтено</td><td>Ниже 60</td><td>F</td><td>Неудовлетворительно</td></tr>
</table>

8 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

8.1 Перечень литературы, необходимой для освоения дисциплины

1 **Вавренюк А. Б.**
Разрушающие программные воздействия : [учебно - метолич. пособие для вузов]. Электронный ресурс. – Москва: НИЯУ МИФИ. 2011 – точка доступа – ЭБС НИЯУ МИФИ – mehpi.ru

2 **Гинодман В.А.**
От первых вирусов до целевых атак : [учебное пособие]. Электронный ресурс. – Москва : НИЯУ МИФИ. 2014. – 94 с. – точка доступа – ЭБС НИЯУ МИФИ – mehpi.ru

3 **Грибунин В. Г.**
Комплексная система защиты информации на предприятии: [учеб. пособие для вузов]. – М. : Академия. 2009. – 416 с

4 **Куприянов А. И**
Основы защиты информации : [учебное пособие]. – М. : Академия. 2008. – 256 с. (+ заказ май 2015 – 5 книг)

5 **Горбатов В. С.**
Контроль защищенности автоматизированных систем от несанкционированного доступа. Аттестационные испытания : [лабораторный практикум]. Электронный ресурс. – Москва : НИЯУ МИФИ. 2013. – 468с. – точка доступа – ЭБС НИЯУ МИФИ – mehpi.ru

8.2 Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения дисциплины

Наименование ресурса	Электронный адрес ресурса
1) Официальный сайт НТИ НИЯУ МИФИ	http://nsti.ru
2) ЭБС «Лань»	https://e.lanbook.com
3) ЭБС «IPRbooks»	https://iprbooks.ru
4) Образовательная платформа Юрайт	https://urait.ru/bcode/468952
5) Образовательный портал НИЯУ МИФИ	https://online.mephi.ru/
6) Научная библиотека НИЯУ МИФИ	http://library.mephi.ru/

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Для осуществления образовательного процесса по дисциплине необходимо:

1 Лекционные занятия:

- аудитория, оборудованная техническими средствами для демонстрации лекций-визуализаций (проектор, экран, компьютер/ноутбук);
- комплект электронных презентаций/слайдов;

2 Практические занятия:

- компьютерный класс;
- среды программирования

НТИ НИЯУ МИФИ располагает данными средствами в полном объеме.

Учебная дисциплина обеспечена учебно-методической документацией и материалами. Ее содержание представлено в локальной сети института и находится в режиме свободного доступа для студентов. Доступ студентов для тренинга по прохождению тестовых заданий и для самостоятельной подготовки осуществляется через компьютеры дисплейного класса (в стандартной комплектации).

В библиотечном фонде представлены необходимые учебные пособия согласно нормативам ФГОС.

Все рекомендуемые методические пособия и материалы по курсу «Программно-технические средства обеспечения информационной без-опасности», разработанные преподавателями кафедры, имеются в электронном виде, на бумажных носителях, представлены в УМКД. Пособия хранятся на кафедре Автоматизация управления, представлены в электронном читальном зале НТИ НИЯУ МИФИ. Электронные копии пособий также могут индивидуально предоставляться студентам по их запросу на кафедре Автоматизация управления.

Студенты своевременно обеспечиваются индивидуальными вариантами домашних заданий. Варианты заданий имеются в электронном виде и представлены в УМКД (кафедра Автоматизация управления).

Лабораторные работы по курсу осуществляются в компьютерных классах. Задания для выполнения на лабораторных работах представлены в методических пособиях кафедры.

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ

к рабочей программе по курсу
«Программно-технические средства обеспечения информационной без-опасности»
для ООП ВПО 09.03.01

на 20____/20____ уч.год

В рабочую программу вносятся следующие изменения:

_____

_____

_____

_____

_____

Рабочая программа пересмотрена и одобрена на заседании кафедры «__»_____20___г.
Заведующий кафедрой АУ

на 20____/20____ уч.год

В рабочую программу вносятся следующие изменения:

_____

_____

_____

_____

_____

Рабочая программа пересмотрена и одобрена на заседании кафедры «__»_____20___г.
Заведующий кафедрой АУ

на 20____/20____ уч.год

В рабочую программу вносятся следующие изменения:

_____

_____

_____

_____

_____

Рабочая программа пересмотрена и одобрена на заседании кафедры «__»_____20___г.
Заведующий кафедрой АУ

Программа действительна

на 20____/20____ уч.год _____(заведующий кафедрой АУ)

на 20____/20____ уч.год _____(заведующий кафедрой АУ)

на 20____/20____ уч.год _____(заведующий кафедрой АУ)

на 20____/20____ уч.год _____(заведующий кафедрой АУ)

на 20____/20____ уч.год _____(заведующий кафедрой АУ)

ПРИЛОЖЕНИЕ 1. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ.

№	Литература	Год	Курс	Семестр	Кол-во студентов	Кол-во книг	Коэффициент книгообеспеченности
	Основная литература						
1	**Вавренюк А. Б.** Разрушающие программные воздействия : [учебно - методич. пособие для вузов]. Электронный ресурс. – Москва: НИЯУ МИФИ. 2011 – точка доступа – ЭБС НИЯУ МИФИ – mehpi.ru	2011	4	8	7	7	1,0
2	**Гинодман В.А.** От первых вирусов до целевых атак : [учебное пособие]. Электронный ресурс. – Москва : НИЯУ МИФИ. 2014. – 94 с. – точка доступа – ЭБС НИЯУ МИФИ – mehpi.ru	2014	4	8	7	7	1,0
	Дополнительная литература						
1	**Грибунин В. Г.** Комплексная система защиты информации на предприятии: [учеб. пособие для вузов]. – М. : Академия. 2009. – 416 с	2009	4	8	7	5	0,71
2	**Куприянов А. И** Основы защиты информации : [учебное пособие]. – М. : Академия. 2008. – 256 с. (+ заказ май 2015 – 5 книг)	2008	4	8	7	7	1,0
3	**Горбатов В. С.** Контроль защищенности автоматизированных систем от несанкционированного доступа. Аттестационные испытания : [лабораторный практикум]. Электронный ресурс. – Москва : НИЯУ МИФИ. 2013. – 468с. – точка доступа – ЭБС НИЯУ МИФИ – mehpi.ru	2013	4	8	7	7	1,0

ПРИЛОЖЕНИЕ 2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ СТУДЕНТОВ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ.

- стандарт организации СТО НТИ-2-2014. Требования к оформлению текстовой документации;
- методические рекомендации по организации самостоятельной работы обучающихся НТИ НИЯУ МИФИ.

ПРИЛОЖЕНИЕ 3. БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА ОЦЕНКИ.

Таблица 3.1. Распределение баллов текущего рейтинга по видам деятельности студента направления подготовки 09.03.01 при изучении курса "Программно-технические средства обеспечения информационной безопасности"

№ п/п	Наименование раздела	Аттестация	Максимальный балл
1	Основные понятия и определения. Концептуальные основы ИБ и ЗИ	ПР1, ЗЛР1	10
2	Организационно-правовые аспекты ЗИ. Политика безопасности и управление рисками.	ПР2, ЗЛР2	15
3	Стандартизация в сфере ИТ-безопасности	ПР3, ЗЛР3	15
4	Математические методы и модели в задачах защиты информации	ПР4, ЗЛР4	15
5	Многоуровневая защита информации в компьютерных системах и сетях	ПР5, ЗЛР5	15
11	Зачет		30
		ИТОГО	**100**

ПРИЛОЖЕНИЕ 4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Для оценки результатов обучения в зависимости от оцениваемого средства используются следующие шкалы оценок:

Критерии оценок	Шкала оценок
1	2
Зачет	
Полнота знаний теоретического контролируемого материала	При промежуточной аттестации количество баллов определяется количеством правильных ответов на вопросы теста Задание на зачет – макс. *30 баллов* Задание на зачет – ответ на один вопрос из приведенного списка. 30 баллов ставится за полный ответ на вопрос. 15 баллов ставится за достаточно полный ответ на вопрос с незначительными недочетами. 10 баллов ставится в случае неполного ответа на вопрос. 0 баллов ставится, если в беседе со студентом выясняется, что он не знает основных понятий и определений курса. В индивидуальном порядке по теме лекций могут быть заданы на зачете дополнительные вопросы (из перечня).

Материалы, необходимые для оценки результатов обучения

Тестовое задание 1
по дисциплине «Программно-технические средства обеспечения информационной безопасности»

Задание №1
Вопрос:
Какие законы существуют в России в области компьютерного права?
Выберите несколько из 6 вариантов ответа:
1) О государственной тайне
2) об авторском праве и смежных правах
3) о гражданском долге
4) о правовой охране программ для ЭВМ и БД
5) о правовой ответственности
6) об информации, информатизации, защищенности информации
Задание №2
Вопрос:
Какие существуют основные уровни обеспечения защиты информации?
Выберите несколько из 7 вариантов ответа:
1) законодательный
2) административный
3) программно-технический
4) физический
5) вероятностный
6) процедурный
7) распределительный
Задание №3
Вопрос:
Физические средства защиты информации
Выберите один из 4 вариантов ответа:
1) средства, которые реализуются в виде автономных устройств и систем
2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу
3) это программы, предназначенные для выполнения функций, связанных с защитой информации
4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств
Задание №4
Вопрос:
В чем заключается основная причина потерь информации, связанной с ПК?

Выберите один из 3 вариантов ответа:
1) с глобальным хищением информации
2) с появлением интернета
3) с недостаточной образованностью в области безопасности

Задание №5
Вопрос:
Технические средства защиты информации
Выберите один из 4 вариантов ответа:
1) средства, которые реализуются в виде автономных устройств и систем
2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу
3) это программы, предназначенные для выполнения функций, связанных с защитой информации
4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств

Задание №6
Вопрос:
К аспектам ИБ относятся
Выберите несколько из 5 вариантов ответа:
1) дискретность
2) целостность
3) конфиденциальность
4) актуальность
5) доступность

Задание №7
Вопрос:
Что такое криптология?
Выберите один из 3 вариантов ответа:
1) защищенная информация
2) область доступной информации
3) тайная область связи

Задание №8
Вопрос:
Что такое несанкционированный доступ (нсд)?
Выберите один из 5 вариантов ответа:
1) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа
2) Создание резервных копий в организации
3) Правила и положения, выработанные в организации для обхода парольной защиты
4) Вход в систему без согласования с руководителем организации
5) Удаление не нужной информации

Задание №9
Вопрос:
Что является основой для формирования государственной политики в сфере информации? (Ответьте 1 словом)
Запишите ответ:
_____

Задание №10
Вопрос:
Что такое целостность информации?
Выберите один из 4 вариантов ответа:
1) Свойство информации, заключающееся в возможности ее изменения любым субъектом
2) Свойство информации, заключающееся в возможности изменения только единственным пользователем
3) Свойство информации, заключающееся в ее существовании в виде единого набора файлов
4) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)

Задание №11
Вопрос:
Кто является знаковой фигурой в сфере информационной безопасности
Выберите один из 4 вариантов ответа:
1) Митник
2) Шеннон
3) Паскаль
4) Беббидж

Задание №12
Вопрос:
В чем состоит задача криптографа?
Выберите один из 2 вариантов ответа:
1) взломать систему защиты
2) обеспечить конфиденциальность и аутентификацию передаваемых сообщений

Задание №13
Вопрос:
Под ИБ понимают
Выберите один из 3 вариантов ответа:
1) защиту от несанкционированного доступа
2) защиту информации от случайных и преднамеренных воздействий естественного и искуственного характера
3) защиту информации от компьютерных вирусов

Задание №14
Вопрос:
Что такое аутентификация?
Выберите один из 5 вариантов ответа:
1) Проверка количества переданной и принятой информации
2) Нахождение файлов, которые изменены в информационной системе несанкционированно
3) Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).
4) Определение файлов, из которых удалена служебная информация
5) Определение файлов, из которых удалена служебная информация
Задание №15
Вопрос:
"Маскарад"- это
Выберите один из 2 вариантов ответа:
1) осуществление специально разработанными программами перехвата имени и пароля
2) выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями
Задание №16
Вопрос:
Верификация -
Выберите один из 3 вариантов ответа:
1) это проверка принадлежности субъекту доступа предъявленного им идентификатора.
2) проверка целостности и подлинности инф, программы, документа
3) это присвоение имени субъекту или объекту
Задание №17
Вопрос:
Кодирование информации -
Выберите один из 2 вариантов ответа:
1) представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д.
2) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом
Задание №18
Вопрос:
Утечка информации
Выберите один из 3 вариантов ответа:
1) несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу
2) ознакомление постороннего лица с содержанием секретной информации
3) потеря, хищение, разрушение или неполучение переданных данных
Задание №19
Вопрос:
Под изоляцией и разделением (требование к обеспечению ИБ) понимают
Выберите один из 2 вариантов ответа:
1) разделение информации на группы так, чтобы нарушение одной группы информации не влияло на безопасность других групп информации (документов)
2) разделение объектов защиты на группы так, чтобы нарушение защиты одной группы не влияло на безопасность других групп
Задание №20
Вопрос:
К аспектам ИБ относятся
Выберите несколько из 5 вариантов ответа:
1) дискретность
2) целостность
3) конфиденциальность
4) актуальность
5) доступность
Задание №21
Вопрос:
Линейное шифрование -
Выберите один из 3 вариантов ответа:
1) несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу
2) криптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому
3) криптографическое преобразование информации в целях ее защиты от ознакомления **и модификации посторонними лицами**
Задание №22
Вопрос:
Прочность защиты в АС
Выберите один из 3 вариантов ответа:
1) вероятность не преодоления защиты нарушителем за установленный промежуток времени
2) способность системы защиты информации обеспечить достаточный уровень своей безопасности
3) группа показателей защиты, соответствующая определенному классу защиты
Задание №23
Вопрос:
Уровень секретности - это
Выберите один из 2 вариантов ответа:
1) ответственность за модификацию и НСД информации

2) административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов

Задание №24

Вопрос:

Угроза - это

Выберите один из 2 вариантов ответа:

1) возможное событие, действие, процесс или явление, которое может привести к ущербу чьих-либо интересов
2) событие, действие, процесс или явление, которое приводит к ущербу чьих-либо интересов

Задание №25

Вопрос:

Под ИБ понимают

Выберите один из 3 вариантов ответа:

1) защиту от несанкционированного доступа
2) защиту информации от случайных и преднамеренных воздействий естественного и искуственного характера
3) защиту информации от компьютерных вирусов

Задание №26

Вопрос:

Что такое криптография?

Выберите один из 3 вариантов ответа:

1) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом
2) область доступной информации
3) область тайной связи, с целью защиты от ознакомления и модификации посторонним лицом

Задание №27

Вопрос:

Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации называется

Выберите один из 4 вариантов ответа:

1) кодируемой
2) шифруемой
3) недостоверной
4) защищаемой

Задание №28

Вопрос:

Продолжите фразу: "Административная и законодательная мера, соответствующая мере ответственности лица за потерю конкретной секретной информации, регламентирующаяся специальным документом с учетом государственных и военно-стратегических, коммерческих или частных интересов - это..."

Запишите ответ:

_____

Задание №29

Вопрос:

Продолжите фразу: " Последовательность символов, недоступная для посторонних, предназначенная для идентификации и аутентификации субъектов и объектов между собой - это..."

Запишите ответ:

_____

Задание №30

Вопрос:

Способ представления информации в вычислительных системах

Запишите ответ:

_____

Задание №31

Вопрос:

Вставьте пропущенное слово:

Информация может быть защищена без аппаратных и программных средств защиты с помощью _____ преобразований.

Запишите ответ:

_____

Задание №32

Вопрос:

Абстрактное содержание какого-либо высказывания, описание, указание, сообщение либо известие - это

Выберите один из 4 вариантов ответа:

1) текст
2) данные
3) информация
4) пароль

Задание №33

Вопрос:

Какие атаки предпринимают хакеры на программном уровне?

Выберите несколько из 4 вариантов ответа:

1) атаки на уровне ОС
2) атаки на уровне сетевого ПО
3) атаки на уровне пакетов прикладных программ
4) атаки на уровне СУБД

Задание №34
Вопрос:
Организационные угрозы подразделяются на
Выберите несколько из 4 вариантов ответа:
1) угрозы воздействия на персонал
2) физические угрозы
3) действия персонала
4) несанкционированный доступ
Задание №35
Вопрос:
Виды технической разведки (по месту размещения аппаратуры)
Выберите несколько из 7 вариантов ответа:
1) космическая
2) оптическая
3) наземная
4) фотографическая
5) морская
6) воздушная
7) магнитометрическая
Задание №36
Вопрос:
Основные группы технических средств ведения разведки
Выберите несколько из 5 вариантов ответа:
1) радиомикрофоны
2) фотоаппараты
3) электронные "уши"
4) дистанционное прослушивание разговоров
5) системы определения местоположения контролируемого объекта
Задание №37
Вопрос:
Разновидности угроз безопасности
Выберите несколько из 6 вариантов ответа:
1) техническая разведка
2) программные
3) программно-математичекие
4) организационные
5) технические
6) физические
Задание №38
Вопрос:
Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется
Выберите один из 4 вариантов ответа:
1) угрозой;
2) опасностью;
3) намерением;
4) предостережением.
Задание №39
Вопрос:
Какая угроза возникает в результате технологической неисправности за пределами информационной системы?
Запишите ответ:
_____
Задание №40
Вопрос:
Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?
Выберите один из 4 вариантов ответа:
1) операционной системы, сетевого программного обеспечения
2) операционной системы, сетевого программного обеспечения и системы управления базами данных;
3) операционной системы, системы управления базами данных;
4) сетевого программного обеспечения и системы управления базами данных.
Задание №41
Вопрос:
Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется
Выберите один из 4 вариантов ответа:
1) системой угроз;
2) системой защиты;
3) системой безопасности;
4) системой уничтожения.
Задание №42
Вопрос:
К угрозам какого характера относятся действия, направленные на сотрудников компании или осуществляемые сотрудниками компании с целью получения конфиденциальной информации или нарушения функции бизнес-процессов?

Запишите ответ:

_____

Задание №43
Вопрос:
К видам защиты информации относятся:
Выберите несколько из 4 вариантов ответа:
1) правовые и законодательные:
2) морально-этические;
3) юридические;
4) административно-организационные;
Задание №44
Вопрос:
Доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации называется
Запишите ответ:

_____

Задание №45
Вопрос:
К методам защиты от НСД относятся
Выберите несколько из 5 вариантов ответа:
1) разделение доступа;
2) разграничение доступа;
3) увеличение доступа;
4) ограничение доступа.
5) аутентификация и идентификация
Задание №46
Вопрос:
Метод пароля и его модификация, метод вопрос-ответ, метод секретного алгоритма - это методы
Запишите ответ:

_____

Задание №47
Вопрос:
Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности называется
Выберите один из 4 вариантов ответа:
1) политикой информации
2) защитой информации
3) политикой безопасности
4) организацией безопасности
Задание №48
Вопрос:
Выделите группы, на которые делятся средства защиты информации:
Выберите один из 3 вариантов ответа:
1) физические, аппаратные, программные, криптографические, комбинированные;
2) химические, аппаратные, программные, криптографические, комбинированные;
3) физические, аппаратные, программные, этнографические, комбинированные;
Задание №49
Вопрос:
Техническое, криптографическое, программное и иное средство, предназначенное для защиты информации, средство, в котором оно реализовано, а также средство контроля эффективности защиты информации- все это есть
Запишите ответ:

_____

Задание №50
Вопрос:
Что такое компьютерный вирус?
Выберите один из 4 вариантов ответа:
1) Разновидность программ, которые способны к размножению
2) Разновидность программ, которые самоуничтожаются
3) Разновидность программ, которые не работают
4) Разновидность программ, которые плохо работают
Задание №51
Вопрос:
Как подразделяются вирусы в зависимости от деструктивных возможностей?
Выберите один из 4 вариантов ответа:
1) Сетевые, файловые, загрузочные, комбинированные
2) Безвредные, неопасные, опасные, очень опасные
3) Резидентные, нерезидентные
4) Полиморфные, макровирусы, вирусы-невидимки, "паразитические", "студенческие", "черви", компаньон-вирусы
Задание №52
Вопрос:
Нежелательная цепочка носителей информации, один или несколько из которых являются правонарушителем или его специальной аппаратурой называется
Запишите ответ:

Задание №53
Вопрос:
Установите соответствие
Укажите соответствие для всех 4 вариантов ответа:
1) это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок
2) это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов
3) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей
4) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии
__ защита информации от утечки по акустическому каналу
Защита информации от утечки по визуально-оптическому каналу
__ Защита информации от утечки по электромагнитным каналам
__ Защита информации от утечки по материально-вещественному каналу
Задание №54
Вопрос:
Надежным средством отвода наведенных сигналов на землю служит
Запишите ответ:

Задание №55
Вопрос:
Установите соответствие
Укажите соответствие для всех 2 вариантов ответа:
1) наука о скрытой передаче информации путем сохранения в тайне самого факта передачи
2) наука скрывающая содержимое секретного сообщения
__ стеганография
__ криптография