



Первый проректор-проректор по учебной работе

25 " 09 20 26 г.

Б1.0.04.02 «Основы информационной безопасности»

Самара 2026

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы	4
2. Место дисциплины (модуля) в структуре образовательной программы	4
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся	4
4. Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий	5
4.1 Содержание лекционных занятий	5
4.2 Содержание лабораторных занятий	7
4.3 Содержание практических занятий	7
4.4. Содержание самостоятельной работы	7
5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю)	8
6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения	9
7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем	9
8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)	10
9. Методические материалы	10
10. Фонд оценочных средств по дисциплине (модулю)	11

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Общепрофессиональные компетенции			
Информационно-коммуникационные технологии для профессиональной деятельности	ОПК-3 Способен понимать и применять современные информационные технологии, в том числе отечественные, при создании программных продуктов и программных комплексов различного назначения	ОПК-3.1 Знать: современные информационные технологии и программные средства	Знать основные понятия информационной безопасности, виды угроз и уязвимостей, организационные, процедурные и программно-технические методы защиты информации
		ОПК-3.2 Уметь: использовать современные информационные технологии на всех этапах разработки программных систем	Уметь определять типовые угрозы и выбирать базовые меры защиты информации при создании и эксплуатации программных и информационных систем
		ОПК-3.3 Владеть: информационными технологиями и программными средствами при решении задач профессиональной деятельности	Владеть базовыми приемами безопасного использования программного обеспечения, управления доступом и защиты данных при решении профессиональных задач
	ОПК-6 Способен использовать в педагогической деятельности научные основы знаний в сфере информационно-коммуникационных технологий	ОПК-6.1 Знать: прикладное программное обеспечение для разработки методической документации для педагогической деятельности	Знать базовые требования информационной безопасности при использовании прикладного ПО и подготовке электронной документации
		ОПК-6.2 Уметь: автоматизировать задачи в области педагогической деятельности, разрабатывать и сопровождать информационные системы для поддержки педагогической деятельности	Уметь учитывать требования защиты информации при автоматизации задач и сопровождении информационных систем, используемых для организации педагогической деятельности
		ОПК-6.3 Владеть: системными знаниями в области информационно-коммуникационных технологий для организации педагогической деятельности	Владеть системным представлением о безопасном применении информационно-коммуникационных технологий и защите данных в электронной информационно-образовательной среде

2. Место дисциплины (модуля) в структуре образовательной программы

Место дисциплины (модуля) в структуре образовательной программы: **обязательная часть**

Код компетенции	Предшествующие дисциплины	Параллельно осваиваемые дисциплины	Последующие дисциплины
ОПК-3	Основы программирования	Системы искусственного интеллекта	Подготовка к процедуре защиты и защита выпускной квалификационной работы
ОПК-6	Основы программирования		Подготовка к процедуре защиты и защита выпускной квалификационной работы

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

Вид учебной работы	Всего часов / часов в электронной форме	3 семестр часов / часов в электронной форме
Аудиторная контактная работа (всего), в том числе:	32	32
Лекции	32	32
Внеаудиторная контактная работа, КСР	2	2
Самостоятельная работа (всего), в том числе:	38	38
подготовка к зачету	6	6
подготовка к лекциям	32	32
Контроль	36	36
Итого: час	108	108
Итого: з.е.	3	3

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

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы				
		ЛЗ	ЛР	ПЗ	СРС	Всего часов
1	Теоретические основы информационной безопасности и анализ угроз	10	0	0	13	23
2	Организационные и процедурные меры обеспечения информационной безопасности	8	0	0	12	20
3	Программно-технические методы защиты информации	14	0	0	13	27
	КСР	0	0	0	0	2
	Контроль	0	0	0	0	36
	Итого	32	0	0	38	108

4.1 Содержание лекционных занятий

№ занятия	Наименование раздела	Тема лекции	Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов / часов в электронной форме
3 семестр				

1	Теоретические основы информационной безопасности и анализ угроз	Информация как объект защиты	Понятие информации. Виды защищаемой информации. Конфиденциальность, целостность и доступность информации. Информационная система как объект защиты.	2
2	Теоретические основы информационной безопасности и анализ угроз	Информационная безопасность в системе национальной безопасности	Интересы личности, общества и государства в информационной сфере. Роль информационной безопасности в системе национальной безопасности. Основные направления государственной политики.	2
3	Теоретические основы информационной безопасности и анализ угроз	Классификация угроз информационной безопасности	Понятия угрозы и уязвимости. Классификация угроз по источнику, объекту и способу реализации. Внутренние и внешние источники угроз.	2
4	Теоретические основы информационной безопасности и анализ угроз	Способы нарушения безопасности информации	Нарушение конфиденциальности, целостности и доступности информации. Несанкционированный доступ. Удалённые атаки. Каналы утечки и искажения информации.	2
5	Теоретические основы информационной безопасности и анализ угроз	Анализ и оценка рисков информационной безопасности	Активы, угрозы, уязвимости и последствия. Качественная оценка риска. Модель угроз. Выбор мер обработки риска.	2
6	Организационные и процедурные меры обеспечения информационной безопасности	Организационные основы обеспечения информационной безопасности	Административный уровень защиты информации. Цели и задачи системы защиты. Распределение ролей и ответственности. Политика информационной безопасности.	2
7	Организационные и процедурные меры обеспечения информационной безопасности	Правовое регулирование защиты информации	Информация ограниченного доступа. Персональные данные. Коммерческая тайна. Обязанности организации и пользователей. Локальные нормативные документы.	2
8	Организационные и процедурные меры обеспечения информационной безопасности	Управление доступом и действия пользователей	Регистрация и учет пользователей. Предоставление и прекращение доступа. Принцип минимальных привилегий. Правила работы с носителями и документами.	2
9	Организационные и процедурные меры обеспечения информационной безопасности	Реагирование на инциденты информационной безопасности	Понятия события и инцидента информационной безопасности. Обнаружение и регистрация инцидентов. Первичные действия при инциденте. Восстановление работоспособности. Анализ причин инцидента.	2
10	Программно-технические методы защиты информации	Защита от вредоносного программного обеспечения	Вирусы, сетевые черви и троянские программы. Другие виды вредоносного программного обеспечения. Источники и признаки заражения. Способы распространения вредоносного программного обеспечения.	2
11	Программно-технические методы защиты информации	Защита от вредоносного программного обеспечения	Обнаружение вредоносного программного обеспечения. Антивирусная защита. Обновление программного обеспечения. Резервное копирование. Правила безопасной эксплуатации программного обеспечения.	2

12	Программно-технические методы защиты информации	Идентификация, аутентификация и разграничение доступа	Идентификация и аутентификация пользователей. Парольная защита. Многофакторная аутентификация. Модели и механизмы разграничения доступа.	2
13	Программно-технические методы защиты информации	Основы криптографической защиты информации	Назначение криптографической защиты информации. Симметричное и асимметричное шифрование. Криптографическое хеширование. Электронная подпись. Области применения криптографических средств.	2
14	Программно-технические методы защиты информации	Защита информации в компьютерных сетях	Сетевые угрозы. Межсетевое экранирование. Защищенные сетевые протоколы. Безопасное удалённое взаимодействие. Базовые меры сетевой защиты.	2
15	Программно-технические методы защиты информации	Защита операционных систем и прикладного программного обеспечения	Уязвимости программного обеспечения. Установка обновлений. Настройка защитных механизмов. Антивирусные средства. Журналирование событий. Безопасная конфигурация программного обеспечения.	2
16	Программно-технические методы защиты информации	Организация комплексной системы защиты информации	Организационные, процедурные и программно-технические меры защиты. Оценка состояния защищенности. Контроль эффективности применяемых мер. Комплексная защита информации.	2
Итого за семестр:				32
Итого:				32

4.2 Содержание лабораторных занятий

Учебные занятия не реализуются.

4.3 Содержание практических занятий

Учебные занятия не реализуются.

4.4. Содержание самостоятельной работы

Наименование раздела	Вид самостоятельной работы	Содержание самостоятельной работы (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов
3 семестр			

Теоретические основы информационной безопасности и анализ угроз	Подготовка к лекционному занятию	Основные понятия информационной безопасности. Виды защищаемой информации. Конфиденциальность, целостность и доступность информации. Интересы личности, общества и государства в информационной сфере. Классификация и источники угроз. Каналы утечки информации. Активы, угрозы, уязвимости и последствия. Последовательность анализа и качественной оценки рисков.	11
Организационные и процедурные меры обеспечения информационной безопасности	Подготовка к лекционному занятию	Нормативные и локальные документы в области информационной безопасности. Политика информационной безопасности. Роли и ответственность участников. Процедуры управления доступом. Правила работы с информацией. Обнаружение и регистрация инцидентов. Реагирование на инциденты. Восстановление после инцидентов. Разбор типовых ситуаций.	10
Программно-технические методы защиты информации	Подготовка к лекционному занятию	Виды вредоносного программного обеспечения. Источники и признаки заражения. Способы распространения вредоносного программного обеспечения. Меры защиты от вредоносного программного обеспечения. Идентификация и аутентификация. Разграничение доступа. Основы криптографической защиты. Основы сетевой защиты. Защита операционных систем и прикладного программного обеспечения. Состав комплексной системы защиты информации.	11
Теоретические основы информационной безопасности и анализ угроз	Подготовка к зачету	Изучение теоретического материала	2
Организационные и процедурные меры обеспечения информационной безопасности	Подготовка к зачету	Изучение теоретического материала	2
Программно-технические методы защиты информации	Подготовка к зачету	Изучение теоретического материала	2
Итого за семестр:			38
Итого:			38

5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю)

№ п/п	Библиографическое описание	Ресурс НТБ СамГТУ (ЭБС СамГТУ, IPRbooks и т.д.)
Основная литература		
1	Прохорова, Ольга Витольдовна Информационная безопасность и защита информации : учеб. [для 2 курса специальности 230400.62 "Информ. системы и технологии"] [Текст] / Самар. гос. архитектур.-строит. ун-т (СГАСУ), Каф. приклад. математики и вычисл. техники.- Самара, СГАСУ, 2014.- 112 с.: ил.	Книжный фонд
2	Сычев, Юрий Николаевич Защита информации и информационная безопасность : учеб. пособие для студентов вузов [Текст] .- Москва, Инфра-М, 2021.- 200 с.: ил.	Книжный фонд
Дополнительная литература		
3	Запечников , С.В. Криптографические методы защиты информации : учеб. пособие для академ.бакалавриата / С. В. Запечников,О. В. Казарин, А. А. Тарасов.- М., Юрайт, 2015.- 309 с.	Книжный фонд
4	Олифер, В.Г. Компьютерные сети : принципы,технологии,протоколы:учеб.пособие / В. Г. Олифер, Н. А. Олифер .- 4-е изд..- М., Питер , 2015.- 943 с.	Книжный фонд
5	Организационное и правовое обеспечение информационной безопасности : учеб. и практикум для бакалавриата и магистратуры / под ред.Т. А. Поляковой, А. А. Стрельцова.- М., Юрайт, 2017.- 325 с.	Книжный фонд

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

При проведении лекционных занятий используется мультимедийное оборудование.

Организовано взаимодействие обучающегося и преподавателя с использованием электронной ин-формационной образовательной среды университета.

№ п/п	Наименование	Производитель	Способ распространения
1	Microsoft Office	Microsoft Corporation (Зарубежный)	Лицензионное
2	Python	Python Software Foundation (Зарубежный)	Свободно распространяемое
3	Kaspersky Endpoint Security	Kaspersky Lab (Отечественный)	Лицензионное
4	Антиплагиат.ВУЗ	АО «Антиплагиат» (Отечественный)	Лицензионное

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

№ п/п	Наименование	Краткое описание	Режим доступа
1	Библиотека учебно-методической литературы системы "Единое окно"	http://window.edu.ru/	Ресурсы открытого доступа
2	Научная электронная библиотека	http://elibrary.ru/	Ресурсы открытого доступа
3	Научная электронная библиотека «Киберленинка»	https://cyberleninka.ru	Ресурсы открытого доступа
4	Банк данных "Библиотека копий официальных публикаций правовых актов"	http://lib.ksrf.ru/	Ресурсы открытого доступа

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия

- аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук);
- аудитория, оснащенная учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя.

Самостоятельная работа

- компьютерный класс, оснащенный компьютерами с доступом в Интернет и обеспечивающие доступ в электронно-информационную образовательную среду СамГТУ читальный зал НТБ СамГТУ (ауд. 200 корпус № 8; ауд. 125 корпус № 1; ауд. 41, 31, 34, 35 Главный корпус библиотеки; ауд. 83а, 414, 416, 0209 12 корпус; ауд. 401 корпус № 10);
- материально-техническое обеспечение НТБ СамГТУ;
- ресурсы УИТ СамГТУ.

9. Методические материалы

Методические рекомендации при работе на лекции

До лекции студент должен просмотреть учебно-методическую и научную литературу по теме лекции с тем, чтобы иметь представление о проблемах, которые будут разбираться в лекции.

Перед началом лекции обучающимся сообщается тема лекции, план, вопросы, подлежащие рассмотрению, доводятся основные литературные источники. Весь учебный материал, сообщаемый преподавателем, должен не просто прослушиваться. Он должен быть активно воспринят, т.е. услышан, осмыслен, понят, зафиксирован на бумаге и закреплён в памяти. Приступая к слушанию нового учебного материала, полезно мысленно установить его связь с ранее изученным. Следя за техникой чтения лекции (акцент на существенном, повышение тона, изменение ритма, пауза и т.п.), необходимо вслед за преподавателем уметь выделять основные категории, законы и определять их содержание, проблемы, предполагать их возможные решения, доказательства и выводы. Осуществляя такую работу, можно значительно облегчить себе понимание учебного материала, его конспектирование и дальнейшее изучение.

Конспектирование лекции позволяет обработать, систематизировать и лучше сохранить полученную информацию с тем, чтобы в будущем можно было восстановить в памяти основные,

содержательные моменты. Типичная ошибка, совершаемая обучающимся, дословное конспектирование речи преподавателя. Как правило, при записи «слово в слово» не остается времени на обдумывание, анализ и синтез информации. Отбирая нужную информацию, главные мысли, проблемы, решения и выводы, необходимо сокращать текст, строить его таким образом, чтобы потом можно было легко в нем разобраться. Желательно оставить в рабочих конспектах поля, на которых можно будет делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С окончанием лекции работа над конспектом не может считаться завершенной. Нужно еще восстановить отдельные места, проверить, все ли понятно, уточнить что-то на консультации и т.п. с тем, чтобы конспект мог быть использован в процессе подготовки к практическим занятиям, зачету, экзамену. Конспект лекции – незаменимый учебный документ, необходимый для самостоятельной работы.

Методические рекомендации по выполнению самостоятельной работы

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению с учетом потребностей и возможностей обучающегося.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

Самостоятельная работа реализуется:

- непосредственно в процессе аудиторных занятий;
- на лекциях, практических занятиях;
- в контакте с преподавателем вне рамок расписания;
- на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.;
- в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.

10. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств представлен в приложении № 1.

Приложение 1 к рабочей программе дисциплины
Б1.О.04.02 «Основы информационной
безопасности»

**Фонд оценочных средств
по дисциплине
Б1.О.04.02 «Основы информационной безопасности»**

Код и направление подготовки (специальность)	02.03.03 Математическое обеспечение и администрирование информационных систем
Направленность (профиль)	Анализ данных в бизнес-аналитике
Квалификация	Бакалавр
Форма обучения	Очная
Год начала подготовки	2026
Институт / факультет	Институт инженерно-экономического и гуманитарного образования
Выпускающая кафедра	кафедра "Высшая математика"
Кафедра-разработчик	кафедра "Высшая математика"
Объем дисциплины, ч. / з.е.	108 / 3
Форма контроля (промежуточная аттестация)	Зачет

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Общепрофессиональные компетенции			
Информационно-коммуникационные технологии для профессиональной деятельности	ОПК-3 Способен понимать и применять современные информационные технологии, в том числе отечественные, при создании программных продуктов и программных комплексов различного назначения	ОПК-3.1 Знать: современные информационные технологии и программные средства	Знать основные понятия информационной безопасности, виды угроз и уязвимостей, организационные, процедурные и программно-технические методы защиты информации
		ОПК-3.2 Уметь: использовать современные информационные технологии на всех этапах разработки программных систем	Уметь определять типовые угрозы и выбирать базовые меры защиты информации при создании и эксплуатации программных и информационных систем
		ОПК-3.3 Владеть: информационными технологиями и программными средствами при решении задач профессиональной деятельности	Владеть базовыми приемами безопасного использования программного обеспечения, управления доступом и защиты данных при решении профессиональных задач
	ОПК-6 Способен использовать в педагогической деятельности научные основы знаний в сфере информационно-коммуникационных технологий	ОПК-6.1 Знать: прикладное программное обеспечение для разработки методической документации для педагогической деятельности	Знать базовые требования информационной безопасности при использовании прикладного ПО и подготовке электронной документации
		ОПК-6.2 Уметь: автоматизировать задачи в области педагогической деятельности, разрабатывать и сопровождать информационные системы для поддержки педагогической деятельности	Уметь учитывать требования защиты информации при автоматизации задач и сопровождении информационных систем, используемых для организации педагогической деятельности
		ОПК-6.3 Владеть: системными знаниями в области информационно-коммуникационных технологий для организации педагогической деятельности	Владеть системным представлением о безопасном применении информационно-коммуникационных технологий и защите данных в электронной информационно-образовательной среде

Матрица соответствия оценочных средств запланированным результатам обучения

Код индикатора достижения компетенции	Результаты обучения	Оценочные средства	Текущий контроль успеваемости	Промежуточная аттестация
Теоретические основы информационной безопасности и анализ угроз				
ОПК-3.1 Знать: современные информационные технологии и программные средства	Знать основные понятия информационной безопасности, виды угроз и уязвимостей, организационные, процедурные и программно-технические методы защиты информации	Подготовка к ЛЗ, подготовка к зачету	Да	Да
ОПК-3.2 Уметь: использовать современные информационные технологии на всех этапах разработки программных систем	Уметь определять типовые угрозы и выбирать базовые меры защиты информации при создании и эксплуатации программных и информационных систем	Подготовка к ЛЗ, подготовка к зачету	Да	Да
ОПК-3.3 Владеть: информационными технологиями и программными средствами при решении задач профессиональной деятельности	Владеть базовыми приемами безопасного использования программного обеспечения, управления доступом и защиты данных при решении профессиональных задач	Подготовка к ЛЗ, подготовка к зачету	Да	Да

ОПК-6.1 Знать: прикладное программное обеспечение для разработки методической документации для педагогической деятельности	Знать базовые требования информационной безопасности при использовании прикладного ПО и подготовке электронной документации	Подготовка к ЛЗ, подготовка к зачету	Да	Да
ОПК-6.2 Уметь: автоматизировать задачи в области педагогической деятельности, разрабатывать и сопровождать информационные системы для поддержки педагогической деятельности	Уметь учитывать требования защиты информации при автоматизации задач и сопровождении информационных систем, используемых для организации педагогической деятельности	Подготовка к ЛЗ, подготовка к зачету	Да	Да
ОПК-6.3 Владеть: системными знаниями в области информационно-коммуникационных технологий для организации педагогической деятельности	Владеть системным представлением о безопасном применении информационно-коммуникационных технологий и защите данных в электронной информационно-образовательной среде	Подготовка к ЛЗ, подготовка к зачету	Да	Да
Организационные и процедурные меры обеспечения информационной безопасности				
ОПК-3.1 Знать: современные информационные технологии и программные средства	Знать основные понятия информационной безопасности, виды угроз и уязвимостей, организационные, процедурные и программно-технические методы защиты информации	Подготовка к ЛЗ, подготовка к зачету	Да	Да
ОПК-3.2 Уметь: использовать современные информационные технологии на всех этапах разработки программных систем	Уметь определять типовые угрозы и выбирать базовые меры защиты информации при создании и эксплуатации программных и информационных систем	Подготовка к ЛЗ, подготовка к зачету	Да	Да
ОПК-3.3 Владеть: информационными технологиями и программными средствами при решении задач профессиональной деятельности	Владеть базовыми приемами безопасного использования программного обеспечения, управления доступом и защиты данных при решении профессиональных задач	Подготовка к ЛЗ, подготовка к зачету	Да	Да
ОПК-6.1 Знать: прикладное программное обеспечение для разработки методической документации для педагогической деятельности	Знать базовые требования информационной безопасности при использовании прикладного ПО и подготовке электронной документации	Подготовка к ЛЗ, подготовка к зачету	Да	Да
ОПК-6.2 Уметь: автоматизировать задачи в области педагогической деятельности, разрабатывать и сопровождать информационные системы для поддержки педагогической деятельности	Уметь учитывать требования защиты информации при автоматизации задач и сопровождении информационных систем, используемых для организации педагогической деятельности	Подготовка к ЛЗ, подготовка к зачету	Да	Да

ОПК-6.3 Владеть: системными знаниями в области информационно-коммуникационных технологий для организации педагогической деятельности	Владеть системным представлением о безопасном применении информационно-коммуникационных технологий и защите данных в электронной информационно-образовательной среде	Подготовка к ЛЗ, подготовка к зачету	Да	Да
Программно-технические методы защиты информации				
ОПК-3.1 Знать: современные информационные технологии и программные средства	Знать основные понятия информационной безопасности, виды угроз и уязвимостей, организационные, процедурные и программно-технические методы защиты информации	Подготовка к ЛЗ, подготовка к зачету	Да	Да
ОПК-3.2 Уметь: использовать современные информационные технологии на всех этапах разработки программных систем	Уметь определять типовые угрозы и выбирать базовые меры защиты информации при создании и эксплуатации программных и информационных систем	Подготовка к ЛЗ, подготовка к зачету	Да	Да
ОПК-3.3 Владеть: информационными технологиями и программными средствами при решении задач профессиональной деятельности	Владеть базовыми приемами безопасного использования программного обеспечения, управления доступом и защиты данных при решении профессиональных задач	Подготовка к ЛЗ, подготовка к зачету	Да	Да
ОПК-6.1 Знать: прикладное программное обеспечение для разработки методической документации для педагогической деятельности	Знать базовые требования информационной безопасности при использовании прикладного ПО и подготовке электронной документации	Подготовка к ЛЗ, подготовка к зачету	Да	Да
ОПК-6.2 Уметь: автоматизировать задачи в области педагогической деятельности, разрабатывать и сопровождать информационные системы для поддержки педагогической деятельности	Уметь учитывать требования защиты информации при автоматизации задач и сопровождении информационных систем, используемых для организации педагогической деятельности	Подготовка к ЛЗ, подготовка к зачету	Да	Да
ОПК-6.3 Владеть: системными знаниями в области информационно-коммуникационных технологий для организации педагогической деятельности	Владеть системным представлением о безопасном применении информационно-коммуникационных технологий и защите данных в электронной информационно-образовательной среде	Подготовка к ЛЗ, подготовка к зачету	Да	Да

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы

Формы текущего контроля успеваемости

Текущий контроль осуществляется выполнением аудиторных контрольных работ и тестовых заданий по материалам дисциплины.

Пример контрольной работы при изучении раздела «Теоретические основы информационной безопасности».

1. Для предложенных ситуаций определить, какое свойство информации нарушено: конфиденциальность, целостность или доступность.
2. Для заданного информационного ресурса выделить актив, угрозу, уязвимость и возможные последствия реализации угрозы.
3. Классифицировать перечисленные угрозы по источнику возникновения и способу реализации.
4. По описанным признакам определить возможное заражение вредоносным программным обеспечением и назвать первичные действия пользователя.
5. Для описанной информационной системы предложить базовые меры обработки выявленного риска.

Пример контрольной работы при изучении раздела «Организационные и процедурные основы защиты информации».

1. Сформулировать основные положения политики информационной безопасности небольшой организации.
2. Установить последовательность регистрации пользователя, предоставления ему прав доступа, пересмотра полномочий и прекращения доступа.
3. Применить принцип минимальных привилегий при распределении прав между пользователями информационной системы.
4. Установить последовательность обнаружения, регистрации, локализации и анализа инцидента информационной безопасности.
5. Определить вид информации ограниченного доступа и указать организационные документы, регулирующие работу с ней.

Пример контрольной работы при изучении раздела «Программно-технические методы защиты информации».

1. Выбрать подходящий способ аутентификации для предложенного сценария и обосновать выбор.
2. Сопоставить симметричное и асимметричное шифрование с задачами их практического применения.
3. Объяснить назначение хеширования и электронной подписи при контроле целостности и подтверждении авторства документа.
4. Для заданной схемы сетевого взаимодействия предложить базовые меры защиты соединения и разграничения доступа.
5. Сформировать минимальный комплекс организационных, процедурных и программно-технических мер защиты информационной системы.

Семестр 3

Форма промежуточной аттестации — зачёт. Зачёт проводится в письменно-устной форме. Обучающийся получает билет и после подготовки отвечает по билету и на дополнительные вопросы преподавателя. Зачётный билет состоит из трёх вопросов: первый и второй вопросы теоретические, третий содержит практическое задание.

Федеральное государственное бюджетное образовательное учреждение высшего образования Самарский государственный технический университет
ЗАЧЁТНЫЙ БИЛЕТ № 1 по дисциплине Б1.О.04.02 «Основы информационной безопасности» Направление подготовки 02.03.03 Математическое обеспечение и администрирование информационных систем
1. Понятия угрозы и уязвимости. Классификация угроз информационной безопасности.
2. Идентификация, аутентификация и разграничение доступа. Парольная и многофакторная аутентификация.
3. Практическое задание. Пользователь сообщил о подозрительном входе в учётную запись. Опишите порядок регистрации события, первичные меры локализации, восстановление доступа и анализ причин.

Вопросы к зачёту (3 семестр)

1. Информация как объект защиты. Виды защищаемой информации. Конфиденциальность, целостность и доступность.
2. Информационная безопасность в системе национальной безопасности. Интересы личности, общества и государства.
3. Понятия угрозы и уязвимости. Классификация угроз информационной безопасности.
4. Способы нарушения конфиденциальности, целостности и доступности информации. Каналы утечки и искажения информации.
5. Активы, угрозы, уязвимости и последствия. Основы анализа и качественной оценки рисков.
6. Виды вредоносного программного обеспечения, источники и признаки заражения, способы распространения.
7. Обнаружение вредоносного программного обеспечения и базовые меры защиты от него.
8. Административный уровень защиты. Цели и задачи системы защиты. Политика информационной безопасности.
9. Правовое регулирование защиты информации. Информация ограниченного доступа и локальные нормативные документы.
10. Регистрация и учёт пользователей. Предоставление и прекращение доступа. Принцип минимальных привилегий.
11. События и инциденты информационной безопасности. Обнаружение, регистрация, реагирование и восстановление.
12. Идентификация, аутентификация и разграничение доступа. Парольная и многофакторная аутентификация.
13. Назначение криптографической защиты. Симметричное и асимметричное шифрование, хеширование и электронная подпись.
14. Сетевые угрозы, межсетевое экранирование, защищённые протоколы и безопасное удалённое взаимодействие.
15. Защита операционных систем и прикладного программного обеспечения. Обновления, безопасная конфигурация и журналирование.
16. Организация комплексной системы защиты информации. Сочетание организационных, процедурных и программно-технических мер.

Типовые практические задания к зачёту

1. Для информационной системы указаны случаи раскрытия данных, несанкционированного изменения записей и недоступности сервиса. Соотнесите каждый случай с нарушением конфиденциальности, целостности или доступности и предложите по одной базовой мере защиты.
2. Организация внедряет новый информационный сервис. Выделите защищаемые активы, назовите типовые угрозы и уязвимости, оцените возможные последствия и предложите базовые меры обработки риска.

3. На рабочем компьютере обнаружены признаки заражения вредоносным программным обеспечением. Опишите последовательность первичных действий пользователя и администратора без уничтожения сведений об инциденте.
4. Для небольшой организации определите основные положения политики информационной безопасности. Укажите цели защиты, роли и ответственность, порядок предоставления доступа и базовые правила работы с информацией.
5. Пользователь сообщил о подозрительном входе в учётную запись. Опишите порядок регистрации события, первичные меры локализации, восстановление доступа и анализ причин.
6. Информационная система хранит данные и электронные учебно-методические материалы. Предложите минимальный комплекс организационных, процедурных и программно-технических мер защиты.

Тесты по компетенциям
по дисциплине Б1.О.04.02 «Основы информационной безопасности»
(шифр и наименование дисциплины)

№ задания	Содержание задания	Ключ к ответу	Наименование темы РПД	Семестр																										
ОПК-3 Способен понимать и применять современные информационные технологии, в том числе отечественные, при создании программных продуктов и программных комплексов различного назначения																														
1	Установите последовательность первичных действий при обнаружении инцидента информационной безопасности: А. сообщить ответственному лицу и зарегистрировать событие Б. выполнить первичную локализацию инцидента В. определить последствия и сохранить сведения об инциденте Г. восстановить работоспособность и устранить причину Запишите соответствующую последовательность букв слева направо.	АБВГ	Реагирование на инциденты информационной безопасности	3																										
2	Прочитайте вопрос и выберите один правильный ответ: При обследовании информационной системы обнаружен устаревший программный компонент с известным недостатком безопасности. Как следует классифицировать этот недостаток? А. источник угрозы Б. уязвимость В. политика информационной безопасности Г. инцидент информационной безопасности	Б	Классификация угроз информационной безопасности	3																										
3	Установите соответствие между свойством защищаемой информации и обеспечивающей его мерой: <table border="1"><thead><tr><th>Свойство</th><th>Мера</th></tr></thead><tbody><tr><td>А. Конфиденциальность</td><td>1. Резервирование и восстановление</td></tr><tr><td>Б. Целостность</td><td>2. Разграничение доступа</td></tr><tr><td>В. Доступность</td><td>3. Контроль хеш-значения</td></tr><tr><td>Г. Комплексная защита</td><td>4. Сочетание организационных и технических мер</td></tr></tbody></table> Запишите выбранные цифры под соответствующими буквами в виде таблицы: <table border="1"><tr><td>А</td><td>Б</td><td>В</td><td>Г</td></tr><tr><td></td><td></td><td></td><td></td></tr></table>	Свойство	Мера	А. Конфиденциальность	1. Резервирование и восстановление	Б. Целостность	2. Разграничение доступа	В. Доступность	3. Контроль хеш-значения	Г. Комплексная защита	4. Сочетание организационных и технических мер	А	Б	В	Г					<table border="1"><tr><td>А</td><td>Б</td><td>В</td><td>Г</td></tr><tr><td>2</td><td>3</td><td>1</td><td>4</td></tr></table>	А	Б	В	Г	2	3	1	4	Информация как объект защиты	3
Свойство	Мера																													
А. Конфиденциальность	1. Резервирование и восстановление																													
Б. Целостность	2. Разграничение доступа																													
В. Доступность	3. Контроль хеш-значения																													
Г. Комплексная защита	4. Сочетание организационных и технических мер																													
А	Б	В	Г																											
А	Б	В	Г																											
2	3	1	4																											
4	Прочитайте текст и выберите три правильных варианта ответа: Какие меры снижают риск запуска вредоносного программного обеспечения в информационной системе организации? А. своевременная установка обновлений безопасности Б. ограничение прав пользователей и контроль запуска приложений В. отключение журналирования событий Г. проверка файлов и почтовых вложений средствами защиты Д. использование общей учётной записи администратора	А, Б, Г	Защита от вредоносного программного обеспечения	3																										
5	Прочитайте текст вопроса и дополните фразу: Предоставление пользователю только тех прав, которые необходимы для выполнения его задач, называется принципом _____.	минимальных привилегий	Управление доступом и действия пользователей	3																										
6	Прочитайте вопрос и дайте развёрнутый ответ: Какие основные элементы необходимо определить при качественной оценке риска информационной безопасности?	Защищаемые активы, угрозы, уязвимости, возможные последствия и существующие либо необходимые меры защиты.	Анализ и оценка рисков информационной безопасности	3																										
7	Прочитайте и решите ситуационную задачу: Аналитику были предоставлены права, превышающие его должностные обязанности. Используя эти права, он изменил справочные данные, что привело к искажению отчёта. Укажите нарушенное свойство информации и принцип управления доступом, который не был соблюден.	Нарушена целостность информации; не соблюден принцип минимальных привилегий.	Способы нарушения безопасности информации	3																										
8	Установите последовательность действий при обнаружении признаков заражения рабочего компьютера: А. изолировать компьютер от сети Б. сообщить ответственному лицу и зарегистрировать событие В. провести проверку и определить последствия Г. восстановить работоспособность и устранить причину Запишите соответствующую последовательность букв слева направо.	АБВГ	Защита от вредоносного программного обеспечения	3																										
9	Прочитайте текст и выберите два правильных варианта ответа: Какие механизмы могут применяться для контроля целостности и подтверждения подлинности электронного документа? А. криптографическая хеш-функция Б. электронная подпись В. переименование файла Г. изменение расширения файла	А, Б	Основы криптографической защиты информации	3																										

№ задания	Содержание задания	Ключ к ответу	Наименование темы РПД	Семестр																										
10	Прочитайте вопрос и выберите один правильный ответ, затем кратко обоснуйте выбор: Каково основное назначение межсетевого экрана? А. резервное копирование файлов Б. фильтрация сетевого трафика по установленным правилам В. создание электронной подписи Г. редактирование документов	Б; межсетевого экран разрешает или блокирует сетевой трафик в соответствии с заданными правилами.	Защита информации в компьютерных сетях	3																										
ОПК-6 Способен использовать в педагогической деятельности научные основы знаний в сфере информационно-коммуникационных технологий																														
11	Установите соответствие между риском для электронной учебно-методической документации и наиболее подходящей мерой защиты: <table><tr><th>Угроза</th><th>Мера защиты</th></tr><tr><td>А. Компрометация пароля преподавателя</td><td>1. Версионное резервное копирование</td></tr><tr><td>Б. Удаление или повреждение актуальной версии документа</td><td>2. Ролевое разграничение и периодический пересмотр прав</td></tr><tr><td>В. Доступ сотрудника сверх его должностных полномочий</td><td>3. Многофакторная аутентификация</td></tr><tr><td>Г. Получение документа с вредоносным вложением</td><td>4. Фильтрация вложений и защита конечного устройства</td></tr></table> Запишите выбранные цифры под соответствующими буквами в виде таблицы: <table><tr><td>А</td><td>Б</td><td>В</td><td>Г</td></tr><tr><td></td><td></td><td></td><td></td></tr></table>	Угроза	Мера защиты	А. Компрометация пароля преподавателя	1. Версионное резервное копирование	Б. Удаление или повреждение актуальной версии документа	2. Ролевое разграничение и периодический пересмотр прав	В. Доступ сотрудника сверх его должностных полномочий	3. Многофакторная аутентификация	Г. Получение документа с вредоносным вложением	4. Фильтрация вложений и защита конечного устройства	А	Б	В	Г					<table><tr><td>А</td><td>Б</td><td>В</td><td>Г</td></tr><tr><td>3</td><td>1</td><td>2</td><td>4</td></tr></table>	А	Б	В	Г	3	1	2	4	Организация комплексной системы защиты информации	3
Угроза	Мера защиты																													
А. Компрометация пароля преподавателя	1. Версионное резервное копирование																													
Б. Удаление или повреждение актуальной версии документа	2. Ролевое разграничение и периодический пересмотр прав																													
В. Доступ сотрудника сверх его должностных полномочий	3. Многофакторная аутентификация																													
Г. Получение документа с вредоносным вложением	4. Фильтрация вложений и защита конечного устройства																													
А	Б	В	Г																											
А	Б	В	Г																											
3	1	2	4																											
12	Прочитайте текст и выберите три правильных варианта ответа: Перед открытой публикацией электронной учебно-методической документации необходимо: А. исключить или обезличить персональные данные Б. проверить установленные права доступа В. разрешить редактирование всем пользователям Г. проверить содержание и целостность документа Д. разместить пароль в имени файла	А, Б, Г	Правовое регулирование защиты информации	3																										
13	Прочитайте текст вопроса и дополните фразу: Модель разграничения доступа, при которой права предоставляются в соответствии с функциональными обязанностями и назначенной ролью пользователя, называется _____ моделью.	ролевой	Управление доступом и действия пользователей	3																										
14	Прочитайте вопрос и выберите один правильный ответ: Какой способ предпочтителен для удалённой передачи учебно-методических материалов ограниченного доступа? А. открытая общедоступная ссылка Б. защищённый канал и доступ после аутентификации В. публикация пароля рядом со ссылкой Г. неизвестный общедоступный сервис без ограничений	Б	Защита информации в компьютерных сетях	3																										
15	Установите последовательность действий при обнаружении подозрительного входа в учётную запись преподавателя: А. сообщить ответственному лицу и зарегистрировать инцидент Б. сменить пароль и завершить посторонние сеансы В. проверить журналы входа и возможные последствия Г. включить или повторно настроить многофакторную аутентификацию Запишите соответствующую последовательность букв слева направо.	АБВГ	Реагирование на инциденты информационной безопасности	3																										
16	Прочитайте вопрос и дайте развёрнутый ответ: Какой минимальный комплекс мер следует предусмотреть для подсистемы электронной информационно-образовательной среды, в которой размещаются учебно-методические материалы и фиксируются действия пользователей?	Индивидуальные учётные записи, ролевое разграничение доступа, обновление программного обеспечения, резервное копирование с проверкой восстановления, защита от вредоносного ПО, журналирование значимых событий и установленный порядок реагирования на инциденты.	Организация комплексной системы защиты информации	3																										
17	Прочитайте и решите ситуационную задачу: Преподаватель подготовил документ с результатами обучающихся и разместил его в облачном хранилище с доступом по открытой ссылке. Укажите, какие действия необходимо выполнить до передачи ссылки обучающимся.	Исключить либо обезличить избыточные персональные данные, ограничить доступ установленной группой пользователей, проверить права на просмотр и изменение и только после этого передать ссылку адресатам.	Правовое регулирование защиты информации	3																										

№ задания	Содержание задания	Ключ к ответу	Наименование темы РПД	Семестр																										
18	Прочитайте текст и выберите три правильных варианта ответа: Какие меры целесообразно применять для защищённого ведения электронного хранилища учебно-методической документации? А. ролевое разграничение доступа Б. журналирование операций просмотра и изменения В. резервное копирование с периодической проверкой восстановления Г. использование общей учётной записи подразделения Д. отключение обновлений программного обеспечения	А, Б, В	Организационные основы обеспечения информационной безопасности	3																										
19	Прочитайте текст вопроса и дополните фразу: Практическая проверка пригодности резервной копии путём восстановления данных в контролируемой среде называется _____.	тестовым восстановлением	Реагирование на инциденты информационной безопасности	3																										
20	Установите соответствие между объектом контроля информационной безопасности в электронной информационно-образовательной среде и способом его проверки: <table><tr><th>Объект контроля</th><th>Способ проверки</th></tr><tr><td>А. Актуальность прав доступа пользователей</td><td>1. Анализ журналов событий</td></tr><tr><td>Б. Целостность электронной документации</td><td>2. Сверка контрольных сумм или электронной подписи</td></tr><tr><td>В. Возможность восстановления данных</td><td>3. Проведение тестового восстановления</td></tr><tr><td>Г. События входа и изменения материалов</td><td>4. Периодический пересмотр ролевой матрицы</td></tr></table> Запишите выбранные цифры под соответствующими буквами в виде таблицы: <table><tr><th>А</th><th>Б</th><th>В</th><th>Г</th></tr><tr><td></td><td></td><td></td><td></td></tr></table>	Объект контроля	Способ проверки	А. Актуальность прав доступа пользователей	1. Анализ журналов событий	Б. Целостность электронной документации	2. Сверка контрольных сумм или электронной подписи	В. Возможность восстановления данных	3. Проведение тестового восстановления	Г. События входа и изменения материалов	4. Периодический пересмотр ролевой матрицы	А	Б	В	Г					<table><tr><th>А</th><th>Б</th><th>В</th><th>Г</th></tr><tr><td>4</td><td>2</td><td>3</td><td>1</td></tr></table>	А	Б	В	Г	4	2	3	1	Организационные основы обеспечения информационной безопасности	3
Объект контроля	Способ проверки																													
А. Актуальность прав доступа пользователей	1. Анализ журналов событий																													
Б. Целостность электронной документации	2. Сверка контрольных сумм или электронной подписи																													
В. Возможность восстановления данных	3. Проведение тестового восстановления																													
Г. События входа и изменения материалов	4. Периодический пересмотр ролевой матрицы																													
А	Б	В	Г																											
А	Б	В	Г																											
4	2	3	1																											

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций

Оценка достижения запланированных результатов обучения производится по итогам отдельных видов текущего контроля и промежуточной аттестации.

Шкала оценивания

«Зачтено» выставляется, если сформированность заявленных знаний, умений и навыков обучающегося составляет 60% и более и ни одна обязательная часть зачёта не оценена «неудовлетворительно».

«Отлично» (95–100%) выставляется, если обучающийся показал прочные систематизированные знания, самостоятельно решает практические задачи повышенной сложности, свободно использует справочную литературу, аргументирует решение и делает обоснованные выводы.

«Хорошо» (75–94%) выставляется, если обучающийся показал прочные знания, самостоятельно решает предусмотренные рабочей программой практические задачи, ориентируется в рекомендованной литературе и правильно оценивает полученные результаты, допуская отдельные неточности.

«Удовлетворительно» (60–74%) выставляется, если обучающийся знает основные положения учебного материала, знаком с рекомендованной литературой и способен получить правильное решение типовой практической задачи самостоятельно или с ограниченной помощью преподавателя.

«Неудовлетворительно» или «не зачтено» (менее 60%) выставляется, если выявлены существенные пробелы в знаниях основных положений учебного материала и обучающийся не может получить правильное решение типовой практической задачи с помощью преподавателя.

Ответы и решения обучающихся оцениваются по следующим общим критериям: распознавание проблемы; определение значимой информации; анализ проблемы; аргументированность; использование подходящей стратегии; правильность решения; обоснованность выводов; творческий подход; общая грамотность.

Текущий контроль

Результат тестирования определяется как доля набранных баллов от максимально возможного количества баллов. Положительным считается результат не менее 60%. Практическое или ситуационное задание оценивается с учётом правильности решения, полноты анализа, самостоятельности, аргументированности и качества выводов.

Промежуточная аттестация

Зачёт проводится по вопросам и практическим заданиям дисциплины. Теоретическая и практическая части оцениваются по традиционной шкале. При проведении зачёта могут учитываться положительные результаты текущего контроля за семестр.

Уровень освоения	Традиционная оценка	Оценка при зачёте
95–100%	5 — отлично	Зачтено
75–94%	4 — хорошо	Зачтено
60–74%	3 — удовлетворительно	Зачтено
Менее 60%	2 — неудовлетворительно	Не зачтено

Обучающиеся выполняют задания в сроки, установленные преподавателем. Оценка «зачтено» может выставляться при неполной сформированности отдельных компетенций, если их формирование продолжается на последующих этапах образовательной программы.