

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Юров Сергей Серафимович Автономная некоммерческая организация высшего образования

Должность: ректор

Дата подписания: 01.11.2022 15:24:56

Уникальный программный ключ:

3cba11a39f7f7fadc578ee5ed1f72a427b45709d10da52f2f114bf9bf44b8f14

**“ИНСТИТУТ БИЗНЕСА И ДИЗАЙНА”**

ФАКУЛЬТЕТ УПРАВЛЕНИЯ БИЗНЕСОМ



УТВЕРЖДАЮ

Ректор  С.С. Юров

«24» февраля 2022 г.

## **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

### **Б1.О.22 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**Для направления подготовки:**

09.03.02 Информационные системы и технологии  
(уровень бакалавриата)

**Типы задач профессиональной деятельности:**

*производственно-технологический; организационно-управленческий; проектный.*

**Направленность (профиль):**

Информационные системы и технологии в бизнесе

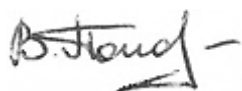
**Форма обучения:**

очная, заочная

**Москва – 2022**

Разработчик: Попов Владимир Иванович кандидат физико-математических наук, доцент кафедры гуманитарных и естественно-научных дисциплин АНО ВО «Институт бизнеса и дизайна».

«15» января 2022 г.



/В.И.Попов/

СОГЛАСОВАНО:

Декан факультета



(подпись)

/Н.Е. Козырева /

Заведующий кафедрой  
разработчика РПД



(подпись)

/Е.С.Мальцева /

Протокол заседания кафедры № 6 от «27» января 2022 г.

## 1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

### Цель:

формирование у студентов знаний об информационной безопасности, роль и значении обеспечения информационной безопасности в профессиональной деятельности.

### Задачи:

- получение знаний о современных информационных системах, нормативно-правовых документах РФ, методах и средствах обеспечения информационной безопасности;
- умений выявлять возможные угрозы, влияющие на состояние информационной безопасности;
- организовывать мероприятия по выполнению требований нормативных и руководящих документов РФ;
- проведении политики безопасности предприятия в области обеспечения информационной безопасности;
- владеть практическими навыками по использованию современных методов и средств обеспечения информационной безопасности.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

### 2.1. Место дисциплины в учебном плане:

**Блок:** Блок 1. Дисциплины (модули).

**Часть:** Обязательная часть.

**Осваивается:** 2 семестр очная форма обучения, 3 семестр - заочная форма обучения

## 3. КОМПЕТЕНЦИИ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-3 – способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

## 4. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМСЯ

Код и наименование компетенции	Индикаторы достижения компетенции	Результаты обучения
<b>ОПК-3</b> Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	<b>ОПК-3.1</b> 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 <b>ОПК-3.2</b> Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с	<b>Знает:</b> 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. <b>Умеет:</b> решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий

	<p>учетом основных требований информационной безопасности</p> <p><b>ОПК-3.3</b></p> <p>Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности</p>	<p>и учетом основных требований информационной безопасности.</p> <p><b>Владеет:</b></p> <p>практическими навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.</p>
--	---	---

## 5. ОБЪЕМ ДИСЦИПЛИНЫ И РАСПРЕДЕЛЕНИЕ ВИДОВ УЧЕБНОЙ РАБОТЫ ПО СЕМЕСТРАМ

Общая трудоемкость дисциплины «Основы информационной безопасности» для студентов всех форм обучения, реализуемых в АНО ВО «Институт бизнеса и дизайна» по направлению подготовки 09.03.02 Информационные системы и технологии: 5 з.е. / 180 час.

Вид учебной работы	Всего число часов и (или) зачетных единиц (по формам обучения)	
	Очная	Заочная
<b>Аудиторные занятия</b>	64	14
<i>в том числе:</i>		
Лекции	32	6
Практические занятия	32	8
Лабораторные работы	-	
<b>Самостоятельная работа</b>	80	157
<i>в том числе:</i>		
часы на выполнение КР / КП	-	-
<b>Промежуточная аттестация:</b>		
Вид	Экзамен	Экзамен
Трудоемкость (час.)	36	9
<b>Общая трудоемкость з.е. / часов</b>	5 з.е. / 180 час.	5 з.е. / 180 час.

## 6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Темы дисциплины		Количество часов (по формам обучения)							
№	Наименование	Очная				Заочная			
		Лекции	Практические занятия	Лабораторные работы	Самост. работа (в т.ч. КР / КП)	Лекции	Практические занятия	Лабораторные работы	Самост. работа (в т.ч. КР / КП)
1	Актуальность проблемы информационной безопасности	2	2			1			15

Темы дисциплины		Количество часов (по формам обучения)							
№	Наименование	Очная				Заочная			
		Лекции	Практические занятия	Лабораторные работы	Самост. работа (в т.ч. КР / КП)	Лекции	Практические занятия	Лабораторные работы	Самост. работа (в т.ч. КР / КП)
2	Основные термины и определения категории «безопасность», виды безопасности	2	2			1			15
3	Национальная безопасность Российской Федерации. Место информационной безопасности в системе Национальной безопасности Российской Федерации.	2	2				1		15
4	Государственная система обеспечения информационной безопасности Российской Федерации	2	2			1	1		16
5	Законодательные акты Российской Федерации в области информационной безопасности, государственная тайна, конфиденциальная информация	4	4				1		16
6	Информация, как объект защиты, источники угроз, угрозы информационной безопасности	4	4			1	1		16
7	Правовой уровень обеспечения информационной безопасности	4	4				1		16
8	Административный уровень, политика информационной безопасности предприятия	4	4				1		16
9	Процедурный уровень информационной безопасности	4	4			1	1		16
10	Программно-технический уровень, сервисы информационной безопасности	4	4			1	1		16
Итого (часов)		32	32		80	6	8		157
<b>Форма контроля:</b>		<i>экзамен</i>			36	<i>экзамен</i>			9
<b>Всего по дисциплине:</b>		180 / 5 з.е.				180 / 5 з.е.			

## СОДЕРЖАНИЕ ТЕМ ДИСЦИПЛИНЫ

### ***Тема 1. Актуальность проблемы информационной безопасности.***

Современный этап развития информационного общества, Этапы развития информационных технологий (ИТ). методов и средств обеспечения информационной безопасности. Проблемы и актуальность обеспечения информационной безопасности.

### ***Тема 2. Основные термины и определения категории «безопасность», виды безопасности***

Понятие, источники, формы, виды, свойства информации. Национальная безопасность, информационная безопасность, цель и решаемые задачи. Жизненно важные интересы личности, общества, государства в сфере информационной безопасности. Объекты защиты. Опасность, ущерб, источники угроз, угроза информационной безопасности.

### ***Тема 3 Национальная безопасность Российской Федерации. Место информационной безопасности в системе Национальной безопасности Российской Федерации.***

Ценности и модели развития глобальной конкуренции. Глобальное информационное противоборство. Значение информационной безопасности в обеспечении национальной безопасности Российской Федерации. Положения основных нормативных документов Российской Федерации в области национальной, и информационной безопасности.

### ***Тема 4. Государственная система обеспечения информационной безопасности Российской Федерации.***

Основные элементы системы государственной информационной безопасности Российской Федерации. Законодательные органы Российской Федерации. Значение и роль судебных органов Российской Федерации в обеспечении информационной безопасности и защиты информации. Органы исполнительной власти Российской Федерации в проведении единой технической политики в области информационной безопасности и защиты информации.

### ***Тема 5. Законодательные акты Российской Федерации в области информационной безопасности, государственная тайна, конфиденциальная информация.***

Основные нормативные акты Российской Федерации, назначение и основные положения. Классификация информации по своей доступности и распространенности в соответствии с Российским законодательством, Правовой институт тайн в Российской Федерации. Государственная тайна, содержание, основные понятия. Конфиденциальная информация, основные понятия, виды конфиденциальной информации.

### ***Тема 6. Информация, как объект защиты, источники угроз, угрозы информационной безопасности.***

Понимание информации как объекта защиты, юридические свойства информации. Информационное право как юридическая отрасль права, цели, задачи, принципы информационного права. Правовое регулирование субъектов по отношению к объектам интеллектуальной собственности. Каналы утечки, методы и способы несанкционированного доступа к защищаемой информации, объектам защиты. Источники угроз воздействия на объект защиты. Угрозы, влияющие на состояние информационной безопасности, методы и способы реализации угроз.

### ***Тема 7. Правовой уровень обеспечения информационной безопасности.***

Назначение, цели и задачи правового уровня обеспечения информационной безопасности. Международные и российские стандарты в области информационной безопасности. Нормативно-правовые и руководящие документы ФСТЭК РФ по защите информации от несанкционированного доступа (НСД) к информационным системам. Классификация автоматизированных систем (АС) по уровню защищенности от

несанкционированного доступа (НСД). Классификация средств вычислительной техники (СВТ) по уровню защищенности от несанкционированного доступа (НСД). Классификация межсетевых экранов по уровню защищенности от несанкционированного доступа (НСД). Классификация программного обеспечения по уровню контроля отсутствия не декларированных возможностей.

***Тема 8. Административный уровень, политика информационной безопасности предприятия.***

Политика информационной безопасности, как концептуальный документ по обеспечению информационной безопасности на предприятии. Состав и содержание политики информационной безопасности. Состав и содержание программы информационной безопасности. Анализ и оценка рисков, управление рисками по исключению реализации угроз информационной безопасности. Цели, задачи и основные мероприятия по построению системы обеспечения информационной безопасности на предприятии.

***Тема 9. Процедурный уровень информационной безопасности.***

Основные классы мер процедурного уровня информационной безопасности (ИБ). Управление персоналом, назначение, основные положения. Физическая защита, назначение, основные положения. Поддержание работоспособности информационных систем. Реагирование на нарушения режима безопасности. Планирование восстановительных работ системы обработки и защиты информации.

***Тема 10. Программно-технический уровень, сервисы информационной безопасности.***

Назначение, цель, решаемые задачи программно-технического уровня обеспечения информационной безопасности. Сервисы информационной безопасности от несанкционированного доступа к информационным ресурсам (ИР). Идентификация и аутентификация пользователей, как передовой рубеж защиты информации. Модели разграничения доступа к информационным ресурсам в области информационно-коммуникационных технологий. Протоколирование и аудит информационных систем (ИС), назначение, решаемые задачи. Экранирование информации в информационно-телекоммуникационных сетях (ИТС). Методы шифрования информации. Процедура формирования электронной подписи. Вредоносные программы: компьютерные вирусы, черви, троянский конь, классификация, методы и средства противодействия. Управление высокой доступности к информационно-коммуникационным системам.

## **7. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ РАБОТ**

Курсовая работа не предусмотрена

### **8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ: Приложение 1.**

### **9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:**

#### **9.1. Рекомендуемая литература:**

1. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с.

Режим доступа: [https://biblioclub.ru/index.php?page=book\\_red&id=562348](https://biblioclub.ru/index.php?page=book_red&id=562348)

2. Гульятеева, Т. А. Основы информационной безопасности : учебное пособие : [16+] / Т. А. Гульятеева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с.

Режим доступа: [https://biblioclub.ru/index.php?page=book\\_red&id=574729](https://biblioclub.ru/index.php?page=book_red&id=574729)

3. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие : [16+] / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с.

Режим доступа: [https://biblioclub.ru/index.php?page=book\\_red&id=571485](https://biblioclub.ru/index.php?page=book_red&id=571485)

## **9.2. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень лицензионного и свободно распространяемого программного обеспечения.**

При осуществлении образовательного процесса по данной учебной дисциплине предполагается использование:

### **Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства:**

1. Windows 10 Pro Professional (Договор: Tr000391618, срок действия с 20.02.2020 г. по 28.02.2023 г., Лицензия: V8732726);
2. Microsoft Office Professional Plus 2019 (Договор: Tr000391618, срок действия с 20.02.2020 г. по 28.02.2023 г., Лицензия: V8732726).
3. Браузер Google Chrome;
4. Браузер Yandex;
5. Adobe Reader - программа для просмотра, печати и комментирования документов в формате PDF

## **9.3. Перечень современных профессиональных баз данных, информационных справочных систем и ресурсов информационно-телекоммуникационной сети «Интернет»**

1. <https://biblioclub.ru/> - университетская библиотечная система online Библиоклуб.py
2. <http://window.edu.ru/> - единое окно доступа к образовательным ресурса
3. <https://uisrussia.msu.ru/> - база данных и аналитических публикаций университетской информационной системы Россия
4. <https://www.elibrary.ru/> - электронно-библиотечная система eLIBRARY.RU, крупнейшая в России электронная библиотека научных публикаций
5. <http://www.consultant.ru/> - справочная правовая система КонсультантПлюс
6. <https://gufo.me/> - справочная база энциклопедий и словарей
7. <https://slovaronline.com> - поисковая система по всем доступным словарям и энциклопедиям
8. <https://www.tandfonline.com/> - коллекция журналов Taylor&Francis Group включает в себя около двух тысяч журналов и более 4,5 млн. статей по различным областям знаний
9. <https://openedu.ru> - «Национальная платформа открытого образования» (ресурсы открытого доступа)
10. <https://www.rsl.ru> - Российская Государственная Библиотека (ресурсы открытого доступа)
11. <https://link.springer.com> - Международная реферативная база данных научных изданий Springerlink (ресурсы открытого доступа)
12. <https://zbmath.org> - Международная реферативная база данных научных изданий zbMATH (ресурсы открытого доступа)



## **10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

1. Оборудованные учебные аудитории, в том числе с использованием видеопроектора и подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Института.

2. Аудитории для самостоятельной работы с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Института.

3. Компьютерный класс с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Института.

4. Аудио и видеоаппаратура.

### **№ 409**

Учебная аудитория для проведения учебных занятий. Аудитория оснащена оборудованием и техническими средствами обучения:

а) учебной мебелью: столы, стулья, доска маркерная учебная

б) стационарный широкоформатный мультимедиа-проектор Epson EB-X41, экран, колонки.

в) 11 компьютеров, подключенных к сети

«Интернет», с обеспечением доступа в электронную информационно-образовательную среду АНО ВО «Институт бизнеса и дизайна»

### **№ 402**

Помещение для самостоятельной работы. Аудитория оснащена оборудованием и техническими средствами обучения:

а) учебной мебелью: столы, стулья, доска маркерная учебная

б) стационарный широкоформатный мультимедиа-проектор Epson EB-X41, экран, колонки.

в) 11 компьютеров, подключенных к сети «Интернет», с обеспечением доступа в электронную информационно-образовательную среду АНО ВО «Институт бизнеса и дизайна»

## **11. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ**

В процессе освоения дисциплины студенту необходимо посетить все виды занятий, предусмотренные рабочей программой дисциплины и выполнить контрольные задания, предлагаемые преподавателем для успешного освоения дисциплины. Также следует изучить рабочую программу дисциплины, в которой определены цели и задачи дисциплины, компетенции обучающегося, формируемые в результате освоения дисциплины и планируемые результаты обучения. Рассмотреть содержание тем дисциплины; взаимосвязь тем лекций и практических занятий; бюджет времени по видам занятий; оценочные средства для текущей и промежуточной аттестации; критерии итоговой оценки результатов освоения дисциплины. Ознакомиться с методическими материалами, программно-информационным и материально-техническим обеспечением дисциплины.

Лекционные занятия включают изложение, обсуждение и разъяснение основных направлений и вопросов изучаемой дисциплины, знание которых необходимо в ходе реализации всех остальных видов занятий и в самостоятельной работе студентов. На лекциях студенты получают самые необходимые знания по изучаемой проблеме. Непременным условием для глубокого и прочного усвоения учебного материала является умение студентов сосредоточенно слушать лекции, активно, творчески воспринимать излагаемые сведения. Внимательное слушание лекций предполагает интенсивную умственную деятельность

студента. Краткие записи лекций, конспектирование их помогает усвоить материал. Конспект является полезным тогда, когда записано самое существенное, основное. Запись лекций рекомендуется вести по возможности собственными формулировками.

Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях. Конспект лучше подразделять на пункты, параграфы, соблюдая красную строку. Принципиальные места, определения, формулы следует сопровождать замечаниями. Работая над конспектом лекций, всегда следует использовать не только основную литературу, но и ту литературу, которую дополнительно рекомендовал лектор.

#### Практические занятия

Подготовку к практическому занятию следует начинать с ознакомления с лекционным материалом, с изучения плана практических занятий. Определившись с проблемой, следует обратиться к рекомендуемой литературе. Владение понятийным аппаратом изучаемого курса является необходимым, поэтому готовясь к практическим занятиям, студенту следует активно пользоваться справочной литературой: энциклопедиями, словарями и др. В ходе проведения практических занятий, материал, излагаемый на лекциях, закрепляется, расширяется и дополняется при подготовке сообщений, рефератов, выполнении тестовых работ. Степень освоения каждой темы определяется преподавателем в ходе обсуждения ответов студентов.

#### Самостоятельная работа

Студент в процессе обучения должен не только освоить учебную программу, но и приобрести навыки самостоятельной работы. Самостоятельная работа студентов играет важную роль в воспитании сознательного отношения самих студентов к овладению теоретическими и практическими знаниями, привитии им привычки к направленному интеллектуальному труду. Самостоятельная работа проводится с целью углубления знаний по дисциплине. Материал, законспектированный на лекциях, необходимо регулярно дополнять сведениями из литературных источников, представленных в рабочей программе. Изучение литературы следует начинать с освоения соответствующих разделов дисциплины в учебниках, затем ознакомиться с монографиями или статьями по той тематике, которую изучает студент, и после этого – с брошюрами и статьями, содержащими материал, дающий углубленное представление о тех или иных аспектах рассматриваемой проблемы. Для расширения знаний по дисциплине студенту необходимо использовать Интернет-ресурсы и специализированные базы данных: проводить поиск в различных системах и использовать материалы сайтов, рекомендованных преподавателем на лекционных занятиях.

#### Подготовка к сессии

Основными ориентирами при подготовке к промежуточной аттестации по дисциплине являются конспект лекций и перечень рекомендуемой литературы. При подготовке к сессии студенту следует так организовать учебную работу, чтобы перед первым днем начала сессии были сданы и защищены все практические работы. Основное в подготовке к сессии – это повторение всего материала курса, по которому необходимо пройти аттестацию. При подготовке к сессии следует весь объем работы распределять равномерно по дням, отведенным для подготовки, контролировать каждый день выполнения работы.

### ***Методические рекомендации для обучающихся с ОВЗ и инвалидов по освоению дисциплины***

В АНО ВО «Институт бизнеса и дизайна» созданы специальные условия для получения высшего образования по образовательным программам обучающимися с ограниченными возможностями здоровья (ОВЗ).

Для перемещения инвалидов и лиц с ограниченными возможностями здоровья в АНО ВО «Институт бизнеса и дизайна» созданы специальные условия для беспрепятственного доступа в учебные помещения и другие помещения, а также их пребывания в указанных помещениях с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

При получении образования обучающимся с ограниченными возможностями здоровья при необходимости предоставляются бесплатно специальные учебники и учебные пособия,

иная учебная литература. Также имеется возможность предоставления услуг ассистента, оказывающего обучающимся с ограниченными возможностями здоровья необходимую техническую помощь, в том числе услуг сурдопереводчиков и тифлосурдопереводчиков.

Получение доступного и качественного высшего образования лицами с ограниченными возможностями здоровья обеспечено путем создания в институте комплекса необходимых условий обучения для данной категории обучающихся. Информация о специальных условиях, созданных для обучающихся с ограниченными возможностями здоровья, размещена на сайте института (<https://obe.ru/sveden/ovz/>).

Для обучения инвалидов и лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата обеспечиваются и совершенствуются материально-технические условия беспрепятственного доступа в учебные помещения, столовую, туалетные, другие помещения, условия их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и др.).

Для адаптации к восприятию обучающимися инвалидами и лицами с ОВЗ с нарушенным слухом справочного, учебного материала, предусмотренного образовательной программой по выбранным направлениям подготовки, обеспечиваются следующие условия:

для лучшей ориентации в аудитории, применяются сигналы, оповещающие о начале и конце занятия (слово «звонок» пишется на доске);

внимание слабослышащего обучающегося привлекается педагогом жестом (на плечо кладется рука, осуществляется нерезкое похлопывание);

разговаривая с обучающимся, педагог смотрит на него, говорит ясно, короткими предложениями, обеспечивая возможность чтения по губам.

Компенсация затруднений речевого и интеллектуального развития слабослышащих инвалидов и лиц с ОВЗ проводится за счет:

использования схем, диаграмм, рисунков, компьютерных презентаций с гиперссылками, комментирующими отдельные компоненты изображения;

регулярного применения упражнений на графическое выделение существенных признаков предметов и явлений;

обеспечения возможности для обучающегося получить адресную консультацию по электронной почте по мере необходимости.

Для адаптации к восприятию инвалидами и лицами с ОВЗ с нарушениями зрения справочного, учебного, просветительского материала, предусмотренного образовательной программой АНО ВО «Институт бизнеса и дизайна» по выбранной специальности, обеспечиваются следующие условия:

ведется адаптация официального сайта в сети Интернет с учетом особых потребностей инвалидов по зрению, обеспечивается наличие крупношрифтовой справочной информации о расписании учебных занятий;

в начале учебного года обучающиеся несколько раз проводятся по зданию АНО ВО «Институт бизнеса и дизайна» для запоминания месторасположения кабинетов, помещений, которыми они будут пользоваться;

педагог, его собеседники, присутствующие представляются обучающимся, каждый раз называется тот, к кому педагог обращается;

действия, жесты, перемещения педагога коротко и ясно комментируются;

печатная информация предоставляется крупным шрифтом (от 18 пунктов), тотально озвучивается; обеспечивается необходимый уровень освещенности помещений;

предоставляется возможность использовать компьютеры во время занятий и право записи объяснения на диктофон (по желанию обучающегося).

Форма проведения текущей и промежуточной аттестации для обучающихся с ОВЗ определяется преподавателем в соответствии с учебным планом. При необходимости обучающемуся с ОВЗ с учетом его индивидуальных психофизических особенностей дается возможность пройти промежуточную аттестацию устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п., либо предоставляется дополнительное время для подготовки ответа.

Автономная некоммерческая организация высшего образования  
«ИНСТИТУТ БИЗНЕСА И ДИЗАЙНА»

Факультет управления бизнесом

**Фонд оценочных средств**

Текущего контроля и промежуточной аттестации  
по дисциплине (модулю)

**Б1.О.22 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**Для направления подготовки:**

09.03.02 Информационные системы и технологии  
(уровень бакалавриата)

**Типы задач профессиональной деятельности:**

производственно-технологический; организационно-управленческий; проектный.

**Направленность (профиль):**

Информационные системы и технологии в бизнесе

**Форма обучения:**

очная, заочная

## Результаты обучения по дисциплине

Код и наименование компетенции	Индикаторы достижения компетенции	Результаты обучения
<p><b>ОПК-3</b> Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p>	<p><b>ОПК-3.1</b> 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</p> <p><b>ОПК-3.2</b> Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p> <p><b>ОПК-3.3</b> Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности</p>	<p><b>Знает:</b> 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.</p> <p><b>Умеет:</b> решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</p> <p><b>Владеет:</b> практическими навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.</p>

### Типовые оценочные средства, необходимые для оценки планируемых результатов обучения по дисциплине (модулю):

#### ТЕКУЩИЙ КОНТРОЛЬ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ (МОДУЛЮ)

##### Тест для формирования «ОПК-3.1»

Вопрос №1 .

Аудит информационной безопасности.

*Варианты ответов:*

1. Состояние сохранности информационных ресурсов и защищенности законных прав личности общества в информационной сфере.
2. Системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности автоматизированной системы в соответствии с определёнными критериями и показателями безопасности.
3. Оба варианта верны. Вопрос №2 .  
Безопасность информационных ресурсов.

*Варианты ответов:*

1. Безопасность всего, что используется целевым образом.
2. Безопасность документов и массивов документов в информационных системах (библиотеках, архивах, фондах, банках данных, депозитариях, музейных хранилищах и т. п.).

3. Оба варианта не верны. Вопрос №3 . Вычислительные сети *Варианты ответов:*

1. Система, обеспечивающая обмен данными между вычислительными устройствами — компьютерами, серверами, маршрутизаторами и другим оборудованием или программным обеспечением.
2. Логически самостоятельная выделенная сеть использующей ресурсы другой физической сети.
3. Оба варианта верны. Вопрос №4 .  
Угроза информационной безопасности.

*Варианты ответов:*

1. Совокупность условий и факторов, создающих опасность нарушения информационной безопасности.
2. Возможное событие, действие (воздействие), процесс или явление, которые могут привести к нанесению ущерба чьим-либо интересам.

3. Оба варианта верны. Вопрос №5 .

Защита информации.

*Варианты ответов:*

1. Практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.
2. Отсутствие недопустимого риска, связанного с возможностью нанесения ущерба.
3. Оба варианта не верны.

### Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	от 0% до 30% правильных ответов из общего числа тестовых заданий
Удовлетворительно	от 31% до 50% правильных ответов из общего числа тестовых заданий
Хорошо	от 51% до 80% правильных ответов из общего числа тестовых заданий
Отлично	от 81% до 100% правильных ответов из общего числа тестовых заданий

### Выполнение реферата для формирования «ОПК-3.2»

1. Информация - фактор существования и развития общества. Основные формы проявления информации, её свойства как объекта безопасности.
2. Понятие безопасности и её составляющие. Безопасность информации.
3. Обеспечение информационной безопасности: содержание и структура понятия.
4. Национальные интересы в информационной сфере.
5. Источники и содержание угроз в информационной сфере.
6. Соотношение понятий «информационная безопасность» и «национальная безопасность»
7. Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности.

### Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не раскрыл материал по теме задания или материал раскрыт поверхностно, излагаемый материал не систематизирован, выводы недостаточно аргументированы, обучающийся не высказывал своего мнения, не проявил способность к анализу, имеются смысловые и речевые ошибки в реферате
Удовлетворительно	Обучающийся демонстрирует логичность и доказательность изложения материала по теме задания, но допускает отдельные неточности при использовании ключевых понятий. Обучающийся не продемонстрировал способность к научному анализу, не высказывал в работе своего мнения, допустил ошибки в логическом обосновании своего ответа
Хорошо	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, в работе присутствуют ссылки на научные источники, мнения известных учёных в данной области
Отлично	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, при разработке реферата использовано не менее 5-8 научных источников. В работе выдвигаются новые идеи и трактовки, демонстрируется способность обучающегося анализировать материал, выражается его мнение по проблеме

#### Выполнение реферата для формирования «ОПК-3.2»

1. Методы борьбы с фишинговыми атаками. 2. Законодательство о персональных данных.
3. Защита авторских прав.
4. Назначение, функции и типы систем видеозащиты.
5. Как подписывать с помощью ЭЦП электронные документы различных форматов. 6. Обзор угроз и технологий защиты Wi-Fi-сетей.
7. Проблемы внедрения дискового шифрования.
8. Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.
9. Особенности процессов аутентификации в корпоративной среде.
10. Квантовая криптография.
11. Утечки информации: как избежать. Безопасность смартфонов. 12. Безопасность применения пластиковых карт - законодательство и практика.
13. Защита CD- и DVD-дисков от копирования. 14. Современные угрозы и защита электронной почты.
15. Программные средства анализа локальных сетей на предмет уязвимостей. 16. Безопасность применения платежных систем - законодательство и практика. 17. Аудит программного кода по требованиям безопасности.
18. Антишпионское ПО (antispware). 19. Обеспечение безопасности Web-сервисов. 20. Защита от внутренних угроз.
21. Технологии RFID.
22. Уничтожение информации на магнитных носителях.
23. Ботнеты - плацдарм современных кибератак.
24. Цифровые водяные знаки в изображениях. 25. Электронный документооборот. Модели нарушителя. 26. Идентификация по голосу. Скрытые возможности.
27. Безопасность океанских портов. 28. Безопасность связи.
29. Безопасность розничной торговли. 30. Банковская безопасность.

31. Информатизация управления транспортной безопасностью. 32. Биопаспорт.  
 33. Обзор современных платформ архивации данных. 34. Что такое консалтинг в области ИБ.  
 35. Бухгалтерская отчетность как источник рассекречивания информации. 36. Управление рисками: обзор потребительских подходов.  
 37. Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности.  
 38. Распределенные атаки на распределенные системы. 39. Оценка безопасности автоматизированных систем. 40. Windows и Linux: что безопаснее?  
 41. Функциональная безопасность программных средств.  
 42. Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств.  
 43. Информационная безопасность: экономические аспекты.

### Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не раскрыл материал по теме задания или материал раскрыт поверхностно, излагаемый материал не систематизирован, выводы недостаточно аргументированы, обучающийся не высказывал своего мнения, не проявил способность к анализу, имеются смысловые и речевые ошибки в реферате
Удовлетворительно	Обучающийся демонстрирует логичность и доказательность изложения материала по теме задания, но допускает отдельные неточности при использовании ключевых понятий. Обучающийся не продемонстрировал способность к научному анализу, не высказывал в работе своего мнения, допустил ошибки в логическом обосновании своего ответа
Хорошо	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, в работе присутствуют ссылки на научные источники, мнения известных учёных в данной области
Отлично	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, при разработке реферата использовано не менее 5-8 научных источников. В работе выдвигаются новые идеи и трактовки, демонстрируется способность обучающегося анализировать материал, выражается его мнение по проблеме

### Выполнение реферата для формирования «ОПК-3.2»

1. Аттестация объектов информатизации по требованиям безопасности информации.
2. Понятие интеллектуальной собственности, ее виды и объекты образования (авторские и лицензионные договоры).
3. Основы авторского права. Основные положения патентного права.
4. Законодательство об интеллектуальной собственности.
5. Особенности правового регулирования общественных отношений при использовании современных технических средств обработки информации и при разработке шифрсредств.
6. Правовое регулирование использования электронной цифровой подписи и защиты информации в системах и средствах электронного документооборота.
7. Статус и организация деятельности удостоверяющих центров.
8. Правовое регулирование защиты информации в системах связи.
9. Использование персональных данных владельцев доменных имен сети Интернет и



проблемы защиты конституционных прав граждан на неприкосновенность персональных данных.

10. Основные понятия и система сертификации продукции и услуг в сфере информационной безопасности.
11. Особенности сертификации средств защиты информации по требованиям безопасности.
12. Аккредитация испытательных лабораторий и органов по сертификации средств защиты информации
13. Отрасли права, обеспечивающие законность в области защиты информации.
14. Конституция и Гражданский кодекс Российской Федерации о правах и обязанностях граждан России в сфере обеспечения информационной безопасности.
15. Международное законодательство в области защиты информации.
16. Основные понятия, положения, организационная структура системы государственного лицензирования.
17. Аттестация объектов информатизации по требованиям безопасности информации.
18. Причины и условия, обуславливающие правонарушения в сфере информационной безопасности(защиты конфиденциальной информации, обеспечение режима секретности)
19. Характеристика личности правонарушителя в сфере информационной безопасности.
20. Понятие и виды юридической ответственности за нарушение правовых норм в области защиты информации.
21. Уголовная ответственность за нарушение правовых норм в сфере информационной безопасности.
22. Административная ответственность за нарушение правовых норм в сфере информационной безопасности.
23. Проведение административного расследования по фактам нарушения установленного порядка обеспечения информационной безопасности.
24. Особенности юридической ответственности за нарушение правовых норм информационной безопасности в области трудовых и гражданско-правовых отношений.
25. Меры предупреждение правонарушений
26. Актуальность проблемы правового регулирования в сфере информационной безопасности.
27. Факторы и проблемы правового регулирования в сфере информационной безопасности.
28. Состояние и закономерности практики правового регулирования информационной безопасности.
29. Направления развития теоретических аспектов законодательства в сфере информационной безопасности
30. Методология и организация исследований в области правового регулирования информационной безопасности.
31. Факторы и проблемы правового регулирования в сфере информационной безопасности.
32. Состояние и закономерности практики правового регулирования информационной безопасности.
33. Направления развития теоретических аспектов законодательства в сфере информационной безопасности.
34. Развитие информационного права как эффективного инструментария регулирования конституционных прав человека в информационной сфере.

### **Критерии оценки выполнения задания**

Оценка	Критерии оценивания
--------	---------------------

Неудовлетворительно	Обучающийся не раскрыл материал по теме задания или материал раскрыт поверхностно, излагаемый материал не систематизирован, выводы недостаточно аргументированы, обучающийся не высказывал своего мнения, не проявил способность к анализу, имеются смысловые и речевые ошибки в реферате
Удовлетворительно	Обучающийся демонстрирует логичность и доказательность изложения материала по теме задания, но допускает отдельные неточности при использовании ключевых понятий. Обучающийся не продемонстрировал способность к научному анализу, не высказывал в работе своего мнения, допустил ошибки в логическом обосновании своего ответа
Хорошо	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, в работе присутствуют ссылки на научные источники, мнения известных учёных в данной области
Отлично	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, при разработке реферата использовано не менее 5-8 научных источников. В работе выдвигаются новые идеи и трактовки, демонстрируется способность обучающегося анализировать материал, выражается его мнение по проблеме

### **Выполнение реферата для формирования «ОПК-3.2»**

1. Объект и предмет информационного права.
2. Источники, информационного права.
3. Задачи, принципы, институты информационного права
4. Система информационного законодательства.
5. Структура и состав информационного Законодательства.
6. Международные актами информационного Законодательства.
7. Информационно-правовые нормы Конституции России.
8. Отрасли законодательства, нормативные правовые акты посвященные информационной сфере.
9. Отдельные информационные правовые нормы в составе нормативных правовых актов отраслей законодательств.
10. Содержание основных нормативных правовых актов информационного законодательства
11. Основные понятия, виды и источники информации, подлежащей защите.
12. Характеристики правонарушений режима защиты конфиденциальной информации.
13. Причины, классификация и характеристики возможных каналов утечки конфиденциальной информации.
14. Информация как объект правоотношений.
15. Понятие информационной безопасности
16. Угрозы информационной безопасности личности, общества, государства.
17. Место информационной безопасности в системе национальной безопасности России.
18. Основные термины, определения и правовые категории информационной безопасности объектов информатизации.
19. Понятие и виды защищаемой информации.
20. Содержание, функции организационного и правового регулирования информационной безопасности и его место в системе комплексной защиты информации.
21. Назначение, структура, методы правового обеспечения защиты информации.
22. Информация, информационные системы и ресурсы - объекты правового регулирования информатизации информационной безопасности.

23. Правовые основы защиты государственной, коммерческой, служебной, профессиональной и личной тайны, персональных данных.
24. Пути развития правовой информатизации и информационной безопасности.
25. Концепция правовой информатизации субъектов Российской Федерации как основа информационной безопасности личности, общества, государства.
26. Программа правовой информатизации.
27. Формирование государственной системы правового регулирования информационной безопасности в Российской Федерации.

### Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не раскрыл материал по теме задания или материал раскрыт поверхностно, излагаемый материал не систематизирован, выводы недостаточно аргументированы, обучающийся не высказывал своего мнения, не проявил способность к анализу, имеются смысловые и речевые ошибки в реферате
Удовлетворительно	Обучающийся демонстрирует логичность и доказательность изложения материала по теме задания, но допускает отдельные неточности при использовании ключевых понятий. Обучающийся не продемонстрировал способность к научному анализу, не высказывал в работе своего мнения, допустил ошибки в логическом обосновании своего ответа
Хорошо	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, в работе присутствуют ссылки на научные источники, мнения известных учёных в данной области
Отлично	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, при разработке реферата использовано не менее 5-8 научных источников. В работе выдвигаются новые идеи и трактовки, демонстрируется способность обучающегося анализировать материал, выражается его мнение по проблеме

### Выполнение реферата для формирования «ОПК-3.2»

1. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.
2. Система обеспечения информационной безопасности. Обеспечение информационной безопасности Российской Федерации.
3. Понятие информационной войны. Проблемы информационной войны.
4. Информационное оружие и его классификация.
5. Цели информационной войны, её составные части и средства её ведения. Объекты воздействия информационной войне.
6. Уровни ведения информационной войны. Информационные операции. Психологические операции. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети.
7. Основные положения государственной информационной политики Российской Федерации. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.
8. Виды защищаемой информации в сфере государственного и муниципального управления.
9. Обеспечение информационной безопасности организации.

### Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Обучающийся не раскрыл материал по теме задания или материал раскрыт поверхностно, излагаемый материал не систематизирован, выводы недостаточно аргументированы, обучающийся не высказывал своего мнения, не проявил способность к анализу, имеются смысловые и речевые ошибки в реферате
Удовлетворительно	Обучающийся демонстрирует логичность и доказательность изложения материала по теме задания, но допускает отдельные неточности при использовании ключевых понятий. Обучающийся не продемонстрировал способность к научному анализу, не высказывал в работе своего мнения, допустил ошибки в логическом обосновании своего ответа
Хорошо	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, в работе присутствуют ссылки на научные источники, мнения известных учёных в данной области
Отлично	Реферат написан грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения обучающегося обоснована, при разработке реферата использовано не менее 5-8 научных источников. В работе выдвигаются новые идеи и трактовки, демонстрируется способность обучающегося анализировать материал, выражается его мнение по проблеме

### Практическое задание для формирования «ОПК-3.3»

Центральный банк РФ для анализа экономической ситуации запросил у АО «Тюмень Нефть» информацию о количестве полученной прибыли за прошедший год и о прогнозах объёма добычи нефти на текущий год. Однако АО не предоставило истребуемой информации, мотивировав тем, что информация отнесена к коммерческой тайне. Имеет ли право Банк России получать данную информацию, и несёт ли ответственность Банк России, а также его должностные лица и работники за разглашение коммерческой тайны.

### Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объём выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объёма, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объёме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочётов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объёме без ошибок с соблюдением необходимой последовательности действий

### Практическое задание для формирования «ОПК-3.3»

Проведите анализ информационно-правовой нормы и определите вид формы предписания: организация должна определять действия, необходимые для устранения причин потенциальных несоответствий требованиям системы менеджмента информационной безопасности, с целью предотвратить их повторное появление.

#### Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

### Практическое задание для формирования «ОПК-3.3»

При реализации политики удаленного доступа определите, какими возможностями должен обладать межсетевой экран при передаче информации с грифом «особой важности» и к какому соответствующему классу он должен относиться.

#### Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

### Практическое задание для формирования «ОПК-3.3»

Определите, соответствуют ли ситуация принципам правового регулирования отношений в сфере информации, информационных технологий и защиты информации: после проведения аудиторской проверки в государственной организации было выявлено нецелевое использование бюджетных средств. Местные средства массовой информации подготовили публикацию об

использовании бюджетных средств, однако руководитель организации запретил публиковать данную информацию.

### Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

### Практическое задание для формирования «ОПК-3.3»

Определите, соответствуют ли ситуация принципам правового регулирования отношений в сфере информации, информационных технологий и защиты информации: в предисловии к роману писателя коротко была изложена биография автора, где были собраны сведения из его жизни, они соответствовали действительности, однако до их публикации у автора не было получено разрешение автора.

### Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

## **Вопросы для проведения промежуточной аттестации по итогам освоения дисциплины**

### *Тема 1. Актуальность проблемы информационной безопасности*

1. Перечислите этапы развития информационных технологий и методов обеспечения безопасности информации.
2. Назовите проблемы обеспечения информационной безопасности на современном этапе развития общества.
3. Определите значение информационной безопасности в развитии общества.
4. Назовите основные положения по обеспечению информационной безопасности на современном этапе.

### *Тема 2. Основные термины и определения категории «безопасность», виды безопасности*

5. Назовите источники, формы, виды, свойства информации.
6. Перечислите цели и решаемые задачи в обеспечении национальной безопасности.
7. Дайте определение информационной безопасности, цель и решаемые задачи.
8. Назовите жизненно важные интересы личности, общества, государства в сфере информационной безопасности.
9. Назовите объекты защиты в области информационной безопасности.
10. Назовите виды источников угроз информационной безопасности.
11. Назовите виды угроз информационной безопасности.

### *Тема 3. Национальная безопасность Российской Федерации. Место информационной безопасности в системе Национальной безопасности Российской Федерации.*

12. Назовите ценности и модели развития глобальной конкуренции
13. Дайте определение глобальное информационное противоборство на международной арене.
14. Дайте определение информационная безопасность в обеспечении национальной безопасности Российской Федерации.
15. Перечислите базовые нормативно-правовые документы Российской Федерации в области национальной, информационной безопасности.

### *Тема 4. Государственная система обеспечения информационной безопасности Российской Федерации*

16. Назовите органы власти которые входят в государственную систему обеспечения информационной безопасности Российской Федерации.
17. Назовите законодательные органы Российской Федерации.
18. Назначение и роль судебных органов Российской Федерации в обеспечении информационной безопасности и защиты информации.
19. Перечислите органы исполнительной власти Российской Федерации, которые проводят единую техническую политику в области информационной безопасности и защиты информации,
20. Назовите министерства, ведомства, федеральные службы, которые разрабатывают нормативные и руководящие документы в области информационной безопасности и защиты информации.

### *Тема 5. Законодательные акты Российской Федерации в области информационной безопасности, государственная тайна, конфиденциальная информация*

21. Перечислите основные нормативные акты РФ в области информационной безопасности, назначение и основные положения.
22. Перечислите нормативно-правовые и руководящие документы органов исполнительной власти РФ, назначение и основные положения в сфере информационной безопасности.
23. Перечислите виды тайн.
24. Дайте определение государственная тайна.
25. Дайте определение персональные данные.
26. Дайте определение коммерческая тайна.
27. Дайте определение служебная тайна.

### *Тема 6. Информация, как объект защиты, источники угроз, угрозы информационной безопасности*

28. Дайте определение - информация, как объекта защиты.
29. Дайте определение и назначение информационного право в обеспечении информационной безопасности, цели, задачи, принципы информационного права.
30. Значение и роль правового регулирования субъектов к объектам интеллектуальной собственности.
31. Приведите классификацию источников угроз информационной безопасности.
32. Приведите классификацию угроз информационной безопасности, методы и способы реализации угроз,
33. Назовите возможные каналы утечки, методы и способы несанкционированного доступа к защищаемой информации.

*Тема 7. Правовой уровень обеспечения информационной безопасности*

34. Назовите назначение, цели и задачи правового уровня обеспечения информационной безопасности.
35. Перечислите основные международные и российские стандарты в области информационной безопасности.
36. Основные положения по защите информации от несанкционированного доступа к объектам защиты.
37. Дайте классификацию информационных систем, цель и решаемые задачи.
38. Дайте классификацию автоматизированных систем (АС) по уровню защищенности от несанкционированного доступа (НСД).
39. Дайте классификацию средств вычислительной техники (СВТ) по уровню защищенности от несанкционированного доступа (НСД).
40. Дайте классификацию межсетевых экранов по уровню защищенности от несанкционированного доступа (НСД)
41. Дайте классификацию программного обеспечения по уровню контроля отсутствия не декларированных возможностей.

*Тема 8. Административный уровень, политика информационной безопасности предприятия*

42. Назовите назначение политики информационной безопасности в производственной деятельности предприятия.
43. Дайте определение политика информационной безопасности, назначение, состав и содержание документа.
44. Назовите назначение и содержание программы информационной безопасности, состав и содержание документа.
45. Перечислите методики анализа и оценки рисков, влияющих на состояние информационных безопасности.
46. Перечислите методы управление рисками по исключению реализации угроз информационной безопасности.
47. Перечислите основные мероприятия по построению системы обеспечения информационной безопасности на предприятии.

*Тема 9. Процедурный уровень информационной безопасности*

48. Перечислите меры процедурного уровня информационной безопасности, основные классы мер процедурного уровня.
49. Назовите методы и принципы управления персоналом.
50. Перечислите основные меры обеспечения физической защиты, направления обеспечения физической защиты, цель, решаемые задачи.
51. Перечислите основные меры поддержания работоспособности, реагирование на нарушения режима безопасности: назначение, цель, решаемые задачи.
52. Назовите основные меры планирования восстановительных работ: цель, решаемые задачи, методы по обеспечению работоспособностью информационных систем.

*Тема 10. Программно-технический уровень, сервисы информационной безопасности*

53. Дайте определение программно-технический уровень информационной безопасности, назначение, цели, решаемые задачи.



54. Назовите принципы архитектурной безопасности и сервисы информационной безопасности.
55. Дайте определение аутентификации, определение, назначение, решаемые задачи.
56. Перечислите методы управление доступом к информационным ресурсам, определение, назначение, решаемые задачи.
57. Дайте определение протоколирование и аудит, назначение, решаемые задачи.
58. Дайте определение вредоносные программ, классификация вредоносных программ, методы противодействия вредоносным программам.
59. Дайте определение криптографическая защита информации (шифрование), назначение, методы криптографической защиты информации.
60. Дайте определение электронная подпись, назначение, решаемые задачи.
61. Дайте определение межсетевое экранирование, назначение, решаемые задачи.
62. Перечислите методы обеспечения отказоустойчивости и безопасного восстановления информационных систем;
63. Дайте определение обеспечение высокой доступности (надежности) пользователей к информационно-коммуникационным системам.

### **Уровни и критерии итоговой оценки результатов освоения дисциплины**

	Критерии оценивания	Итоговая оценка
Уровень 1. Недостаточный	Незнание значительной части программного материала, неумение даже с помощью преподавателя сформулировать правильные ответы на задаваемые вопросы, невыполнение практических заданий	Неудовлетворительно/ Незачтено
Уровень 2. Базовый	Знание только основного материала, допустимы неточности в ответе на вопросы, нарушение логической последовательности в изложении программного материала, затруднения при решении практических задач	Удовлетворительно/ зачтено
Уровень 3. Повышенный	Твердые знания программного материала, допустимые несущественные неточности при ответе на вопросы, нарушение логической последовательности в изложении программного материала, затруднения при решении практических задач	Хорошо/ зачтено
Уровень 4. Продвинутый	Глубокое освоение программного материала, логически стройное его изложение, умение связать теорию с возможностью ее применения на практике, свободное решение задач и обоснование принятого решения	Отлично/ зачтено