Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Байханов Исмаил Баутдинович
Должность: Ректор
Дата подписания: 10.07.2023 17:36:55
Уникальный программный ключ:
442c337cd125e1d014b2698e9a813e302097f64

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ЧЕЧЕНСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»

КАФЕДРА ЭКОЛОГИИ И БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ

Утверждаю:
Зав. каф.: Мицаев Ш.Ш.
_____
Протокол № 9 заседания
кафедры от 28.04.2023г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.08.02.06 «Информационная безопасность»

Направление подготовки
44.03.05 Педагогическое образование

Профили подготовки
«Биология» и «Безопасность жизнедеятельности»

Квалификация (степень выпускника):
бакалавр

Форма обучения: очная/заочная

Год набора: 2023 г.

Грозный, 2023 г.

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ / МОДУЛЯ

1.1. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Б.1.О.08.02.06 «Информационная безопасность» является обязательной для изучения студентами факультета естествознания и относится к дисциплинам базовой части Блока 1 учебного плана образовательной программы по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки «Биология и Безопасность жизнедеятельности») и изучается на 4 курсе (8 семестр).

Для освоения дисциплины обучающиеся используют знания и умения, сформированные в процессе изучения дисциплины Б1.0.08.02.01 «Концептуальные основы безопасности жизнедеятельности».

Приобретенные знания, умения и навыки применяются студентами при освоении дисциплин предметного модуля вариативной части учебных планов, в том числе, Б1.О.08.02.15 «Основы обороны государства и военной службы», а также необходимы для прохождения учебной практики в образовательных организациях.

Виды профессиональной деятельности: педагогическая, проектная

1.2. Цель освоения дисциплины (модуля)

. Целью освоения дисциплины является формирование общепрофессиональных и профессиональных компетенций в области информационной безопасности личности, организации, общества, государства и основных мерах по её обеспечению.

1.3. Планируемые результаты обучения по дисциплине (модулю)

Достижение цели освоения дисциплины (модуля) обеспечивается через формирование следующих компетенций – ОПК-1, ПК-1.

Таблица-1

Код и наименованиекомпетенции	Код и наименование индикатора достижения компетенции	Показатели достижения компетенции
ОПК-1. Способен осуществлять профессиональную деятельность в соответствии с нормативно-правовыми актами в сфере образования и нормами профессиональной этики. .	ОПК-1.1. Понимает и объясняет сущность приоритетных направлений развития образовательной системы Российской Федерации, законов и иных нормативно-правовых актов, регламентирующих образовательную деятельность в Российской Федерации, нормативных документов по вопросам обучения и воспитания детей и молодежи, федеральных государственных образовательных стандартов дошкольного, начального общего, основного общего, среднего общего, среднего	**Знать:** - нормативно-правовые акты по информационной безопасности в образовании; - роль и значение информационной безопасности в образовательном процессе. **Уметь:** - анализировать и практически использовать нормативно-правовые акты по информационной безопасности в образовании; - проводить оценку информации с точки зрения её соответствия нормативно-правовым актам. **Владеть:** - навыками работы с законодательными и иными нормативно-правовыми актами по информационной безопасности в системе

	профессионального образования, профессионального обучения, законодательства о правах ребенка, трудового законодательства. ОПК-1.2. Применяет в своей деятельности основные нормативно-правовые акты в сфере образования и нормы профессиональной этики, обеспечивает конфиденциальность сведений о субъектах образовательных отношений, полученных в процессе профессиональной деятельности	образования; - способами предупреждения информационных правонарушений
ПК-1. Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач.	ПК-1.1. Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета). ПК-1.2. Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО. ПК-1.3. Демонстрирует умение разрабатывать различные формы учебных занятий, применять методы, приемы и технологии обучения, в том числе информационные.	**Знать:** - основы государственной политики обеспечения информационной безопасности; - виды и источники опасностей и угроз в сфере информационных процессов и систем; - понятия информационной безопасности. **Уметь:** - защищаться от негативного информационного воздействия; - принимать решения на основе анализа и оценки информации. **Владеть:** - методами формирования у учащихся знаний и умений в области информационной безопасности; - методами и средствами обеспечения информационной безопасности.

1.4.Объем дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 академ. часа)

Таблица 2

Вид учебной работы	**Количество академ. часов**	
	Очно	**Заочно**
4.1. Объем контактной работы обучающихся с преподавателем	**40**	**14**
4.1.1. аудиторная работа	**40**	**14**
в том числе:		
лекции	**10**	**6**
практические занятия, семинары, в том числе практическая подготовка	**30**	**8**
лабораторные занятия		
4.1.2. внеаудиторная работа		
в том числе:		

индивидуальная работа обучающихся с преподавателем		
курсовое проектирование/работа		
групповые, индивидуальные консультации и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем		
4.2. Объем самостоятельной работы обучающихся	68	**90**
в том числе часов, выделенных на подготовку к экзамену		

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Таблица 3

2.1. Тематическое планирование дисциплины (модуля):

№	Наименование темы (раздела) дисциплины (модуля)	Общая трудоёмкость в акад.часах		Трудоёмкость по видам учебных занятий (в акад.часах							
				Лек.		Лаб.		Пр.		СР	
		Оч-но	Заоч-но	Оч-но	Заоч-но	Оч-но	Заоч-но	Оч-но	Заоч-но	Оч-но	Заоч-но
1	Информация и информационная безопасность в современном мире.	18	19	2	2			4	2	12	15
2	Обеспечение информационной безопасности РФ	20	17	2				6	2	12	15
3	Информационная безопасность человека	18	17	2	2			4		12	15
4	Криптографические способы защиты информации	20	17	2				6	2	12	15
5.	Антивирусная защита	18	17	2	2			4		12	15
6.	Сетевая безопасность	14	17	-				6	2	8	15
	Подготовка к зачету	*Х*	*Х*							*Х*	*Х*
ИТОГО		108		10	6			30	8	68	90

2.2.Содержание разделов дисциплины (модуля):

Таблица 4

№ п/п	**Наименование раздела дисциплины**	**Содержание дисциплины (дидактические единицы)** *(для педагогических профилей наполняется с учетом ФГОС основного общего и среднего общего образования*
1.	Информация и информационная безопасность в современном мире	Понятие информации и информационной безопасности. Окружающая среда как источник информации. Восприятие информации человеком. Роль информации в развитии общества. Понятие информационного общества. Образование в информационном обществе. (ОПК-1, ПК-1).
2.	Обеспечение информационной безопасности РФ	Информация как объект правового регулирования. Информационная безопасность РФ. Правовое обеспечение информационной безопасности РФ. Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 5 декабря 2016 г. № 646). Защита государственной тайны. Конфиденциальная информация и её защита. Защита интеллектуальной собственности. Служебная тайна. Коммерческая тайна. Профессиональная тайна. Информационная война. Психологическая война. (ОПК-1, ПК-1).

3.	Информационная безопасность человека	Концепция информационной безопасности детей. ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию". Неприкосновенность частной жизни граждан. Персональные данные и их защита. Технологии идентификации человека. Применение паролей в механизме аутентификации человека. Влияние средств массовой информации на человека. Влияние рекламы на человека. Цифровая зависимость. Правила кибергигиены. Деструктивные течения и деятельность в Интернете и их профилактика. Опасный и запрещенный контент в Интернете и его признаки. Правила цифрового поведения, необходимого для предотвращения рисков и угроз при использовании Интернета (кибербуллинга, вербовки в различные организации и группы). Принятие решений в повседневной жизни и в чрезвычайных ситуациях. Информационные и компьютерные преступления. (ОПК-1, ПК-1).
4.	Криптографические способы защиты информации	Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Простые числа. Квадратичное сравнение. Криптографическая система RSA. Криптосистемы. Простые криптосистемы. Шифрование методом замены (подстановки). Одноалфавитная подстановка. Многоалфавитная одноконтурная обыкновенная подстановка. Таблицы Вижинера. Многоалфавитная одноконтурная монофоническая подстановка. Многоалфавитная многоконтурная подстановка. Шифрование методом перестановки. Простая перестановка. Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard. Режимы работы алгоритма DES. Алгоритм шифрования данных IDEA. Общая схема алгоритма IDEA. (ОПК-1, ПК-1).
5.	Антивирусная защита	Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ. Основы работы антивирусных программ: Сигнатурный и эвристический анализ. Тестирование работы антивируса. Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы. (ОПК-1, ПК-1).
6.	Комплексная безопасность образовательного учреждения	Защита информации в локальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты. Уровень защиты рабочих станций и сетевых серверов. Уровень защиты почты. Уровень защиты шлюзов. Централизованное управление антивирусной защитой. Логическая сеть. Схема сбора статистики в системе антивирусной защиты. Управление ключами шифрования и безопасность сети. Целостность сообщения и установление подлинности сообщения. Криптографические хэш-функции. Цифровая подпись. Установление подлинности объекта. Управление ключами. Безопасность на прикладном уровне:

		PGP и S/MIME. Безопасность на транспортном уровне: SSL и TLS. Безопасность на сетевом уровне: IP SEC. Брандмауэры. Определение типов брандмауэров. Разработка конфигурации межсетевого экрана. Построение набора правил межсетевого экрана. Система обнаружения вторжений (IDS). Узловые IDS. Анализаторы журналов. Датчики признаков. Анализаторы системных вызовов. Анализаторы поведения приложений. Контроллеры целостности файлов. Сетевые IDS. Установка IDS. Определение целей применения IDS. Управление IDS. (ОПК-1, ПК-1).

3.УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ)

3.1. Учебно-методическое обеспечение самостоятельной работы обучающихся

Таблица 5

№ п/п	Наименование раздела дисциплины	Вид самостоятельной работы обучающихся
1.	Информация и информационная безопасность в современном мире.	Самостоятельное изучение материалов темы 1 «Информация и информационная безопасность в современном мире». Подготовка к семинарскому занятию (изучение вопросов, выносимых для обсуждения на семинарское занятие). Подготовка доклада на заданную преподавателем тему для представления и обсуждения на семинарском занятии. Подготовка глоссария по теме 1 «Информация и информационная безопасность в современном мире»
2.	Обеспечение информационной безопасности РФ	Самостоятельное изучение материала темы 2 «Обеспечение информационной безопасности РФ». Подготовка к семинарскому занятию (изучение вопросов, выносимых для обсуждения на семинарское занятие). Подготовка докладов на заданную преподавателем тему для представления и обсуждения на семинарском занятии. Подготовка и написание контрольной работы по теме 2 «Обеспечение информационной безопасности РФ»
3.	Информационная безопасность человека	Самостоятельное изучение материалов темы 3 «Информационная безопасность человека». Подготовка к семинарским занятиям (изучение вопросов, выносимых для обсуждения на семинарское занятие). Подготовка докладов и презентации по теме 3 для представления и обсуждения на семинарских занятиях. Подготовка и написание контрольной работы по теме 3 «Информационная безопасность человека»
4.	Криптографические способы защиты информации	Самостоятельное изучение материалов темы 4 «Криптографические способы защиты информации». Подготовка к семинарскому занятию (изучение вопросов, выносимых для обсуждения на семинарское занятие). Подготовка докладов и презентации по теме 4 для представления и обсуждения на семинарских занятиях. Подготовка и написание контрольной работы по теме 4 «Криптографические способы защиты информации»
5.	Антивирусная защита	Самостоятельное изучение материалов темы 5 «Антивирусная защита». Подготовка презентации к практическому занятию. Подготовка и написание контрольной работы по теме 5 «Антивирусная защита»
6.	Сетевая безопасность	Самостоятельное изучение материалов темы 6 «Сетевая безопасность». Подготовка к деловой игре (в соответствии с распределенными между студентами ролями и заданием преподавателя)

7.	Подготовка студентами рефератов по темам из предлагаемого перечня [1]

3.1 Учебно-методическое и информационное обеспечение программы дисциплины (модуля)

3.1.1. Основная и дополнительная литература

Таблица 6

Виды литературы	Автор, название литературы, город, издательство, год	Количество часов, обеспеченных указанной литературой	Количество обучающихся	Количество экземпляров в библиотеке университета	Режим доступа ЭБС/ электронный носитель (CD,DVD)	Обеспеченность обучающихся литературой,
1	2	3	4	5	6	7
	Основная литература					
1	*Зенков, А. В.* Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный //	40/68	25		https://urait.ru/bcode/497002	100%
2	*Суворова, Г. М.* Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный //	40/68	25		https://urait.ru/bcode/496741	100%
3	*Лунева, Е. В.* Информационное обеспечение молодежной политики : учебное пособие для вузов / Е. В. Лунева. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 163 с. — (Высшее образование). — ISBN 978-5-534-14106-1. — Текст : электронный //	40/68	25		https://urait.ru/bcode/496776	100%
	Дополнительная литература					
1	Бармин А.Н. Байраков И.А. Пучков М.Ю. Автаева Т.А. Иолин М.М. Мантаев Х.З.Локтионова Е.А. Безопасность жизнедеятельности. – Грозный:ЧГПИ, 2015.-344с	40/68	25	10		50%

2	*Чернова, Е. В.* Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный //	40/68	25		https://urait.ru/bcode/495922	100%
3	Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный //	40/68	25		https://urait.ru/bcode/498844	100%
4.	*Корабельников, С. М.* Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2022. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный //	40/68	25		https://urait.ru/bcode/496492	100%
5.	*Рассолов, И. М.* Информационное право : учебник и практикум для вузов / И. М. Рассолов. — 6-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 415 с. — (Высшее образование). — ISBN 978-5-534-14327-0. — Текст : электронный //	40/68	25		https://urait.ru/bcode/488767	100%

3.1.2. Интернет-ресурсы

. Цифровой образовательный ресурс IPR SMART (www.iprbookshop.ru)
2. Образовательная платформа «ЮРАЙТ» https://urait.ru/).
3. Электронно-библиотечная система «Лань» (https://e.lanbook.com/).
4. МЭБ (Межвузовская электронная библиотека) НГПУ. (https://icdlib.nspu.ru/).
5. НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА eLIBRARY.RU(https://www.elibrary.ru/)
6. СПС «КонсультантПлюс» (http://www.consultant.ru)

3.2. Материально-техническое обеспечение дисциплины

Для осуществления образовательного процесса по дисциплине необходима следующая материально-техническая база:

Таблица 7

Помещения для осуществления образовательного процесса	**Перечень основного оборудования (с указанием кол-ва посадочных мест)**	**Адрес (местоположение)**
Аудитория для проведения лекционных занятий		
Ауд. 5-11	Учебная мебель (столы ученические, стулья ученические) на 24 посадочных	ул. Субры Кишиевой, № 33

	мест, компьютер- 1 с выходом в интернет, проектор -1, стеллажей – 4, интерактивная доска	
Аудитории для проведения практических занятий, контроля успеваемости		
Ауд. 5-03	Учебная мебель (столы ученические, стулья ученические) на 24 посадочных мест,шкаф для учебников – 2, интерактивная доска -1, компьютер с выходом в интернет - 1, телевизор, DVD диски, графопроектор -1, наглядное пособие, скелет-1, микроскопы, микропрепараты, скелет – 1, набор позвонков – 1, модели органов, барельефные модели различных органов и систем органов, тонометр – 1, секундомер – 1, таблицы	ул. Субры Кишиевой, № 33
Помещения для самостоятельной работы		
Ауд.4-01	Учебная мебель (столы ученические, стулья ученические) на 24 посадочных мест, компьютер- 1 с выходом в интернет, проектор -1, стеллажей – 8, интерактивная доска	ул. СубрыКишиевой, № 33

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ / МОДУЛЯ

4.1. Характеристика оценочных средств

Контроль и оценка результатов освоения дисциплины / модуля осуществляется преподавателем в процессе проведения практических и лабораторных занятий, контрольных работ, а также выполнения обучающимися индивидуальных заданий, проектов. исследо

№ п/п	Наименование темы (раздела) с контролируемым содержанием	Код и наименование проверяемых компетенций	Оценочные средства	
			текущий контроль	промежуточная аттестация
1.	Информация и информационная безопасность в	ОПК-1, ПК-1	Глоссарий	
2.	Обеспечение информационной	ОПК-1, ПК-1	Тестирование	
3.	Информационная безопасность человека	ОПК-1, ПК-1	Презентация	
4.	Криптографические способы защиты	ОПК-1, ПК-1	Контрольная работа	Тестирование
5.	Антивирусная защита	ОПК-1, ПК-1	Доклады	
6.	Сетевая безопасность	ОПК-1, ПК-1	Деловая игра	Письменная работа

4.2. Оценочные средства для проведения текущего контроля успеваемости

4.2.1. Наименование оценочного средства: тест

Примерные вопросы для тестирования

1. Какой вид идентификации и аутентификации получил наибольшее распространение:
а) системы PKI
б) постоянные пароли
в) одноразовые пароли
2. Под какие системы распространение вирусов происходит наиболее динамично:
а) Windows
б) Mac OS
в) Android
3. Заключительным этапом построения системы защиты является:
а) сопровождение
б) планирование
в) анализ уязвимых мест
4. Какие угрозы безопасности информации являются преднамеренными:
а) ошибки персонала
б) открытие электронного письма, содержащего вирус
в) не авторизованный доступ
5. Какой подход к обеспечению безопасности имеет место:
а) теоретический
б) комплексный
в) логический
6. Системой криптографической защиты информации является:
а) BFox Pro
б) CAudit Pro
в) Крипто Про
7. Какие вирусы активизируются в самом начале работы с операционной системой:
а) загрузочные вирусы
б) троянцы
в) черви
8. Stuxnet – это:
а) троянская программа
б) макровирус
в) промышленный вирус
9. Таргетированная атака – это:
а) атака на сетевое оборудование
б) атака на компьютерную систему крупного предприятия +
в) атака на конкретный компьютер пользователя
10. Под информационной безопасностью понимается:
а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре
б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
в) нет верного ответа

Критерии оценивания результатов тестирования

Таблица 9

Уровень освоения	***Критерии***	***Баллы***
Максимальный уровень	Выполнены правильно все задания теста (тест зачтен)	2
Средний уровень	Выполнено правильно больше половины заданий (тест зачтен)	1
Минимальный уровень	Выполнено правильно меньше половины заданий (тест не зачтен)	0

4.2.2. Наименование оценочного средства: Реферат и презентация

Примерная тематика рефератов.

1.Информация - фактор существования и развития общества.
2.Основные формы проявления информации, её свойства как объекта безопасности.
3.Понятие безопасности и её составляющие. Безопасность информации.
4.Обеспечение информационной безопасности: содержание и структура понятия.
5.Национальные интересы в информационной сфере.
6.Источники и содержание угроз в информационной сфере.
7.Соотношение понятий «информационная безопасность» и «национальная безопасность»
8.Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности.
9.Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.
10.Система обеспечения информационной безопасности. Обеспечение информационной безопасности Российской Федерации.

Критерии оценивания результатов выполнения реферата

Таблица 10

Уровень освоения	***Критерии***	***Баллы***
Максимальный уровень	Задание выполнено правильно: выводы аргументированы, основаны на знании материала, владении категориальным аппаратом	*3*
Средний уровень	Задание выполнено в целом правильно: но допущены ошибки в аргументации, обнаружено поверхностное владение терминологическим аппаратом	*2*
Минимальный уровень	Задание выполнено с ошибками в формулировке тезисов и аргументации, обнаружено слабое владение терминологическим аппаратом	*1*
Минимальный уровень не достигнут	Задание не выполнено или выполнено с серьёзными ошибками	*0*

Темы презентаций:

1.Понятие информационной войны. Проблемы информационной войны.
2.Информационное оружие и его классификация.
3.Цели информационной войны, её составные части и средства её ведения. Объекты воздействия в информационной войне.
4.Уровни ведения информационной войны. Информационные операции. Психологические операции. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети.
5.Основные положения государственной информационной политики Российской Федерации. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.
6.Виды защищаемой информации в сфере государственного и муниципального управления.
7.Обеспечение информационной безопасности организации.
8.Управление и защита информации в информационно-телекоммуникационных сетях.
9.Характеристика эффективных стандартов по безопасности. Требования к полноте эффективных стандартов по безопасности.
10.Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере.

Критерии и шкалы оценивания доклада/сообщения (в форме презентации):

Таблица 11

Уровень освоения	***Критерии***	***Баллы***
Максимальный уровень	– продемонстрировано умение выступать перед аудиторией; – содержание выступления даёт полную информацию о теме; – продемонстрировано умение выделять ключевые идеи; – умение самостоятельно делать выводы, использовать актуальную	3

	научную литературу; – высокая степень информативности, компактность слайдов	
Средний уровень	– продемонстрирована общая ориентация в материале; – достаточно полная информация о теме; – продемонстрировано умение выделять ключевые идеи, но нет самостоятельных выводов; – невысокая степень информативности слайдов; – ошибки в структуре доклада; – недостаточное использование научной литературы	2
Минимальный уровень	– продемонстрирована слабая (с фактическими ошибками) ориентация в материале; – ошибки в структуре доклада; – научная литература не привлечена	1
Минимальный уровень не достигнут	– выступление не содержит достаточной информации по теме; – продемонстрировано неумение выделять ключевые идеи; – неумение самостоятельно делать выводы, использовать актуальную научную литературу.	0

4.2.3. Наименование оценочного средства: *контрольная работа*

Примерная тематика контрольных работ.

1. Покажите на примерах значение информации в развитии общества
2. Что такое информационное общество?
3. Что такое информационное неравенство людей в информационной среде? Каковы его причины?
4. Покажите на примерах значение информационной безопасности в обеспечении национальной безопасности государства
5. Какие нормативно-правовые акты обеспечивают информационную безопасность на территории РФ?
6. Покажите на примерах значение информации в условиях войны
7. Каковы цели и задачи информационной войны в мирное и в военное время?
8. Какие методы биометрической идентификации человека вам известны? Насколько они могут быть точны?
9. Почему защита информации о частной жизни граждан стала проблемой в наше время?
10. Почему в обеспечении защиты информации человек является «самым слабым звеном»?

Критерии оценивания результатов контрольной работы

Таблица 12

Балл (интервал баллов)	**Уровень освоения**	**Критерии оценивания уровня освоения компетенций***
10	Максимальный уровень (интервал)	Контрольная работа оформлена в соответствии с предъявляемыми требованиями, содержит 1-2 мелких ошибки; ответы студента правильные, четкие, содержат 1-2 неточности
[6-8]	Средний уровень (интервал)	Контрольная работа содержит одну принципиальную или 3 или более недочетов; ответы студента правильные, но их формулирование затруднено и требует наводящих вопросов от преподавателя
[3-5]	Минимальный уровень (интервал)	Контрольная работа оформлена в соответствии с предъявляемыми требованиями, неполное раскрытие темы в теоретической части и/или в практической части контрольной работы; ответы студенты формально правильны, но поверхностны, плохо сформулированы, содержат более одной принципиальной ошибки
Менее 3	Минимальный уровень (интервал) не достигнут.	Контрольная работа содержит более одной принципиальной ошибки моделей решения задачи; контрольная работа оформлена не в соответствии с предъявляемыми требованиями; ответы студента путанные, нечеткие, содержат множество ошибок, или ответов нет совсем; несоответствие варианту.

4.2.4. Наименование оценочного средства: практико-ориентированное задание

1. Бывший сотрудник химико-биологического предприятия вместе со своим приятелем-программистом скопировали конфиденциальную информацию: состав ингредиентов, их пропорции и формулу нового лекарственного препарата – с целью продажи этой информации конкурирующей организации.

2. П. П. Андреев, сотрудник одного из филиалов ИТ-банка, внедрил в компьютерную банковскую систему вирус, уничтожающий исполняемые файлы (файлы с расширением *.exe). В результате внедрения этого вируса было уничтожено 40 % банковских программных приложений, что принесло банку материальный ущерб в размере 750 000 рублей.

3. Будет ли удовлетворен иск компании «Интермедиа» о привлечении к уголовной ответственности гражданина Р. И. Сизова и выплате им фирме денежной компенсации, если он внедрил в компьютерную сеть компании программу, действие которой заключается в уничтожении исполняемых файлов в какой-либо компьютерной сети? Функционирование данной программы принесло убытки различным организациям на общую сумму 670 ООО рублей.

Критерии оценивания результатов выполнения практико-ориентированного задания

4. Таблица 13

Уровень освоения	Критерии	Баллы
Максимальный уровень	Задание выполнено правильно: выводы аргументированы, основаны на знании материала, владении категориальным аппаратом	5
Средний уровень	Задание выполнено в целом правильно: но допущены ошибки в аргументации, обнаружено поверхностное владение терминологическим аппаратом	3
Минимальный уровень	Задание выполнено с ошибками в формулировке тезисов и аргументации, обнаружено слабое владение терминологическим аппаратом	2
Минимальный уровень не достигнут	Задание не выполнено или выполнено с серьёзными ошибками	0

а. Оценочные средства для промежуточной аттестации

Представлено в Приложении 1.

Автор(ы) рабочей программы дисциплины (модуля):

Профессор, доктор сельскохозяйственных наук _____ Оказова З.П.
(подпись)

СОГЛАСОВАНО:
Директор библиотеки _____ Арсагириева Т.А.
(подпись)

Приложение 1.

Приложение 1

Оценочные средства для проведения промежуточной аттестации по дисциплине

«Информационная безопасность»

Направление подготовки

44.03.05 Педагогическое образование

(с двумя профилями подготовки)

Профили подготовки «Биология» и «Безопасность жизнедеятельности

Форма обучения: очная и заочная

Год приема: 2023

4.3.1.Характеристика оценочной процедуры:

Семестр - 8

Форма аттестации – зачет с оценкой

4.3.2.Оценочные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

Вопросы для промежуточной аттестации по дисциплине:

1. Понятие об информации. Роль информации в развитии общества.
2. Понятия информационной безопасности. Цели и задачи информационной безопасности.
3. Виды и источники опасностей и угроз в сфере информационных процессов и систем.
4. Информационная безопасность в системе национальной безопасности государства.
5. Государственная система защиты информации.
6. Информационная безопасность РФ в условиях глобализации.
7. Российское законодательство в области информационной безопасности.
8. Правовая защита интеллектуальной собственности.
9. Международное право в сфере защиты информации.
10. Информационно-психологические операции в войнах и вооруженных конфликтах прошлого.
11. Информационное противоборство в современной войне.
12. Информационная война и ее особенности.
13. Цели и задачи информационной войны в мирное и военное время.
14. Виды информационного оружия и его особенности.
15. Методы и средства современной информационной войны.
16. Глобальная информатизация общества и ее последствия.
17. Информационное общество
18. Информационное неравенство людей в информационной среде.
19. Проблема защиты информации о частной жизни граждан.
20. Информационные технологии и здоровье человека.
21. Информационный стресс. Компьютерная зависимость.
22. Информационное воздействие окружающей среды на человека как фактор деструктивного и агрессивного поведения.
23. Влияние средств массовой информации на человека.
24. Восприятие рекламной информации и формирование поведения потребителей.
25. Способы защиты человека от негативного влияния информации.
26. Цифровая зависимость.
27. Правила кибергигиены.
28. Информационная преступность (компьютерные преступления).
29. Методы и средства защиты обычной и электронной информации.

30. Информационная безопасность в сети Internet.
31. Информационная изоляция человека в ЧС.
32. Возникновение и распространение слухов в ЧС.
33. Сбор, анализ и оценка информации для принятия решения в ЧС.
34. Этапы принятия и реализации решения.
35. Особенности индивидуального принятия решений в ЧС.
36. Особенности группового принятия решений в ЧС.

4.3.3.Критерии и шкала оценивания устного ответа обучающегося на экзамене (зачете)

Максимальное количество баллов на экзамене (зачете) – 30, из них:
1. Ответ на первый вопрос, содержащийся в билете – 15 баллов.
2. Ответ на второй вопрос, содержащийся в билете – 15 баллов.

Таблица 13

№ п/п	Характеристика ответа	Баллы
1.	Ответ на поставленный вопрос правильный, полный (исчерпывающий) с пояснениями и примерами	13-15
2.	Ответ на поставленный вопрос правильный и полный, в формулировках имеют место неточности, не приведены пояснения и (или) примеры	10-12
3	Ответ на поставленный вопрос не полный, в формулировках имеют место ошибки	7-9
4.	Ответ на поставленный вопрос не полный, в формулировках имеют место существенные ошибки и неоднозначность	6 и менее

Расчет итоговой рейтинговой оценки

Таблица 14

До 50 баллов включительно	«неудовлетворительно»
От 51 до 70 баллов	«удовлетворительно»
От 71 до 85 баллов	«хорошо»
От 86 до 100 баллов	«отлично»

4.3.4.Уровни сформированности компетенций по итогам освоения дисциплины (модуля)

Код и наименование компетенции и для ОП ВО, индикаторы достижения компетенции (ИДК)	Шкала оценивания			
	«отлично»	«хорошо»	«удовлетворительно»	«неудовлетворительно»
Компетенция (шифр и индикаторы) ОПК-1, ОПК-1.1, ОПК-1.2.ПК-1, ПК-1.1, ПК-1.2,	выставляется обучающемуся, который в процессе изучения дисциплины и по результатам	выставляется обучающемуся, который в процессе изучения дисциплины и по результатам	выставляется обучающемуся, который в процессе изучения дисциплины и по результатам	выставляется обучающемуся, который в процессе изучения дисциплины и по результатам

ПК-1.3.	промежуточной аттестации обнаружил системные знания по всем разделам программы дисциплины, продемонстрировал способность к их самостоятельному пополнению, в том числе в рамках учебно-исследовательской и научно-исследовательской деятельности	промежуточной аттестации обнаружил системные знания по всем разделам программы дисциплины, продемонстрировал способность к их самостоятельному пополнению в процессе учебной деятельности, за исключением учебно-исследовательской и научно-исследовательской деятельности	промежуточной аттестации обнаружил фрагментарные знания по всем разделам программы дисциплины	промежуточной аттестации обнаружил отсутствие знаний по основным разделам программы дисциплины;
	представил результаты выполнения всех заданий для самостоятельной работы полностью и качественно, на творческом уровне, выразил личностную значимость деятельности	представил результаты выполнения всех заданий для самостоятельной работы, но на репродуктивном уровне	представил результаты выполнения более 70 % всех заданий для самостоятельной работы	выполнил менее 50% предусмотренных рабочей программой дисциплины задания для самостоятельной работы
	при устном ответе высказал самостоятельное суждение на основе исследования теоретических источников, логично и аргументированно изложил материал, связал теорию с	при устном ответе высказал самостоятельное суждение на основе исследования теоретических источников, логично и аргументированно изложил материал,	при устном ответе высказал репродуктивное суждение по предлагаемому вопросу из теоретических источников, не смог связать теорию с практикой (не привел примеров), в	при устном ответе допустил фактические ошибки в использовании научной терминологии и изложении учебного содержания, сделал ложные выводы

	практикой посредством иллюстрирующих примеров, свободно ответил на дополнительные вопросы	испытывал затруднение связать теорию с практикой посредством иллюстрирующих примеров, ответить на дополнительные вопросы	ответе на дополнительные вопросы испытывал затруднение	

4.3.5.Рейтинг-план изучения дисциплины

Таблица 16

I	БАЗОВАЯ ЧАСТЬ РЕЙТИНГОВОЙ СИСТЕМЫ		
Виды контроля	**Контрольные мероприятия**	**Мин. кол-во баллов на занятиях**	**Макс. кол-во баллов на занятиях**
Текущий контроль № 1	Тема1. Информация и информационная безопасность в современном мире Тема 2. Обеспечение информационной безопасности РФ	0	10
Текущий контроль № 2	Тема3. Информационная безопасность человека	0	8
Рубежный контроль: контрольная работа №1 (Темы 1-3)		0	10
Текущий контроль №3	Тема 4. Криптографические способы защиты Тема 5. Антивирусная защита	0	10
Текущий контроль №4	Тема 6. Сетевая безопасность	0	10
Рубежный контроль: контрольная работа №2 (Темы 4-6)		0	10
Допуск к промежуточной аттестации		**Мин 36**	
II	**ДОПОЛНИТЕЛЬНАЯ ЧАСТЬ РЕЙТИНГОВОЙ СИСТЕМЫ**	**Мин.**	**Макс.**
1	**Поощрительные баллы**	**0-10**	**10**
	Подготовка доклада с презентацией по дисциплине	0-1	1
	Посещаемость лекций (100%)	0-2	2
	Участие в работе круглого стола, студенческой конференции	0-2	2
	Соц.-личностный рейтинг	0-3	3
	Участие в общественной, культурно-массовой и спортивной работе	0-2	2

2	**Штрафные баллы**		**0-3**	**3**
	Пропуск учебных лекций	за пропуск лекции снимается балльная стоимость лекции (2:8=0,25)	0,25 x N (N – количество пропущенных лекций	
	Несвоевременное выполнение контрольной (аттестационной) работы №1	минус 5% от максимального балла	- 0,5	
	Несвоевременное выполнение контрольной (аттестационной) работы №2	минус 5% от максимального балла	- 0,5	
III	**ИТОГОВЫЙ КОНТРОЛЬ**		**0-30**	**30**
Форма итогового контроля:	Зачет с оценкой		0-30	**30**
Итого баллов за семестр			0-100	

Приложение 2.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ / МОДУЛЯ

«Информационная безопасность»

(наименование дисциплины / модуля)

Направление подготовки __44.03.05 Педагогическое образование
Профили »Биология» и «Безопасность жизнедеятельности»
(год набора __2023, форма обучения очная/заочная)
на 2023/ 2024учебный год

В рабочую программу дисциплины / модуля вносятся следующие изменения:

№ n/n	Раздел рабочей программы (пункт)	Краткая характеристика вносимых изменений	Основание для внесения изменений