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.
« 03» марта 2023 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

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 от «02» марта 2023 г. № 3.0)

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

Составитель (ли): профессор департамента ПИиИИ 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
2023

Оборотная сторона титульного листа РПД

1. Рабочая программа пересмотрена и утверждена на заседании Департамента программной инженерии и искусственного интеллекта, протокол от «___»_____20__г. №____

2. Рабочая программа пересмотрена и утверждена на заседании Департамента программной инженерии и искусственного интеллекта, протокол от «___»_____20__г. №____

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	**ОПК-4** 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	*Знает* современные подходы к верификации ПО, их достоинства и недостатки. *Умеет* применять подходы к уменьшению количества уязвимостей в исходном коде на основе систем типов. *Владеет* 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	**ПК-12** 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	*Знает* новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях *Умеет* разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях *Владеет* методами создания кода программного обеспечения в соответствии с проектом
ПК-12.2 Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для	*Знает* 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	*Умеет* модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях *Владеет* методами модернизации программного обеспечения

1. Трудоёмкость 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						Формы промежуточной аттестации
			Лек	Лаб	Пр	ОК	СР	Контроль из часов на СР	
1	Тема 1. Задачи и методы обеспечения информационной безопасности	2	6		6		12		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	27	
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	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 “троянские кони”. Модели нарушителя. Основные функции систем защиты информации. Процедура проверки подлинности субъектов и объектов, параметры парольной идентификации, особенности аутентификации в вычислительных сетях: задачи аутентификации, авторизации и акаунтинга (AAA). 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. Методы аутентификации и разграничения доступа в операционных системах Windows и Linux.
2.	Тема 2. Теоретические основы информационной безопасности операционных систем и баз данных	Строгие протоколы аутентификации. Протокол Нидхема-Шредера для симметричной и асимметричной криптографии. Протоколы на основе ключевых хеш-функций. Использование цифровой подписи. Матрица доступа, пятимерное пространства безопасности Хартсона, модели HRU и Take-Grant, основные результаты, их достоинства и недостатки, основные направления развития. MLS модель «военной безопасности», модель Белла-ЛаПадулы, решетки безопасности Деннинг. Модель Биба. Тематические классификаторы и решетки мультирубрик. Использование функциональной структуры организации для управления доступом, индивидуально групповая модель управления доступом.

3.	Тема 3. Информационная безопасность вычислительных сетей	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. 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. 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. Построение VPN, протоколы SSL,SSH,TLS,IPSec. Сети с открытым доступом к каналам связи. Аутентификация, Авторизация – повышенные требования для WiFi, GSM, LTE сетей. Контроль доступа. Основные уязвимости и риски.
4.	Тема 4. Методическое и организационное обеспечение информационной безопасности	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. 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. 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. 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

		защиты, стойкость функций безопасности.
5.	Тема 5. Проблемные вопросы обеспечения информационной безопасности автоматизированных систем и вычислительных сетей	Виртуальные вычисления в центрах обработки данных, «облачные вычисления». Понятие, виды (по памяти, по времени, статистические), обнаружение и методы противодействия; утечки информации в статистических БД; теоретико-вероятностная модель «невыводимости» и «невлияния». Понятие анонимных сетей. Примеры анонимных сетей. TOR. I2P. Уязвимости. Обнаружение. Безопасность SDN. Разделение потока данных и управляющего потока. Возможные виды атак. Скрытые каналы**.**
6.	Тема 6. Использование средств машинного обучения и искусственного интеллекта в управлении информационной безопасностью.	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: • байесовская модель; • деревья решения (решающие деревья); • метод опорных векторов; • искусственные нейронные сети, включая сверточные нейронные сети, сети глубокого обучения, машину Больцмана, сети Хопфилда, сети Кохонена и другие решения, основанные на использовании искусственных нейронов; • бустинг и бэггинг. Возможности и ограничения при использовании ИИ в управлении ИБ (классификация, кластеризация, регрессия, распознавание образов, ведение полноценных диалогов и т.д.). 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 сеты сетевого трафика: KDD Cup 1999, NSL-KDD (2009), UNSW-NB15 (2015), CAIDA (2002-2016), CSE-CIC-IDS2018 и др. Дата сеты интернет трафика: MAWI (2011)URL (2016), Tor-nonTor (2017), UMASS (2018). Дата сеты VPN трафика: VPN-nonVPN (2016). Метрики оценки качества обучения.

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 “троянские 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

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
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

Самостоятельная работа определяется как индивидуальная или коллективная учебная деятельность, осуществляемая без непосредственного руководства педагога, но по его заданиям и под его контролем. Самостоятельная работа – это познавательная учебная деятельность, когда последовательность мышления студента, его умственных и практических операций и действий зависит и определяется самим студентом.

Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровней, что в итоге приводит к развитию навыка самостоятельного планирования и реализации деятельности.

Целью самостоятельной работы студентов является овладение необходимыми компетенциями по своему направлению подготовки, опытом творческой и исследовательской деятельности.

Формы самостоятельной работы студентов:

- работа с основной и дополнительной литературой, интернет-ресурсами;
- самостоятельное ознакомление с лекционным материалом, представленным на электронных носителях, в библиотеке образовательного учреждения;
- подготовка к экзамену;
- другие виды деятельности, организуемые и осуществляемые образовательным учреждением и органами студенческого самоуправления.

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.

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.

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	*Знает* современные подходы к верификации ПО, их достоинства и недостатки. *Умеет* применять подходы к уменьшению количества уязвимостей в исходном коде на основе систем типов. *Владеет* методами визуализации результатов работы с применением современного программного обеспечения с учетом требований информационной безопасности	Работа на практическом занятии: УО-1 собеседование (опрос)	Экзамен
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	*Знает* новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях *Умеет* разрабатывать программное и аппаратное обеспечение технологий и систем искусственного	Работа на практическом занятии: УО-1 собеседование (опрос)	Экзамен

		различных предметных областях	интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях *Владеет* методами создания кода программного обеспечения в соответствии с проектом		
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	*Знает* особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях *Умеет* модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях *Владеет* методами модернизации программного обеспечения	Работа на практическом занятии: УО-1 собеседование (опрос)	Экзамен

* Формы оценочных средств:
собеседование (УО-1)

6. СПИСОК ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1. Анисимов А.А. Менеджмент в сфере информационной безопасности : учебное пособие / Анисимов А.А.. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 211 с. — ISBN 978-5-4497-0328-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89443.html — Режим доступа: для авторизир. пользователей

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2020. —

325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/450371

3. Черников, Б. В. Управление качеством программного обеспечения : учебник / Б. В. Черников. — Москва : ФОРУМ : ИНФРА-М, 2019. — 240 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0499-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1018037 – Режим доступа: по подписке

4. Шилов А.К. Управление информационной безопасностью : учебное пособие / Шилов А.К.. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2018. — 120 с. — ISBN 978-5-9275-2742-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87643.html — Режим доступа: для авторизир. пользователей

Дополнительная литература

1. Абденов, А.Ж. Современные системы управления информационной безопасностью : учебное пособие / Абденов А.Ж., Дронова Г.А., Трушин В.А.. — Новосибирск : Новосибирский государственный технический университет, 2017. — 48 с. — ISBN 978-5-7782-3236-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/91427.html — Режим доступа: для авторизир. пользователей

2. Девянин, П. Н. Модели безопасности компьютерных систем: учебное пособие для вузов / П. Н. Девянин. - М. : Академия, 2005. - 143 с. - https://lib.dvfu.ru/lib/item?id=chamo:263487&theme=FEFU

3. Дронов, В.Ю. Международные и отечественные стандарты по информационной безопасности : учебно-методическое пособие / Дронов В.Ю.. — Новосибирск : Новосибирский государственный технический университет, 2016. — 34 с. — ISBN 978-5-7782-3112-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/91395.html — Режим доступа: для авторизир. пользователей

4. Жукова, М. Н. Управление информационной безопасностью. Ч. 2: Управление инцидентами информационной безопасности : учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/463061 – Режим доступа: по подписке.

5. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2020. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1018665 – Режим доступа: по подписке.

6. Нестеров, С. А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft : учебное пособие / С. А. Нестеров. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 250 с. — ISBN 978-5-4497-0300-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89416.html — Режим доступа: для авторизир. пользователей

7. Петренко, В.И. Теоретические основы защиты информации : учебное пособие / Петренко В.И.. — Ставрополь : Северо-Кавказский федеральный университет, 2015. — 222 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/63138.html — Режим доступа: для авторизир. пользователей

8. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2012. — 592 с. — ISBN 978-5-94074-637-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/3032 — Режим доступа: для авториз. пользователей.

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. 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 - 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 - 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 работа на практических занятиях, собеседование (опрос).

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

Студент считается аттестованным по дисциплине при условии выполнения всех видов текущего контроля и самостоятельной работы, предусмотренных учебной программой.

Шкала оценивания сформированности образовательных результатов по дисциплине представлена в фонде оценочных средств (ФОС).

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 лицензионного программного обеспечения
690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус D, ауд. D 733,733а. Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 13) Оборудование: ЖК-панель 47", Full HD, LG M4716 CCBA – 1 шт. Доска аудиторная, Моноблок Lenovo C360G-i34164G500UDK с лицензионными программами Microsoft Office 2013(13 шт.) и аудиовизуальными средствами проектор Panasonic DLPProjectorPT-D2110XE	1С Предприяти8 (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,Inscape0.91,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 Photoshope CS3,DVD-студия Windows,GoogleChrome,Internet Explorer,ITMOproctor,Mozilla Firefox, Visual Studio Installer,Windows Media Center, WinSCP
690922, Приморский край, г. Владивосток, остров	Моноблок Lenovo C360G-i34164G500UDK – 115 шт.;	Microsoft Windows 7 Pro MAGic 12.0 Pro, Jaws for Windows 15.0 Pro, Open book 9.0,

Русский, полуостров Саперный, поселок Аякс, 10, корпус А ауд. А1042 аудитория для самостоятельной работы студентов	Интегрированный сенсорный дисплей Polymedia FlipBox; Копир-принтер-цветной сканер в e-mail с 4 лотками Xerox WorkCentre 5330 (WC5330C; Полноцветный копир-принтер-сканер Xerox WorkCentre 7530 (WC7530CPS Оборудование для инвалидов и лиц с ограниченными возможностями здоровья: Дисплей Брайля Focus-40 Blue – 3 шт.; Дисплей Брайля Focus-80 Blue; Рабочая станция Lenovo ThinkCentre E73z – 3 шт.; Видео увеличитель ONYX Swing-Arm PC edition; Маркер-диктофон Touch Memo цифровой; Устройство портативное для чтения плоскопечатных текстов PEarl; Сканирующая и читающая машина для незрячих и слабовидящих пользователей SARA; Принтер Брайля Emprint SpotDot - 2 шт.; Принтер Брайля Everest - D V4; Видео увеличитель ONYX Swing-Arm PC edition; Видео увеличитель Topaz 24” XL стационарный электронный; Обучающая система для детей тактильно-речевая, либо для людей с ограниченными возможностями здоровья; Увеличитель ручной видео RUBY портативный – 2 шт.; Экран Samsung S23C200B; Маркер-диктофон Touch Memo цифровой	Duxbury BrailleTranslator, Dolphin Guide (контракт № А238-14/2); Неисключительные права на использование ПО Microsoft рабочих станций пользователей (контракт ЭА-261-18 от 02.08.2018): - лицензия на клиентскую операционную систему; - лицензия на пакет офисных продуктов для работы с документами включая формат.docx , .xlsx , .vsd , .ptt.; - лицензия па право подключения пользователя к серверным операционным системам , используемым в ДВФУ : Microsoft Windows Server 2008/2012; - лицензия на право подключения к серверу Microsoft Exchange Server Enterprise; - лицензия па право подключения к внутренней информационной системе документооборота и порталу с возможностью поиска информации во множестве удаленных и локальных хранилищах, ресурсах, библиотеках информации, включая портальные хранилища, используемой в ДВФУ: Microsoft SharePoint; - лицензия на право подключения к системе централизованного управления рабочими станциями, используемой в ДВФУ: Microsoft System Center

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.