

Частное образовательное учреждение высшего образования  
«САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ ТЕХНОЛОГИЙ  
УПРАВЛЕНИЯ И ЭКОНОМИКИ»

---

РАССМОТРЕНО И ОДОБРЕНО

На заседании кафедры информаци-  
онных технологий и математики  
Протокол № 9 от 25.05.2023

УТВЕРЖДАЮ

Первый проректор  
Авдашкевич С.В.  
28.06.2023

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина:	Б1.В.ДВ.02.02 Информационная безопасность и защита информации
Направление подготовки:	38.03.02 Менеджмент
Направленность (профиль):	«Маркетинг»
Уровень высшего образования:	Бакалавриат
Программа:	Прикладного бакалавриата
Форма обучения:	Очная, заочная
Разработчики:	Кандидат экономических наук, доцент Удахина С.В.

### 1. Цели и задачи дисциплины:

Цель дисциплины: формирование у студентов методически правильных основ знаний и практических навыков по основам информационной безопасности (ИБ), необходимых выпускникам университета, занимающимся эксплуатацией корпоративных информационных систем. Дисциплина является важной составной частью теоретической подготовки бакалавра и занимает существенное место в его будущей практической деятельности.

Задачи дисциплины:

- получение студентами необходимых для их работы теоретических знаний о современных средствах, методах и технологиях обеспечения информационной безопасности корпоративных информационных систем;
- формирование у студентов практических навыков организации работ по обеспечению основ информационной безопасности и защиты информации на предприятиях.

### 2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы высшего образования

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код компетенции	Содержание компетенции
ОПК-7	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК-11	владением навыками анализа информации о функционировании системы внутреннего документооборота организации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов

Планируемые результаты обучения:

Код компетенции	Основные признаки освоения		
	Знать	Уметь	Владеть
ОПК-7	<ul style="list-style-type: none"> <li>- основные угрозы и методы обеспечения информационной безопасности;</li> <li>- основные методики, направленные на обеспечение информационной безопасности на различных направлениях деятельности современного предприятия;</li> <li>- перспективы развития технологий обеспечения информационной безопасности.</li> </ul>	<ul style="list-style-type: none"> <li>- анализировать и выбирать адекватные модели информационной безопасности, планировать их реализацию на базе требований к современному уровню ИБ;</li> <li>- ориентироваться в инфраструктуре проекта по разработке и внедрению средств обеспечения информационной безопасности;</li> <li>- формулировать задачи по обеспечению ИБ, исходя из поставленных целей.</li> </ul>	<ul style="list-style-type: none"> <li>- навыками анализа информационной безопасности;</li> <li>- навыками работы с современными информационными системами и средствами обеспечения их информационной безопасности;</li> <li>- приемами анализа степени выполнения задач по обеспечению информационной безопасности.</li> </ul>
ПК-11	<ul style="list-style-type: none"> <li>- способы анализа информации о функционировании системы внутреннего документооборота организации;</li> <li>- основы и средства формирования информационного обеспечения участников ор-</li> </ul>	<ul style="list-style-type: none"> <li>- оценивать функционирование системы внутреннего документооборота организации;</li> <li>- анализировать состояние информационного обеспечения участников организационных проектов и применять</li> </ul>	<ul style="list-style-type: none"> <li>- навыками анализа информации о функционировании системы внутреннего документооборота организации;</li> <li>- навыками ведения баз данных по различным показателям и формирования ин-</li> </ul>

38.03.02 Менеджмент, направленность «Маркетинг»  
 Программа прикладного бакалавриата  
 Рабочая программа дисциплины  
 Дисциплина: Б1.В.ДВ.02.02 Информационная безопасность и защита информации  
 Форма обучения: очная, заочная  
 Разработана для приема 2019/2020, 2020/2021 учебного года  
 Обновлено на 2023/2024 учебный год

	ганизационных проектов.	средства по его формирова- нию.	формационного обеспече- ния участников организаци- онных проектов.
--	-------------------------	------------------------------------	--

### 3. Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность и защита информации» входит в Блок 1 «Дисциплины (модуля)» (Вариативная часть) образовательной программы высшего образования по направлению 38.03.02 Менеджмент направленность (профиль) «Маркетинг».

*При изучении данной дисциплины обучающийся использует знания, умения и навыки, которые формируются в процессе изучения следующих дисциплин (практик):*

Информатика, Информационные технологии в менеджменте, Основы информационной культуры

*Знания, умения и навыки, приобретенные в процессе изучения данной дисциплины, будут использованы обучающимся при изучении дисциплин (практик):*

Информационные системы в маркетинге, Производственная практика: технологическая практика, Производственная практика: преддипломная практика

### 4. Объем дисциплины

*Очная форма обучения:*

Вид учебной работы	Всего часов	Семестр
		2
<b>Аудиторные занятия (АЗ):</b>	54	54
В том числе:		
Лекционные занятия (Лек)	18	18
Лабораторные занятия (Лаб)	0	0
Практические занятия (Пр)	36	36
<b>Самостоятельная работа студента (СР)</b>	49	49
В том числе:		
Курсовая работа	0	
Другие виды самостоятельной работы*	49	49
<b>Контроль самостоятельной работы (КСР)</b>	5	5
<b>Контактная работа (КоР)</b>	59	59
<b>Форма промежуточной аттестации</b>		Экзамен
<b>Подготовка к экзамену и сдача экзамена (СР, КоР)</b>	36	36
<b>Общая трудоемкость дисциплины, часы/ЗЕТ</b>	144/4	144/4

\* - подготовка к аудиторным занятиям, подготовка к зачету (при наличии)..

*Заочная форма обучения:*

Вид учебной работы	Всего часов	Курс
		1
<b>Аудиторные занятия (АЗ):</b>	8	8
В том числе:		
Лекционные занятия (Лек)	4	4
Лабораторные занятия (Лаб)	0	0
Практические занятия (Пр)	4	4
<b>Самостоятельная работа студента (СР)</b>	123	123

38.03.02 Менеджмент, направленность «Маркетинг»  
 Программа прикладного бакалавриата  
 Рабочая программа дисциплины  
 Дисциплина: Б1.В.ДВ.02.02 Информационная безопасность и защита информации  
 Форма обучения: очная, заочная  
 Разработана для приема 2019/2020, 2020/2021 учебного года  
 Обновлено на 2023/2024 учебный год

В том числе:		
Курсовая работа	0	
Другие виды самостоятельной работы*	123	123
<b>Контроль самостоятельной работы (КСР)</b>	4	4
<b>Контактная работа (КоР)</b>	12	12
<b>Форма промежуточной аттестации</b>		Экзамен
<b>Подготовка к экзамену/зачету и сдача экзамена/зачета (СР, КоР)</b>	9	9
<b>Общая трудоемкость дисциплины, часы/ЗЕТ</b>	144/4	144/4

\* - подготовка к аудиторным занятиям.

## 5. Содержание дисциплины

*Очная форма обучения:*

№ п/п	Наименование темы дисциплины	Семестр/ Курс	Количество учебных часов				СР	Практическая подготовка*
			В том числе по видам аудиторных занятий					
			Лек	Пр	Лаб			
1	Основные направления формирования информационной безопасности современного предприятия.	2	4	8	0	12	8	
2	Защищенная информационная система. Уровни и структура информационной безопасности.	2	4	8	0	12	8	
3	Модели и стандарты в сфере информационной безопасности и управления рисками информационной безопасности.	2	4	10	0	12	10	
4	Технологии и методы обеспечения информационной безопасности. Комплексная защита информационных систем.	2	6	10	0	13	10	
Итого:			18	36	0	49	36	

\* Практическая подготовка при реализации дисциплин организована путем проведения практических занятий и (или) выполнения лабораторных и (или) курсовых работ и предусматривает выполнение работ, связанных с будущей профессиональной деятельностью.

*Заочная форма обучения:*

№ п/п	Наименование темы дисциплины	Семестр/ Курс	Количество учебных часов				СР	Практическая подготовка*
			В том числе по видам аудиторных занятий					
			Лек	Пр	Лаб			
1	Основные направления формирования информационной безопасности современного предприятия.	1	2	0	0	31	8	
2	Защищенная информационная система. Уровни и структура информационной безопасности.	1	2	2	0	31	8	
3	Модели и стандарты в сфере информационной безопасности и управления рисками информационной безопасности.	1	0	2	0	31	10	
4	Технологии и методы обеспечения информационной безопасности. Комплексная защита информационных систем.	1	0	0	0	30	10	
Итого:			4	4	0	123	36	

\* Практическая подготовка при реализации дисциплин организована путем проведения практических занятий и (или) выполнения лабораторных и (или) курсовых работ и (или) путем выделения часов из часов, отведен-

38.03.02 Менеджмент, направленность «Маркетинг»  
 Программа прикладного бакалавриата  
 Рабочая программа дисциплины  
 Дисциплина: Б1.В.ДВ.02.02 Информационная безопасность и защита информации  
 Форма обучения: очная, заочная  
 Разработана для приема 2019/2020, 2020/2021 учебного года  
 Обновлено на 2023/2024 учебный год

ных на самостоятельную работу, и предусматривает выполнение работ, связанных с будущей профессиональной деятельностью.

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия обучающихся, курсовая работа	Компетенции	Оценочное средство текущего контроля
1	2	3	4
Тема 1: Основные направления формирования информационной безопасности современного предприятия.	<p>Предпосылки становления предметной области информационной безопасности. Ключевые вопросы информационной безопасности. Концепция информационной безопасности Российской Федерации. Разработка корпоративной концепции информационной безопасности</p> <p>Правовые аспекты информационной безопасности. Международное и российское законодательство в сфере информационной безопасности</p> <p><b>Практические занятия/ Самостоятельная работа</b> Основные вопросы информационной безопасности.</p> <p>Международное законодательство в сфере информационной безопасности.</p> <p>Корпоративная концепция информационной безопасности.</p> <p><b>Лабораторная работа: -</b></p>	ОПК-7,ПК-11	Тестирование №1; Контрольная работа №1
Тема 2: Защищенная информационная система. Уровни и структура информационной безопасности.	<p>Виды защищаемой информации. Модель угроз и модель информационной безопасности</p> <p>Понятие защищенной информационной системы.</p> <p>Программа информационной безопасности</p> <p>Организационно-распорядительные документы в сфере информационной безопасности.</p> <p>Политика информационной безопасности.</p> <p><b>Практические занятия/ Самостоятельная работа</b> Модели угроз и информационной безопасности.</p> <p>Программа и политика информационной безопасности на международном рынке.</p> <p><b>Лабораторная работа: -</b></p>	ОПК-7,ПК-11	Тестирование №1; Коллоквиум №1
Тема 3: Модели и стандарты в сфере информационной безопасности и управления рисками информационной безопасности.	<p>Управление информационными рисками.</p> <p>Стандартизация в сфере информационной безопасности.</p> <p><b>Практические занятия/ Самостоятельная работа</b> Управление информационными рисками в области международных финансов.</p> <p><b>Лабораторная работа: -</b></p>	ОПК-7,ПК-11	Тестирование №1; Коллоквиум №2
Тема 4: Технологии и методы	Защита информационной инфраструктуры от атак. Антивирусные средства защиты.	ОПК-7,ПК-11	Рефераты №1

38.03.02 Менеджмент, направленность «Маркетинг»  
 Программа прикладного бакалавриата  
 Рабочая программа дисциплины  
 Дисциплина: Б1.В.ДВ.02.02 Информационная безопасность и защита информации  
 Форма обучения: очная, заочная  
 Разработана для приема 2019/2020, 2020/2021 учебного года  
 Обновлено на 2023/2024 учебный год

обеспечения информационной безопасности. Комплексная защита информационных систем.	Оценка эффективности средств защиты информации. <b>Практические занятия/ Самостоятельная работа</b> Антивирусные средства защиты информационной безопасности. Комплексная защита информационной инфраструктуры и ресурсов в сфере международных финансов. <b>Лабораторная работа: -</b>		
Курсовая работа	Не предусмотрено учебным планом		

### 6. Формы проведения занятий

При реализации дисциплины применяются инновационные формы учебных занятий, развивающих у обучающихся навыки командной работы, межличностной коммуникации, принятия решений, лидерские качества.

*Очная форма обучения:*

№ п/п	Наименование темы/ лекционного (практического) занятия	Тип занятия	Кол-во часов	Форма проведения занятий
1	Защищенная информационная система. Уровни и структура информационной безопасности.: Модели угроз и информационной безопасности. Программа и политика информационной безопасности на международном рынке.	Пр	8	Дискуссия
2	Модели и стандарты в сфере информационной безопасности и управления рисками информационной безопасности.: Управление информационными рисками в области международных финансов.	Пр	10	Деловая игра

*Заочная форма обучения:*

№ п/п	Наименование темы/ лекционного (практического) занятия	Тип занятия	Кол-во часов	Форма проведения занятий
1	Защищенная информационная система. Уровни и структура информационной безопасности.: Модели угроз и информационной безопасности. Программа и политика информационной безопасности на международном рынке.	Пр	2	Дискуссия
2	Модели и стандарты в сфере информационной безопасности и управления рисками информационной безопасности.: Управление информационными рисками в области международных финансов.	Пр	2	Деловая игра

### 7. Способ реализации дисциплины

Без использования онлайн-курса.

### 8. Учебно-методическое обеспечение дисциплины:

*Основная литература:*

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2023. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт].

38.03.02 Менеджмент, направленность «Маркетинг»  
Программа прикладного бакалавриата  
Рабочая программа дисциплины  
Дисциплина: Б1.В.ДВ.02.02 Информационная безопасность и защита информации  
Форма обучения: очная, заочная  
Разработана для приема 2019/2020, 2020/2021 учебного года  
Обновлена на 2023/2024 учебный год

---

— URL: <https://urait.ru/bcode/519780>

2. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/495922>

3. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/511998>

#### *Дополнительная литература:*

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/490277>

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/498844>

3. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2023. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/520063>

### **9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения**

1. Операционная система
2. Пакет прикладных офисных программ
3. Антивирусное программное обеспечение
4. Oracle VM Virtualbox

Дополнительно при применении электронного обучения, дистанционных образовательных технологий используются:

1. LMS Moodle.
2. Вебинарная платформа

### **10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», информационных справочных систем и профессиональных баз данных, необходимых для освоения дисциплины**

1. [ibooks.ru](http://ibooks.ru) : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: <https://ibooks.ru>. - Текст: электронный

2. Электронно-библиотечная система СПбУТУиЭ : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: <http://libume.ru>. - Текст: электронный

3. Юрайт : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: <https://urait.ru>. - Текст: электронный

4. [eLibrary.ru](http://eLibrary.ru) : научная электронная библиотека [Электронный ресурс] : профессиональ-

38.03.02 Менеджмент, направленность «Маркетинг»  
Программа прикладного бакалавриата  
Рабочая программа дисциплины  
Дисциплина: Б1.В.ДВ.02.02 Информационная безопасность и защита информации  
Форма обучения: очная, заочная  
Разработана для приема 2019/2020, 2020/2021 учебного года  
Обновлена на 2023/2024 учебный год

---

ная база данных. - Режим доступа: <http://elibrary.ru>. - Текст: электронный

5. Архив научных журналов НЭИКОН [Электронный ресурс] : профессиональная база данных. - Режим доступа: [arhiv.neicon.ru](http://arhiv.neicon.ru). - Текст: электронный

6. КиберЛенинка : научная электронная библиотека [Электронный ресурс] : информационная справочная система. - Режим доступа: <http://cyberleninka.ru>. - Текст: электронный

7.Лань : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: <https://e.lanbook.com>. - Текст: электронный

8. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс] : профессиональная база данных. - Режим доступа: <https://rkn.gov.ru/>. - Текст: электронный

9. it-world.ru [Электронный ресурс] : информационная справочная система. - Режим доступа: <https://www.it-world.ru/>. - Текст: электронный

10. Бизнес-информатика [Электронный ресурс] : информационная справочная система. - Режим доступа: <https://bijournal.hse.ru/>. - Текст: электронный

### **11. Материально-техническое обеспечение дисциплины**

Учебные аудитории для проведения занятий лекционного типа, семинарского типа - практических занятий, для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оборудованные: рабочими местами для обучающихся, оснащенными специальной мебелью; рабочим местом преподавателя, оснащенного специальной мебелью, персональным компьютером с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета, программным обеспечением; техническими средствами обучения - мультимедийным оборудованием (проектор, экран, колонки) и маркерной доской.

Учебная аудитория для проведения занятий семинарского типа - практических занятий – компьютерный класс, оборудованный рабочими местами для обучающихся, оснащенными специальной мебелью, персональными компьютерами с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета, программным обеспечением; рабочим местом преподавателя, оснащенного специальной мебелью, персональным компьютером с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета, программным обеспечением; техническими средствами обучения - мультимедийным оборудованием (проектор, экран, колонки) и маркерной доской.

Помещение для самостоятельной работы, оборудованное специальной мебелью, персональными компьютерами с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета, программным обеспечением.

При применении электронного обучения, дистанционных образовательных технологий используются: виртуальные аналоги учебных аудиторий - вебинарные комнаты на вебинарных платформах, рабочее место преподавателя, оснащенное персональным компьютером (планшет, мобильное устройство) с возможностью подключения к сети «Интернет», доступом к электронной информационно-образовательной среде Университета и к информационно-образовательному portalу Университета [imeos.ru](http://imeos.ru), веб-камерой, микрофоном и гарнитурой (в т.ч. интегрированными в устройствами), программным обеспечением; рабочее место обучающегося оснащено персональным компьютером (планшет, мобильное устройство) с возможностью подключения к сети «Интернет», доступом к электронной информационно-образовательной среде Университета и к информационно-образовательному portalу Университета [imeos.ru](http://imeos.ru), веб-камерой, микрофоном и гарнитурой (в т.ч. интегрированными в устройства),



38.03.02 Менеджмент, направленность «Маркетинг»  
 Программа прикладного бакалавриата  
 Рабочая программа дисциплины  
 Дисциплина: Б1.В.ДВ.02.02 Информационная безопасность и защита информации  
 Форма обучения: очная, заочная  
 Разработана для приема 2019/2020, 2020/2021 учебного года  
 Обновлено на 2023/2024 учебный год

программным обеспечением. Авторизация на информационно-образовательном портале Университета [umeos.ru](http://umeos.ru) и начало работы осуществляются с использованием персональной учетной записи (логина и пароля).

## 12. Оценочные материалы по дисциплине

### 1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

*Очная форма обучения:*

Код компетенции	Название дисциплины	Форма промежуточной аттестации	Семестр/курс	Этап формирования компетенции
ОПК-7	Информатика	экзамен	1	1
ОПК-7	Информационные технологии в менеджменте	экзамен	2	2
ОПК-7	Основы информационной культуры	экзамен	2	2
ОПК-7	Информационная безопасность и защита информации			
ОПК-7	Информационные системы в маркетинге	экзамен	6	3
ПК-11	Информатика	экзамен	1	1
ПК-11	Информационные технологии в менеджменте	экзамен	2	2
ПК-11	Основы информационной культуры	экзамен	2	2
ПК-11	Информационная безопасность и защита информации			
ПК-11	Информационные системы в маркетинге	экзамен	6	3
ПК-11	Производственная практика: технологическая практика	зачет с оценкой	8	4
ПК-11	Производственная практика: преддипломная практика	зачет с оценкой	8	4

*Заочная форма обучения:*

Код компетенции	Название дисциплины	Форма промежуточной аттестации	Семестр/курс	Этап формирования компетенции
ОПК-7	Основы информационной культуры	экзамен	1	1
ОПК-7	Информационная безопасность и защита информации			
ОПК-7	Информатика	экзамен	2	2
ОПК-7	Информационные технологии в менеджменте	экзамен	3	3
ОПК-7	Информационные системы в маркетинге	экзамен	4	4
ПК-11	Основы информационной культуры	экзамен	1	1
ПК-11	Информационная безопасность и защита информации			
ПК-11	Информатика	экзамен	2	2
ПК-11	Информационные технологии в менеджменте	экзамен	3	3
ПК-11	Информационные системы в маркетинге	экзамен	4	4
ПК-11	Производственная практика: технологическая практика	зачет с оценкой	5	5
ПК-11	Производственная практика: преддипломная практика	зачет с оценкой	5	5

### 2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования в процессе изучения дисциплины, описание шкал оценивания

## 2.1 Текущий контроль

### ТЕСТИРОВАНИЕ

Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.

Выполнение теста оценивается по следующим показателям:

- Правильность выполнения заданий теста за отведенный промежуток времени.

#### Критерии и шкала оценивания теста

Выполнение заданий теста оценивается по единой схеме, основанной на вычислении коэффициента результативности (КР) учебных достижений. Для этого подсчитывается количество правильных ответов к заданиям теста (А), при этом каждое тестовое задание оценивается в бинарной шкале «правильно – не правильно». Далее фиксируется максимальное количество заданий данного теста (А<sub>max</sub>).

Величина коэффициента результативности учебных достижений студентов в рамках тестирования вычисляется по следующей формуле:  $KP = A / A_{max}$  (значения КР изменяются в пределах от 0 до 1).

<b>Коэффициент результативности (КР)</b>	КР < 0,4	0,4 ≤ КР < 0,6	0,6 ≤ КР ≤ 0,8	0,8 < КР ≤ 1
<b>Баллы в БРС университета</b>	0	6	8	10
<b>Уровень сформированности компетенций</b>	Не сформирована	Пороговый	Высокий	Повышенный

### КОЛЛОКВИУМ

Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.

Коллоквиум оценивается по следующим показателям:

1. Глубокое и прочное усвоение программного материала;
2. Полные, последовательные, грамотные и логически излагаемые ответы при видоизменении задания;
3. Владение разносторонними навыками и приемами выполнения практических работ;
4. Владение профессиональной терминологией;
5. Полный конспект лекционных материалов.

#### Критерии оценивания коллоквиума

Студент полностью раскрыл содержание материала в объеме, предусмотренном программой, изложил материал грамотным языком в определенной логической последовательности, точно используя терминологию и символику; продемонстрировал сформированность и устойчивость полученных знаний. Возможны одна-две неточности при ответе на дополнительные вопросы, которые студент легко исправил по замечанию преподавателя.	20 баллов
Ответ студента имеет один из недостатков: в изложении вопроса допущены небольшие пробелы, не исказившие содержание ответа; допущены один-два недочета при освещении основного содержания ответа, не исправленные по замечанию преподавателя; допущены ошибка или более двух недочетов при освещении дополнительных вопросов, легко исправленные по замеча-	15 баллов

38.03.02 Менеджмент, направленность «Маркетинг»  
 Программа прикладного бакалавриата  
 Рабочая программа дисциплины  
 Дисциплина: Б1.В.ДВ.02.02 Информационная безопасность и защита информации  
 Форма обучения: очная, заочная  
 Разработана для приема 2019/2020, 2020/2021 учебного года  
 Обновлено на 2023/2024 учебный год

нию преподавателя.	
Студент неполно раскрыл содержание вопроса, но показал общее понимание материала и продемонстрировал умения, достаточные для дальнейшего усвоения программного материала; имеет затруднения или допустил ошибки в определении понятий, использовании терминологии и исправил их после нескольких наводящих вопросов преподавателя.	10 баллов
Студент обнаружил полное незнание и непонимание изучаемого учебного материала по дисциплине или не смог ответить ни на один из дополнительных вопросов по изучаемому материалу.	0 баллов

### Шкала оценивания коллоквиума

Зависимость баллов и уровня сформированности компетенции на данном этапе изучения дисциплины представлены в следующей таблице:

<b>Баллы в БРС Университета</b>	20	15	10	0
<b>Уровень сформированности компетенции</b>	Повышенный	Высокий	Пороговый	Не сформированы

### КОНТРОЛЬНАЯ РАБОТА

Самостоятельная письменная аналитическая работа студента, которая способствует закреплению и систематизации знаний по одной или нескольким темам дисциплины. Цель контрольной работы – получить специальные знания и продемонстрировать навыки их практического применения.

Контрольная работа оценивается по следующим показателям:

1. Выполнение работы в полном объеме и без ошибок;
2. Зрелая, творческая, полностью самостоятельная работа;
3. Выполнение работы в соответствии с требованиями к оформлению.

### Критерии оценивания контрольной работы

Полное, правильное и обоснованное решение; полностью самостоятельная работа; работа выполнена в соответствии с требованиями к оформлению	10 баллов
Решение в целом правильное и обоснованное, но допущены незначительные ошибки либо решение является неполным, допускается незначительная подсказка со стороны преподавателя; работа выполнена в соответствии с требованиями к оформлению	8 баллов
Решение содержит обоснование, ход рассуждений в целом верный, но при этом допущены существенные ошибки, студент продемонстрировал недостаточное умение правильно применять знания, полученные в процессе изучения дисциплины, либо работа выполнена при существенной помощи преподавателя; работа выполнена с некоторыми нарушениями требований к оформлению	6 баллов
Отсутствует решение задачи, либо отсутствует обоснование решения, либо решение содержит обоснование, но допущены грубые ошибки, приведшие к абсолютно неверной квалификации; работа выполнена без учета требований к оформлению	0 баллов

### Шкала оценивания контрольной работы

Зависимость баллов и уровня сформированности компетенций на данном этапе изучения дисциплины представлены в следующей таблице:

<b>Баллы в БРС Университета</b>	10	8	6	0
<b>Уровень сформированности компетенции</b>	Повышенный	Высокий	Пороговый	Не сформированы

### РЕФЕРАТ

38.03.02 Менеджмент, направленность «Маркетинг»  
 Программа прикладного бакалавриата  
 Рабочая программа дисциплины  
 Дисциплина: Б1.В.ДВ.02.02 Информационная безопасность и защита информации  
 Форма обучения: очная, заочная  
 Разработана для приема 2019/2020, 2020/2021 учебного года  
 Обновлено на 2023/2024 учебный год

Самостоятельная письменная аналитическая работа, выполняемая на основе преобразования документальной информации и раскрывающая суть изучаемой темы; представляет собой краткое изложение содержания книги, научной работы, результатов изучения научной проблемы важного социально-культурного, народнохозяйственного или политического значения. Реферат отражает различные точки зрения на исследуемый вопрос, в том числе точку зрения самого автора.

### Показатели и критерии оценивания реферата

№ п/п	Показатели оценки	Критерии оценивания
1	<b>Новизна текста</b> (актуальность темы исследования; новизна и самостоятельность в постановке проблемы, формулирование нового аспекта известной проблемы в установлении новых связей (межпредметных, внутрипредметных, интеграционных); умение работать с исследованиями, критической литературой, систематизировать и структурировать материал; самостоятельность оценок и суждений).	Каждый из предложенных показателей оценивается по критерию « <b>выполнен - частично выполнен - не выполнен</b> », что соответствует следующему распределению баллов « <b>2 балла - 1 балл - 0 баллов</b> »
2	<b>Степень раскрытия сущности вопроса</b> (соответствие плана теме реферата; соответствие содержания теме и плану реферата; полнота и глубина знаний по теме; умение обобщать, делать выводы, сопоставлять различные точки зрения по одному проблеме).	
3	<b>Обоснованность выбора источников</b> (оценка использованной литературы: привлечены ли наиболее известные работы по теме исследования, в т.ч. журнальные публикации последних лет, последние статистические данные, сводки, справки и т.д.).	
4	<b>Соблюдение требований к оформлению</b> (насколько верно оформлены ссылки на используемую литературу, список литературы; оценка грамотности и культуры изложения, в т.ч. орфографической, пунктуационной, стилистической культуры, владение терминологией; соблюдение требований к объёму реферата).	
5	<b>Ответы на дополнительные вопросы</b>	

### Шкала оценивания реферата

Зависимость баллов и уровня сформированности компетенции на данном этапе изучения дисциплины за реферат представлены в следующей таблице:

Баллы в БРС Университета	10-9	8-7	6-5	Менее 5
Уровень сформированности компетенции	Повышенный	Высокий	Пороговый	Не сформированы

#### 2.2 Курсовая работа

Не предусмотрено учебным планом.

#### 2.3 Промежуточная аттестация в форме зачета

Не предусмотрено учебным планом.

#### 2.4 Промежуточная аттестация в форме экзамена

Экзамен проводится в форме группового бланкового тестирования (письменный экзамен). Процедура проведения экзамена изложена в «Положении о текущем контроле успеваемости, промежуточной аттестации и балльно-рейтинговой системе оценки учебных достижений студентов».

Выполнение теста оценивается по следующим показателям:

38.03.02 Менеджмент, направленность «Маркетинг»  
 Программа прикладного бакалавриата  
 Рабочая программа дисциплины  
 Дисциплина: Б1.В.ДВ.02.02 Информационная безопасность и защита информации  
 Форма обучения: очная, заочная  
 Разработана для приема 2019/2020, 2020/2021 учебного года  
 Обновлено на 2023/2024 учебный год

- Правильность выполнения заданий теста за отведенный промежуток времени.

### Критерии и шкала оценивания теста

Выполнение заданий теста оценивается по единой схеме, основанной на вычислении коэффициента результативности (КР) учебных достижений. Для этого подсчитывается количество правильных ответов к заданиям теста (А), при этом каждое тестовое задание оценивается в бинарной шкале «правильно – не правильно». Далее фиксируется максимальное количество заданий данного теста (А<sub>max</sub>).

Величина коэффициента результативности учебных достижений студентов в рамках тестирования вычисляется по следующей формуле:  $KP = A / A_{max}$  (значения КР изменяются в пределах от 0 до 1).

<b>Коэффициент результативности (КР)</b>	$KP < 0,4$	$0,4 \leq KP < 0,6$	$0,6 \leq KP \leq 0,8$	$0,8 < KP \leq 1$
<b>Баллы в БРС университета</b>	0	18	24	30
<b>Уровень сформированности компетенций</b>	Не сформирована	Пороговый	Высокий	Повышенный

<b>Баллы по дисциплине*</b>	60 и менее		61-73		74-90		91-100
<b>Итоговая оценка по дисциплине*</b>	Неудовлетворительно		Удовлетворительно		Хорошо		Отлично
<b>Баллы в международной шкале ECTS с буквенным обозначением уровня</b>	<50	51-60	61-67	68-73	74-83	84-90	91-100
	F	Fx	E	D	C	B	A
<b>Уровень сформированности компетенций</b>	Не сформированы		Пороговый		Высокий		Повышенный

\*Оценка, полученная студентом за промежуточную аттестацию, выставляется с учетом баллов, полученных за текущий контроль (сумма баллов за экзамен и текущий контроль).

### 2.5 Описание показателей и критериев оценивания компетенций, сформированных дисциплиной

После выполнения студентом всех видов оценочных средств, указанных в рабочей программе дисциплины, производится оценка уровня сформированности компетенций по дисциплине:

Код компетенции	Уровень сформированности компетенции	Основные признаки освоения компетенций		
		Знать	Уметь	Владеть

38.03.02 Менеджмент, направленность «Маркетинг»  
 Программа прикладного бакалавриата  
 Рабочая программа дисциплины  
 Дисциплина: Б1.В.ДВ.02.02 Информационная безопасность и защита информации  
 Форма обучения: очная, заочная  
 Разработана для приема 2019/2020, 2020/2021 учебного года  
 Обновлено на 2023/2024 учебный год

ОПК-7	Пороговый	<ul style="list-style-type: none"> <li>- основные понятия и определения, используемые при изучении дисциплины;</li> <li>- законодательную и нормативную базу информационной безопасности;</li> <li>- иметь представление о значении информационной безопасности для современного предприятия.</li> </ul>	<ul style="list-style-type: none"> <li>- анализировать и выбирать адекватные модели информационной безопасности;</li> <li>- ориентироваться в инфраструктуре проекта по разработке и внедрению средств обеспечения информационной безопасности;</li> <li>- оценивать состояние организационной защиты информации.</li> </ul>	<ul style="list-style-type: none"> <li>- приемами реализации мероприятий по обеспечению на предприятии (в организации) деятельности в области защиты информации;</li> <li>- навыками работы с современными информационными системами и средствами обеспечения их информационной безопасности.</li> </ul>
	Высокий	<ul style="list-style-type: none"> <li>- основные виды и источники угроз информации в компьютерных сетях;</li> <li>- основные направления формирования информационной безопасности современного предприятия;</li> <li>- модели и стандарты в сфере информационной безопасности;</li> <li>- перспективы развития технологий обеспечения информационной безопасности.</li> </ul>	<ul style="list-style-type: none"> <li>- классифицировать основные угрозы безопасности информации;</li> <li>- анализировать и выбирать адекватные модели информационной безопасности;</li> <li>- ориентироваться в инфраструктуре проекта по разработке и внедрению средств обеспечения информационной безопасности.</li> </ul>	<ul style="list-style-type: none"> <li>- навыками анализа информационной безопасности;</li> <li>- навыками работы с современными информационными системами и средствами обеспечения их информационной безопасности.</li> </ul>
	Повышенный	<ul style="list-style-type: none"> <li>- основные угрозы и методы обеспечения информационной безопасности;</li> <li>- основные методики, направленные на обеспечение информационной безопасности на различных направлениях деятельности современного предприятия;</li> <li>- перспективы развития технологий обеспечения информационной безопасности.</li> </ul>	<ul style="list-style-type: none"> <li>- анализировать и выбирать адекватные модели информационной безопасности, планировать их реализацию на базе требований к современному уровню ИБ;</li> <li>- ориентироваться в инфраструктуре проекта по разработке и внедрению средств обеспечения информационной безопасности;</li> <li>- формулировать задачи по обеспечению ИБ, исходя из поставленных целей.</li> </ul>	<ul style="list-style-type: none"> <li>- навыками анализа информационной безопасности;</li> <li>- навыками работы с современными информационными системами и средствами обеспечения их информационной безопасности;</li> <li>- приемами анализа степени выполнения задач по обеспечению информационной безопасности.</li> </ul>
ПК-11	Пороговый	<ul style="list-style-type: none"> <li>- основные понятия и принципы функционирования системы внутреннего документооборота организации;</li> <li>- основы формирования информационного обеспечения участников организационных проектов.</li> </ul>	<ul style="list-style-type: none"> <li>- проводить анализ информации о состоянии системы внутреннего документооборота организации;</li> <li>- оценивать состояние информационного обеспечения участников организационных проектов.</li> </ul>	<ul style="list-style-type: none"> <li>- навыками анализа информации об отдельных сторонах функционирования системы внутреннего документооборота организации;</li> <li>- приемами организации информационного обеспечения участников организационных проектов.</li> </ul>

38.03.02 Менеджмент, направленность «Маркетинг»  
 Программа прикладного бакалавриата  
 Рабочая программа дисциплины  
 Дисциплина: Б1.В.ДВ.02.02 Информационная безопасность и защита информации  
 Форма обучения: очная, заочная  
 Разработана для приема 2019/2020, 2020/2021 учебного года  
 Обновлено на 2023/2024 учебный год

	Высокий	- способы анализа информации об отдельных сторонах функционирования системы внутреннего документооборота организации; - основы формирования информационного обеспечения участников организационных проектов.	- проводить анализ информации о функционировании системы внутреннего документооборота организации; - оценивать состояние информационного обеспечения участников организационных проектов.	- навыками анализа информации о функционировании системы внутреннего документооборота организации; - средствами формирования информационного обеспечения участников организационных проектов; - навыками ведения баз данных.
	Повышенный	- способы анализа информации о функционировании системы внутреннего документооборота организации; - основы и средства формирования информационного обеспечения участников организационных проектов.	- оценивать функционирование системы внутреннего документооборота организации; - анализировать состояние информационного обеспечения участников организационных проектов и применять средства по его формированию.	- навыками анализа информации о функционировании системы внутреннего документооборота организации; - навыками ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов.

### 3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

**Методика формирования оценки по дисциплине.** Успеваемость студента оценивается в баллах и состоит из:

- суммы баллов за выполнение заданий текущего контроля (обучающийся может получить в сумме не более 70 баллов);
- баллов за посещаемость (не более 10 баллов);
- баллов за активность на занятиях (занятия в интерактивной форме – п. 6. Формы проведения занятий), выполнение дополнительных заданий и пр. по усмотрению преподавателя, ведущего дисциплину – премиальные баллы (не более 20 баллов).

Полученные итоговые баллы по дисциплине переводятся в оценку по традиционной пятибалльной шкале оценивания и по 100-балльной шкале оценок Европейской системы перевода и накопления баллов (ECTS) в соответствии с таблицами, представленными в п.Таблицами. 1, 2. Оценки в пятибалльной шкале выставляются в ведомости и зачетные книжки, в 100-балльной – в ведомости.

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности приводятся в соответствующих методических материалах и локальных нормативных актах Университета (Положение «О текущем контроле успеваемости, промежуточной аттестации и балльно-рейтинговой системе оценки учебных достижений студентов», Положение «Об оценочных средствах», Положение «О контроле самостоятельности выполнения письменных работ обучающимися университета с использованием системы «Антиплагиат ВУЗ» и др.).

Уровень сформированности компетенции № 1 (№ N) определяется перечнем оценочных средств:

Оценочное средство (в том числе экзамен, зачет с оценкой при наличии)	Уровень сформированности компетенции*			Средний уровень сформированности компетенций по каждому оценочному средству
	Студент №1	...	Студент № N	

38.03.02 Менеджмент, направленность «Маркетинг»  
 Программа прикладного бакалавриата  
 Рабочая программа дисциплины  
 Дисциплина: Б1.В.ДВ.02.02 Информационная безопасность и защита информации  
 Форма обучения: очная, заочная  
 Разработана для приема 2019/2020, 2020/2021 учебного года  
 Обновлено на 2023/2024 учебный год

.....	.....			
<b>Итоговый уровень:</b>	.....			

\* пороговый, высокий или повышенный

Итоговый (общий/средний) уровень рассчитывается как среднее арифметическое с округлением в сторону более высокого уровня.

Далее делается вывод об общем уровне освоения компетенций студентами в ходе изучения дисциплины:

#### Оценочный лист по дисциплине

ФИО студента	Уровень сформированности компетенций								
	Общекультурные компетенции			Общепрофессиональные компетенции			Компетенции по видам деятельности		
	№ 1	№ N	Уровень сформированности общекультурных компетенций	№ 1	№ N	Уровень сформированности общепрофессиональных компетенций	№ 1	№ N	Уровень сформированности компетенций по виду деятельности № 1
Студент № 1									
Студент № 2									
.....									

4. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

#### Контрольная работа №1.

1. Естественные и искусственные угрозы безопасности информации. Уязвимости информационных систем.
2. Основные направления и способы защиты информации.
3. Понятия идентификации и аутентификации.
4. Требования к парольной защите.
5. Основные направления технической защиты информации.
6. Понятие технического канала утечки информации

#### Тематика рефератов №1

1. Классификация угроз информационной безопасности по базовым признакам.
2. Угрозы нарушения конфиденциальности.
3. Угрозы нарушения целостности данных.
4. Угрозы отказа служб (угрозы отказа в доступе).
5. Понятие политики безопасности информационных систем. Назначение политики безопас-



- ности.
6. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
  7. Законодательный уровень обеспечения информационной безопасности.
  8. Основные законодательные акты РФ в области защиты информации

### **Тематика вопросов к коллоквиуму №1**

#### *Основные вопросы*

1. Основные понятия и определения информационной безопасности. Виды информации ограниченного доступа.
2. Цели и задачи защиты информации.
3. Естественные и искусственные угрозы безопасности информации. Уязвимости информационных систем.
4. Основные направления и способы защиты информации.
5. Понятия идентификации и аутентификации.
6. Требования к парольной защите.
7. Основные направления технической защиты информации.
8. Понятие технического канала утечки информации.
9. Угрозы утечки информации по техническим каналам.
10. Характеристики объектов информатизации.
11. Побочные электромагнитные излучения и наводки.
12. Классификация технических каналов утечки информации.
13. Понятие политики безопасности организации.
14. Сертификация средств защиты информации.
15. Категорирование информационных объектов по степени важности и конфиденциальности защищаемой информации.

#### *Дополнительные вопросы*

1. Программы внутренней защиты. Программы ядра системы безопасности.
2. Интегральная безопасность информационных систем.
3. Комплексная защита объектов.
4. Механические системы защиты.
5. Системы оповещения.

### **Тематика вопросов к коллоквиуму №2.**

#### *Основные вопросы*

1. Аттестация объектов по выполнению требований обеспечения безопасности информации.
2. Основные разделы документов, характеризующих политику безопасности организации.
3. Задачи технических средств защиты информации.
4. Пассивные и активные средства и способы защиты информации.
5. Методы выявления закладочных устройств.
6. Устройства защиты телефонных переговоров. Генераторы пространственного зашумления.
7. Генераторы акустического и виброакустического зашумления.
8. Сетевые фильтры.
9. Подавители диктофонов.

### *Дополнительные вопросы*

1. Системы опознавания.
2. Основы физической защиты объектов.
3. Интегральный комплекс физической защиты объектов..

### **Тестирование №1.**

#### *Вариант 1*

- 1) Что входит в понятие “безопасность информации”
  - a) исключение ознакомления с информацией сотрудников АСОИ
  - b) предотвращение ознакомления с информацией лиц к ней не допущенных
  - c) исключение изменений информации
  - d) исключение утечки информации за счет излучений и наводок
- 2) Конфиденциальность информации обеспечивается путем
  - a) содержания критической информации в секрете
  - b) ограничения доступа в специальные помещения
  - c) организации мониторинга сети
- 3) Информационная безопасность информации достигается обеспечением
  - a) конфиденциальности
  - b) доступности
  - c) комплексирования средств ЗИ
  - d) целостности информации
- 4) Защита целостности потоков данных осуществляется с использованием
  - a) дополнительных форм нумерации
  - b) меток времени
  - c) повтором сообщений
  - d) включением дополнительных признаков к сообщению
- 5) Для обеспечения защиты от анализа трафика могут быть использованы
  - a) механизм заполнения текста
  - b) генерация фиктивных сообщений
  - c) ограничение доступа в выделенные помещения
- 6) Если сеть централизованная, то защита должна
  - a) централизованной
  - b) распределенной
- 7) При схеме управления защитой информации **“длинные руки”** полномочия пользователей на каждом компьютере устанавливаются
  - a) администратором удаленно со своего рабочего места
  - b) самим пользователем системы
  - c) пользователем системы после действий администратора безопасности
- 8) Схема отложенного централизованного управления доступом требует, чтобы компьютеры пользователей на момент изменения полномочий были
  - a) включены
  - b) выключены
  - c) безразлично
- 9) Для облегчения работы администратора безопасности по контролю за состоянием безопасности АС необходимо предусмотреть следующие возможности
  - a) селекцию определенных событий из системных журналов

- b) ограничение перечня событий, регистрируемых СЗИ
  - c) семантическое сжатие данных в журналах регистрации
  - d) автоматическую подготовку отчетных документов
- 10) Реальные возможности нарушителя определяются
- a) психологическим состоянием нарушителя
  - b) состоянием объекта защиты,
  - c) наличием потенциальных каналов утечки информации,
  - d) качеством средств защиты информации
- 11) В качестве показателя эффективности системы защиты информации может быть использованы
- a) вероятность обнаружения нарушения
  - b) своевременность реакции на каждый вид нарушения
  - c) доказуемость нарушения
- 12) Для осуществления несанкционированного доступа в информационную систему требуется провести подготовительные действия
- a) собрать сведения о системе
  - b) выполнить пробные попытки вхождения в систему
  - c) выявить организационную структуру предприятия
- 13) Программы ЦП характеризуются следующими параметрами
- a) криптостойкостью
  - b) количеством операторов
  - c) временем работы
  - d) функциональными возможностями
- 14) Время работы алгоритма ЦП складывается из времени
- a) набора текста
  - b) генерации ключей
  - c) проверки подписи
  - d) постановки подписи
- 15) С увеличением криптостойкости системы ЦП временные характеристики
- a) падают
  - b) увеличиваются

#### *Вариант 2*

- 1) Конечная цель защиты информации
- a) уменьшение возможных точек атак
  - b) сведение к минимуму потерь в управлении
  - c) формирование системы информационной безопасности
  - d) минимизация риска
- 2) Основные принципы построения системы защиты информации
- a) принцип совместимости средств защиты информации
  - b) принцип непрерывного совершенствования СЗИ
  - c) принцип открытости
  - d) принцип комплексного использования средств защиты
- 3) Принцип непрерывности совершенствования СЗИ заключается в
- a) постоянном контроле функционирования СЗИ
  - b) выявлении слабых мест в СЗИ
  - c) анализе рынка услуг в области защиты информации

- d) обновлении и дополнении механизма защиты
- 4) Вероятные угрозы техническому обеспечению
  - a) изменение конфигурации
  - b) изменение маршрутизации
  - c) физический съём информации с каналов
  - d) искажение входных данных
- 5) Вероятные угрозы информационному обеспечению
  - a) Съём и использование выходной информации
  - b) Подмена протоколов
  - c) Изменение топологии
  - d) Перегрузка канала или устройства
- 6) Вероятные угрозы прикладным программам
  - a) ознакомление и изменение программ решения
  - b) изменение прав и полномочий на доступ к ресурсам
  - c) искажение входных данных
- 7) Администратор безопасности
  - a) осуществляет эксплуатацию средств защиты информации
  - b) обеспечивает непрерывность процесса обработки информации
  - c) восстанавливает работоспособность компьютерной системы
  - d) осуществляет допуск в специальные помещения
- 8) В случае возникновения нарушения в компьютерной системе администратор безопасности
  - a) изменяет пароли пользователей
  - b) локализует нарушение
  - c) определяет причину возникновения нарушения
  - d) вызывает представителей МВД
- 9) Источники получения информации для администратора безопасности
  - a) от пользователей
  - b) из системного журнала
  - c) кадровых органов
- 10) Нарушитель это лицо, предпринявшее попытку выполнения запрещенных операций
  - a) по ошибке
  - b) незнанию
  - c) осознанно
  - d) с использованием служебного положения
- 11) Облик нарушителя по совершению противоправных действий определяется
  - a) мотивацией и намерениями,
  - b) совокупностью знаний, умений и навыков (способов) совершения нарушений
  - c) возможностями технических средств снятия информации
  - d) умением пользоваться средствами технической разведки
- 12) Реальные возможности нарушителя определяются
  - a) психологическим состоянием нарушителя
  - b) состоянием объекта защиты,
  - c) наличием потенциальных каналов утечки информации,
  - d) качеством средств защиты информации
- 13) Цифровая подпись это
  - a) полученная хэш-функция
  - b) хэш-функция, прошедшая математическую обработку

- с) электронная версия фактической подписи
- 14) Цифровая подпись может храниться
- вместе с документом
  - в отдельном файле
  - в закрытой области памяти
- 15) Проверка ЦП включает в себя проверку соотношения, связывающего
- хэш-функцию и подпись под документом
  - подпись под документом и открытый ключ
  - хэш-функцию и открытый ключ
  - хэш-функцию, подпись и открытый ключ

### Примерный перечень теоретических и практических заданий для экзамена

№	Задание	Варианты ответа	Кол-во баллов
1.	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее, это ...	а) Уязвимость проектирования б) Атака в) Угроза безопасности информации г) Тревога	1
2.	Не относится к уровням обеспечения информационной безопасности:	а) нормативно-правовой б) организационный в) социальный г) технический	1
3	Принцип, состоящий в том, что ни один сотрудник организации не должен иметь полномочий, позволяющих ему единолично выполнять критичные операции, называется ...	а) Непрерывность защиты б) Разделение функций в) Разумная достаточность г) Персональная ответственность	1
4	Не является сервисом безопасности:	а) экранирование б) управление доступом в) туннелирование г) кодирование	1
5	Комплекс предупредительных мер по обеспечению ИБ организации, включающий руководящие принципы, правила и процедуры в области безопасности, это ...	а) Программа безопасности б) Политика безопасности в) Кодекс безопасности г) Защита информации	1
6	Зашифровать слово БЕЗОПАСНОСТЬ перестановкой согласно таблице.	а) ПНАТЪСООЗЪЕС б) ПНАСБТООЗЪЕС	2

38.03.02 Менеджмент, направленность «Маркетинг»  
 Программа прикладного бакалавриата  
 Рабочая программа дисциплины  
 Дисциплина: Б1.В.ДВ.02.02 Информационная безопасность и защита информации  
 Форма обучения: очная, заочная  
 Разработана для приема 2019/2020, 2020/2021 учебного года  
 Обновлено на 2023/2024 учебный год

	<table border="1"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td> </tr> <tr> <td>5</td><td>8</td><td>6</td><td>11</td><td>1</td><td>10</td><td>9</td><td>4</td><td>3</td><td>12</td><td>2</td><td>7</td> </tr> </table>	1	2	3	4	5	6	7	8	9	10	11	12	5	8	6	11	1	10	9	4	3	12	2	7	в) ПОАТЬСНОЗЬЕС г) ПНАТЬБСООЗЕС	
1	2	3	4	5	6	7	8	9	10	11	12																
5	8	6	11	1	10	9	4	3	12	2	7																
7	При моноалфавитной замене получен шифрокод ЗЖРЦ. Расшифровать слово, если известно, что смещение <b>к</b> является нечетным числом.	а) ФЛЭШ б) БАЙТ в) ЛОГИН г) СТЭК	2																								
8	Зашифровать слово НАИФ способом простой замены, используя таблицу. <table border="1"> <tr> <td><b>A</b></td><td><b>B</b></td><td><b>C</b></td><td><b>D</b></td><td><b>E</b></td><td><b>F</b></td><td><b>G</b></td><td><b>H</b></td><td><b>I</b></td><td><b>J</b></td> </tr> <tr> <td><b>F</b></td><td><b>I</b></td><td><b>L</b></td><td><b>O</b></td><td><b>R</b></td><td><b>U</b></td><td><b>X</b></td><td><b>A</b></td><td><b>D</b></td><td><b>Q</b></td> </tr> </table>	<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>	<b>F</b>	<b>G</b>	<b>H</b>	<b>I</b>	<b>J</b>	<b>F</b>	<b>I</b>	<b>L</b>	<b>O</b>	<b>R</b>	<b>U</b>	<b>X</b>	<b>A</b>	<b>D</b>	<b>Q</b>	а) FOID б) AFDX в) FOAD г) AFDU	2				
<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>	<b>F</b>	<b>G</b>	<b>H</b>	<b>I</b>	<b>J</b>																		
<b>F</b>	<b>I</b>	<b>L</b>	<b>O</b>	<b>R</b>	<b>U</b>	<b>X</b>	<b>A</b>	<b>D</b>	<b>Q</b>																		
9	Зашифровать сообщение (2,3) методом RSA, если открытый ключ $(K_0, N) \rightarrow (7, 33)$ .	а) (27,4) б) (29,9) в) (29,4) г) (29,2)	2																								
10	Расшифровать криптограмму (3,1) методом RSA, если секретный ключ $(K_c, N) \rightarrow (3, 22)$ .	а) (5, 1) б) (7, 5) в) (7, 1) г) (9, 11)	2																								
11	Зашифровать методом Виженера сообщение ШИФРЫ ЗАМЕНЫ. Ключ – ХАКЕР (Таблицу см. в приложении).	а) МИЮФЛЫАЦКЭР б) МИЮФЛЫАЦЛЭР в) МИЭХЛЫАШКЭР г) МИЮХЛЫАЦКЭР	3																								
12	Определить ключ слова ТЕХНОЛОГИЯ, шифрокод которого по методу Виженера: ФКЯПУХРИТА.	а) ТПК б) ВОЛЬТ в) ВЕК г) СТО	3																								
13	Зашифровать сообщение ИНТЕРНЕТ способом Гронсфельда. <table border="1"> <tr> <td>№ позиции</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td> </tr> <tr> <td>Ключ</td><td>5</td><td>2</td><td>4</td><td>8</td><td>1</td><td>3</td><td>6</td><td>7</td> </tr> </table>	№ позиции	1	2	3	4	5	6	7	8	Ключ	5	2	4	8	1	3	6	7	а) МОХЛРПЙШ б) МОЧЛРСЙШ в) НПЦМСРКЦ г) НПЦМКРКЦ	3						
№ позиции	1	2	3	4	5	6	7	8																			
Ключ	5	2	4	8	1	3	6	7																			
14	Получить шифрокод слова УНИВЕРСИТЕТ методом гаммирования, если гаммой шифра является ХЕШИРОВАНИЕ.	а) БЗПЙЭЦРЗЬОФ б) БЗСЙЦЭРЗЬОФ в) БЗПЙЦЭРЗЬОФ г) БЗСЙЦЭРТЬОФ	3																								
15	Определить гамму, если шифрокоду ТЕСТ соответствует информация КРАХ.	а) ХЦТД б) ЧЦТД в) ЧФТД г) ЧЦРД	3																								

38.03.02 Менеджмент, направленность «Маркетинг»  
Программа прикладного бакалавриата  
Рабочая программа дисциплины  
Дисциплина: Б1.В.ДВ.02.02 Информационная безопасность и защита информации  
Форма обучения: очная, заочная  
Разработана для приема 2019/2020, 2020/2021 учебного года  
Обновлена на 2023/2024 учебный год

---