МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ЧЕЧЕНСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ ФИЗИКИ, МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
КАФЕДРА ПРИКЛАДНОЙ ИНФОРМАТИКИ

Утверждаю:
Зав.каф.: Юшаев С-Э.С-М.
Протокол № 8 заседания
кафедры от 24 апреля 2023

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Основы информационной безопасности
(наименование дисциплины (модуля))

направление подготовки:
38.03.04- Государственное и муниципальное управление

Профиль «Государственное и муниципальное управление»
Квалификация
Бакалавр

Форма обучения
Очная, очно-заочная

Год набора 2023

Грозный, 2023

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ / МОДУЛЯ

Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Информационная безопасность и защита информации» Б1.П.02.02 относится к дисциплинам по выбору, части, формируемая участниками образовательных отношений. Дисциплина (модуль) изучается на 3 курсе в 5 семестре.

Цель освоения дисциплины (модуля)

Целью: является формирование у студентов принципов информационной безопасности государства, подходов к анализу его информационной инфраструктуры, принципов организации, проектирования и анализа систем защиты информации, освоения основ их комплексного построения на различных уровнях защиты и особенностей степеней защиты для государственного и частного назначения.

Планируемые результаты обучения по дисциплине (модулю)

Достижение цели освоения дисциплины (модуля) обеспечивается через формирование следующих компетенций *(с указанием шифра компетенции):*

Таблица 1

Код и наименование компетенции	Код и наименование индикатора достижения компетенций, которые формирует дисциплина (модуль)	Планируемые результаты обучения
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и Библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	ОПК-3.1. Применяет принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с использованием информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ОПК-3.2. Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. ОПК-3.3. Имеет опыт подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	ОПК-3-З1 основы информационной безопасности и защиты информации; ОПК-3-З2 главные требования к организации эффективного функционирования системы ИБ ОПК-3-З3 методы анализа информационных рисков и структур нарушения ИБ ОПК-3-З4 методы оценки уровня безопасности корпоративной информационной системы ОПК-3-З5 современные информационные технологии и программные средства при решении задач профессиональной деятельности ОПК-3-З6 описание прикладных процессов и информационного обеспечения решения прикладных задач ОПК-3-У1 выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации ОПК-3-У2 пользоваться современной научно-технической информацией по исследуемым проблемам и задачам

Объем дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет 108ч / 3з.е. (академ. часов)

Таблица 2

Вид учебной работы	Количество академ. часов	
	Очно	Очно-заочно
4.1. Объем контактной работы обучающихся с преподавателем	**108**	108
4.1.1. аудиторная работа	**32**	32
в том числе:		
Лекции	16	16
практические занятия, семинары, в том числе практическая подготовка	16	16
лабораторные занятия		
4.1.2. внеаудиторная работа	76	76
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		
в том числе часов, выделенных на подготовку к экзамену		

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Тематическое планирование дисциплины (модуля):

Таблица 3

№ п/п	Наименование темы (раздела) дисциплины (модуля)	Общая трудоѐмкость в акад.часах		Лекции		Практ. занятия		Лаб. занятия		Сам. работа	
		Очно	Очно-заочно	Очно	Очно-заочно	Очно	Очно-заочно	Очно	Очно-заочно	Очно	Очно-заочно
1.	**Раздел 1.Введение в информационную безопасность.** Основные составляющие информационной безопасности. Понятие «информационная безопасность». Проблема информационной безопасности общества.	10	10	5	5	5	5			25	25
2.	**Раздел 2. Уровни компьютерной безопасности.** Угрозы информационной безопасности Основные определения и критерии классификации	10	10	5	5	5	5			25	25

	угроз. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности. Вредоносное программное обеспечение. Вирусы как угроза информационной безопасности. Классификация компьютерных вирусов. Характеристики «вирусоподобных» программ. Антивирусные программы. Профилактика компьютерных вирусов и обнаружение неизвестного вируса.										
3.	**Раздел 3. Правовые основы информационной безопасности.** Основы международного законодательства в области информационной безопасности и защиты информации. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Ответственность за нарушения в сфере информационной безопасности. Стандарты и спецификации в области информационной	12	12	6	6	6	6			26	26

	безопасности. Административный уровень обеспечения информационной безопасности: цели, задачи, содержание, разработка политики информационной безопасности. Управление рисками. Процедурный уровень информационной безопасности. Основные программно-технические меры.										
	Подготовка к экзамену (зачету)										
	Итого:	108	108	16	16	16	16			76	76

Содержание разделов дисциплины (модуля):

Таблица 4

№ п/п	Наименование темы (раздела) дисциплины	Содержание дисциплины (дидактические единицы) *(для педагогических профилей наполняется с учетом ФГОС основного общего и среднего общего образования)*
1.	**Раздел 1.Введение в информационную безопасность.**	Основные составляющие информационной безопасности. Понятие «информационная безопасность». Проблема информационной безопасности общества.
2.	**Раздел 2. Уровни компьютерной безопасности.**	Угрозы информационной безопасности Основные определения и критерии классификации угроз. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности. Вредоносное программное обеспечение. Вирусы как угроза информационной безопасности. Классификация компьютерных вирусов. Характеристики «вирусоподобных» программ. Антивирусные программы. Профилактика компьютерных вирусов и обнаружение неизвестного вируса.
3.	**Раздел 3. Правовые основы информационной безопасности.**	Основы международного законодательства в области информационной безопасности и защиты информации. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Ответственность за нарушения в сфере информационной безопасности. Стандарты и спецификации в области информационной безопасности. Административный уровень обеспечения информационной безопасности: цели, задачи, содержание, разработка политики информационной

		безопасности. Управление рисками. Процедурный уровень информационной безопасности. Основные программно-технические меры.

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ)

Учебно-методическое обеспечение самостоятельной работы обучающихся

Таблица 5

№ п/п	Наименование раздела дисциплины	Вид самостоятельной работы обучающихся
1.	**Раздел 1.Введение в информационную безопасность.**	Устный опрос Выполнение практико-ориентированных заданий
2.	**Раздел 2. Уровни компьютерной безопасности.**	Устный опрос. Выполнение практико-ориентированных заданий
3.	**Раздел 3. Правовые основы информационной безопасности.**	Устный опрос Выполнение практико-ориентированных заданий

Учебно-методическое и информационное обеспечение программы дисциплины (модуля)

Основная и дополнительная литература

Таблица 6

Виды литературы	Автор, название литературы, город, издательство, год	Количество часов, обеспеченных указанной литературой Аудит./самост.	Количество обучающихся	Количество экземпляров в библиотеке университета	Режим доступа ЭБС/ электронный носитель (CD,DVD)	Обеспеченность обучающихся литературой, (5гр./4гр.)х100%))
1	2	3	4	5	6	7
	Основная литература					

1	Нестеров, С. А. Основы информационной безопасности: учебник для вузов / С. А. Нестеров. - Санкт-Петербург: Лань, 2021. - 324 с. - ISBN 978-5-8114-6738-9.- Текст: электронный //	108	25		Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837	100%
2	Никифоров, С. Н. Методы защиты информации. Шифрование данных: учебное пособие / С. Н. Никифоров. - 2-е изд., стер. - Санкт-Петербург: Лань, 2022. - 160 с. - ISBN 978-5-8114-4042-9. - Текст: электронный//	108	25		Лань: электронно-библиотечная система. - URL: https://e.lanbook.com/book/206285	100%
3	Петренко, В. И. Защита персональных данных в информационных системах. Практикум: учебное пособие для вузов / В. И. Петренко, И. В. Мандрица. - 3-е изд., стер. - Санкт-Петербург: Лань, 2021. - 108 с. - ISBN 978-5-8114-8370-9. - Текст: электронный //	108	25		Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/175506	100%
4	Прохорова, О. В. Информационная безопасность и защита информации: учебник для вузов / О. В. Прохорова. - 4-е изд., стер. - Санкт-Петербург: Лань, 2022. - 124 с. - ISBN 978-5-507-44201-0. - Текст: электронный//	108	25		Лань: электронно-библиотечная система. - URL: https://e.lanbook.com/book/217445	100%
	Дополнительная литература					

1	Прохорова, О. В. Информационная безопасность и защита информации: учебник для вузов / О. В. Прохорова. - 3-е изд., стер. - Санкт-Петербург: Лань, 2021. - 124 с. - ISBN 978-5-8114-7970-2.- Текст: электронный//	108	25		Лань: электронно-библиотечная система. - URL: https://e.lanbook.com/book/169817	100%
2	Титова, Л. Н. Информационная безопасность и защита информации: учебно-методическое пособие / Л. Н. Титова. - Уфа: БГПУ имени М. Акмуллы, 2013. - 108 с.- Текст: электронный //	108	25		Лань: электронно-библиотечная система. - URL: https://e.lanbook.com/book/56704	100%
3	Фомин, Д. В. Информационная безопасность: учебник / Д. В. Фомин. - Москва: Ай Пи Ар Медиа, 2022. - 222 с. - ISBN 978-5-4497-1548-7. - Текст: электронный //	108	25		Цифровой образовательный ресурс IPR SMART: [сайт]. - URL: https://www.iprbookshop.ru/118876.html	100%

Интернет-ресурсы

1. eLIBRARY.RU [Электронный ресурс]: научная электронная библиотека. – Режим доступа: http://elibrary.ru/defaultx.asp, свободный.
2. EqWorld. TheWorldofMathematicalEguations [Электронный ресурс]: Международный научно-образовательный сайт. – Режим доступа: http://eqworld.impnet.ru, свободный.
3. Prezentacya.ru [Электронный ресурс]: образовательный портал. – Режим доступа: http://prezentacya.ru/, свободный.
4. Единая коллекция цифровых образовательных ресурсов [Электронный ресурс]: федеральный портал. – Режим доступа: http://school-collection.edu.ru/, свободный.
5. КиберЛенинка [Электронный ресурс]: научная электронная библиотека. – Режим доступа: http://cyberleninka.ru, свободный

6. Российский общеобразовательный портал [Электронный ресурс]: образовательный портал. – Режим доступа: http://www.school.edu.ru/, свободный.

7. Российское образование [Электронный ресурс]: федеральный портал. – Режим доступа: http://www.edu.ru/, свободный.

8. Федеральный центр информационно-образовательных ресурсов [Электронный ресурс]: Единое окно доступа к образовательным ресурсам. – Режим доступа: http://fcior.edu.ru, свободный.

9. Цифровая техника в радиосвязи [Электронный ресурс]: сайт. – Режим доступа: http://digteh.ru, свободный.

Материально-техническое обеспечение дисциплины

При необходимости для проведения занятий используется аудитория, оборудованная компьютером с доступом к сети Интернет с установленным на нем необходимым программным обеспечением и браузером, проектор (интерактивная доска) для демонстрации презентаций и мультимедийного материала. В соответствии с содержанием практических (лабораторных) занятий при их проведении используется аудитория, рабочие места обучающихся в которой оснащены компьютерной техникой, имеют широкополосный доступ в сеть Интернет и программное обеспечение, соответствующее решаемым задачам.

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		
5-04	• стандартно оборудованные лекционные аудитории с видеопроектором и настенным экраном • персональный компьютер или ноутбук под управлением MS Windows XP Pro, MS Windows 7, пакет Microsoft Office с возможностью подключения проектора 40 посадочных мест	Чеченская Республика г. Грозный, ул. Ляпидевского 9. Учебный корпус №3
Аудитории для проведения практических занятий, контроля успеваемости		
3-18	• класс персональных компьютеров под управлением MS Windows XP Pro (Win7), включенных в корпоративную сеть университета 25 посадочных мест	Чеченская Республика г. Грозный, ул. Ляпидевского 9. Учебный корпус №3
Помещения для самостоятельной работы		
Компьютерный центр	Компьютерная мебель на 52 посадочных мест, 52 компьютеров с выходом в Интернет, системный блок (52 шт.), клавиатура (52 штук), мышь (52 штук)	Чеченская Республика г. Грозный, ул. СубрыКишиевой, № 33

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ / МОДУЛЯ

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, исследований и т.д.

Таблица 8

№ п/п	Наименование темы (раздела) с контролируемым содержанием	Код и наименование проверяемых компетенций	Оценочные средства	
			текущий контроль	промежуточная аттестация
1.	**Раздел 1.Введение в информационную безопасность.** Основные составляющие информационной безопасности. Понятие «информационная безопасность». Проблема информационной безопасности общества.	ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и Библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	тестирование, практико-ориентированное задание, доклад	контрольная работа

2.	**Раздел 2. Уровни компьютерной безопасности.** Угрозы информационной безопасности Основные определения и критерии классификации угроз. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности. Вредоносное программное обеспечение. Вирусы как угроза информационной безопасности. Классификация компьютерных вирусов. Характеристики «вирусоподобных»	ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и Библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	тестирование, практико-ориентированное задание, доклад	контрольная работа

	программ. Антивирусные программы. Профилактика компьютерных вирусов и обнаружение неизвестного вируса.			
3.	**Раздел 3. Правовые основы информационной безопасности.** Основы международного законодательства в области информационной безопасности и защиты информации. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Ответственность за нарушения в сфере информационной безопасности. Стандарты и спецификации в области информационной безопасности. Административный уровень обеспечения информационной безопасности: цели, задачи, содержание, разработка политики информационной безопасности. Управление рисками. Процедурный уровень информационной безопасности. Основные программно-технические меры.	ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и Библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	тестирование, практико-ориентированное задание, доклад	контрольная работа

Оценочные средства для проведения текущего контроля успеваемости

Наименование оценочного средства: *тест*

Методические материалы: приводятся вопросы и/или типовые задания, критерии оценки.

Примерные вопросы для тестирования

Правильный вариант ответа отмечен знаком +

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

тест 10) Принципом информационной безопасности является принцип недопущения:

+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

- Компьютерный сбой
+ Логические закладки («мины»)
- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
+ Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

- Электронно-цифровой преобразователь
+ Электронно-цифровая подпись
- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелицензионного ПО
+ Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
+ Сбой (отказ) оборудования, нелегальное копирование данных

тест_20) Наиболее распространены средства воздействия на сеть офиса:

- Слабый трафик, информационный обман, вирусы в интернет
+ Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:

+ Потерей данных в системе
- Изменением формы информации

- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

+ Целостность
- Доступность
- Актуальность

23) Угроза информационной системе (компьютерной сети) – это:

+ Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

- Регламентированной
- Правовой
+ Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

+ Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

+ Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

+ Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
+ Аудит, анализ уязвимостей, риск-ситуаций

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*

Наименование оценочного средства: практико-ориентированное задание

Методические материалы: приводятся вопросы и/или типовые задания, критерии оценки.

Примерные практико-ориентированные задания

1. Законодательство РФ в области информационной безопасности
2. Изучение положений о государственном лицензировании деятельности в области защиты информации

3. Система сертификации средств криптографической защиты информации
4. Изучения положения о сертификации средств вычислительной техники и связи
5. Изучение положения по аттестации объектов информатизации по требованиям безопасности информации
6. Изучение особенностей аттестации помещений по требованиям безопасности информации

Критерии оценивания результатов выполнения практико-ориентированного задания

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 серьѐзными ошибками*	*0*

Наименование оценочного средства: ***доклад/сообщение***

Методические материалы: приводятся вопросы и/или типовые задания, критерии оценки

Темы докладов:

1. Информация - фактор существования и развития общества. Основные формы проявления информации, еѐ свойства как объекта безопасности.
2. Понятие безопасности и еѐ составляющие. Безопасность информации.
3. Обеспечение информационной безопасности: содержание и структура понятия.
4. Национальные интересы в информационной сфере.
5. Источники и содержание угроз в информационной сфере.
6. Соотношение понятий «информационная безопасность» и «национальная безопасность»
7. Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности.
8. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.
9. Система обеспечения информационной безопасности.
10. Обеспечение информационной безопасности Российской Федерации.
11. Понятие информационной войны. Проблемы информационной войны.
12. Информационное оружие и его классификация.
13. Цели информационной войны, еѐ составные части и средства еѐ ведения. Объекты воздействия в информационной войне.

14. Уровни ведения информационной войны. Информационные операции. Психологические операции.

15. Уровни ведения информационной войны. Оперативнаямаскировка. Радиоэлектронная борьба. Воздействие на сети.

16. Основные положения государственной информационной политики Российской Федерации.

17. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.

18. Виды защищаемой информации в сфере государственного и муниципального управления.

19. Обеспечение информационной безопасности организации.

20. Характеристика эффективных стандартов по безопасности.

21. Требования к полноте эффективных стандартов по безопасности.

22. Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере.

23. Информация - фактор существования и развития общества.

24. Обеспечение информационной безопасности: содержание и структура понятия.

25. Система обеспечения информационной безопасности. Обеспечение информационной безопасности организации.

26. Обеспечение информационной безопасности Российской Федерации.

27. Международная нормативная база обеспечения безопасности. Федеральная нормативная база обеспечения безопасности

28. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.

29. Административный уровень обеспечения информационной безопасности.

30. Организационные структуры системы обеспечения информационной безопасности предприятия (организации).

31. Корпоративная нормативная база по защите информации.

32. Основные организационные мероприятия по обеспечению информационной безопасности организации (предприятия).

33. Основные организационные мероприятия по обеспечению информационной безопасности организации (предприятия).

34. Нормативно-методические документы по обеспечению безопасности информации.

35. Управление персоналом на предприятиях и в организациях.

36. Подбор и расстановка кадров.

37. Мотивация добросовестной деятельности сотрудников.

38. Порядок проведения служебных расследований.

39. Организация подготовки кадров и повышения квалификации в области обеспечения информационной безопасности.

40. Категорирование объектов информатизации.

41. Общие положения по категорированию объектов информатизации. Порядок проведения категорирования объектов на предприятий.

42. Классификация автоматизированных систем в составе объектов вычислительной техники.

43. Правовые основы лицензирования. Основные понятия и принципы лицензирования. Общие положения по организации лицензирования.

44. Государственная система лицензирования. Система лицензирования деятельности в области защиты государственной тайны.

45. Правовые основы сертификации и аттестации средств защиты информации.

46. Основные понятия и принципы сертификации.

47. Организация и проведение сертификации.

48. Организация и проведение лицензирования, сертификации и аттестации.

49. Требования к объектам информатизации и необходимость проведения их аттестации. Порядок проведения аттестации объектов информатизации.

50. Права и обязанности органов системы аттестации объектов информатизации.

51. Проведение аттестационных испытаний.

52. Основы организации и обеспечения работ по технической защите информации.

53. Цели и задачи защиты информации.

54. Организация защиты конфиденциальной информации.

55. Концепция безопасности предприятия и ее содержание.

56. Организация работы подразделений (служб) обеспечения информационной безопасности.

57. Организация защиты информации на предприятии.

58. Выявление и классификация угроз.

59. Принципы обеспечения информационной безопасности.

60. Управление информационной безопасностью.

61. Политика безопасности.

62. Разработка и внедрение системы управления информационной безопасности. Обеспечение информационной безопасности организации.

63. Характеристика эффективных стандартов по безопасности.

64. Требования к полноте эффективных стандартов по безопасности.

65. Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере.

66. Информация - фактор существования и развития общества.

67. Обеспечение информационной безопасности: содержание и структура понятия.

68. Система обеспечения информационной безопасности. Обеспечение информационной безопасности организации.

69. Обеспечение информационной безопасности Российской Федерации.

70. Международная нормативная база обеспечения безопасности. Федеральная нормативная база обеспечения безопасности

71. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.

72. Административный уровень обеспечения информационной безопасности.

73. Общие положения по категорированию объектов информатизации. Порядок проведения категорирования объектов на предприятий.

74. Классификация автоматизированных систем в составе объектов вычислительной техники.

75. Правовые основы лицензирования. Основные понятия и принципы лицензирования. Общие положения по организации лицензирования.

76. Государственная система лицензирования. Система лицензирования деятельности в области защиты государственной тайны.

77. Правовые основы сертификации и аттестации средств защиты информации.

78. Основные понятия и принципы сертификации.

79. Организация и проведение сертификации.

80. Организация и проведение лицензирования, сертификации и аттестации.

81. Уровни ведения информационной войны. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети.

82. Основные положения государственной информационной политики Российской Федерации.

83. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.

84. Виды защищаемой информации в сфере государственного и муниципального управления.

85. Международная нормативная база обеспечения безопасности. Федеральная нормативная база обеспечения безопасности

86. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.

87. Административный уровень обеспечения информационной безопасности.

Наименование оценочного средства: ***контрольная работа***

Методические материалы: приводятся вопросы и/или типовые задания, критерии оценки.

Примерное задание для контрольной работы:

- ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ
- ИСТОРИЯ И СОВРЕМЕННЫЕ ЦЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
- КЛАССИФИКАЦИЯ ВИРУСОВ И ВРЕДОНОСНЫХ ПРОГРАММ
- КОНТРОЛЬНАЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВАРИАНТ
- МЕТОДЫ ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

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.*

Оценочные средства для промежуточной аттестации

Представлено в приложении №1.

Автор(ы) рабочей программы дисциплины (модуля):

Ст. преподаватель кафедры ПИ _____ Мурадова П.Р.
(подпись)

СОГЛАСОВАНО:

Директор библиотеки _____ Арсагериева Т.А.
(подпись)

Приложение 1

Оценочные средства
для проведения промежуточной аттестации по дисциплине
Информационная безопасность и защита информации
направление подготовки:
09.03.03- Прикладная информатика

Профиль «Прикладная информатика в экономике»
Форма обучения: очная, заочная
Год приема: 2023

1. Характеристика оценочной процедуры:
Семестр - _4_
Форма аттестации – _зачет_

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

Вопросы для промежуточной аттестации по дисциплине:

1. Информационная безопасность в системе национальной безопасности.
2. Обеспечение информационной безопасности объектов информационной сферы государства
3. Общая характеристика компьютерной безопасности.
4. Испытание программного и аппаратного уровней компьютерной безопасности.
5. Система физической защиты компьютерных систем.
6. Организация и аудит безопасности компьютерных систем.

Структура экзаменационного билета (примерная):

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.	Если ответ студента показывает глубокое и систематическое знание всего программного материала и структуры конкретного вопроса, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой. Студент демонстрирует отчетливое и свободное владение концептуально-понятийным аппаратом, научным языком и терминологией соответствующей научной области. Знание основной литературы и знакомство с дополнительно рекомендованной литературой. Логически корректное и убедительное изложение ответа	**13-15**
2.	Если студент показывает знание узловых проблем программы и	**10-12**

	основного содержания лекционного курса; умение пользоваться концептуально-понятийным аппаратом в процессе анализа основных проблем в рамках данной темы; знание важнейших работ из списка рекомендованной литературы. В целом логически корректное, но не всегда точное и аргументированное изложение ответа	
3	Если студент показывает фрагментарные, поверхностные знания важнейших разделов программы и содержания лекционного курса; затруднения с использованием научно-понятийного аппарата и терминологии учебной дисциплины; неполное знакомство с рекомендованной литературой; частичные затруднения с выполнением предусмотренных программой заданий; стремление логически определенно и последовательно изложить ответ	**7-9**
4.	Если студент показывает незнание, либо отрывочное представление о данной проблеме в рамках учебно-программного материала; неумение использовать понятийный аппарат; отсутствие логической связи в ответе	**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. Уровни сформированности компетенций по итогам освоения дисциплины (модуля)

Таблица 15

Индикаторы достижения компетенции (ИДК)	**Уровни сформированности компетенций**			
	«отлично»	**«хорошо»**	**«удовлетворительно»**	**«неудовлетворительно»**
	86-100	**71-85**	**51-70**	**Менее 51**
	«зачтено»			**«не зачтено»**
ОПК-3 Способен решать стандартныезадачи профессиональной деятельности на основе информационной и Библиографическойкультуры с применением информационно- коммуникационныхтехнологий и с учетом основных требований информационной безопасности.				
ОПК-3.1. Применяет принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с использованием информационно-коммуникационных технологий и с учетом основных требований информационной безопасности ОПК-3.2. Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно - коммуникационных технологий и с учетом основных требований	*Критерий* 1 Обладает твердым и полным знанием материала, владеет дополнительной информацией. Дает полный, развернутый ответ	*Критерий* 1 Знает материал в запланированном объѐме. Ответ достаточно полный, но не отражает некоторые аспекты.	*Критерий* 1 Допускает неточности в формулировках. Знает только основной материал.	*Критерий* 1 Не знает значительной части материала. Отвечает на вопрос частично. Не отвечает на поставленные вопросы.

информационной безопасности. ОПК-3.3. Имеет опыт подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.				
	Критерий 2 Раскрывает структуру и состав изучаемых разделов информатики, демонстрирует сформированные системные знания. Успешно справляется с решением всех Поставленных математических задач	*Критерий 2* Раскрывает структуру и состав некоторых изучаемых разделов информатики. При решении предметных задач допускает единичные ошибки	*Критерий 2* Фрагментарно описывает структуру и состав изучаемых разделов информатики. Допускает множественные ошибки при решении предметных задач	*Критерий 2* Не знает структуру и содержание изучаемых разделов информатики. Не справляется с решением предложенных предметных задач
	Критерий 3 Обладает фактическими и теоретическими знаниями	*Критерий 3* Знает основные понятия и	*Критерий 3* Обладает базовыми общими знаниями и	*Критерий 3* Неспособен самостоятельно

	в пределах изучаемой области с пониманием границ применимости. Обладает диапазоном практических умений, требуемых для решения определенных проблем в нестандартной ситуации.	ключевые факты в пределах изучаемой области. Обладает диапазоном практических умений, требуемых для решения определенных проблем в пределах изучаемой области.	основными умениями, требуемыми для выполнения простых задач	продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.
Код и наименование формируемой компетенции				

5. Рейтинг-план изучения дисциплины

I	**БАЗОВАЯ ЧАСТЬ РЕЙТИНГОВОЙ СИСТЕМЫ**		
Виды контроля	**Контрольные мероприятия**	**Мин. кол-во баллов на занятиях**	**Макс. кол-во баллов на занятиях**
Текущий контроль № 1	Тема № 1-2. Основные составляющие информационной безопасности. Понятие «информационная безопасность». Проблема информационной безопасности общества.	0	10
Текущий контроль № 2	Тема № 3. Угрозы информационной безопасности Основные определения и критерии классификации угроз.	0	10
	Тема № 4. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.		
Рубежный контроль №1: контрольная работа (Темы 1-4)		0	10
Текущий	Тема 5. Вредоносное программное обеспечение. Вирусы как		10

контроль №3	угроза информационной безопасности.		0	
	Тема 6. Основы международного законодательства в области информационной безопасности и защиты информации.			
	Тема 7. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации.			
Текущий контроль №4	Тема 8. Ответственность за нарушения в сфере информационной безопасности. Стандарты и спецификации в области информационной безопасности. Административный уровень обеспечения информационной безопасности: цели, задачи, содержание, разработка политики информационной безопасности.		0	10
Рубежный контроль №2: контрольная работа (Темы 5-9)			0	10
Допуск к промежуточной аттестации			**Мин 36**	
II	**ДОПОЛНИТЕЛЬНАЯ ЧАСТЬ РЕЙТИНГОВОЙ СИСТЕМЫ**			
1	**Поощрительные баллы**		**0-10**	**10**
	Подготовка доклада с презентацией		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		0-30	**30**
ИТОГО БАЛЛОВ ЗА СЕМЕСТР:			**0-100**	

Приложение 2

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ / МОДУЛЯ
Информационная безопасность и защита информации
(наименование дисциплины / модуля)
направление подготовки:
09.03.03- Прикладная информатика
Профиль «Прикладная информатика в экономике»
(год набора 2023, форма обучения очная, заочная)
на 2023 / 2024 учебный год

В рабочую программу дисциплины / модуля вносятся следующие изменения:

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