

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Таныгин Максим Олегович

Должность: и.о. декана факультета фундаментальной и прикладной информатики

Дата подписания: 2025.01.10 10:00:00

Уникальный программный ключ:

65ab2aa0d384efe8480e6a4c688eddbc475e411a

## **Аннотация к рабочей программе**

### **дисциплины: «Информационно-аналитические системы безопасности»**

#### **Цель преподавания дисциплины**

Целью преподавания дисциплины «Информационно-аналитические системы безопасности» является овладение знаниями и практическими навыками в области информационно-аналитического обеспечения безопасности бизнеса, создание и эксплуатация современных программных и информационных систем, компьютерных технологий, изучение основ базовая подготовки в области информационной безопасности.

#### **Задачи изучения дисциплины**

- изучение методов и средств защиты информации, возможностей применения новых информационных технологий, информационно-аналитическое обеспечение безопасности бизнеса;
- изучение основ устройства и принципов функционирования автоматизированных систем (АС), методологии проектирования и построения защищенных АС, критериев и методов оценки защищенности АС, средств и методов защиты от несанкционированного доступа (НСД) к информации.
- создание и обеспечение работы узловых элементов национальной системы по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма на всех уровнях (международном, государственном, первичном).

#### **Компетенции, формируемые в результате освоения дисциплины**

Способен управлять рисками информационной безопасности (ПК-8);


Способен оценивать эффективность механизмов безопасности в информационных системах (ПК-10).

#### **Разделы дисциплины**

Сущность, структура и задачи аналитики СБ. Аналитика как интерфейс между теорией и практикой. Принципы организации аналитической деятельности в СБ. Технологический цикл информационно-аналитической работы. Аналитический режим потребления информации. Синтез информационно-аналитических СБ. Информационно-аналитические системы аутентификации. Информационно-аналитические системы защиты от несанкционированного доступа (НСД).

МИНОБРНАУКИ РОССИИ  
Юго-Западный государственный университет

УТВЕРЖДАЮ:  
Декан факультета  
фундаментальной и прикладной  
*(наименование ф-та полностью)*  
информатики



М.О. Таныгин

*(подпись, инициалы, фамилия)*

« 30 » 08 2022 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационно-аналитические системы безопасности  
*(наименование дисциплины)*

ОПОП ВО

10.04.01 Информационная безопасность  
*шифр и наименование направления подготовки (специальности)*

Защищённые информационные системы  
*наименование направленности (профиля, специализации)*

форма обучения

очная

*очная, очно-заочная, заочная*

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО – магистратура по направлению подготовки 10.04.01 Информационная безопасность на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищенные информационные системы», одобренного Ученым советом университета (протокол № 7 «28» февраля 2022 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы» на заседании кафедры информационной безопасности № 11 «30» июня 2022 г.

Зав. кафедрой \_\_\_\_\_ Таныгин М.О.

Разработчик программы \_\_\_\_\_  
к.т.н., доцент \_\_\_\_\_ Марухленко А.Л.  
*(ученая степень и ученое звание, Ф.И.О.)*

Директор научной библиотеки \_\_\_\_\_ Макаровская В.Г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол № 7 «28» 02 20 22 г., на заседании кафедры ИБ протокол № 1 от 30.08.2023  
*(наименование кафедры, дата, номер протокола)*

Зав. кафедрой \_\_\_\_\_

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол № « » 20 г., на заседании кафедры  
*(наименование кафедры, дата, номер протокола)*

Зав. кафедрой \_\_\_\_\_

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе на основании учебного плана ОПОП ВО 10.04.01 Информационная безопасность, профиль «Защищённые информационные системы», одобренного Ученым советом университета протокол № « » 20 г., на заседании кафедры  
*(наименование кафедры, дата, номер протокола)*

Зав. кафедрой \_\_\_\_\_

## **1 Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы**

### **1.1 Цель дисциплины**

Целью преподавания дисциплины «Информационно-аналитические системы безопасности» является овладение знаниями и практическими навыками в области информационно-аналитического обеспечения безопасности бизнеса, создание и эксплуатация современных программных и информационных систем, компьютерных технологий, изучение основ базовая подготовки в области информационной безопасности.

### **1.2 Задачи изучения дисциплины**

Задачи изучения учебной дисциплины:

- изучение методов и средств защиты информации, возможностей применения новых информационных технологий, информационно-аналитическое обеспечение безопасности бизнеса;
- изучение основ устройства и принципов функционирования автоматизированных систем (АС), методологии проектирования и построения защищенных АС, критериев и методов оценки защищенности АС, средств и методов защиты от несанкционированного доступа (НСД) к информации.
- создание и обеспечение работы узловых элементов национальной системы по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма на всех уровнях (международном, государственном, первичном).

### **1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы**

Таблица 1.3 – Результаты обучения по дисциплине

<i>Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной)</i>		<i>Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной</i>	<i>Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций</i>
<i>код комп-ии</i>	<i>наименование компетенции</i>		

ПК-8	Способен управлять рисками информационной безопасности	ПК-8.1 Формирует перечень угроз для защищаемой информационной системы	<b>Знать:</b> Методику анализа перечня угроз для защищаемой информационной системы <b>Уметь:</b> Анализировать и формировать перечень угроз для защищаемой информационной системы. <b>Владеть (или Иметь опыт деятельности):</b> методом формулировки перечня угроз для защищаемой информационной системы.
		ПК-8.2 Формирует критерии оценки каждого вида угроз в защищаемой системе	<b>Знать:</b> Методику формирования критериев оценки каждого вида угроз в защищаемой системе. <b>Уметь:</b> Анализировать критерии оценки каждого вида угроз в защищаемой системе. <b>Владеть (или Иметь опыт деятельности):</b> Навыками формирования критериев оценки каждого вида угроз в защищаемой системе.
		ПК-8.3 Классифицирует угрозы информационной безопасности исходя из существующих и оригинальных методик	<b>Знать:</b> Методику анализа классификации угрозы информационной безопасности исходя из существующих и оригинальных методик. <b>Уметь:</b> Анализировать и оформлять и классификации угрозы информационной безопасности исходя из существующих и оригинальных методик. <b>Владеть (или Иметь опыт деятельности):</b> Навыками классификации угрозы информационной безопасности исходя из существующих и оригинальных методик.
		ПК-8.4 Формирует перечень нарушителей информационной безопасности и их возможностей	<b>Знать:</b> Методику анализа формирования перечня нарушителей информационной безопасности и их возможностей. <b>Уметь:</b> Анализировать и формировать перечень нарушителей информационной безопасности и их возможностей. <b>Владеть (или Иметь опыт деятельности):</b> Навыками формирования перечня нарушителей информационной безопасности и их возможностей.
ПК-10	Способен оценивать эффективность механизмов безопасности в информационных системах	ПК-10.1 Оценивает эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик	<b>Знать:</b> Методику анализа оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик. <b>Уметь:</b> Анализировать оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик.

			<p><b>Владеть (или Иметь опыт деятельности):</b> навыками оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик.</p>
		<p>ПК-10.2 Оценивает соответствие механизмов безопасности системы требованиям нормативных документов и рискам</p>	<p><b>Знать:</b> Методику анализа и оценки соответствия механизмов безопасности системы требованиям нормативных документов и рискам. <b>Уметь:</b> Анализировать и оценивать соответствие механизмов безопасности системы требованиям нормативных документов и рискам.</p> <p><b>Владеть (или Иметь опыт деятельности):</b> навыками оценки соответствия механизмов безопасности системы требованиям нормативных документов и рискам.</p>
		<p>ПК-10.3 Формулирует критерии оценки эффективности механизмов безопасности, используемых в информационных системах</p>	<p><b>Знать:</b> Методику анализа критериев оценки эффективности механизмов безопасности, используемых в информационных системах. <b>Уметь:</b> Анализировать и формулировать критерии оценки эффективности механизмов безопасности, используемых в информационных системах. <b>Владеть (или Иметь опыт деятельности):</b> навыками анализа, управления и формулировки критериев оценки эффективности механизмов безопасности, используемых в информационных системах.</p>
		<p>ПК-10.4 Формулирует предложения по повышению эффективности механизмов безопасности, используемых в информационных системах</p>	<p><b>Знать:</b> Методику анализа формулировки предложения по повышению эффективности механизмов безопасности, используемых в информационных системах. <b>Уметь:</b> Анализировать формулировки предложения по повышению эффективности механизмов безопасности, используемых в информационных системах. <b>Владеть (или Иметь опыт деятельности):</b> навыками формулировки предложения по повышению эффективности механизмов безопасности, используемых в информационных системах.</p>



## 2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Информационно-аналитические системы безопасности» входит в базовую часть, формируемую участниками образовательных отношений, блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы магистратуры 10.04.01.Информационная безопасность профиль «Защищённые информационные системы». Дисциплина «Информационно-аналитические системы безопасности» изучается на 2 курсе в 3 семестре.

## 3 Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоёмкость (объём) дисциплины составляет 3 зачётные единицы, 108 часа

Таблица 3.1 – Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоёмкость дисциплины	108
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего)	54
в том числе:	
лекции	18
лабораторные занятия	
практические занятия	36
Самостоятельная работа обучающихся (всего)	53,9
Контроль (подготовка к экзамену)	36
Контактная работа по промежуточной аттестации (всего АттКР)	0,1
в том числе:	
зачет	0,1
зачет с оценкой	не предусмотрен
курсовая работа (проект)	не предусмотрена
экзамен (включая консультацию перед экзаменом)	не предусмотрен

## 4 Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

### 4.1 Содержание дисциплины

Таблица 4.1 – Содержание дисциплины, структурированное по темам (разделам)

/п	Раздел (тема) Дисциплины	Содержание
1.	Сущность, структура и задачи аналитики СБ.	Понятие и сущность аналитики СБ, структура и задачи аналитики СБ, информационно-аналитические технологии СБ, их задачи.
2.	Аналитика как интерфейс между теорией и практикой	Методы структурирования информации, методы поэтапной структуризации задач и группа морфологических методов, методы обработки и анализа числовых данных.
3.	Принципы организации аналитической деятельности в СБ.	Задачи и определения информационно-аналитического (ИА) обеспечения СБ, организационные формы субъектов ИА работы; системы, управляемые потоком событий
4.	Технологический цикл информационно-аналитической работы.	Поиск, отбор и анализ данных; неструктурированные текстовые данные; структурированные текстовые данные; анализ информативности источников.
5.	Аналитический режим потребления информации.	Режимы восприятия информации; средства автоматизации информационно-аналитической работы.
6.	Синтез информационно-аналитических СБ.	Создание информационно-аналитических СБ (ИА СБ); составные части ИА СБ; стадии и технология создания ИА СБ.
7.	Информационно-аналитические системы аутентификации.	Задачи аутентификации, понятие протокола аутентификации, основные схемы протоколов аутентификации.
8.	Информационно-аналитические системы защиты от несанкционированного доступа (НСД).	Основные принципы построения систем защиты от НСД, классификация уровней защиты от НСД, программно-аппаратный состав средств защиты от НСД.



Таблица 4.2 – Содержание дисциплины и ее методическое обеспечение

п/п	Раздел (тема) Дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости (по неделям семестра)	Компетенции
		ек., час	пр.	лб.			
	2				6	7	8
1.	Сущность, структура и задачи аналитики СБ.	2			У-1-5	С (1-2)	ПК-8 ПК-10
2.	Аналитика как интерфейс между теорией и практикой	2			У-1-5	С (3-4)	ПК-8 ПК-10
3.	Принципы организации аналитической деятельности в СБ.	2	1		У-1-5 МУ-1-5	С, ЗПР (5-6)	ПК-8 ПК-10
4.	Технологический цикл информационно-аналитической работы.	2			У-1-5	С (7-8)	ПК-8 ПК-10
5.	Аналитический режим потребления информации.	2	2		У-1-5 МУ-1-5	С, ЗПР (9-10)	ПК-8 ПК-10
6.	Синтез информационно-аналитических СБ.	2	3		У-1-5 МУ-1-5	С, ЗПР (11-12)	ПК-8 ПК-10
7.	Информационно аналитические системы аутентификации	2			У-1-5	С (13-15)	ПК-8 ПК-10
8.	Информационно аналитические системы защиты от несанкционированного доступа (НСД).	4	4		У-1-5 МУ-1-5	С, ЗПР (16-18)	ПК-8 ПК-10
	Итого	18	-	-	-	-	-

С – собеседование, ЗПР – защита практической работы

## 4.2 Лабораторные работы и практические занятия

Таблица 4.3 – Практические занятия

	Наименование практической работы	Объем, час.
1.	Анализ информации на предприятии	8
2.	Применение навыков анализа на примере Business Objects	8
3.	Основные понятия информационно-аналитических систем	10
4.	Оперативный анализ данных	10
Итого		36

## 4.3 Самостоятельная работа студентов (СРС)

Таблица 4.4 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Сущность, структура и задачи аналитики СБ.	1 неделя	6
2.	Аналитика как интерфейс между теорией и практикой	2 неделя	6
3.	Принципы организации аналитической деятельности в СБ.	4 неделя	6
4.	Технологический цикл информационно-аналитической работы.	5-7 неделя	6
5.	Аналитический режим потребления информации.	8-11 неделя	6
6.	Синтез информационно-аналитических СБ.	12-13 неделя	7
7.	Информационно аналитические системы аутентификации	14-15 неделя	8
8.	Информационно аналитические системы защиты от несанкционированного доступа (НСД).	16-18 неделя	8,9
Итого			53,9

## **5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине**

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала за счёт выкладывания на сайт кафедры ИБ в интернете;

- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

- путем разработки вопросов к зачету

- методических указаний к выполнению практических работ.

типографией университета

- путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы;

путем удовлетворения потребностей в тиражировании научной, учебной, учебно-методической литературы.

- и научной, учебной, учебно-методической литературы.

## **6 Образовательные технологии.**

Реализация компетентного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования общепрофессиональных компетенций обучающихся. В рамках дисциплины предусмотрены выполнение в ходе лабораторных работ практико-ориентированных заданий.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объём, час.
1.	Выполнение практической работы №1 «Анализ информации на предприятии»	Выполнение студентом интерактивных заданий по анализу информации на предприятии.	4
2.	Выполнение практической работы №2 «Применение навыков анализа на примере Business Objects»	Выполнение студентом интерактивных заданий по Применению навыков анализа информации на примере Business Objects.	4
3.	Выполнение практической работы №3 «Основные понятие информационно-аналитических систем»	Групповое обсуждение с элементами дискуссии рассматриваемых на лекции вопросов	4
4.	Выполнение практической работы №4 «Оперативный анализ данных»	Групповое обсуждение с элементами дискуссии рассматриваемых на лекции вопросов	4
	Итого		16

### **Технологии использования воспитательного потенциала дисциплины**

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует правовому, экономическому, профессионально-трудовому, воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

– целенаправленный отбор преподавателем и включение в лекционный материал, материал для практических и (или) лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки (производства, экономики, культуры), высокого профессионализма ученых (представителей производства, деятелей культуры), их ответственности за результаты и последствия деятельности для человека и

общества; примеры подлинной нравственности людей, причастных к развитию науки и производства;

– применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, (командная работа, разбор конкретных ситуаций);

– личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

## **7 Фонд оценочных средств для проведения промежуточной аттестации**

### **7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы**

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
Способен управлять рисками информационной безопасности (ПК-8).	Оценка защищённости информационных систем Теоретические основы компьютерной безопасности Информационно-аналитические системы безопасности Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем		Производственная преддипломная практика
Способен оценивать эффективность механизмов безопасности в информационных системах (ПК-10).	Технологии обеспечения информационной безопасности объектов Информационно-аналитические системы безопасности Экспертные системы комплексной оценки безопасности информационных и телекоммуникационных систем		Производственная преддипломная практика

## 7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 7.2 – Показатели и критерии оценивания компетенций, шкала оценивания

Код компетенции/ этап (указываются название этапа из п.7.1)	Показатели оценивания компетенций (индикаторы достижения компетенций, закрепленные за дисциплиной)	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно»)	Продвинутый уровень (хорошо)	Высокий уровень («отлично»)
1	2	3	4	5
ПК-8 /основной	ПК-8.1 Формирует перечень угроз для защищаемой информационной системы	<b>Знать:</b> Методику анализа перечня угроз для защищаемой информационной системы <b>Уметь:</b> Анализировать перечень угроз для защищаемой информационной системы. <b>Владеть (или Иметь опыт деятельности):</b> методом анализа каких-либо угроз.	<b>Знать:</b> Методику анализа перечня угроз для защищаемой информационной системы <b>Уметь:</b> Анализировать и формировать перечень угроз для защищаемой информационной системы. <b>Владеть (или Иметь опыт деятельности):</b> методом анализа каких-либо угроз.	<b>Знать:</b> Методику анализа перечня угроз для защищаемой информационной системы <b>Уметь:</b> Анализировать и формировать перечень угроз для защищаемой информационной системы. <b>Владеть (или Иметь опыт деятельности):</b> методом формулировки перечня угроз для защищаемой информационной системы.
	ПК-8.2 Формирует критерии оценки каждого вида угроз в защищаемой системе	<b>Знать:</b> Методику формирования критериев оценки угроз в защищаемой системе. <b>Уметь:</b> Анализировать критерии оценки угроз в защищаемой системе.	<b>Знать:</b> Методику формирования критериев оценки каждого вида угроз в защищаемой системе. <b>Уметь:</b> Анализировать критерии оценки каждого вида угроз в	<b>Знать:</b> Методику формирования критериев оценки каждого вида угроз в защищаемой системе. <b>Уметь:</b> Анализировать критерии оценки каждого вида угроз в защищаемой системе.

		<b>Владеть (или Иметь опыт деятельности):</b> Навыками формирования критериев оценки угроз.	защищаемой системе. <b>Владеть (или Иметь опыт деятельности):</b> Навыками формирования критериев оценки любого вида угроз в защищаемой системе.	<b>Владеть (или Иметь опыт деятельности):</b> Навыками формирования критериев оценки каждого вида угроз в защищаемой системе.
ПК-8.3 Классифицирует угрозы информационной безопасности исходя из существующих и оригинальных методик	<b>Знать:</b> Методику анализа классификации угрозы информационной безопасности. <b>Уметь:</b> Анализировать и оформлять и классификации угрозы информационной безопасности исходя из существующих и оригинальных методик. <b>Владеть (или Иметь опыт деятельности):</b> Навыками классификации угрозы информационной безопасности.	<b>Знать:</b> Методику анализа классификации угрозы информационной безопасности исходя из существующих и оригинальных методик. <b>Уметь:</b> Анализировать и оформлять и классификации угрозы информационной безопасности исходя из существующих и оригинальных методик. <b>Владеть (или Иметь опыт деятельности):</b> Навыками классификации угрозы информационной безопасности.	<b>Знать:</b> Методику анализа классификации угрозы информационной безопасности исходя из существующих и оригинальных методик. <b>Уметь:</b> Анализировать и оформлять и классификации угрозы информационной безопасности исходя из существующих и оригинальных методик. <b>Владеть (или Иметь опыт деятельности):</b> Навыками классификации угрозы информационной безопасности исходя из существующих и оригинальных методик.	<b>Знать:</b> Методику анализа классификации угрозы информационной безопасности исходя из существующих и оригинальных методик. <b>Уметь:</b> Анализировать и оформлять и классификации угрозы информационной безопасности исходя из существующих и оригинальных методик. <b>Владеть (или Иметь опыт деятельности):</b> Навыками классификации угрозы информационной безопасности исходя из существующих и оригинальных методик.
ПК-8.4 Формирует перечень нарушителей информационной безопасности и их возможностей	<b>Знать:</b> Методику анализа формирования перечня нарушителей информационной безопасности. <b>Уметь:</b> Анализировать и	<b>Знать:</b> Методику анализа формирования перечня нарушителей информационной безопасности и их возможностей. <b>Уметь:</b>	<b>Знать:</b> Методику анализа формирования перечня нарушителей информационной безопасности и их возможностей. <b>Уметь:</b>	<b>Знать:</b> Методику анализа формирования перечня нарушителей информационной безопасности и их возможностей. <b>Уметь:</b>



		<p>формировать перечень нарушителей информационной безопасности.</p> <p><b>Владеть (или Иметь опыт деятельности):</b></p> <p>Навыками формирования перечня нарушителей информационной безопасности.</p>	<p>Анализировать и формировать перечень нарушителей информационной безопасности и их возможностей.</p> <p><b>Владеть (или Иметь опыт деятельности):</b></p> <p>Навыками формирования перечня нарушителей информационной безопасности.</p>	<p>Анализировать и формировать перечень нарушителей информационной безопасности и их возможностей.</p> <p><b>Владеть (или Иметь опыт деятельности):</b></p> <p>Навыками формирования перечня нарушителей информационной безопасности и их возможностей.</p>
ПК-10 / основной	ПК-10.1	<p>Оценивает эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик</p> <p><b>Знать:</b> Методику анализа оценки эффективности применяемых программно-аппаратных средств защиты информации.</p> <p><b>Уметь:</b></p> <p>Анализировать оценки эффективности применяемых программно-аппаратных средств защиты информации.</p> <p><b>Владеть (или Иметь опыт деятельности):</b></p> <p>навыками оценки эффективности применяемых программно-аппаратных средств защиты информации.</p>	<p>Оценивает эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик.</p> <p><b>Знать:</b> Методику анализа оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик.</p> <p><b>Уметь:</b></p> <p>Анализировать оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик.</p> <p><b>Владеть (или Иметь опыт деятельности):</b></p> <p>навыками оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик.</p>	<p>Оценивает эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик.</p> <p><b>Знать:</b> Методику анализа оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик.</p> <p><b>Уметь:</b></p> <p>Анализировать оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик.</p> <p><b>Владеть (или Иметь опыт деятельности):</b></p> <p>навыками оценки эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик.</p>
	ПК-10.2	<p><b>Знать:</b> Методику</p>	<p><b>Знать:</b> Методику</p>	<p><b>Знать:</b> Методику</p>

	<p>Оценивает соответствие механизмов безопасности системы требованиям нормативных документов и рискам</p>	<p>оценки соответствия механизмов безопасности системы требованиям нормативных документов <b>Уметь:</b> оценивать соответствие механизмов безопасности системы требованиям нормативных документов <b>Владеть (или Иметь опыт деятельности):</b> навыками оценки механизмов безопасности системы.</p>	<p>анализа и оценки соответствия механизмов безопасности системы требованиям нормативных документов и рискам. <b>Уметь:</b> оценивать соответствие механизмов безопасности системы требованиям нормативных документов. <b>Владеть (или Иметь опыт деятельности):</b> навыками оценки механизмов безопасности системы.</p>	<p>анализа и оценки соответствия механизмов безопасности системы требованиям нормативных документов и рискам. <b>Уметь:</b> Анализировать и оценивать соответствие механизмов безопасности системы требованиям нормативных документов и рискам. <b>Владеть (или Иметь опыт деятельности):</b> навыками оценки соответствия механизмов безопасности системы требованиям нормативных документов и рискам.</p>
ПК-10.3 Формулирует критерии оценки эффективности механизмов безопасности.	<p><b>Знать:</b> Методику анализа критериев оценки эффективности механизмов безопасности информационных системах. <b>Уметь:</b> Анализировать и формулировать критерии оценки эффективности механизмов безопасности, используемых в информационных системах. <b>Владеть (или</b></p>	<p><b>Знать:</b> Методику анализа критериев оценки эффективности механизмов безопасности, используемых в информационных системах. <b>Уметь:</b> Анализировать и формулировать критерии оценки эффективности механизмов безопасности, используемых в информационных системах.</p>	<p><b>Знать:</b> Методику анализа критериев оценки эффективности механизмов безопасности, используемых в информационных системах. <b>Уметь:</b> Анализировать и формулировать критерии оценки эффективности механизмов безопасности, используемых в информационных системах.</p>	<p><b>Знать:</b> Методику анализа критериев оценки эффективности механизмов безопасности, используемых в информационных системах. <b>Уметь:</b> Анализировать и формулировать критерии оценки эффективности механизмов безопасности, используемых в информационных системах.</p>

		<p><b>Иметь опыт деятельности):</b> навыками анализа, и формулировки критериев оценки эффективности механизмов безопасности.</p>	<p><b>Владеть (или Иметь опыт деятельности):</b> навыками анализа, и формулировки критериев оценки эффективности механизмов безопасности.</p>	<p><b>Владеть (или Иметь опыт деятельности):</b> навыками анализа, управления и формулировки критериев оценки эффективности механизмов безопасности, используемых в информационных системах.</p>
ПК-10.4 Формулирует предложения по повышению эффективности механизмов безопасности, используемых в информационных системах	<p><b>Знать:</b> Методику анализа формулировки предложения по повышению эффективности механизмов безопасности. <b>Уметь:</b> Анализировать формулировки предложения по повышению эффективности механизмов безопасности. <b>Владеть (или Иметь опыт деятельности):</b> навыками формулировки предложения по повышению эффективности механизмов безопасности.</p>	<p><b>Знать:</b> Методику анализа формулировки предложения по повышению эффективности механизмов безопасности, используемых в информационных системах. <b>Уметь:</b> Анализировать формулировки предложения по повышению эффективности механизмов безопасности, используемых в информационных системах. <b>Владеть (или Иметь опыт деятельности):</b> навыками формулировки предложения по повышению эффективности механизмов безопасности.</p>	<p><b>Знать:</b> Методику анализа формулировки предложения по повышению эффективности механизмов безопасности, используемых в информационных системах. <b>Уметь:</b> Анализировать формулировки предложения по повышению эффективности механизмов безопасности, используемых в информационных системах. <b>Владеть (или Иметь опыт деятельности):</b> навыками формулировки предложения по повышению эффективности механизмов безопасности, используемых в информационных системах.</p>	

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

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля успеваемости

П/П	Раздел дисциплины (тема)	Код контролируемой компетенции (или её части)	Технология формирования	Оценочные средства		Описание шкал оценивания
				наименование	№ заданий	
1	2	3	4	5	6	7
1.	Сущность, структура и задачи аналитики СБ.	ПК-8 ПК-10	Лекция, СРС	ВС	1-5	Согласно табл.7.2
2.	Аналитика как интерфейс между теорией и практикой	ПК-8 ПК-10	Лекция, СРС	ВС	1-5	Согласно табл.7.2
3.	Принципы организации аналитической деятельности в СБ.	ПК-8 ПК-10	Лекция, СРС, практическая работа	ВС, КВЗПР	1-5 1-5	Согласно табл.7.2
4.	Технологический цикл информационно-аналитической работы.	ПК-8 ПК-10	Лекция, СРС	ВС	1-5	Согласно табл.7.2
5.	Аналитический режим потребления информации.	ПК-8 ПК-10	Лекция, СРС, практическая работа	ВС, КВЗПР	1-5 1-5	Согласно табл.7.2
6.	Синтез информационно-аналитических СБ.	ПК-8 ПК-10	Лекция, СРС, практическая работа	ВС, КВЗПР	1-5	Согласно табл.7.2
7.	Информационно-аналитические системы аутентификации.	ПК-8 ПК-10	Лекция, СРС	ВС	1-5	Согласно табл.7.2
8.	Информационно-аналитические системы защиты от несанкционированного доступа (НСД).	ПК-8 ПК-10	Лекция, СРС, практическая работа	ВС, КВЗПР	1-5 1-5	Согласно табл.7.2

ВС- вопросы для собеседования, КВЗПР- контрольные вопросы для защиты практической работы

## Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для собеседования по теме 1 «Сущность, структура и задачи  
аналитики СБ.».

1. Назовите сущность аналитики СБ.
2. Перечислите основные и дополнительные задачи аналитики СБ.
3. Понятие аналитики СБ.
4. Структура аналитики СБ.
5. Соотношение аналитики СБ и смежных категорий.

Контрольные вопросы для защиты практической работы №3  
«Основные понятие информационно-аналитических систем»

1. Что такое аналитика в целом?
2. Что такое информационно-аналитическая система? Приведите примеры.
3. Что такое OSINT?
4. В чем заключается сущность и задачи информации?
5. Основные схемы сертификации средств защиты информации.

Типовые задания для проведения промежуточной аттестации  
обучающихся

*Промежуточная аттестация* по дисциплине проводится в форме зачета. Зачет проводится в виде компьютерного тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 4 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

*Умения, навыки (или опыт деятельности) и компетенции* проверяются с помощью компетентностно-ориентированных задач (ситуационных,

производственных или кейсового характера) и различного вида конструкторов.

Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

### Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

Для чего производится предварительное обследование объекта автоматизации?

- 1) для формирования концепции создания системы
- 2) для создания прототипа системы
- 3) для выяснения готовности предприятия к автоматизации
- 4) для формирования команды, которая будет работать над созданием системы

Задание в открытой форме:

1. В структуру информационного обеспечения входит...
2. На этапе хранения данных информационная система охватывает...
3. База данных-это...

Задание на установление правильной последовательности

Установить последовательность этапов внедрения системы безопасности

1. Внедрение организационных мер защиты информации, в том числе, разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ходе эксплуатации объекта
2. Выявление и анализ уязвимостей программных и технических средств, принятие мер по их устранению
3. Установка и настройка средств защиты информации
4. Испытания и опытная эксплуатация системы защиты информации

Задание на установление соответствия:  
Установите взаимно однозначное соответствие

1.	Выявление критически важной информации	А	на этом этапе выполняется непосредственно специалистами, проводящими аудит. От результатов этой работы зависит выбор схемы построения информационной безопасности
2	Выявление слабых мест в корпоративной безопасности	Б	Это завершающий этап аудита, в ходе которого на основании проведенного анализа составляется список конкретных мер, которые необходимо принять для охраны корпоративных секретов компании
3	Оценка возможностей защиты информации	В	на этом этапе происходит определение тех документов и данных, безопасность которых имеет огромное значение для компании, а утечка – несет огромные убытки.

Компетентностно-ориентированная задача:

Настроить и описать все этапы установления межсетевого взаимодействия между двумя защищенными сетевыми инфраструктурами системы.

Полностью оценочные материалы и оценочные средства для проведения промежуточной аттестации обучающихся представлены в УММ по дисциплине.

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

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016 «О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ»;



– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля успеваемости* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	Балл	примечание	балл	примечание
Выполнение практической работы №1 «Анализ информации на предприятии»	4	Выполнил, доля правильных ответов менее 50%	8	Выполнил и доля правильных ответов более 50%
Выполнение практической работы №2 «Применение навыков анализа на примере Business Objects»	4	Выполнил, доля правильных ответов менее 50%	8	Выполнил и доля правильных ответов более 50%
Выполнение практической работы №3 «Основные понятие информационно-аналитических систем»	4	Выполнил, доля правильных ответов менее 50%	8	Выполнил и доля правильных ответов более 50%
Выполнение практической работы №4 «Оперативный анализ данных»	4	Выполнил, доля правильных ответов менее 50%	8	Выполнил и доля правильных ответов более 50%
Собеседование по теме 1-2	2	Доля правильных ответов менее 50%	4	Доля правильных ответов более 50%
Собеседование по теме 3-4	2	Доля правильных ответов менее 50%	4	Доля правильных ответов более 50%
Собеседование по теме 5-6	2	Доля правильных ответов менее 50%	4	Доля правильных ответов более 50%
Собеседование по теме 7-8	2	Доля правильных ответов менее 50%	4	Доля правильных ответов более 50%
<b>ИТОГО</b>	<b>24</b>		<b>48</b>	

Для *промежуточной аттестации обучающихся*, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ –16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме – 2 балла,
  - задание в открытой форме – 2 балла,
  - задание на установление правильной последовательности – 2 балла,
  - задание на установление соответствия – 2 балла,
  - решение компетентностно-ориентированной задачи – 6 баллов.
- Максимальное количество баллов за тестирование – 36 баллов.

## **8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины**

### **8.1 Основная литература**

- 1) Ипатова, Э. Р. Методологии и технологии системного проектирования информационных систем : учебник / Э. Р. Ипатова, Ю. В. Ипатов. – 3-е изд., стер. – Москва : ФЛИНТА, 2021. – 256 с. – URL: <https://biblioclub.ru/index.php?page=book&id=79551> (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.
- 2) Технологии обеспечения безопасности информационных систем : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. – URL: <https://biblioclub.ru/index.php?page=book&id=598988> (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

### **8.2 Дополнительная литература**

- 3) Аверченков, В. И. История развития системы государственной безопасности России : учебное пособие / В. И. Аверченков, В. В. Ерохин, О. М. Голембиовская ; науч. ред. Ю. Т. Трифанков. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 193 с. – URL: <https://biblioclub.ru/index.php?page=book&id=93267> (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.
- 4) Алдохина, О. И. Информационно-аналитические системы и сети : учебное пособие / О. И. Алдохина, О. Г. Басалаева. – Кемерово : КемГУКИ, 2010. – Часть 1. Информационно-аналитические системы. – 148 с. - URL: <https://biblioclub.ru/index.php?page=book&id=227684> (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.
- 5) Ветошкин, А. Г. Нормативное и техническое обеспечение безопасности жизнедеятельности: учебно-практическое пособие : в 2 частях / А. Г. Ветошкин. – Москва ; Вологда : Инфра-Инженерия, 2017. – Часть 1. Нормативно-управленческое обеспечение безопасности жизнедеятельности. – 471 с. – URL: <https://biblioclub.ru/index.php?page=book&id=466497> (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.

### 8.3 Перечень методических указаний

1) Анализ информации на предприятии [Электронный ресурс] : методические указания по выполнению практических работ по дисциплине «Информационно-аналитические системы безопасности», для студентов направления подготовки 10.04.01 / Юго-Зап. гос. ун-т ; сост.: И. В. Калущкий, А.А. Татаринцева - Курск : ЮЗГУ, 2017. - 21 с. - Библиогр.: с. 21.

2) Применение навыков анализа на примере Business Objects [Электронный ресурс] : методические указания по выполнению практических работ по дисциплине «Информационно-аналитические системы безопасности», для студентов направления подготовки 10.04.01 / Юго-Зап. гос. ун-т ; сост.: И. В. Калущкий, А.А. Ус - Курск : ЮЗГУ, 2017. - 7 с. - Библиогр.: с. 7.

3) Основные понятия информационно-аналитических систем [Электронный ресурс] : методические указания по выполнению практических работ по дисциплине «Информационно-аналитические системы безопасности», для студентов направления подготовки 10.04.01 / Юго-Зап. гос. ун-т ; сост.: И. В. Калущкий, А.А. Ус - Курск : ЮЗГУ, 2017. - 20 с. - Библиогр.: с. 20.

4) Оперативный анализ данных [Электронный ресурс] : методические указания по выполнению практических работ по дисциплине «Информационно-аналитические системы безопасности», для студентов направления подготовки 10.04.01 / Юго-Зап. гос. ун-т ; сост.: И. В. Калущкий, А.А. Татаринцева - Курск : ЮЗГУ, 2017. - 25 с. - Библиогр.: с. 25.

5) Основные аспекты информационно-аналитических систем безопасности [Электронный ресурс] : методические указания по выполнению самостоятельных работ по дисциплине «Информационно-аналитические системы безопасности», для студентов направления подготовки 10.04.01 / Юго-Зап. гос. ун-т ; сост.: И. В. Калущкий Е.М. Чуденко, А.А. Чеснокова. - Курск : ЮЗГУ, 2017. - 13 с. - Библиогр.: с. 12.

### 9 Перечень ресурсов информационно-телекоммуникационной сети Интернет

1. Федеральная служба безопасности [официальный сайт]. Режим доступа: <http://www.fsb.ru/>

6) Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: <http://fstec.ru/>

7) Корпорация Microsoft [официальный сайт]. Режим доступа: <http://microsoft.com/>

8) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: <http://biblioclub.ru>

9) Компания «Консультант Плюс» [официальный сайт]. Режим доступа: <http://www.consultant.ru>

- 10) Научно-информационный портал ВИНТИ РАН [официальный сайт]. Режим доступа: <http://www.consultant.ru/>
- 11) База данных "Патенты России"
- 12) Компания Cisco [официальный сайт] [https://www.cisco.com/c/ru\\_ru/index.html](https://www.cisco.com/c/ru_ru/index.html)
- 13) ЗАО «Лаборатория Касперского» [корпоративный блог] <https://www.kaspersky.ru/blog/>
- 14) Аналитический раздел компании «Код Безопасности» <https://www.securitycode.ru/documents/analytics/>
- Сайт для IT-специалистов [www.habrahabr.ru](http://www.habrahabr.ru)

## **10 Методические указания для обучающихся по освоению дисциплины**

Основными видами аудиторной работы студента при изучении дисциплины «Информационно-аналитические системы безопасности» являются лекции, практические работы. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают практические занятия и тестирования, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Практическому занятию предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по практическим работам.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Информационно-аналитические системы безопасности»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у

студентов умения работать с учебником и литературой. Изучение литературы и справочной документации составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немислима серьезная работа над литературой. Систематическое конспектирование помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Безопасность операционных систем» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Информационно-аналитические системы безопасности» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

## **11 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)**

- Libreoffice (Бесплатная, GNU General Public License) -  
<https://ru.libreoffice.org/> ;

- Microsoft Office 2016. Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»;

- Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,

- Windows 7, договор IT000012385;

## **12 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

Учебная аудитория для проведения занятий лекционного и практического типа или лаборатории кафедры информационная безопасность, оснащенные мебелью: столы, стулья для обучающихся; стол,

стул для преподавателя; доска, проектор для демонстрации презентаций. Помещение для самостоятельной работы Компьютер PDC2160/iC33/2\*512Mb/HDD 160Gb/DVD-ROM/FDD/ATX350W/ K/m/ OFF/L 7" TFT E700 (6 шт)

### **13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья**

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

*Для лиц с нарушением слуха* возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

*Для лиц с нарушением зрения* допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

*Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата,* на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочесть задание, оформить ответ, общаться с преподавателем).

**14 Лист дополнений и изменений, внесенных в рабочую программу дисциплины**

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	изменённых	заменённых	аннулированных	новых			