ЦЕНТРАЛЬНЫЙ УНИВЕРСИТЕТ

УТВЕРЖДЕНА

Решением Ученого совета
АНО ВО «Центральный университет»
«25» мая 2026 г.
Протокол №2

Рабочая программа дисциплины (модуля)
«Информационная безопасность»

Направление подготовки: *02.03.01 Математика и компьютерные науки*

Направленность (профиль) подготовки: *Прикладной искусственный интеллект*

Квалификация (степень) выпускника: *бакалавр*

Форма обучения: *очная*

Срок освоения программы: *4 года*

Год набора: *2026*

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0215B0C000D1B3FEB44A37EE631E0C27D4
Владелец: Ивашкевич Евгений Васильевич
Действителен: с 13.01.2026 до 13.04.2027

Электронный документ

Москва
2026

Содержание

1. Краткая характеристика дисциплины (модуля)

Рабочая программа дисциплины (модуля) «Информационная безопасность» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению 02.03.01 «Математика и компьютерные науки», профиль «Прикладной искусственный интеллект», утвержденный приказом Министерства науки и высшего образования Российской Федерации № 807 от 23.08.2017 года.

Изучение дисциплины (модуля) «Информационная безопасность» позволяет защитить информационные ресурсы и данные от несанкционированного доступа, предотвращая угрозы и кибератаки. Это обеспечивает сохранность конфиденциальности, целостности и доступности информации, что критично для стабильной работы организаций и безопасности пользователей.

Дисциплина (модуль) «Информационная безопасность» разработана и утверждена совместно с АО «Лаборатория Касперского».

Место дисциплины (модуля) в структуре образовательной программы

Настоящая дисциплина (модуль) включена в учебные планы по программам подготовки бакалавриата по направлению 02.03.01 «Математика и компьютерные науки», профиль «Прикладной искусственный интеллект» и входит в вариативную часть Блока 1, формируемую участниками образовательных отношений, как дисциплина по выбору.

Дисциплина (модуль) является выборной и доступна для изучения на 3 или 4 курсе в 5,6,7 или 8 семестрах на выбор после успешного освоения дисциплины «Основы промышленной разработки».

Цель изучения дисциплины (модуля): формирование знаний и навыков по защите информации и информационных систем от различных угроз и несанкционированного доступа.

Задачи изучения дисциплины (модуля):

— изучить основные понятия, угрозы и принципы информационной безопасности, включая модели защиты и стандарты;

— практические методы и технологии защиты информации, таких как шифрование, аутентификация и контроль доступа;

— научиться анализировать законодательные и этические аспектов информационной безопасности, а также развитие умений по выявлению и предотвращению киберугроз.

В результате освоения дисциплины (модуля) обучающийся должен:

знать:

— классификацию основных угроз информационной безопасности

— стратегии защиты информации

— виды нормативных документов, регламентирующие защиту информации;

уметь:

— разрабатывать требования по обеспечению информационной безопасности

— вести учет затрат и рисков при выработке стратегий защиты информации;

владеть:

— навыками аудита информационной безопасности информационных систем;

— практикой построения комплексной системы защиты информации.

2. Перечень планируемых результатов обучения

Компетенции, формируемые в результате освоения дисциплины (модуля) при проведении учебных занятий в форме контактной работы обучающихся с педагогическими работниками Университета и в форме самостоятельной работы обучающихся:

Код и содержание компетенции	**Индикатор компетенции и перечень планируемых результатов обучения по дисциплине (модулю)**
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Знает методы поиска и анализа информации в области разработки, основные принципы критической оценки источников информации и их релевантности.
	УК-1.2. Умеет критически оценивать источники информации и синтезировать данные из различных источников для решения задач, применять системный подход к анализу и решению комплексных проблем.
	УК-1.3. Имеет практический опыт работы с современными инструментами и технологиями для обработки информации, формулировании и структурировании задач на основе полученной информации.
УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде *(соответствует УНК-02)*	УК-3.1. (УНК-02.01.) Принимает участие в групповом взаимодействии в ходе профессиональной деятельности (базовый) УНК-02.01.01. У-1. Проявляет понимание своей роли в команде УНК-02.01.01. У-2. Умеет ясно выражать свои мысли в группе УНК-02.01.01. У-3. Способен слушать и учитывать мнения других участников команды. УНК-02.01.01. У-4. Умеет давать конструктивную обратную связь УНК-02.01.01. У-5. Умеет работать в команде, проявлять инициативу и поддерживать коллег УНК-02.01.01. У-6. Обладает навыками разрешения конфликтных ситуаций и поиска компромиссов УНК-02.01.01. З-1. Знает основы командной работы, роли и ответственности каждого участника.
	УК-3.2. (УНК-02.02.) Проявляет лидерство и осуществляет наставничество (базовый) УНК-02.02.01. У-1. Умеет мотивировать и вдохновлять команду для достижения общих целей УНК-02.02.01. У-2. Способен организовывать работу группы, распределять обязанности и контролировать выполнение задач УНК-02.02.01. У-3. Умеет делиться знаниями и опытом, оказывать поддержку и осуществлять наставничество коллегам УНК-02.02.01. У-4. Способен принимать ответственные решения и демонстрировать пример профессионализма УНК-02.02.01. З-1. Знает основы лидерства, мотивации и командообразования УНК-02.02.01. З-2. Знает принципы эффективного наставничества и развития персонала УНК-02.02.01. З-3. Знает методы оценки эффективности работы команды и индивидуальных участников
ОПК-6. Способен разрабатывать алгоритмы и компьютерные программы,	ОПК-6.1. Знает принципы алгоритмизации, основные структуры данных, парадигмы программирования, методы разработки, тестирования и отладки компьютерных программ.

пригодные для практического применения	ОПК-6.2. Умеет разрабатывать, документировать, тестировать и отлаживать алгоритмы и компьютерные программы, пригодные для практического применения, с использованием современных языков и сред разработки.
	ОПК-6.3. Имеет практический опыт разработки и сопровождения компьютерных программ и программных комплексов для решения прикладных задач.
ППК-ДА3. Способен проводить аналитические исследования с применением технологий больших данных	ППК-ДА3.1. – Применяет методы машинного обучения и статистического анализа (базовый) ППК-ДА3.1. З-1. Знает основные алгоритмы машинного обучения
	ППК-ДА3.2. – Обеспечивает соответствие результатов анализа бизнес-задачам заказчика (средний) ППК-ДА3.2. З-2. Знает ключевые бизнес-метрики в предметной области
ППК-Р5. Способен разрабатывать требования и проектировать программное обеспечение	ППК-Р5.1. Анализирует возможности реализации требований к компьютерному программному обеспечению (средний) ППК-Р5.1. З-1. Знает возможности существующей программно-технической архитектуры. ППК-Р5.1. З-2. Знает возможности современных и перспективных средств разработки программных продуктов, технических средств. ППК-Р5.1. З-3. Знает методологии разработки компьютерного программного обеспечения и технологии программирования. ППК-Р5.1. У-1. Умеет проводить сбор и систематизацию требований к компьютерному программному обеспечению. ППК-Р5.1. У-2. Умеет выявлять взаимосвязи и документировать требования к компьютерному программному обеспечению ППК-Р5.1. У-3. Умеет вырабатывать варианты реализации требований к компьютерному программному обеспечению.
	ППК-Р5.2. Разрабатывает технические спецификаций на программные компоненты и их взаимодействие (средний) ППК-Р5.2. З-1. Знает методы и средства проектирования компьютерного программного обеспечения. ППК-Р5.2. З-2. Знает методы и средства проектирования программных интерфейсов. ППК-Р5.2. У-1. Умеет выбирать средства реализации требований к компьютерному программному обеспечению. ППК-Р5.2. У-2. Умеет вырабатывать варианты реализации компьютерного программного обеспечения. ППК-Р5.2. У-3. Умеет проводить оценку и обоснование рекомендуемых решений.
	ППК-Р5.3. Проектирует компьютерное программное обеспечение (продвинутый) ППК-Р5.3. З-1. Знает принципы построения и виды архитектуры компьютерного программного обеспечения. ППК-Р5.3. З-2. Знает типовые решения, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке компьютерного программного обеспечения. ППК-Р5.3. З-3. Знает нормативно-технические документы (стандарты), определяющие требования к технической

	документации на компьютерное программное обеспечение. ППК-Р5.3. З-4. Знает методы и средства проектирования компьютерного программного обеспечения. ППК-Р5.3. У-1. Умеет разрабатывать и изменять архитектуру компьютерного программного обеспечения и согласовывать ее с системным аналитиком и архитектором программного обеспечения. ППК-Р5.3. У-2. Умеет проектировать структуры данных. ППК-Р5.3. У-3. Умеет проектировать программные интерфейсы.
	ППК-Р5.4. Выполняет логическое проектирование системы (продвинутый) ППК-Р5.4. З-1. Знает устройство и функционирование ИТ-систем/продуктов ППК-Р5.4. З-2. Знает методы моделирования и описания устройства и функционирования ИТ-систем/продуктов, их частей, обеспечения и окружения ППК-Р5.4. З-3. Знает базовые технологии взаимодействия и интеграции систем и компонентов ППК-Р5.4. З-4. Знает методы функциональной декомпозиции ИТ-систем ППК-Р5.4. У-1. Умеет декомпозировать ИТ-системы и ИТ-продукты на подсистемы и элементы поставки ППК-Р5.4. У-2. Умеет описывать интерфейсы пользователя на логическом уровне ППК-Р5.4. У-1. Умеет описывать интеграции со смежными системами на логическом уровне
ППК-Р6. Способен участвовать в промышленной разработке программного обеспечения	ППК-Р6.1. Работает в соответствии с промышленными методологиями разработки (средний) ППК-Р6.1. З-1. Знает принципы Agile и их применение в промышленных проектах. ППК-Р6.1. З-2. Знает процессы code review, принципы коллективного владения кодом (collective code ownership). ППК-Р6.1. У-1. Умеет оценивать объем задачи и срок ее выполнения, участвовать в планировании спринтов. ППК-Р6.1. У-2. Умеет работать в команде с использованием инструментов управления проектами.
	ППК-Р6.3. Разрабатывает масштабируемый и поддерживаемый код (продвинутый) ППК-Р6.3. З-1. Знает принципы чистого кода, SOLID, DRY, KISS и др. ППК-Р6.3. З-2. Знает принципы предметно-ориентированного проектирования (ПОП) программного обеспечения. ППК-Р6.3. З-3. Знает паттерны проектирования и антипаттерны. ППК-Р6.3. У-1. Умеет разрабатывать модульный и тестируемый программный код. ППК-Р6.3. У-2. Умеет выполнять модульное, интеграционное и нагрузочное тестирование. ППК-Р6.3. У-3. Умеет проводить рефакторинг для повышения качества кода. ППК-Р6.3. У-4. Умеет применять принципы ПОП при разработке программного обеспечения на языках программирования высокого уровня абстракций и в LowCode и NoCode системах.

	ППК-Р6.4. Участвует в развертывании и поддержке программного обеспечения (продвинутый) ППК-Р6.4. З-1. Знает стратегии развертывания промышленного программного обеспечения. ППК-Р6.4. З-2. Знает основы работы с облачными платформами. ППК-Р6.4. У-1. Умеет развертывать приложения в облаке. ППК-Р6.4. У-2. Умеет обнаруживать и устранять инциденты с работой продуктивного программного обеспечения.
ППК-Р7. Способен применять искусственный интеллект (ИИ) для генерации и отладки программного кода	ППК-Р7.1. Применяет ИИ-инструменты для генерации программного кода (базовый) ППК-Р7.1. З-1. Знает принципы работы современных генеративных ИИ-моделей для генерации кода. ППК-Р7.1. У-1. Умеет формулировать корректные текстовые запросы (промты) для генерации кода. ППК-Р7.1. У-2. Умеет интегрировать ИИ-инструменты в среду разработки.
	ППК-Р7.2. Использует ИИ для анализа и отладки кода (средний) ППК-Р7.2. З-1. Знает методы ИИ-анализа кода. ППК-Р7.2. З-2. Знает форматы и инструменты для автоматизированного тестирования с ИИ.
ППК-ДА4. Способен выявлять бизнес-проблемы или бизнес-возможности	ППК-ДА4.2. Выявление истинных бизнес-проблем или бизнес-возможностей (продвинутый) ППК-ДА4.2. З-1. Знает предметную область и специфику деятельности организации в объеме, достаточном для решения задач бизнес-анализа ППК-ДА4.2. З-2. Знает инструменты, техники анализа бизнес-ситуации и предметной области, включая анализ данных.
РГ-1. Способен руководить процессами разработки компьютерного программного обеспечения	РГ-1.2. Руководит проверкой работоспособности компьютерного программного обеспечения (средний) РГ-1.2. З-1. Знает основные методы измерения и оценки характеристик компьютерного программного обеспечения РГ-1.2. З-2. Знает методы и средства проверки работоспособности компьютерного программного обеспечения РГ-1.2. У-2. Умеет оценивать результаты проверки работоспособности компьютерного программного обеспечения РГ-1.2. У-3. Умеет принимать управленческие решения по результатам проверки работоспособности компьютерного программного обеспечения об исправлении ошибок, рефакторинге, оптимизации и инспекции кода РГ-1.2. У-4. Умеет включать поиск возможных отказов из воздействий внутреннего или внешнего нарушителя (хакер, неосторожный пользователь, программист, поставщик компонентов) в процедуры инспекции программного кода.
	РГ-1.3. Руководит интеграцией программных модулей и компонентов компьютерного программного обеспечения (продвинутый) РГ-1.3. З-1. Знает методы и средства сборки модулей и компонентов компьютерного программного обеспечения РГ-1.3. З-2. Знает методы и программные интерфейсы взаимодействия компьютерного программного обеспечения с внешними программными компонентами РГ-1.3. З-3. Знает методы проектирования и разработки

	программных интерфейсов взаимодействия внутренних модулей компьютерного программного обеспечения РГ-1.3. З-4. Знает методы и средства разработки процедур для развертывания компьютерного программного обеспечения.
РГ-4. Способен организовать промышленную разработку программного обеспечения	РГ-4.4. Организует развертывание и поддержку программного обеспечения (продвинутый) РГ-4.4. У-2. Умеет управлять обнаружением и устранением инцидентов с работой продуктивного программного обеспечения.

1. Тематический план

№п/п	Наименование раздела дисциплины (модуля)	Трудоемкость, академические часы				ТКУ (текущий контроль успеваемости)
		Очная форма				
		Аудиторная работа		Контроль	Самостоятельная работа	
		Лекции	Практические занятия			
1	Основы безопасности корпоративной инфраструктуры	6	6		26	Домашние задания
2	Вредоносное программное обеспечение	6	6		26	Домашние задания
3	Криптографическая защита информация	6	6		26	Домашние задания
4	Методы защиты информации	6	6	1	24	Домашние задания Аудиторная работа
5	Аудит безопасности информационных систем	6	6	1	24	Домашние задания Коллоквиум
	Зачет с оценкой			2		
	Итого:	***30***	***30***	***4***	***126***	
Объем дисциплины (модуля) (в ак. ч.)		***190***				
Объем дисциплины (модуля) (в зач. ед.)		***5***				

2. Содержание дисциплины (модуля)

№п/п	Наименование раздела дисциплины (модуля)	Содержание дисциплины (модуля) по темам
1	Основы безопасности корпоративной инфраструктуры	Администрирование ОС: Windows, Linux. Сети передачи данных. Модель OSI. Виртуализация и контейнеры
2	Вредоносное программное обеспечение	Классификация вредоносного программного обеспечения. Социальная инженерия и фишинг. Анализ вредоносных программ (реверс-инжиниринг).
3	Криптографическая защита информация	Основы криптографической защиты информации. Управление доступом: идентификация, аутентификация, авторизация. Управление ключами и PKI
4	Методы защиты информации	Классификация программных средств защиты информации. Мониторинг и реагирование на инциденты (цифровая криминалистика). Риск-ориентированный подход при построении системы защиты. Планирование финансовых ресурсов.
5	Аудит безопасности информационных систем	Нормативные основы защиты информации в РФ. Модель угроз и злоумышленника. Тестирование на проникновение - методология и программный инструментарий. Безопасность приложений

3. Учебно-методическое обеспечение

Университет располагает полным набором лицензионного и свободно распространяемого программного обеспечения, включая продукты отечественного производства.

Каждый студент в течение всего периода обучения получает индивидуальный неограниченный доступ к электронно-библиотечной системе и электронной информационно-образовательной среде университета. Эти системы предоставляют возможность доступа к ресурсам из любой точки, где есть подключение к сети Интернет, как на территории университета, так и за его пределами.

Студентам обеспечен удаленный доступ к современным профессиональным базам данных и информационным справочным системам.

Основная литература:

1. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588374.

2. Бондаренко, И. С. Информационная безопасность : учебник / И. С. Бондаренко. - Москва : Издательский Дом НИТУ «МИСиС», 2023. - 255 с. - ISBN 978-5-907560-71-0. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2148212.

3. Аверченков, В. И. Аудит информационной безопасности : учебное пособие для вузов / В. И. Аверченков. - 4-е изд., стер. - Москва : ФЛИНТА, 2021. - 269 с. - ISBN 978-5-9765-1256-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1843184.

Дополнительная литература:

1. Козырь, Н. С. Анализ и оценка рисков информационной безопасности : учебник для вузов / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2025. — 154 с. — (Высшее образование). — ISBN 978-5-534-17866-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/581502.

2. Козырь, Н. С. Оценка рисков и аудит информационной безопасности : учебник для вузов / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2025. — 186 с. — (Высшее образование). — ISBN 978-5-534-17864-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/581501.

4. Материально-техническое обеспечение

Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

Помещения, которые представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Изучение дисциплины (модуля) обеспечивается в учебных аудиториях, оснащенных:

— столами и стульями;

— компьютерной техникой;

— механическими калькуляторами;

— специализированным оборудованием, включая демонстрационное оборудование.

Помещения для самостоятельной работы обучающихся, в том числе приспособленные для использования инвалидами и лицами с ограниченными возможностями здоровья, оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.

Обучающимся предоставляется доступ (в том числе удаленный) к ресурсам информационно-телекоммуникационной сети «Интернет», электронным ресурсам (в том числе электронным библиотечным системам, современным профессиональным базам данных и информационным справочным системам):

№	Наименование портала (издания, курса, документа)	Ссылка
1.	Научная электронная библиотека elibrary.ru библиотека	https://elibrary.ru/defaultx.asp
2.	База данных для IT-специалистов	https://habr.com
3.	База данных ScienceDirect	https://www.sciencedirect.com
4.	Официальный сайт Министерства науки и высшего образования Российской Федерации	https://minobrnauki.gov.ru/
5.	Федеральный портал «Российское образование"	https://www.edu.ru/
6.	Информационная система "Единое окно доступа к образовательным ресурсам"	http://window.edu.ru/
7.	Единая коллекция цифровых образовательных ресурсов	http://school-collection.edu.ru/
8.	Федеральный центр информационно - образовательных ресурсов	http://fcior.edu.ru/

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), в том числе комплект лицензионного программного обеспечения, современные профессиональные базы данных и информационные справочные системы:

Наименование ПО	Производство	Лицензионное / свободно распространяемое
Операционные системы:		
Microsoft Imagine (Windows Client, Server)	зарубежное	лицензионное
Браузеры:		
Яндекс.Браузер	отечественное	свободно распространяемое
Google Chrome	зарубежное	свободно распространяемое
Офисные приложения:		
Microsoft Imagine (Visio, OneNote)	зарубежное	лицензионное
TeXstudio	зарубежное	свободно распространяемое
Adobe Acrobat Reader	зарубежное	свободно распространяемое
Программное обеспечение для планирования и учета времени:		
Toggle app	зарубежное	свободно распространяемое
Системы управления проектами:		
Microsoft Imagine (Project)	зарубежное	лицензионное
Системы управления базами данных:		
Microsoft Imagine (SQL Server)	зарубежное	лицензионное
Системы резервного копирования (backup):		
Acronis Backup Advanced for HyperV	зарубежное	лицензионное
Справочно-правовые системы:		

КонсультантПлюс: справочно-правовая система	отечественное	лицензионное
Средства антивирусной защиты:		
Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition	отечественное	лицензионное
Среды разработки:		
Visual Studio Code	зарубежное	свободно распространяемое
Bash (Unix shell)	зарубежное	свободно распространяемое
Anaconda	зарубежное	свободно распространяемое
Robotic Operating System	зарубежное	свободно распространяемое
CopelliaSim	зарубежное	свободно распространяемое
Google Colaboratory	зарубежное	свободно распространяемое
Пакеты программных средств и библиотек:		
AutoPsy	зарубежное	свободно распространяемое
Interactive Disassembler (IDA)	зарубежное	свободно распространяемое
Системы управления библиографической информацией:		
Zotero	зарубежное	свободно распространяемое
Сервисы и службы:		
Bind	зарубежное	свободно распространяемое
Docker	зарубежное	свободно распространяемое

5. Методические и оценочные материалы

Методические указания для обучающихся по освоению дисциплины (модуля)

В процессе изучения дисциплины (модуля) «Информационная безопасность» в рамках текущего контроля успеваемости используются такие виды учебной работы, как лекции, семинары, аудиторная работа, домашние задания, коллоквиум, а также различные виды самостоятельной работы обучающихся по заданию преподавателя, направленные на развитие навыков профессиональной лексики, закрепление практических профессиональных компетенций, поощрение инициатив.

Лекция – систематическое, последовательное, монологическое изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект лекций: кратко и схематично фиксировать основные идеи, выводы и обобщения лекции; выделять важные мысли, ключевые слова и термины. Необходимо отметить вопросы или материалы, которые вызывают затруднения, и попытаться найти ответы в рекомендованной литературе. Если разобраться в материале не удается, следует сформулировать вопрос и задать его преподавателю на консультации или во время семинарского (практического) занятия.

Семинар – это форма учебной деятельности, проводимая в учебном заведении под руководством преподавателя, где студенты активно участвуют в обсуждениях, практических заданиях и других формах взаимодействия.

Для успешной подготовки к семинару рекомендуется заранее ознакомиться с темой занятия и основными материалами, чтобы иметь возможность активно участвовать в обсуждении. Также полезно подготовить вопросы и идеи для обсуждения, что поможет глубже понять материал и продемонстрировать заинтересованность.

Аудиторная работа – активная работа студента на семинаре, его ответы на вопросы преподавателя и участие в дискуссии.

Для успешного участия в семинаре студентам рекомендуется заранее ознакомиться с темой обсуждения, прочитать необходимые материалы и подготовить вопросы. Важно активно слушать и вовлекаться в дискуссию, высказывая свои мнения и аргументируя их.

При ответах на вопросы преподавателя стоит быть уверенным, четким и логичным, опираясь на изученный материал. Также полезно поддерживать диалог с однокурсниками, чтобы обогатить обсуждение и расширить свои знания.

Домашнее задание – набор задач по темам недели.

При работе над домашними заданиями важно внимательно ознакомиться с требованиями и сроками выполнения. Рекомендуется разбивать задания на этапы, чтобы избежать перегрузки и лучше усвоить материал. Использовать различные источники информации, включая учебники и онлайн-ресурсы, для более глубокого понимания темы.

Коллоквиум – устные ответы на вопросы, список которых известен студенту заранее.

В процессе подготовки к коллоквиуму необходимо проанализировать учебные материалы, ознакомившись с лекциями, учебниками и дополнительными источниками, акцентируя внимание на ключевых темах. Рекомендуется создать структурированные конспекты, выделяя основные идеи, термины и формулы.

Самостоятельная работа – работа студентов, направленная на углубленное изучение отдельных тем и вопросов учебной дисциплины (модуля).

В процессе самостоятельной работы студенты взаимодействуют с рекомендованными материалами при минимальном участии преподавателя. Задачи студента включают работу с конспектами лекций (обработка текста), повторное изучение учебных материалов, планов и тезисов ответов, изучение дополнительных тем, выполнение учебно-исследовательских заданий и другое.

Система оценивания результатов обучения по дисциплине (модулю)

Критерии получения уровня и оценивания сформированности компетенций по дисциплине (модулю) «Информационная безопасность»

Оценивание уровня учебных достижений, обучающихся по дисциплине (модулю), осуществляется в виде текущего контроля успеваемости и промежуточной аттестации.

Промежуточная аттестация по дисциплине (модулю) осуществляется в форме ***зачета с оценкой***, при этом проводится оценка компетенций, сформированных по дисциплине.

Для оценивания текущего контроля успеваемости и промежуточной аттестации используется десятибалльная шкала оценивания, которая соотносится с традиционной пятибалльной шкалой следующим образом, если иное не указано в силлабусе дисциплины:

Десятибалльная оценка	Пятибалльная оценка	Общая характеристика результата обучения по дисциплине (модулю)
10	Отлично	Студент полностью владеет знаниями, изложенными в рабочей программе, и глубоко осмысляет дисциплину. Он самостоятельно и логически последовательно отвечает на все вопросы, акцентируя внимание на наиболее важном. Умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя ключевые моменты и устанавливая причинно-следственные связи. Четко
9	Отлично	
8	Отлично	

Десятибалльная оценка	Пятибалльная оценка	Общая характеристика результата обучения по дисциплине (модулю)
		формулирует ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты дисциплины (модуля) с практическими задачами.
7	Хорошо	Студент обладает знаниями предмета почти в полном объеме рабочей программы и самостоятельно, логически последовательно и всесторонне отвечает на все вопросы, акцентируя внимание на наиболее значимых моментах. Он умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя его ключевые аспекты и устанавливая причинно-следственные связи. Формулирует свои ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные ситуационные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты предмета с практическими задачами.
6	Хорошо	
5	Удовлетворительно	Студент обладает базовыми знаниями по дисциплине (модулю), но испытывает трудности при самостоятельных ответах и использует неточные формулировки. В ходе ответов он допускает ошибки, касающиеся сути вопросов. Студент способен решать только самые простые задачи и владеет лишь минимальным набором методов исследования.
4	Удовлетворительно	
3	Не сдан	Студент не овладел обязательным минимумом знаний по предмету и не может ответить на вопросы, даже если преподаватель задает дополнительные наводящие вопросы.
2	Не сдан	
1	Не сдан	

Дисциплина (модуль) «Информационная безопасность» оценивается следующим образом:

Активность	Вес	Количество	Описание
Домашнее задание	40%	15	Набор задач по темам недели
Коллоквиум	25%	1	Устные ответы на вопросы, список которых известен студенту заранее
Аудиторная работа	10%	1	Активная работа студента на занятии

Активность	Вес	Количество	Описание
Зачет с оценкой	25%	1	Письменная или устная работа над заданием, направленным на проверку полученных знаний и навыков по дисциплине (модулю)

Формула расчёта итоговой оценки по дисциплине (модулю) «Информационная безопасность»: «0,4 × среднее за домашние задания + 0,25 × коллоквиум + 0,1 × аудиторная работа + 0,25 × зачет с оценкой».

Текущий контроль успеваемости обучающихся по дисциплине (модулю)

Примерные домашние задания

Домашнее задание 1

1. Проанализируйте реальный случай кибератаки (например, WannaCry или NotPetya) и опишите её последствия для организации.
2. Составьте алгоритм действий по обнаружению и удалению вредоносного ПО на компьютере.
3. Исследуйте современные инструменты для обнаружения вредоносного ПО и сделайте сравнительную таблицу их возможностей.
4. Опишите основные признаки заражения системы вредоносным ПО.
5. Разработайте план восстановления информационной системы после успешной атаки.

Домашнее задание 2

1. Подготовьте доклад о пяти наиболее распространённых методах социальной инженерии с примерами.
2. Составьте сценарий фишингового письма и объясните, как распознать его признаки.
3. Проанализируйте реальные случаи успешных атак с использованием социальной инженерии и выделите ошибки жертв.
4. Разработайте рекомендации для сотрудников по предотвращению атак социальной инженерии.
5. Проведите ролевую игру: один студент выступает в роли злоумышленника, другой — потенциальной жертвы, и проанализируйте результаты.

Домашнее задание 3

Что используем

- Java Spring
- Spring Security
- Keycloak (с PostgreSQL DB)
- Docker + Compose

Что надо сделать

1. Реализовать простое веб-приложение с использованием Java Spring. Тематика – на ваш вкус. Требований к контенту, хранению в БД и т.д. нет. Что должно быть
   a. Главная страница (лендинг), доступный без авторизации всем (а-ля у нас классный сервис, регистрируйтесь)
   b. Страница регистрации и логина (можно брать стандартную из Keycloak, можете свою красивую форму для нее сделать)
   c. Страница, которая доступна любому зарегистрированному пользователю (а-ля личный кабинет, данные какие-то по клиенту и т.д.)
   d. Страница, которая должна быть доступна только администратору (а-ля какая-то админка)
2. Подключить Spring Security и подружить это с Keycloak. Настроить авторизацию и аутентификацию, настроить роли “user” и “admin”
3. Запаковать приложение в docker compose. Главное требование – при проверке должно быть достаточно сделать docker compose up и все должно работать
4. Показать клиентский путь и продемонстрировать со скриншотами в README регистрацию, вход, назначение ему в Keycloak роли администратора (и как меняется веб-приложение при этом действии для него)
5. В вашем приложении должна быть настроена защита от CSRF
6. В вашем приложении должны быть настроены CORS Policy
7. Сделайте так, чтобы в ваше приложение можно было попадать только через NGINX. Рекомендую делать по DNS записям так: «example.com» – ваше приложение, а «api.example.com» – ваше API для него. Добавить такие записи при отсутствии DNS сервера можно через /etc/hosts в UNIX-like системах
8. Настройте на NGINX базовый MTLS. Выпустите свой CA для клиентов и настройте его так, чтобы если к вам обращались без сертификата, то получали бы ошибку 403 (работающий пример - https://smallstep.com/hello-mtls/doc/server/nginx)
9. При помощи переменной `$ssl_client_s_dn` отразите в NGINX логах `log_format` DN сертификата.
10. Выпустите клиентский сертификат, установите в систему CA для доверия и клиентский сертификат. Продемонстрируйте, что при работе с браузером не возникает ошибок самоподписанного сертификата. Проверьте, что в логи NGINX попала запись о ваших похождениях

Как предоставить результаты

- Репозиторий с кодом сервиса на Git
- В репозитории ОБЯЗАТЕЛЬНО должен быть отчет. В отчете ОБЯЗАТЕЛЬНО должны быть картинки с демонстрацией функциональности

Примерные вопросы для подготовки к семинарам

Вопросы к семинару по теме «Основы безопасности корпоративной инфраструктуры»

1. Какие основные модели контроля доступа существуют и в чем их отличия

(например, DAC, MAC, RBAC)?

2. Какие методы аутентификации и авторизации применяются для обеспечения контроля доступа?

3. Каковы основные задачи и методы мониторинга данных в корпоративной сети?

4. Какие инструменты и технологии используются для обнаружения несанкционированного доступа?

5. Каковы основные принципы построения политики контроля доступа и мониторинга для защиты информации?

Вопросы к семинару по теме «Методы защиты информации»

1. Какие этапы включает в себя процесс проведения тестирования на проникновение?
2. В чем разница между белым, серым и черным пентестингом?
3. Какие инструменты и техники используются для сканирования уязвимостей?
4. Как проводится эксплуатация уязвимостей и какие риски при этом возникают?
5. Какие требования предъявляются к отчетности и рекомендациям по итогам пентестинга?

Вопросы к семинару по теме «Вредоносное программное обеспечение»

1. Какие типы фишинговых атак существуют и как они отличаются?
2. Какие признаки позволяют распознать фишинговое письмо или веб-сайт?
3. Какие психологические приемы используют злоумышленники в фишинговых атаках?
4. Какие технические и организационные меры помогают защититься от фишинга?
5. Каковы основные этапы расследования инцидента, связанного с фишинговой атакой?

Примерные задания для коллоквиума

1. Какие основные виды вредоносного программного обеспечения существуют? Приведите примеры.
2. Какие методы распространения вредоносного ПО наиболее распространены?
3. Каковы типичные последствия заражения системы троянами и ransomware?
4. Какие признаки могут свидетельствовать о заражении компьютера вирусом?
5. Опишите основные методы обнаружения и удаления вредоносного ПО.
6. Какие меры защиты от вирусов и другого вредоносного ПО можно применить на уровне пользователя и организации?
7. Что такое социальная инженерия и какие основные методы используются злоумышленниками?
8. Каковы особенности фишинговых атак и как их можно распознать?
9. Какие психологические приёмы применяются в атаках социальной инженерии?
10. Какие превентивные меры помогут снизить риски успешных фишинговых атак?
11. Как повысить осведомлённость пользователей для защиты от социальной инженерии?
12. В чём разница между симметричным и асимметричным шифрованием?
13. Какие алгоритмы симметричного шифрования являются наиболее распространёнными?
14. Как работает алгоритм RSA и где он применяется?
15. Что такое цифровая подпись и как она обеспечивает целостность и аутентичность данных?

Задания для промежуточной аттестации по дисциплине (модулю)

№ п/п	Задание	Ответ	Компетенция	Индикатор
1	Опишите роли участников команды при разработке системы защиты информации и распределении задач по модулям безопасности.	Разработчик пишет код защиты, тестировщик проверяет уязвимости, архитектор проектирует Security Architecture, все несут ответственность за этап	УК-3, УК-1	УК-3.1, УК-1.2
2	Как мотивировать команду и распределить ресурсы при реагировании на инциденты информационной безопасности с ограниченным временем?	Четкое распределение задач, контроль сроков, пример профессионализма, оценка трудоемкости этапов проекта	УК-3, РГ-1	УК-3.2, РГ-1.2
3	Подготовьте презентацию результатов аудита безопасности для стейкхолдеров и руководства компании.	Структура: цель, методы, результаты, выводы, рекомендации с учетом целевых установок заинтересованных сторон	УК-1, ППК-ДА3	УК-1.3, ППК-ДА3.2
4	Оформите документацию по проекту системы защиты согласно профессиональным стандартам и требованиям к техническим спецификациям.	Титульный лист, содержание, введение, основная часть, выводы, список источников, приложения по ГОСТ	УК-1, ППК-Р5	УК-1.3, ППК-Р5.3
5	Дайте определение модели угроз и запишите её смысл в контексте защиты информационной системы.	Модель угроз это описание потенциальных злоумышленников их целей и методов атак на систему	УК-1, ОПК-6	УК-1.2, ОПК-6.1
6	Проанализируйте экономическую информацию для выбора между средствами криптографической защиты для проекта.	Сравнение затрат, производительности, рисков, учет специфики задач, влияние на эффективность бизнес-решений	УК-1, ОПК-6	УК-1.2, ОПК-6.2
7	Обоснуйте экономическое решение о выборе архитектуры системы защиты на основе анализа затрат и выгод.	Решение выбирается если учитывает интересы всех сторон, повышает	УК-1, ОПК-6	УК-1.3, ОПК-6.3

Электронный документ

		защиту инвестора от неблагоприятных изменений		
8	Запишите формулу для расчета риска информационной безопасности и выберите метод анализа данных для оценки.	Формула риска равна вероятность умноженная на ущерб, метод статистического анализа для оценки значимости угроз	ОПК-6, ППК-ДА3	ОПК-6.2, ППК-ДА3.2
9	Оптимизируйте выбор алгоритма шифрования и обоснуйте влияние на бизнес показатели компании.	Выбор алгоритма с максимальной эффективностью, оценка воздействия на ключевые показатели компании, скорость обработки данных	ОПК-6, ППК-Р5	ОПК-6.3, ППК-Р5.3
10	Обоснуйте экономическое решение в учебном проекте с учетом системного мышления при проектировании архитектуры защиты.	Использование модели с учетом взаимосвязей между модулями защиты, политиками и бизнес-целями компании	ОПК-6, РГ-4	ОПК-6.3, РГ-4.4
11	Назовите правовые нормы регулирующие защиту информации в РФ и их смысл для проекта безопасности.	ФЗ-152 О персональных данных, ФЗ-187 О безопасности КИИ, требования регуляторов, ответственность за нарушения	ППК-Р5, УК-1	ППК-Р5.3, УК-1.1
12	Примените правовые нормы при оценке рисков нарушения требований при работе с персональными данными.	Анализ рисков несоблюдения законодательных требований, оценка вероятности и пороговых значений, меры минимизации штрафов	ППК-Р5, ППК-Р6	ППК-Р5.3, ППК-Р6.3
13	Дайте правовую оценку ситуации с нарушением требований по защите информации в проекте компании.	Определение нарушений законодательных актов, применение санкций, влияние на репутацию организации	ППК-Р5, УК-1	ППК-Р5.3, УК-1.3
14	Выберите метод статистического анализа для проверки гипотез о влиянии мер защиты на снижение инцидентов.	A/B тест, проверка гипотез о значимости различий, расчет доверительных интервалов для	ППК-ДА3, ППК-ДА4	ППК-ДА3.2, ППК-ДА4.2

		оценок количества инцидентов		
15	Адаптируйте аналитическую модель оценки системы защиты под бизнес потребности и оцените влияние решений.	Перевод технических метрик в бизнес показатели, оценка воздействия на ключевые показатели компании, оптимизация процессов безопасности	ППК-ДА3, ППК-Р6	ППК-ДА3.2, ППК-Р6.3
16	Выберите тип визуализации для представления данных о результатах аудита и коммуникации с руководством.	График количества инцидентов и доверительных интервалов, интерактивный дашборд для публичной дискуссии о результатах анализа	ППК-ДА3, УК-1	ППК-ДА3.2, УК-1.3
17	Выявите бизнес проблему на основе анализа отклонений в системе защиты и примите решение.	Проблема уязвимости критических систем, выбор стратегии реагирования, решение о корректировке архитектуры или политик безопасности	ППК-ДА4, ППК-Р7	ППК-ДА4.2, ППК-Р7.2
18	Классифицируйте бизнес возможности при масштабировании системы защиты с учетом стратегического планирования.	Оптимизация ресурсов безопасности, разработка плана действий с учетом целей компании, выявление резервов роста защиты	ППК-ДА4, РГ-4	ППК-ДА4.2, РГ-4.4
19	Сформулируйте рекомендации на основе статистических выводов о результатах тестирования для управления продуктом.	При значимом улучшении внедрение изменения, при отсутствии эффекта отказ от изменения для эффективности системы защиты	ППК-Р6, ППК-Р7	ППК-Р6.3, ППК-Р7.2
20	Оцените риски реализации проекта системы защиты и разработайте меры управления.	Анализ вероятности срывов сроков, мониторинг индикаторов успешности, пересмотр плана при выявлении	РГ-1, УК-1	РГ-1.3, УК-1.3

		проблем		