

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Директор по образовательной
деятельности

Князев С.Т. Князев
«7» сентября 2023



РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля	Модуль
1153114	Информационная безопасность

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа Прикладной искусственный интеллект	Код ОП 09.03.03
Направление подготовки Прикладная информатика	Код направления и уровня подготовки 09.03.03

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Круглов Василий Николаевич	кандидат технических наук, доцент	Доцент	департамент информационных технологий и автоматики
2	Спиричева Наталья Рахматулловна	без ученой степени, без ученого звания	Старший преподаватель	департамент информационных технологий и автоматики

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Информационная безопасность

1.1. Аннотация содержания модуля

Целью освоения модуля «Информационная безопасность» является представление основных типов и способов защиты информации, приобретение студентом навыков проектирования систем защиты информации, освоение современных программных и аппаратных средств защиты информации, приобретение знания законодательства Российской Федерации в области защиты информации.

1.2. Структура и объем модуля

Таблица 1

№	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах
1	Информационная безопасность	3
ИТОГО по модулю:		3

1.3. Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	Не предусмотрены
Постреквизиты и кореквизиты модуля	Не предусмотрены

1.4. Распределение компетенций по дисциплинам модуля, планируемые результаты обучения (индикаторы) по модулю

Таблица 2

Перечень дисциплин модуля	Код и наименование компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения
1	2	3	4
Информационная безопасность	УК 13. Способен планировать и организовывать свою деятельность в цифровом пространстве с учетом правовых и этических норм взаимодействия человека и искусственного интеллекта и требований	УК-13.2. Использует технологии сбора, обработки, интерпретации, анализа и обмена информацией с учетом требований информационной безопасности	УК-13.2. 3-1. Знает цели, задачи и предмет, основные понятия информационной безопасности, информационные угрозы, их классификацию, возможные последствия для организаций различных форм собственности и критерии оценки защищенности информационных систем и

	информационной безопасности		<p>систем искусственного интеллекта УК-13.2. У-1. Умеет использовать в профессиональной деятельности и в социальной сфере профессиональные навыки работы с информационными и компьютерными технологиями</p> <p>УК-13.2. У-2. Умеет сознавать опасности и угрозы, возникающие в профессиональной деятельности и в социальной сфере, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны</p> <p>УК-13.2. У-3. Умеет работать с информацией с учетом требований информационной безопасности</p>
--	-----------------------------	--	---

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной форме.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Информационная безопасность

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Круглов Василий Николаевич	кандидат технических наук, доцент	Доцент	департамент информационных технологий и автоматики
2	Широков Сергей Александрович	без ученой степени, без ученого звания	Старший преподаватель	департамент информационных технологий и автоматики

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Круглов Василий Николаевич, Доцент, Департамент информационных технологий и автоматике**
- **Широков Сергей Александрович, Старший преподаватель, Департамент информационных технологий и автоматике**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Смешанная модель обучения с использованием онлайн-курса партнера
- Разноуровневое (дифференцированное) обучение
 - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания; Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.*

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
P1	Введение в информационную безопасность	Что такое информационная безопасность. Уровни решения проблемы информационной безопасности. Содержание основных законов Российской Федерации в сфере компьютерного права. Уровни защиты информации. Меры защиты информационной безопасности. Угрозы для информационной безопасности, связанные с подключением к глобальной компьютерной сети Интернет и меры безопасного использования сервисов Интернета.
P2	Классификация информационных систем	Понятие информационных систем. Процессы, протекающие в информационных системах. Этапы развития информационных систем. Типы информационных систем. Классификация информационных систем по функциональному признаку. Классификация информационных систем по уровням управления.

P3	Матрица доступа. Классификация угроз	Понятие матрицы доступа. Распределение ответственности. Минимизация привилегий. Классификация угроз безопасности информации. Угрозы утечки информации по техническим каналам. Угрозы несанкционированного доступа к информации в информационной системе.
P4	Угрозы утечки информации	Угрозы утечки акустической (речевой) информации. Угрозы утечки видовой информации. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).
P5	Общая характеристика угроз непосредственного доступа	Анализ уязвимостей системы Основные направления и методы реализации угроз Неформальная модель нарушителя
P6	Безопасность мобильного доступа. Средства защиты информации.	Сценарии атаки мобильных устройств. Основные положения и принципы построения технической защиты информации.
P7	Криптография. Симметричная и асимметричная криптография.	Популярные шифры. Полиморфизм. Распространённые алгоритмы. Виды алгоритмов. Квантовая криптография
P8	Хэш-функции. Управление криптографическими ключами. Аутентификация пользователей	Хэш-функции: основные требования к ним и их применение. Генерация ключей. Хранение ключей. Носители ключевой информации. Концепция иерархии ключей. Распределение ключей.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	профориентационная деятельность	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности Технология самостоятельной работы	УК 13. Способен планировать и организовывать свою деятельность в цифровом пространстве с учетом правовых и этических норм взаимодействия человека и искусственного интеллекта и требований	УК-13.2. У-3. Умеет работать с информацией с учетом требований информационной безопасности

			информационной безопасности	
--	--	--	-----------------------------	--

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации.

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Информационная безопасность

Электронные ресурсы (издания)

1. Суворова, , Г. М.; Информационная безопасность : учебное пособие.; Вузовское образование, Саратов; 2019; <http://www.iprbookshop.ru/86938.html> (Электронное издание)
2. Моргунов, А. В.; Информационная безопасность : учебно-методическое пособие.; Новосибирский государственный технический университет, Новосибирск; 2019; <https://biblioclub.ru/index.php?page=book&id=576726> (Электронное издание)
3. Ревнивых, , А. В.; Информационная безопасность в организациях : учебное пособие.; Ай Пи Ар Медиа, Москва; 2021; <http://www.iprbookshop.ru/108227.html> (Электронное издание)
4. Галатенко, , В. А.; Основы информационной безопасности : учебное пособие.; Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, Москва; 2020; <http://www.iprbookshop.ru/97562.html> (Электронное издание)
5. Артемов, А. В.; Информационная безопасность: курс лекций : курс лекций.; Межрегиональная академия безопасности и выживания, Орел; 2014; <https://biblioclub.ru/index.php?page=book&id=428605> (Электронное издание)
6. Прохорова, О. В.; Информационная безопасность и защита информации : учебник.; Самарский государственный архитектурно-строительный университет, Самара; 2014; <https://biblioclub.ru/index.php?page=book&id=438331> (Электронное издание)

Профессиональные базы данных, информационно-справочные системы

- 1) Зональная научная библиотека УрФУ <http://lib.urfu.ru>
- 2) Научная электронная библиотека Elibrary.ru <https://www.elibrary.ru/>
- 3) Электронная библиотечная сеть "Лань" <http://e.lanbook.com/>
- 4) Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии - http://window.edu.ru/catalog/p_rubr=2.2.75.6
- 5) Федеральный центр информационно-образовательных ресурсов <http://eor.edu.ru/>

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

- 1) Государственная публичная научно-техническая библиотека <http://www.gpntb.ru>

- 2) Список библиотек, доступных в Интернет и входящих в проект «Либнет» <http://www.valley.ru/nicr/listrum.htm>
- 3) Российская национальная библиотека <http://www.rsl.ru>
- 4) Портал информационно-образовательных ресурсов УрФУ <http://study.urfu.ru/>
- 5) Энциклопедия Википедия <https://ru.wikipedia.org/>
- 6) Онлайн-курс “Основы обеспечения информационной безопасности”. URL: https://openedu.ru/course/bmstu/MGTU_6/

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Информационная безопасность

Сведения об оснащённости дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащённость специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	<p>Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов</p> <p>Рабочее место преподавателя</p> <p>Доска аудиторная</p> <p>Периферийное устройство</p> <p>Персональные компьютеры по количеству обучающихся</p> <p>Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами</p> <p>Подключение к сети Интернет</p>	<p>Microsoft Windows 8.1 Pro 64-bit RUS OLP NL Acdmc</p> <p>Adobe Acrobat Professional 2017 Multiple Platforms</p> <p>Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES</p>
2	Лабораторные занятия	<p>Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов</p> <p>Рабочее место преподавателя</p> <p>Периферийное устройство</p>	<p>Adobe Acrobat Professional 2017 Multiple Platforms</p> <p>Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES</p>

		<p>Персональные компьютеры по количеству обучающихся</p> <p>Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами</p> <p>Подключение к сети Интернет</p>	
3	Консультации	<p>Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов</p> <p>Рабочее место преподавателя</p> <p>Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами</p> <p>Подключение к сети Интернет</p>	<p>Adobe Acrobat Professional 2017 Multiple Platforms</p> <p>Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES</p>
4	Текущий контроль и промежуточная аттестация	<p>Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов</p> <p>Рабочее место преподавателя</p> <p>Периферийное устройство</p> <p>Персональные компьютеры по количеству обучающихся</p> <p>Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами</p> <p>Подключение к сети Интернет</p>	<p>Adobe Acrobat Professional 2017 Multiple Platforms</p> <p>Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES</p>
5	Самостоятельная работа студентов	<p>Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов</p> <p>Персональные компьютеры по количеству обучающихся</p>	<p>Adobe Acrobat Professional 2017 Multiple Platforms</p> <p>Office 365 EDUA5 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES</p>

		Оборудование, соответствующее требованиям организации учебного процесса в соответствии с санитарными правилами и нормами Подключение к сети Интернет	
--	--	--	--

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ
Информационная безопасность**

Код модуля
1153114(1)

Модуль
Информационная безопасность

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Круглов Василий Николаевич	кандидат технических наук, доцент	Доцент	департамент информационных технологий и автоматике
2	Широков Сергей Александрович	без ученой степени, без ученого звания	Старший преподаватель	департамент информационных технологий и автоматике

Авторы:

- **Круглов Василий Николаевич, Доцент, Департамент информационных технологий и автоматике**
- **Широков Сергей Александрович, Старший преподаватель, Департамент информационных технологий и автоматике**

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Информационная безопасность

1.	Объем дисциплины в зачетных единицах	3	
2.	Виды аудиторных занятий	Лекции Лабораторные занятия	
3.	Промежуточная аттестация	Экзамен	
4.	Текущая аттестация	Контрольная работа	1
		Домашняя работа	1

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Информационная безопасность

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины, указанного в табл. 1.3 РПМ-РПД.

Таблица 1

Код и наименование компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения	Контрольно-оценочные средства для оценивания достижения результата обучения по дисциплине
1	2	3	4
УК 13. Способен планировать и организовывать свою деятельность в цифровом пространстве с учетом правовых и этических норм	УК-13.2. Использует технологии сбора, обработки, интерпретации, анализа и обмена информацией с учетом требований	УК-13.2. 3-1. Знает цели, задачи и предмет, основные понятия информационной безопасности, информационные угрозы, их классификацию, возможные последствия для организаций различных форм собственности и критерии оценки защищенности	Домашняя работа Экзамен Контрольная работа Лабораторные занятия Лекции

взаимодействия человека и искусственного интеллекта и требований информационной безопасности	информационной безопасности	информационных систем и систем искусственного интеллекта УК-13.2. У-1. Умеет использовать в профессиональной деятельности и в социальной сфере профессиональные навыки работы с информационными и компьютерными технологиями УК-13.2. У-2. Умеет сознавать опасности и угрозы, возникающие в профессиональной деятельности и в социальной сфере, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны УК-13.2. У-3. Умеет работать с информацией с учетом требований информационной безопасности	
--	-----------------------------	--	--

3. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ МОДУЛЯ В БАЛЬНО-РЕЙТИНГОВОЙ СИСТЕМЕ (ТЕХНОЛОГИЧЕСКАЯ КАРТА БРС)

3.1. Процедуры текущей и промежуточной аттестации по дисциплине

1. Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0.50		
Текущая аттестация на лекциях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
<i>домашняя работа</i>	7,7	50
<i>контрольная работа</i>	7,14	50
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.50		
Промежуточная аттестация по лекциям – экзамен Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.50		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – не предусмотрено		
Текущая аттестация на практических/семинарских занятиях	Сроки – семестр,	Максимальная оценка в баллах

	учебная неделя	
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– не предусмотрено		
Промежуточная аттестация по практическим/семинарским занятиям–нет		
Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– не предусмотрено		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0.50		
Текущая аттестация на лабораторных занятиях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
<i>выполнение и защита лабораторных работ</i>	7,16	100
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -1.00		
Промежуточная аттестация по лабораторным занятиям –нет		
Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям – 0.00		
4. Онлайн-занятия: коэффициент значимости совокупных результатов онлайн-занятий –не предусмотрено		
Текущая аттестация на онлайн-занятиях	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
Весовой коэффициент значимости результатов текущей аттестации по онлайн-занятиям -не предусмотрено		
Промежуточная аттестация по онлайн-занятиям –нет		
Весовой коэффициент значимости результатов промежуточной аттестации по онлайн-занятиям – не предусмотрено		

3.2. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Текущая аттестация выполнения курсовой работы/проекта	Сроки – семестр, учебная неделя	Максимальная оценка в баллах
Весовой коэффициент текущей аттестации выполнения курсовой работы/проекта– не предусмотрено		
Весовой коэффициент промежуточной аттестации выполнения курсовой работы/проекта– защиты – не предусмотрено		

4. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

4.1. В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 4

Критерии оценивания учебных достижений обучающихся

Результаты обучения	Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Другие результаты	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

4.2 Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5

Шкала оценивания достижения результатов обучения (индикаторов) по уровням

Характеристика уровней достижения результатов обучения (индикаторов)				
№ п/п	Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)	Шкала оценивания		
		Традиционная характеристика уровня		Качественная характеристика уровня
1.	Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам,	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)

	имеются существенные ошибки и замечания, требуется доработка		
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания	Нет результата

5. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПО ДИСЦИПЛИНЕ МОДУЛЯ

5.1. Описание аудиторных контрольно-оценочных мероприятий по дисциплине модуля

5.1.1. Лекции

Самостоятельное изучение теоретического материала по темам/разделам лекций в соответствии с содержанием дисциплины (п. 1.2. РПД)

5.1.2. Лабораторные занятия

Примерный перечень тем

1. Настройка персонального брандмауэра и его использование для обеспечения безопасности сетевого соединения
 2. Обеспечение безопасности в сетях. Списки управления доступом ACL и служба трансляции адресов NAT
 3. Абсолютно стойкий шифр
 4. Снифферы. Методы защиты от перехвата трафика
 5. Сетевые сканеры
 6. Аутентификация пользователей в ОС Windows. Пароли
 7. Система обнаружения атак Snort
- LMS-платформа – не предусмотрена

5.2. Описание внеаудиторных контрольно-оценочных мероприятий и средств текущего контроля по дисциплине модуля

Разноуровневое (дифференцированное) обучение.

Базовый

5.2.1. Контрольная работа

Примерный перечень тем

1. Классификация информационных систем

Примерные задания

Понятие информационных систем

Процессы, протекающие в информационных системах

Этапы развития информационных систем

Типы информационных систем

Классификация информационных систем по функциональному признаку

Классификация информационных систем по уровням управления.

LMS-платформа:

1. https://openedu.ru/course/bmstu/MGTU_6/

5.2.2. Домашняя работа

Примерный перечень тем

1. Хеширование

Примерные задания

Задание 1. Реализация блочного 128-битового шифра.

Задание 2. Хеширование (вычисление сжатого образа сообщения):

Программная реализациям бесключевой 128-битовой функции хеширования на основе реализованного в задании 1 блочного шифра

LMS-платформа:

1. https://openedu.ru/course/bmstu/MGTU_6/

5.3. Описание контрольно-оценочных мероприятий промежуточного контроля по дисциплине модуля

5.3.1. Экзамен

Список примерных вопросов

1. Введение в информационную безопасность

2. Классификация информационных систем

3. Матрица доступа. Классификация угроз

4. Угрозы утечки информации

5. Общая характеристика угроз непосредственного доступа

6. Безопасность мобильного доступа

7. Средства защиты информации

8. Криптография

9. Симметричная криптография

10. Асимметричная криптография

11. Хеш-функции

12. Управление криптографическими ключами

13. Аутентификация пользователей

LMS-платформа – не предусмотрена

5.4 Содержание контрольно-оценочных мероприятий по направлениям воспитательной деятельности

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения	Контрольно-оценочные мероприятия
Профессиональное воспитание	профориентационная деятельность	Технология формирования уверенности и готовности к самостоятельной	УК 13	УК-13.2. У-3	Домашняя работа Лабораторные занятия

		успешной профессиональной деятельности Технология самостоятельной работы			Лекции
--	--	---	--	--	--------