

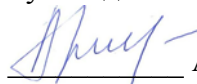


МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное автономное образовательное учреждение  
высшего образования  
«Дальневосточный федеральный университет»  
(ДВФУ)

**ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ (ШКОЛА)**

«СОГЛАСОВАНО»

Руководитель ОП

 Артемьева И.Л.

«Утверждаю»

И.о. директора департамента

 Смагин С.В.  
« 20 » июня 2022 г.



**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**  
**Информационная безопасность**

Направление подготовки 01.04.02 «Прикладная математика и информатика»

(Перспективные методы искусственного интеллекта в сетях передачи и обработки данных)

**Форма подготовки очная**

курс 1 семестр 2  
лекции 36 час.  
практические занятия 36 час.  
лабораторные работы 0 час.  
всего часов аудиторной нагрузки 72 час.  
самостоятельная работа 72 час.  
в том числе на подготовку к экзамену 27 час.  
контрольные работы (количество) не предусмотрены  
курсовая работа/курсовой проект не предусмотрены  
зачет не предусмотрен  
экзамен 2 семестр

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта по направлению подготовки 01.04.02 Прикладная математика и информатика, утвержденного приказом Министерства образования и науки РФ от 10.01.2018 № 13 (с изменениями и дополнениями).

Рабочая программа составлена на основе разработанной и утвержденной Ученым советом факультета вычислительной математики и кибернетики Московского государственного университета имени М.В. Ломоносова (протокол № 7 от «29» сентября 2021 г.) РПД «Информационная безопасность».

Рабочая программа обсуждена на заседании департамента программной инженерии и искусственного интеллекта ИМиКТ ДВФУ, протокол № 6.1а от «17» июня 2022 г.

И.о. директора департамента программной инженерии и искусственного интеллекта ИМиКТ ДВФУ  
к.т.н. Смагин С.В.

Составитель (ли): профессор департамента ПИИИ ИМиКТ ДВФУ д.т.н. Артемьева И.Л.,  
Пилюгин П. Л. к.т.н., с.н.с. факультет ВМК МГУ имени М.В.Ломоносова

Владивосток  
2022

**Оборотная сторона титульного листа РПД**

**I. Рабочая программа пересмотрена на заседании департамента:**

Протокол от «\_\_\_\_\_» \_\_\_\_\_ 200 г. № \_\_\_\_\_

Директор департамента \_\_\_\_\_  
(подпись) (И.О. Фамилия)

**II. Рабочая программа пересмотрена на заседании департамента:**

Протокол от «\_\_\_\_\_» \_\_\_\_\_ 200 г. № \_\_\_\_\_

Директор департамента \_\_\_\_\_  
(подпись) (И.О. Фамилия)

Рабочая программа дисциплины разработана при участии Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М. В. Ломоносова» в рамках Соглашения о предоставлении из федерального бюджета грантов в форме субсидий на разработку программ бакалавриата и программ магистратуры по профилю «искусственный интеллект», а также Программы развития «Образовательного комплекса по Искусственному Интеллекту» МГУ имени М.В. Ломоносова на период 2021-2024 гг. от 27 сентября 2021 г.

### **Цели и задачи освоения дисциплины:**

**Цель:** Формирование у студентов необходимого объема теоретических и практических знаний об основных принципах, методах и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах, умений и навыков практической реализации методов искусственного интеллекта в управлении информационной безопасностью.

#### **Задачи:**

1. ознакомление с основными методами обеспечения информационной безопасности;
2. ознакомление с теоретическими основами информационной безопасности операционных систем и баз данных, вычислительных сетей;
3. ознакомление с методическим и организационным обеспечением информационной безопасности;
4. изучение вопросов обеспечения информационной безопасности;
5. развитие навыков разработки и модификации программного и аппаратного обеспечения технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях;
6. формирование у обучающихся навыков применения методов визуализации результатов работы с применением современного программного обеспечения с учетом требований информационной безопасности.

Изучение дисциплины базируется на освоении знаний по математическому анализу, теории вероятностей, математической статистике.

В результате изучения данной дисциплины у обучающихся формируются следующие компетенции:

Общепрофессиональные компетенции выпускников и индикаторы их достижения:

Наименование категории (группы) общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции (результат освоения)	Код и наименование индикатора достижения компетенции
Информационно-коммуникационные технологии для профессиональной деятельности	<b>ОПК-4</b> Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	ОПК-4.3 Использует современные подходы к верификации ПО в профессиональной деятельности с учетом требований информационной безопасности

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения по дисциплине)
ОПК-4.3 Использует современные подходы к верификации ПО в профессиональной деятельности с учетом требований информационной безопасности	<i>Знает</i> современные подходы к верификации ПО, их достоинства и недостатки. <i>Умеет</i> применять подходы к уменьшению количества уязвимостей в исходном коде на основе систем типов. <i>Владеет</i> методами визуализации результатов работы с применением современного программного обеспечения с учетом требований информационной безопасности

**Профессиональные компетенции выпускников и индикаторы их достижения:**

Тип задач	Код и наименование профессиональной компетенции (результат освоения)	Код и наименование индикатора достижения компетенции
Производственно-технологический	<b>ПК-12</b> Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях	ПК-12.1 Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях
		ПК-12.2 Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения по дисциплине)
ПК-12.1 Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	<i>Знает</i> новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях <i>Умеет</i> разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях <i>Владеет</i> методами создания кода программного обеспечения в соответствии с проектом
ПК-12.2 Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для	<i>Знает</i> особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях

решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	<i>Умеет</i> модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях <i>Владеет</i> методами модернизации программного обеспечения
--	---

## 1. Трудоемкость дисциплины и видов учебных занятий по дисциплине

Общая трудоемкость дисциплины составляет 4 зачётные единицы 144 академических часа, в том числе 72 академических часа, отведенных на контактную работу обучающихся с преподавателем (36 академических часов занятий лекционного типа, 36 академических часов занятий практического типа) и 72 академических часа на самостоятельную работу обучающихся (включая 27 часов на подготовку к экзамену).

(1 зачетная единица соответствует 36 академическим часам).

Видами учебных занятий и работы обучающегося по дисциплине являются:

Обозначение	Виды учебных занятий и работы обучающегося
Лек	Лекции
Пр	Практические занятия
СР:	Самостоятельная работа обучающегося в период теоретического обучения
в том числе контроль	Самостоятельная работа обучающегося и контактная работа обучающегося с преподавателем в период промежуточной аттестации

## Структура дисциплины:

### Форма обучения – очная

	Наименование раздела дисциплины	Семестр	Количество часов по видам учебных занятий и работы обучающегося					Контроль из часов на СР	Формы промежуточной аттестации
			Лек	Лаб	Пр	ОК	СР		
1	Тема 1. Задачи и методы обеспечения информационной безопасности	2	6		6		12	27	Экзамен
2	Тема 2. Теоретические основы информационной безопасности операционных систем и баз данных	2	6		6		12		
3	Тема 3. Информационная безопасность вычислительных сетей	2	6		6		12		
4	Тема 4. Методическое и организационное обеспечение информационной безопасности	2	6		6		12		
5	Тема 5. Проблемные вопросы	2	6		6		12		

	обеспечения информационной безопасности автоматизированных систем и вычислительных сетей							
6	Тема 6. Использование средств машинного обучения и искусственного интеллекта в управлении информационной безопасностью	2	6		6		12	
7	Промежуточная аттестация (экзамен)	2						27
	Итого:		36		36		72	

## 2. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

№ п/п	Наименование разделов (тем) дисциплины	Содержание разделов (тем) дисциплин
1.	Тема 1. Задачи и методы обеспечения информационной безопасности	<p>Термины и определения. Классификация угроз несанкционированного доступа к информации в АС. Общая характеристика источников угроз несанкционированного доступа в АС. Общая характеристика уязвимостей АС и вычислительных сетей. Угрозы программно-математических воздействий. Компьютерные вирусы и “тройские кони”. Модели нарушителя. Основные функции систем защиты информации.</p> <p>Процедура проверки подлинности субъектов и объектов, параметры парольной идентификации, особенности аутентификации в вычислительных сетях: задачи аутентификации, авторизации и акаунтинга (AAA).</p> <p>Модель системы защиты с полным перекрытием, субъектно-объектная модель системы защиты, понятие изолированной системы, особенности моделирования механизмов безопасности операционных систем и баз данных, основные виды моделей и политик управления доступом — ограниченность моделей и проблемы изменения прав доступа.</p> <p>Методы аутентификации и разграничения доступа в операционных системах Windows и Linux.</p>
2.	Тема 2. Теоретические основы информационной безопасности операционных систем и баз данных	<p>Строгие протоколы аутентификации. Протокол Нидхем-Шредера для симметричной и асимметричной криптографии. Протоколы на основе ключевых хеш-функций.</p> <p>Использование цифровой подписи.</p> <p>Матрица доступа, пятимерное пространства безопасности Хартсона, модели HRU и Take-Grant, основные результаты, их достоинства и недостатки, основные направления развития.</p> <p>MLS модель «военной безопасности», модель Белла-ЛаПадулы, решетки безопасности Деннинг. Модель Биба.</p> <p>Тематические классификаторы и решетки мультирубрик.</p> <p>Использование функциональной структуры организации для управления доступом, индивидуально групповая модель управления доступом.</p>

3.	<p>Тема 3. Информационная безопасность вычислительных сетей</p>	<p>Субъекты и объекты компьютерных атак в сетях, виды сетевых атак; методы защиты вычислительных сетей: задачи аутентификации, авторизации и акаунтинга (AAA), сервера безопасности (RADIUS, Kerberos). Задачи фильтрации сетевого трафика. Межсетевые экраны. Фильтрация пакетов. Анализ приложений. Анализ состояний. Прокси сервер. DLP системы. Понятие DMZ.</p> <p>Управление доступом в распределенных системах. Методы оптимизации и методы теории игр при моделировании систем защиты. Теоретико-игровые модели сетевых атак. Модели «доверия» в социальных сетях.</p> <p>Реальность угроз. Типы атак. Структура типовой атаки. Сканирование. Атаки на разных уровнях протокола TCP/IP (ARP-спуффинг, атаки на маршрутизатор, атаки на DNS, атаки HTTP). Методы обнаружения вторжений.</p> <p>Построение VPN, протоколы SSL,SSH,TLS,IPSec.</p> <p>Сети с открытым доступом к каналам связи.</p> <p>Аутентификация, Авторизация – повышенные требования для WiFi, GSM, LTE сетей. Контроль доступа. Основные уязвимости и риски.</p>
4.	<p>Тема 4. Методическое и организационное обеспечение информационной безопасности</p>	<p>Критериальные пространства безопасности. Задача оценки эффективности защиты информации. Понятие риска безопасности, вероятностная модель Клементса. Идентификация рисков, основания для управления рисками для обеспечения непрерывности. Измерение эффективности систем защиты в качественных и количественных шкалах. Экономические модели оценки эффективности. Классификации и упорядоченные классы требований безопасности. Стандарты безопасности.</p> <p>Субъективность оценки эффективности, понятие доверия в безопасности, методы доверия, требования доверия, управление доверием, обеспечение уровня доверия к среде. Принципиальные ограничения моделей эффективности в условиях критических объектов безопасности и угроз инсайдера.</p> <p>Эволюция подходов и моделей управления безопасностью. Процессный характер управления, этапы и факторы управления. Система управления, иерархия политик безопасности. Технологии и инструменты аудита безопасности. Мониторинг безопасности, идентификация событий безопасности, нормализация, корреляция и классификация событий безопасности.</p> <p>Управление фильтрацией прикладного уровня, мониторинг прикладного потока через контур сегмента вычислительной среды, угрозы ошибок фильтрации, задача оптимального фильтра. Технологии управление правами для различных моделей доступа, проблема администратора, расщепление полномочий. Технологии управление безопасностью в виртуальных средах: сертификация среды обработки, доверенный супервизор, функциональная и ресурсная инкапсуляция. Идеология «Общих критериев», сеть высокоуровневых сущностей, диалектика зависимости целей, предположений, угроз и политик для среды и объекта</p>

		защиты, стойкость функций безопасности.
5.	Тема 5. Проблемные вопросы обеспечения информационной безопасности автоматизированных систем и вычислительных сетей	<p>Виртуальные вычисления в центрах обработки данных, «облачные вычисления».</p> <p>Понятие, виды (по памяти, по времени, статистические), обнаружение и методы противодействия; утечки информации в статистических БД; теоретико-вероятностная модель «невыводимости» и «невлияния».</p> <p>Понятие анонимных сетей. Примеры анонимных сетей. TOR. I2P. Уязвимости. Обнаружение.</p> <p>Безопасность SDN. Разделение потока данных и управляющего потока. Возможные виды атак. Скрытые каналы.</p>
6.	Тема 6. Использование средств машинного обучения и искусственного интеллекта в управлении информационной безопасностью.	<p>Методы ИИ в управлении информационной безопасностью. Основные функции и методы управления ИБ. Задачи обнаружения, адаптации и прогнозирования. Роль ИИ в управлении ИБ. Особенности управления ИБ КИИ. Типы ИИ используемые в системах управления ИБ:</p> <ul style="list-style-type: none"> <li>• байесовская модель;</li> <li>• деревья решения (решающие деревья);</li> <li>• метод опорных векторов;</li> <li>• искусственные нейронные сети, включая сверточные нейронные сети, сети глубокого обучения, машину Больцмана, сети Хопфилда, сети Кохонена и другие решения, основанные на использовании искусственных нейронов;</li> <li>• бустинг и бэггинг.</li> </ul> <p>Возможности и ограничения при использовании ИИ в управлении ИБ (классификация, кластеризация, регрессия, распознавание образов, ведение полноценных диалогов и т.д.).</p> <p>Машинное обучение систем управления ИБ . Понятие событий безопасности - элементарные и агрегированные события. Наборы данных (датасеты) для машинного обучения. Состав и методы получения наборов данных (датасетов) для обучения и тестирования качества обучения, различающихся по источникам и типу данных. Дата сетов сетевого трафика: KDD Cup 1999, NSL-KDD (2009), UNSW-NB15 (2015), CAIDA (2002-2016), CSE-CIC-IDS2018 и др. Дата сетов интернет трафика: MAWI (2011)URL (2016), Tor-nonTor (2017), UMASS (2018). Дата сетов VPN трафика: VPN-nonVPN (2016). Метрики оценки качества обучения.</p>



### 3. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА И САМОСТОЯТЕЛЬНОЙ РАБОТЫ

#### Практические занятия

**Практическое занятие 1.** Задачи и методы обеспечения информационной безопасности.

1. Классификация угроз несанкционированного доступа к информации в АС.
2. Общая характеристика источников угроз несанкционированного доступа в АС.
3. Общая характеристика уязвимостей АС и вычислительных сетей.
4. Угрозы программно-математических воздействий.
5. Компьютерные вирусы и “тройные кони”.
6. Модели нарушителя.
7. Основные функции систем защиты информации.
8. Модель системы защиты с полным перекрытием
9. Субъектно-объектная модель системы защиты.
10. Понятие изолированной системы.
11. Моделирование механизмов безопасности операционных систем и баз данных.
12. Проблемы изменения прав доступа.
13. Методы аутентификации и разграничения доступа в операционных системах Windows и Linux.

**Практическое занятие 2.** Теоретические основы информационной безопасности операционных систем и баз данных.

1. Протокол Нидхема-Шредера для симметричной и асимметричной криптографии.
2. Протоколы на основе ключевых хеш-функций.
3. Использование цифровой подписи.
4. Матрица доступа, пятимерное пространства безопасности Хартсона.
5. Модели HRU и Take-Grant.
6. MLS модель «военной безопасности».
7. Модель Белла-ЛаПадулы.
8. Решетки безопасности Деннинг.
9. Модель Биба.
10. Тематические классификаторы и решетки мультирубрик.
11. Использование функциональной структуры организации для управления доступом.

12. Индивидуально групповая модель управления доступом.

**Практическое занятие 3. Информационная безопасность вычислительных сетей**

1. Субъекты и объекты компьютерных атак в сетях.
2. Виды сетевых атак.
3. Методы защиты вычислительных сетей.
4. Задачи фильтрации сетевого трафика.
5. Межсетевые экраны.
6. Фильтрация пакетов.
7. Анализ приложений.
8. Анализ состояний.
9. Прокси сервер.
10. DLP системы.
11. Понятие DMZ.
12. Управление доступом в распределенных системах.
13. Методы оптимизации и методы теории игр при моделировании систем защиты.
14. Теоретико-игровые модели сетевых атак.
15. Модели «доверия» в социальных сетях.
16. Реальность угроз.
17. Типы атак. Структура типовой атаки.
18. Методы обнаружения вторжений.
19. Построение VPN, протоколы SSL,SSH,TLS,IPSec.

**Практическое занятие 4. Методическое и организационное обеспечение информационной безопасности**

1. Критериальные пространства безопасности.
2. Идентификация рисков.
3. Измерение эффективности систем защиты в качественных и количественных шкалах.
4. Экономические модели оценки эффективности.
5. Классификации и упорядоченные классы требований безопасности.
6. Стандарты безопасности.
7. Понятие доверия в безопасности, методы доверия, требования доверия, управление доверием, обеспечение уровня доверия к среде.
8. Принципиальные ограничения моделей эффективности в условиях критических объектов безопасности и угроз инсайдера.
9. Эволюция подходов и моделей управления безопасностью.
10. Система управления, иерархия политик безопасности.

11. Технологии и инструменты аудита безопасности.
12. Мониторинг безопасности, идентификация событий безопасности, нормализация, корреляция и классификация событий безопасности.
13. Технологии управление правами для различных моделей доступа, проблема администратора, расщепление полномочий.
14. Технологии управление безопасностью в виртуальных средах.

**Практическое занятие 5.** Проблемные вопросы обеспечения информационной безопасности автоматизированных систем и вычислительных сетей

1. Виртуальные вычисления в центрах обработки данных.
2. Понятие, виды, обнаружение и методы противодействия.
3. Утечки информации в статистических БД.
4. Теоретико-вероятностная модель «невыводимости» и «невлияния».
5. Анонимные сети. Уязвимости. Обнаружение.
6. Безопасность SDN. Разделение потока данных и управляющего потока. Возможные виды атак. Скрытые каналы.

**Практическое занятие 6.** Использование средств машинного обучения и искусственного интеллекта в управлении информационной безопасностью

1. Методы ИИ в управлении информационной безопасностью.
2. Основные функции и методы управления ИБ.
3. Задачи обнаружения, адаптации и прогнозирования.
4. Роль ИИ в управлении ИБ.
5. Особенности управления ИБ КИИ.
6. Типы ИИ используемые в системах управления ИБ.
7. Возможности и ограничения при использовании ИИ в управлении ИБ.
8. Машинное обучение систем управления ИБ.
9. Наборы данных (датасеты) для машинного обучения.
10. Метрики оценки качества обучения.

### **План-график выполнения самостоятельной работы по дисциплине**

<b>№ п/п</b>	<b>Дата/сроки выполнения</b>	<b>Вид самостоятельной работы</b>	<b>Примерные нормы времени на выполнение</b>	<b>Форма контроля</b>
1	в течение семестра	Работа с основной и дополнительной литературой, интернет-источниками. Подготовка к	72 часа	УО-1 Собеседование;  Экзамен

		практическим занятиям. Самостоятельный разбор заданий, решаемых на практических занятиях. Подготовка к экзамену		
		ИТОГО	72 часа	

#### **4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ**

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине включает в себя критерии оценки выполнения самостоятельной работы.

##### **Рекомендации по самостоятельной работе студентов**

Самостоятельная работа студентов является неотъемлемой частью образовательного процесса и рассматривается как организационная форма обучения.

Самостоятельная работа по дисциплине осуществляется в виде внеаудиторных форм познавательной деятельности.

*Самостоятельная работа включает в себя* повторение теоретического и практического материала дисциплины, заслушиваемого и конспектируемого в ходе аудиторных занятий; изучение основной и дополнительной литературы, указанной в рабочей программе дисциплины, самоконтроль ответов на основные проблемные вопросы по темам занятий; самостоятельный разбор заданий и задач, решаемых на практических занятиях.

Результаты самостоятельной работы представляются в виде ответов на основные положения теоретического и практического материала дисциплины по темам; письменного разбора процесса решения практических заданий и задач; собственных действий, осуществляемых в ходе подготовки к практическим заданиям.

##### **Критерии оценки выполнения самостоятельной работы**

Общие критерии оценки выполнения самостоятельной работы – правильность ответов на вопросы по темам теоретической части дисциплины, верность получаемых ответов в ходе решения практических заданий и задач, достижение правильного результата при осуществлении собственных действий.

Критериями оценок результатов внеаудиторной самостоятельной работы студента являются:

- уровень освоения студентами (магистрантами) учебного материала;

- умения студента (магистранта) использовать теоретические знания при выполнении практических задач;
- сформированность общеучебных умений;
- умения студента (магистранта) активно использовать электронные образовательные ресурсы, находить требующуюся информацию, изучать ее и применять на практике;
- обоснованность и четкость изложения ответа;
- оформление материала в соответствии с требованиями;
- умение ориентироваться в потоке информации, выделять главное;
- умение четко сформулировать проблему, предложив ее решение, критически оценить решение и его последствия;
- умение показать, проанализировать альтернативные возможности, варианты действий;
- умение сформировать свою позицию, оценку и аргументировать ее.

#### *Подготовка к практическому занятию*

В процессе подготовки к практическим занятиям, студентам необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме практического занятия, что позволяет студентам проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

#### *Работа с литературой.*

Рекомендуется использовать различные возможности работы с литературой: фонды научной библиотеки ДВФУ (<http://www.dvfu.ru/library/>) и других ведущих вузов страны, а также доступных для использования научно-библиотечных систем.

В процессе выполнения самостоятельной работы, в том числе при подготовке к практическим занятиям рекомендуется работать со следующими видами изданий:

- а) Научные издания, предназначенные для научной работы и содержащие теоретические, экспериментальные сведения об исследованиях.

Они могут публиковаться в форме: монографий, научных статей в журналах или в научных сборниках;

б) Учебная литература подразделяется на:

- учебные издания (учебники, учебные пособия, тексты лекций), в которых содержится наиболее полное системное изложение дисциплины или какого-то ее раздела;

- справочники, словари и энциклопедии – издания, содержащие краткие сведения научного или прикладного характера, не предназначенные для сплошного чтения. Их цель – возможность быстрого получения самых общих представлений о предмете.

Существуют два метода работы над источниками:

– сплошное чтение обязательно при изучении учебника, глав монографии или статьи, то есть того, что имеет учебное значение. Как правило, здесь требуется повторное чтение, для того чтобы понять написанное. Старайтесь при сплошном чтении не пропускать комментарии, сноски, справочные материалы, так как они предназначены для пояснений и помощи. Анализируйте рисунки (карты, диаграммы, графики), старайтесь понять, какие тенденции и закономерности они отражают;

– метод выборочного чтения дополняет сплошное чтение; он применяется для поисков дополнительных, уточняющих необходимых сведений в словарях, энциклопедиях, иных справочных изданиях. Этот метод крайне важен для повторения изученного и его закрепления, особенно при подготовке к зачету.

Для того чтобы каждый метод принес наибольший эффект, необходимо фиксировать все важные моменты, связанные с интересующей Вас темой.

*Методические указания к собеседованию.*

УО-1 Собеседование. В процессе собеседования магистранту рекомендуется использовать изученные материалы и конспекты лекций. Во время собеседования оценивается содержательность, правильность ответов на вопросы, нормативность высказывания обучающегося.

*Оценивание собеседования проводится по критериям:*

- уровень оперирования научной терминологией;  
- понимание информации, различие главного и второстепенного, сущности и деталей.

**Критерии оценки (устный ответ)**

100-85 баллов - «отлично», «зачтено» - если ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры;

свободное владение монологической речью, логичность и последовательность ответа; умение приводить примеры.

85-76 - баллов - «хорошо», «зачтено» - ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.

75-61 - балл - «удовлетворительно», «зачтено» – оценивается ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа; неумение привести пример развития ситуации, провести связь с другими аспектами изучаемой области.

60-50 баллов - «неудовлетворительно» / «незачет» – ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа; незнание проблематики изучаемой области.

## 5. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы/ темы дисциплины	Код и наименование индикатора достижения	Результаты обучения	Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1.	Темы: 1-6	ОПК-4.3 Использует современные подходы к верификации ПО в профессиональной деятельности с учетом требований информационной безопасности	<i>Знает</i> современные подходы к верификации ПО, их достоинства и недостатки. <i>Умеет</i> применять подходы к уменьшению количества уязвимостей в исходном коде на основе систем типов. <i>Владеет</i> методами визуализации результатов работы с применением	Работа на практическом занятии: УО-1 собеседование (опрос)	Экзамен

			современного программного обеспечения с учетом требований информационной безопасности		
2.	Темы: 1-6	ПК-12.1 Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	<i>Знает</i> новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях <i>Умеет</i> разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях <i>Владеет</i> методами создания кода программного обеспечения в соответствии с проектом	Работа на практическом занятии: УО-1 собеседование (опрос)	Экзамен
3.	Темы: 1-6	ПК-12.2 Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	<i>Знает</i> особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях <i>Умеет</i> модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях <i>Владеет</i> методами модернизации программного обеспечения	Работа на практическом занятии: УО-1 собеседование (опрос)	Экзамен

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также качественные критерии оценивания, которые описывают уровень сформированности компетенций, представлены в разделе 9.

## 6. СПИСОК ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ



## Основная литература

1. Основы управления информационной безопасностью: учебное пособие / Курило А. П., Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. - М.: Горячая Линия-Телеком, 2012. - 244 с.

2. Смелянский, Р. Л. Концепции программного управления и виртуализации сетевых сервисов в современных сетях передачи данных / Смелянский Р. Л., Антоненко В. А. - М. Курсю 2020. - 259с.

3. Ерохин, С. Д. Управление безопасностью критических информационных структур / Ерохин С. Д., Петухов А. Н., Пилюгин П. Л. - М. Горячая Линия-Телеком, 2021. - 239 с.

## Дополнительная литература

1. Грушо, А. А. Теоретические основы защиты информации / Грушо А. А., Тимонина Е. Е. - М.:Яхтсмен, 1996. - 192с.

2. Мельников, Д. А. Информационная безопасность открытых систем [Текст] : Учебник / Д. А. Мельников. - М. : Флинта: Наука, 2013. - 448 с. - ISBN 978-5-9765-1613-7; ISBN 978-5-02-037923-7. 004.056(075.8) - М-482

3. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : [Учеб.пособие] / В. Ф. Шаньгин. - М. : ДМК Пресс, 2012. - 592 с. - Доступ к электронной версии книги открыт на сайте <http://e.lanbook.com/> - ISBN 978-5-94074-637-9.

4. Галатенко, В. А. Стандарты информационной безопасности [Текст] : Курс лекций: Учеб.пособие / В. А. Галатенко ; Под ред. В.Б. Бетелина. - 2-е изд. - М. : Интернет-Университет Информационных технологий, 2012. - 264 с. - 2000 экз. - ISBN 978-5-9556-0053-6 : 262-51; 262-50.

5. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : Учеб.пособие / П. Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с. - Доступ к электронной версии книги открыт на сайте <http://e.lanbook.com/> - ISBN 978-5-9912-0147-6.

## Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. <http://www.mk.cs.msu.ru>
2. <http://www.intuit.ru/studies/courses>
3. <https://xakep.ru/> Сетевой журнал «Хаер»
4. <http://www.inside-zi.ru/> Журнал «Защита информации. Инсайд»

5. [www.jetinfo.ru](http://www.jetinfo.ru). Информационный бюллетень “JetInfo”. Издатель: компания «ИнфосистемыДжет»
6. <http://www.mathnet.ru> - Math-Net.Ru [Электронный ресурс] : общероссийский математический портал / Математический институт им. В. А. Стеклова РАН ; Российская академия наук, Отделение математических наук. - М. : [б. и.], 2010. - Загл. с титул. экрана. - Б. ц.
7. [www.biblioclub.ru](http://www.biblioclub.ru) - Университетская библиотека Online [Электронный ресурс] : электронная библиотечная система / ООО "Директ-Медиа" . - М. : [б. и.], 2001. - Загл. с титул. экрана. - Б. ц.
8. [www.ebiblioteka.ru](http://www.ebiblioteka.ru) - Универсальные базы данных East View [Электронный ресурс] : информационный ресурс / East View Information Services. - М. : [б. и.], 2012. - Загл. с титул. экрана. - Б. ц.
9. <http://www.citforum.ru/> - Электронная библиотека online статей по информационным технологиям. Удобный поиск по разделам, отдельным темам.
10. <http://www.iqlib.ru/> - Интернет-библиотека образовательных изданий. Собраны электронные учебники, справочные и учебные пособия.

### **Перечень информационных технологий и программного обеспечения**

При осуществлении образовательного процесса по дисциплине может быть использовано следующее программное обеспечение:

- Операционная система Ubuntu 18.04.
- Операционная система ALT Linux MATE Starterkit 9 лицензия GPL
- Статистический пакет MATLAB (или свободный аналог Octave)
- Операционная система Microsoft Windows 10 Education академическая лицензия
- Программный продукт Python 3.5.1 (64-bit) Python Software Foundation

### **Профессиональные базы данных и информационные справочные системы**

1. Портал Министерства образования и науки РФ <http://www.edu.ru>
2. Система федеральных образовательных порталов «ИКТ в образовании» <http://www.ict.edu.ru>
3. Российский портал открытого образования <http://www.openet.ru>
4. Министерство образования и науки Российской Федерации <http://www.mon.gov.ru>
5. Федеральное агентство по науке и инновациям <http://www.fasi.gov.ru>
6. База данных Scopus <http://www.scopus.com/home.url>

7. База данных Web of Science <http://apps.webofknowledge.com/>
8. Электронная библиотека диссертаций Российской государственной библиотеки <http://diss.rsl.ru/>
9. Электронные базы данных EBSCO <http://search.ebscohost.com/>

## **7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ**

Основной формой работы при изучении дисциплины являются лекционные и практические занятия.

При организации учебной деятельности на лекционных занятиях широко используются как традиционные, так и современные электронные носители информации, а также возможности информационных и коммуникационных образовательных технологий.

Цели лекционных занятий:

- создать условия для углубления и систематизации знаний по информационной безопасности;
- научить студентов использовать полученные знания для решения задач профессионального характера.

Лекционные и практические занятия проводятся в учебной группе.

Со стороны преподавателя студентам оказывается помощь в формировании навыков работы с литературой, анализа литературных источников.

Следует учитывать, что основной объем информации студент должен усвоить в ходе систематической самостоятельной работы с материалами, размещенными как на электронных, так и на традиционных носителях.

Для углубленного изучения материала курса дисциплины рекомендуется использовать основную и дополнительную литературу.

Литературные источники доступны обучаемым в научной библиотеке (НБ) ДВФУ, а также в электронных библиотечных системах (ЭБС), с доступом по гиперссылкам — ЭБС издательства "Лань" (<http://e.lanbook.com/>), ЭБС Znanium.com НИЦ "ИНФРА-М" (<http://znanium.com/>), ЭБС IPRbooks (<http://iprbookshop.ru/>) и другие ЭБС, используемые в ДВФУ <https://www.dvfu.ru/library/electronic-resources/>

Формами текущего контроля результатов работы студентов по дисциплине является собеседование (опрос, работа на практических занятиях).

Итоговый контроль по дисциплине осуществляется в форме экзамена в конце 2 семестра.

## 8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

ДВФУ располагает соответствующей материально-технической базой, включая современную вычислительную технику, объединенную в локальную вычислительную сеть, имеющую выход в Интернет.

Используются специализированные компьютерные классы, оснащенные современным оборудованием. Материальная база соответствует действующим санитарно-техническим нормам и обеспечивает проведение всех видов занятий (лабораторной, практической, дисциплинарной и междисциплинарной подготовки) и научно-исследовательской работы обучающихся, предусмотренных учебным планом.

### Материально-техническое и программное обеспечение дисциплины

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень программного обеспечения.
<p>690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус D, ауд. D 733,733а.</p> <p>Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации</p>	<p>Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 13)</p> <p>Оборудование: ЖК-панель 47", Full HD, LG M4716 ССВА – 1 шт.</p> <p>Доска аудиторная,</p> <p>Моноблок Lenovo C360G-i34164G500UDK с лицензионными программами Microsoft Office 2013(13 шт.) и аудиовизуальными средствами проектор Panasonic DLPPjectorPT-D2110XE</p>	<p>1С Предприятия8 (8.2), 7-Zip, ABBYY Lingvo12,Alice 3, Anaconda3,Autodesk,CodeBlocks,CorelDRAW X7,Dia,Directum4.8,DosBox-0.74,Farmanager,Firebird 2.5,FlameRobin,Foxit Reader,Free Pascal,Geany,Ghostscript,Git,Greenfoot,gsview,Inscapе0.91,Java,Java development Kit,Kaspersky,Lazarus,LibreOffice4.4,MatLab R2017b,Maxima 5.37.2,Microsoft Expression,Microsoft Office 2013,Microsoft Silverlight,Microsoft Silverlight 5SDK-русский,MicrosoftSistem Center,Microsoft Visial Studio 2012,MikTeX2.9,MySQL,NetBeans,Notepad++,Oracle VM VirtualBox,PascalABC.NET,PostgreSQL 9.4,PTC Mathcad,Putty,PyQt GPL v5.4.1 for Pythonv 3.4,Pyton2.7(3.4,3.6),QGIS Brighton,RStudio,SAM CoDeC Pack,SharePoint,Strawberry Perl,Tecnomatix,TeXnicCenter,TortoiseSVN,Unity2017.3.1f1,Veusz,Vim8.1,Visual Paradigm CE,Visual Studio2013,Windows Kits,Windows Phone SDK8.1,Xilinx Design ToolsAcrobat ReaderDC,AdobeBridge CS3,AdobeDeviceCentralCS3,Adobe ExtendScript Toolkit 2,Adobe Photoshpe CS3,DVD-студия Windows,GoogleChrome,Internet Explorer,ITMOproctor,Mozilla Firefox, Visual Studio Installer,Windows Media Center, WinSCP,</p>

В целях обеспечения специальных условий обучения инвалидов и лиц с ограниченными возможностями здоровья в ДВФУ все здания оборудованы

пандусами, лифтами, подъемниками, специализированными местами, оснащенными туалетными комнатами, табличками информационно-навигационной поддержки.

## **9. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ**

**Текущая аттестация студентов** по дисциплине проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Текущая аттестация проводится в форме собеседования (опроса) на практических занятиях по оцениванию фактических результатов обучения студентов и осуществляется ведущим преподавателем.

Объектами оценивания выступают:

- учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине);
- степень усвоения теоретических знаний;
- результаты самостоятельной работы.

Составляется календарный план контрольных мероприятий по дисциплине. Оценка посещаемости, активности обучающихся на занятиях ведётся на основе журнала, который ведёт преподаватель в течение учебного семестра.

Для текущего контроля используется проведение собеседований (опросов) в рамках практических занятий. Прослушиваются и оцениваются ответы на вопросы.

Для дисциплины используются следующие оценочные средства:

### **1. Собеседование (опрос) (УО-1)**

Собеседование (УО-1) – средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.

### **Перечень вопросов для проведения собеседования (опроса)**

1. Граф «угроза - объект» - как базовая модель СЗИ
2. Основные функции и методы реализации СЗИ
3. Угрозы безопасности КС
4. Процедуры подтверждения подлинности (идентификация и аутентификация)

5. Статические биометрические методы идентификации и их характеристики
6. Динамические биометрические методы идентификации и их характеристики
7. Методы взлома парольной защиты и модификации схемы «простой пароль»
8. Методы парольной аутентификации PAP, CHAP, MsChap
9. ЭЦП как средство аутентификации любых цифровых данных
10. Субъектно-объектная модель компьютерной системы. Монитор безопасности
11. Модели (политики) безопасности в субъектно-объектной модели КС
12. Модели на основе матрицы доступа (варианты принудительного и добровольного управления доступом, проблема «тройских коней»)
13. Модель Харрисона-Руззо-Ульмана (модель HRU). Критерий безопасности и основные теоремы модели HRU
14. Расширения модели HRU
15. Теоретико-графовая модель «take-grant». Распространение (утечка) прав доступа в графе модели «take-grant», состоящем из субъектов
16. Теоретико-графовая модель «take-grant». Распространение (утечка) прав доступа в графе модели «take-grant», состоящем из субъектов и объектов
17. Критерий безопасности и основная теорема модели «take-grant»
18. Расширенная модель Take–Grant, “неявные” информационные потоки.
19. Достоинства и недостатки дискреционных моделей
20. Основные положения моделей мандатного доступа. Решетка уровней и функции безопасности. MLS решетка.
21. Модель Белла-Ла Падулы. Критерий безопасности модели Белла-Ла Падулы.
22. Достоинства и недостатки модели Белла-Ла Падулы
23. Модификации модели Белла-Ла Падулы (Мак-Лин, LWM)
24. Основные ограничения моделей мандатного доступа.
25. Модели безопасности на основе тематической политики доступа
26. Дескрипторная тематическая классификация в модели тематической политики доступа
27. Иерархическая тематическая классификация в модели тематической политики доступа
28. Тематические решетки в модели тематической политики доступа
29. Решетка мультирубрик в модели тематической политики доступа
30. Модели ролевого доступа
31. Модели индивидуально-группового доступа

32. Политики безопасности в Windows и Linux.
33. Понятие скрытых каналов утечки информации в моделях разграничения доступа. Виды скрытых каналов утечки информации. Понятие скрытых каналов по памяти и скрытых каналов по времени.
34. Статистический скрытый канал передачи информации
35. Автоматная модель невлияния Гогена-Месигера (GM-модель)
36. Понятие целостности данных. Мандатная модель целостности Биба.
37. Модели комплексной оценки защищенности КС
38. Угрозы сети традиционные и «типично сетевые»
39. Оценка рисков нарушения ИБ
40. Стандарты в сфере безопасности ИТ (типы объектов, шкалы)
41. Развитие стандартов, ГОСТ и РД.
42. Защищенные протоколы. Уязвимости протоколов интернет.
43. Анонимность в интернет.
44. Анонимные сети
45. Защищенные протоколы.
46. Сертификаты и ЭЦП. Иерархия сертификатов.
47. Аутентификация и авторизация.
48. Протокол аутентификации Kerberos
49. Управление доступом. Межсетевые экраны. DMZ.
50. Сканирование сетей.
51. Перехват данных. Снифинг. Включение в разрыв сети. Методы защиты.
52. Перехват данных. Ложные запросы. Перехват TCP-соединения. Методы защиты.
53. Атаки на отказ в обслуживании. Цели и основные методы атак. Методы защиты

*Методические указания к собеседованию (опросу).*

УО-1 Собеседование (опрос). В процессе собеседования магистранту рекомендуется использовать изученные материалы и конспекты лекций. Во время собеседования оценивается содержательность, правильность ответов на вопросы, нормативность высказывания обучающегося.

*Оценивание собеседования проводится по критериям:*

- уровень оперирования научной терминологией;
- понимание информации, различие главного и второстепенного, сущности и деталей.

**Критерии оценки (устный ответ)**

100-85 баллов - «отлично», «зачтено» - если ответ показывает прочные знания основных процессов изучаемой предметной области, отличается

глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа; умение приводить примеры.

85-76 - баллов - «хорошо», «зачтено» - ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.

75-61 - балл - «удовлетворительно», «зачтено» – оценивается ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа; неумение привести пример развития ситуации, провести связь с другими аспектами изучаемой области.

60-50 баллов - «неудовлетворительно» / «незачет» – ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа; незнание проблематики изучаемой области.

**Промежуточная аттестация студентов** по дисциплине проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

К экзамену допускаются обучающиеся, выполнившие программу обучения по дисциплине, прошедшие все этапы текущей аттестации.

Экзамен принимается ведущим преподавателем. В исключительных случаях, по согласованию с заместителем директора Института по учебной и воспитательной работе, директор департамента имеет право принять экзамен в отсутствие ведущего преподавателя.



Форма проведения экзамена (устная, письменная и др.) утверждается на заседании департамента по согласованию с руководителем в соответствии с рабочей программой дисциплины.

Во время проведения экзамена студенты могут пользоваться рабочей программой дисциплины, а также с разрешения преподавателя, проводящего экзамен, справочной литературой и другими пособиями (учебниками, учебными пособиями, рекомендованной литературой и т.п.).

Время, предоставляемое студенту на подготовку к ответу на экзамене, должно составлять не более 20 минут. По истечении данного времени студент должен быть готов к ответу.

Присутствие на экзамене посторонних лиц (кроме лиц, осуществляющих проверку) без разрешения соответствующих лиц (ректора либо проректора по учебной и воспитательной работе, директора Института, руководителя ОПОП или директора департамента), не допускается. Инвалиды и лица с ограниченными возможностями здоровья, не имеющие возможности самостоятельного передвижения, допускаются к экзамену с сопровождающими.

При промежуточной аттестации обучающимся устанавливается оценка «Неудовлетворительно», «Удовлетворительно», «Хорошо» или «Отлично».

### **Вопросы к экзамену**

1. Эволюция подхода к управлению ИБ: реактивный, системно-сервисный, архитектурный, развитие пространства критериев ИБ, принципиально процессный характер управления ИБ, содержание этапов жизненного цикла управления.

2. Содержание и инструменты уровней управления ИБ, концептуальные принципы безопасности, основания дифференциации защищаемых информационных активов, диалектика и компоненты понятия угрозы, методы формирования модели угроз, виды политик ИБ.

3. Иерархическая классификация объектов защиты и требований безопасности в традиционной идеологии управления ИБ, ограничения традиционной идеологии, стандартизация управления ИБ, система стандартов 27-го подкомитета ISO.

4. Идеология анализа и управления информационными рисками, исчисляемые факторы при двух-, трех- и четырехфакторном анализе рисков, вероятностное расширение модели Клементса, проблемы экспертного оценивания и количественной интерпретации качественных шкал.

5. Модель высокоуровневых понятий в идеологии общих критериев, диалектика взаимодействия угроз, политик, предположений и целей безопасности в профиле защиты, функциональные требования безопасности и требования доверия, оценочные уровни доверия.

6. Управление специальными методами безопасности, безопасность критических объектов информационной инфраструктуры, привлечение фактора необратимости, делегирование управления ИБ, динамические политики ИБ.

7. Управление защитой от угроз инсайдера, принципиальная избыточность полномочий, факторы избыточности, ограниченность мониторинга событий безопасности и традиционных методов защиты, методы компенсации потенциала угроз инсайдера.

### Критерии выставления оценки студенту на экзамене

Оценка	Требования к сформированным компетенциям
«отлично»	выставляется студенту, если даны полные и правильные ответы на все вопросы экзаменационного билета в соответствии с требованиями, предъявляемыми программой; содержание ответа изложено логично и последовательно; существенные фактические ошибки отсутствуют; ответ соответствует нормам русского литературного языка. Студент должен дать исчерпывающие и правильные ответы на уточняющие и дополнительные вопросы по теме вопросов билета.
«хорошо»	выставляется студенту в случае, когда содержание ответа, в основном, соответствует требованиям, предъявляемым к оценке «отлично», т. е. даны полные правильные ответы на вопросы экзаменационного билета с соблюдением логики изложения материала, но при ответе допущены небольшие ошибки и погрешности, не имеющие принципиального характера
«удовлетворительно»	выставляется студенту, не показавшему знания в полном объеме, допустившему ошибки и неточности при ответе на вопросы экзаменационного билета, продемонстрировавшему неумение логически выстроить материал ответа и сформулировать свою позицию. При этом хотя бы по одному из вопросов ошибки не должны иметь принципиального характера
«неудовлетворительно»	выставляется студенту, если он не дал ответа хотя бы на один вопрос экзаменационного билета; дал неверные, содержащие фактические ошибки, ответы на все вопросы; не смог ответить более, чем на половину дополнительных и уточняющих вопросов. Неудовлетворительная оценка выставляется выпускнику, отказавшемуся отвечать на вопросы билета

<b>ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения по дисциплине</b>				
Оценка	2 (не зачтено)	3 (зачтено)	4 (зачтено)	5 (зачтено)
виды оценочных средств				
<b>Знания</b> (виды оценочных средств: опрос, тесты)	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
<b>Умения</b> (виды оценочных средств: практические задания)	Отсутствие умений	В целом успешное, но не систематическое умение	В целом успешное, но содержащее отдельные пробелы умение (допускает неточности не принципиального характера)	Успешное и систематическое умение
<b>Навыки (владения, опыт деятельности)</b>	Отсутствие навыков (владений, опыта)	Наличие отдельных навыков (наличие фрагментарного опыта)	В целом, сформированные навыки (владения), но используемые не в активной форме	Сформированные навыки (владения), применяемые при решении задач