Министерство сельского хозяйства Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Вятский государственный агротехнологический университет"

УТВЕРЖДАЮ
Декан агрономического факультета
_____ А.В. Тюлькин
"15" апреля 2022 г.

Информационная безопасность

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **информационных технологий и статистики**

Учебный план Направление подготовки 19.03.01 Биотехнология
Направленность (профиль) программы бакалавриата "Пищевая биотехнология"

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **7 ЗЕТ**

Часов по учебному плану 252
в том числе:
аудиторные занятия 80
самостоятельная работа 145
часов на контроль 27

Виды контроля в семестрах:
экзамены 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		**7 (4.1)**		Итого	
Недель	17		19			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	16	16	16	16	32	32
Лабораторные			16	16	16	16
Практические	16	16	16	16	32	32
В том числе инт.	4	4	4	4	8	8
Итого ауд.	32	32	48	48	80	80
Контактная работа	32	32	48	48	80	80
Сам. работа	76	76	69	69	145	145
Часы на контроль			27	27	27	27
Итого	108	108	144	144	252	252

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 26ADAA3CADCD154164284BE8B6E56076
Владелец: Симбирских Елена Сергеевна
Действителен: с 06.07.2022 до 29.09.2023

Киров 2022

Программу составил(и):
к.э.н., Доцент кафедры информационных технологий и статистики , Козлова Лариса Алексеевна

Рецензент(ы):
к.э.н, Доцент кафедры экономики и менеджмента, Шиврина Татьяна Борисовна

Рабочая программа дисциплины

Информационная безопасность
разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 19.03.01 Биотехнология (приказ Минобрнауки России от 10.08.2021 г. № 736)

составлена на основании Учебного плана:

Направление подготовки 19.03.01 Биотехнология
Направленность (профиль) программы бакалавриата "Пищевая биотехнология"
одобренного и утвержденного Ученым советом университета от 15.04.2022 протокол № 5.

Рабочая программа дисциплины рассмотрена и одобрена учебно-методической комиссией

Протокол № ____ от "15"апреля 2022 г.

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры

информационных технологий и статистики

Протокол № ____ от "15"апреля 2022 г.

Зав. кафедрой _____к.э.н. доцент Козлова Лариса Алексеевна

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры **информационных технологий и статистики**

Протокол от "__" _____ 2023 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры **информационных технологий и статистики**

Протокол от "__" _____ 2024 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры **информационных технологий и статистики**

Протокол от "__" _____ 2025г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры **информационных технологий и статистики**

Протокол от "__" _____ 2026 г. № __

Зав. кафедрой _____

1. ЦЕЛЬ (ЦЕЛИ) ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Цель учебной дисциплины заключается в получении обучающимися теоретических знаний об основах защиты информации, организационных методах защиты информации, математических методах, лежащих в основе защиты информации с последующим применением в профессиональной сфере

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
Цикл (раздел) ОПОП:	Б1.О.03
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Дисциплины, изученные на предыдущем уровне
2.1.2	Пакеты прикладных программ для профессиональной деятельности
2.1.3	Основы информационных технологий
2.1.4	Технологическая практика
2.1.5	Ознакомительная практика
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Научно-исследовательская работа
2.2.2	Преддипломная практика
2.2.3	Подготовка к процедуре защиты и защита выпускной квалификационной работы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-2	Способен осуществлять поиск, хранение, обработку и анализ профессиональной информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий, включая проведение расчетов и моделирование, с учетом основных требований информационной безопасности
ОПК-2.1	Знает процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); современные инструментальные среды, программно-технические платформы и программные средства, в том числе системы искусственного интеллекта, используемые для решения задач профессиональной деятельности, и принципы их работы
ОПК-2.2	Умеет выбирать и использовать современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы и программные средства для решения задач профессиональной деятельности; анализировать профессиональные задачи, выбирать и использовать подходящие информационные технологии
ОПК-2.3	Владеет навыками работы с данными с помощью информационных технологий; навыками применения современных информационно-коммуникационных и интеллектуальных технологий, инструментальных сред, программно- технических платформ и программных средств для решения задач профессиональной
ПК-4	Способен управлять биотехнологическими процессами и технологическим оборудованием на предприятиях пищевой промышленности для обеспечения качества и безопасности продуктов питания в соответствии с действующими нормативами
ПК-4.4	Использует основы организационного и технологического обеспечения процесса разработки прикладного программного обеспечения

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции (индикаторы)	Литература	Инте ракт.	Примечание
	Раздел 1. Раздел 1.Информационная безопасность						
1.1	Тема 1 Правовые основы информационной безопасности в Российской Федерации Цель: изучить правовые основы информационной безопасности в Российской Федерации Краткое содержание: Нормативно-правовые акты регламентирующие деятельность, связанную с защитой информации на территории РФ. Документы, демонстрирующие государственную политику РФ в сфере защиты информации. /Лек/	6	8	ОПК-2.1 ОПК- 2.2 ОПК-2.3 ПК-4.4	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	2	

1.2	Тема 2 Физические основы передачи информации. Технические средства защиты информации. История технологий шифрования. Модульная арифметика. Элементы коммутативной алгебры. Элементы элементарной теории чисел Цель: изучить физические основы передачи информации, технические средства защиты информации, историю технологий шифрования, модульную арифметику, элементы коммутативной алгебры и элементарной теории чисел. /Лек/	6	8	ОПК-2.1 ОПК- 2.2 ОПК-2.3 ПК-4.4	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	0	
1.3	Тема 1 Правовые основы информационной безопасности в Российской Федерации /Пр/	6	2	ОПК-2.1 ОПК- 2.2 ОПК-2.3 ПК-4.4	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	0	
1.4	Тема 1 Правовые основы информационной безопасности в Российской Федерации /Ср/	6	35	ОПК-2.1 ОПК- 2.2 ОПК-2.3 ПК-4.4	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	0	
1.5	Тема 2 Физические основы передачи информации. Технические средства защиты информации. История технологий шифрования. Модульная арифметика. Элементы коммутативной алгебры. Элементы элементарной теории чисел /Пр/	6	14	ОПК-2.1 ОПК- 2.2 ОПК-2.3 ПК-4.4	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	2	
1.6	Тема 2 Физические основы передачи информации. Технические средства защиты информации. История технологий шифрования. Модульная арифметика. Элементы коммутативной алгебры. Элементы элементарной теории чисел /Ср/	6	41	ОПК-2.1 ОПК- 2.2 ОПК-2.3 ПК-4.4	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	0	
1.7	Тема 3 Алгоритмы симметричного и ассиметричного шифрования. Использование шифрования в системах защиты информации. Особенности программной реализации криптоаналитических алгоритмов и алгоритмов шифрования. Уязвимости интернет страниц. Сетевая безопасность. /Лек/	7	16	ОПК-2.1 ОПК- 2.2 ОПК-2.3 ПК-4.4	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	2	
1.8	Тема 3 Алгоритмы симметричного и ассиметричного шифрования. Использование шифрования в системах защиты информации. Особенности программной реализации криптоаналитических алгоритмов и алгоритмов шифрования. Уязвимости интернет страниц. Сетевая безопасность. /Пр/	7	16	ОПК-2.1 ОПК- 2.2 ОПК-2.3 ПК-4.4	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	2	

1.9	Тема 3 Алгоритмы симметричного и ассиметричного шифрования. Использование шифрования в системах защиты информации. Особенности программной реализации криптоаналитических алгоритмов и алгоритмов шифрования. Уязвимости интернет страниц. Сетевая безопасность /Лаб/	7	16	ОПК-2.1 ОПК- 2.2 ОПК-2.3 ПК-4.4	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	0	
1.10	Тема 3 Алгоритмы симметричного и ассиметричного шифрования. Использование шифрования в системах защиты информации. Особенности программной реализации криптоаналитических алгоритмов и алгоритмов шифрования. Уязвимости интернет страниц. Сетевая безопасность. /Ср/	7	69	ОПК-2.1 ОПК- 2.2 ОПК-2.3 ПК-4.4	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	0	
1.11	/Экзамен/	7	0	ОПК-2.1 ОПК- 2.2 ОПК-2.3 ПК-4.4	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Рабочая программа дисциплины обеспечена фондом оценочных средств для проведения текущего контроля и промежуточной аттестации. Содержание фонда оценочных средств представлено в Приложении 1 и 2.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство,
Л1.1	Суворова, Г. М.	Информационная безопасность: учебное пособие для вузов Режим доступа: https://urait.ru/bcode/467370	Издательство Юрайт, 2021
Л1.2	Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов	Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов Режим доступа: https://urait.ru/bcode/450371	Издательство Юрайт, 2020

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство,
Л2.1	Зенков, А. В.	Информационная безопасность и защита информации: учебное пособие для вузов Режим доступа: https://urait.ru/bcode/477968	Издательство Юрайт, 2021
Л2.2	Чернова, Е. В.	Информационная безопасность человека: учебное пособие для вузов Режим доступа: https://urait.ru/bcode/449350	Издательство Юрайт, 2020

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство,
Л3.1	Ливанов Р.В	Информационная безопасность [Электронный ресурс]: учебно-методическое пособие для лабораторных занятий Режим доступа: http://46.183.163.35/MarcWeb2/Default.asp	Киров, 2022

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Научная электронная библиотека [Электронный ресурс]. - Режим доступа: http://elibrary.ru/defaultx.asp
Э2	Открытое образование.Информатика для инженеров и исследователей [Электронный ресурс]: [Виртуальная обучающая среда] - Режим доступа: https://openedu.ru/course/misis/INF/. - Загл. с экрана

6.3. Перечень информационных технологий

6.3.1 Перечень программного обеспечения

6.3.1.1	Операционная система семейства Windows (Windows Vista Business AO NL, MS Win Prof 7 AO NL, Win Prof 7 AOL NL, Win Home Bas 7 AOL NL LGG, Win Starter 7 AO NL LGG, Win SL 8 AOL NL LGG, Win Prof 8 AOL NL, Win Home 10 All Languages Online Product Key License)
6.3.1.2	Приложения Office (MS Office Prof Plus 2007 AO NL, MS Office Prof Plus 2010 AO NL, MS Office 2013 OL NL, MS OfficeStd 2016 RUS OLP NL Acdmc)

6.3.1.3	Антивирусное ПО Kaspersky Endpoint Security
6.3.1.4	Free Commander 2009/02b
6.3.1.5	Google Chrome 39/0/21/71/65
6.3.1.6	Opera 26/0/1656/24
6.3.1.7	Adobe Reader XI 11/0/09
6.3.1.8	IBM SPSS Statistics
6.3.2 Перечень информационных справочных систем и современных профессиональных баз данных	
6.3.2.1	Информационная справочная система: КонсультантПлюс
6.3.2.2	Информационная справочная система: Гарант
6.3.2.3	Профессиональная база данных: Научная электронная библиотека elibrary.ru Режим доступа: http://elibrary.ru/
6.3.2.4	Профессиональная база данных: Электронный каталог ФГБОУ ВО Вятского ГАТУ Режим доступа: http://46.183.163.35/MarcWeb2
6.3.2.5	Профессиональная база данных: Официальный сайт Министерства сельского хозяйства и продовольствия Кировской области, Режим доступа: http://www.dsx-kirov.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю) представлено в Приложении 3 РПД.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Освоение дисциплины проводится в форме аудиторных занятий и внеаудиторной самостоятельной работы обучающихся.

При проведении аудиторных занятий предусмотрено применение следующих инновационных форм учебных занятий, развивающих у обучающихся навыки командной работы, межличностной коммуникации, принятия решений, лидерские качества.

Внеаудиторная самостоятельная работа осуществляется в следующих формах:

• самостоятельное изучение теоретического материала (тем дисциплины);
• подготовка к лабораторным занятиям;
• подготовка к мероприятиям текущего контроля;
• подготовка к промежуточной аттестации.

При организации самостоятельной работы необходимо, прежде всего, обратить внимание на ключевые понятия, несущие основную смысловую нагрузку в том или ином разделе учебной дисциплины.

1. Самостоятельное изучение тем дисциплины

Для работы необходимо ознакомиться с учебным планом дисциплины и установить, какое количество часов отведено учебным планом в целом на изучение дисциплины, на аудиторную работу с преподавателем на лекционных и практических (семинарских), лабораторных занятиях, а также на самостоятельную работу. С целью оптимальной самоорганизации необходимо сопоставить эту информацию с графиком занятий и выявить наиболее затратные по времени и объему темы, чтобы заранее определить для себя периоды объемных заданий. Целесообразно начать работу с изучения теоретического материала, основных терминов и понятий курса и с письменных ответов на индивидуальные и тестовые задания.

2. Подготовка к лекционным и лабораторным занятиям

Традиционной формой преподнесения материала является лекция. Курс лекций по предмету дает необходимую информацию по изучению закономерностей и тенденций развития объекта и предмета исследования изучаемой дисциплины. Лекционный материал рекомендуется конспектировать. Конспекты позволяют обучающемуся не только получить больше информации на лекции, но и правильно его структурировать, а в дальнейшем - лучше освоить.

Подготовка к лабораторным занятиям носит различный характер как по содержанию, так и по сложности исполнения. Многие лабораторные занятия требуют большой исследовательской работы, изучения дополнительной научной литературы. Прежде чем приступить к выполнению такой работы, обучающемуся необходимо ознакомиться обстоятельно с содержанием задания, уяснить его, оценить с точки зрения восприятия и запоминания все составляющие его компоненты. Результаты эксперимента, графики и т.д. следует стремиться получить непосредственно при выполнении работы в лаборатории. Лабораторная работа считается выполненной только в том случае, когда отчет по ней принят. Чем скорее составлен отчет после проведения работы, тем меньше будет затрачено труда и времени на ее оформление.

3. Подготовка к мероприятиям текущего контроля

В конце изучения каждой темы может проводиться тематическая контрольная работа, которая является средством промежуточного контроля оценки знаний. Подготовка к ней заключается в повторении пройденного материала и повторном решении заданий, которые рассматривались на занятиях, а также в выполнении заданий для самостоятельной работы.

4. Подготовка к промежуточной аттестации

Подготовка к экзамену является заключительным этапом изучения дисциплины. Подготовка к экзамену предполагает изучение конспектов лекций, рекомендуемой литературы и других источников, повторение материалов практических занятий. Обучающийся получает оценку "отлично" в случае, если он ответил исчерпывающее на экзаменационные вопросы и на все дополнительные вопросы; получает оценку "хорошо", в случае, если он ответил на экзаменационные вопросы в достаточно полном объеме и ответил не на все дополнительные вопросы; получает оценку "удовлетворительно", в случае, если он ответил на большинство экзаменационных вопросов в объеме, предусмотренном учебным планом; получает оценку "неудовлетворительно", в случае, если он не ответил на вопросы экзамена в объеме предусмотренном учебным планом.

5. Интерактивные формы

Интерактивные формы обучения по дисциплине представлены в виде деловой игры. Количество часов занятий в интерактивных формах определено учебным планом.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации по дисциплине (модулю)
«Информационная безопасность»

Направление подготовки специальности 19.03.01 Биотехнология
Направленность (профиль) программы «Пищевая биотехнология»
Квалификация бакалавр

1. Описание назначения фонда оценочных средств

Настоящий фонд оценочных средств (ФОС) входит в состав рабочей программы дисциплины/модуля «Информационная безопасность» и предназначен для оценки планируемых результатов обучения, характеризующих этапы формирования компетенций (п.2) в процессе изучения данной дисциплины.

ФОС включает в себя оценочные материалы для проведения промежуточной аттестации в форме экзамена.

ФОС разработан на основании:

- Федерального государственного образовательного стандарта высшего образования по направлению подготовки 19.03.01 Биотехнология (приказ Минобрнауки России от 10.08.2021 №736) – основной профессиональной образовательной программы высшего образования по направлению подготовки 19.03.01 Биотехнология программы бакалавриата «Пищевая биотехнология»;
- Положения «О формировании фонда оценочных средств для промежуточной и итоговой аттестации обучающихся по образовательным программам высшего образования»

2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы:

Общепрофессиональные компетенции:

- Способен осуществлять поиск, хранение, обработку и анализ профессиональной информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий, включая проведение расчетов и моделирование, с учетом основных требований информационной безопасности (ОПК-2);

Профессиональные компетенции:

- Способен управлять биотехнологическими процессами и технологическим оборудованием на предприятиях пищевой промышленности для обеспечения качества и безопасности продуктов питания в соответствии с действующими нормативами (ПК-4).

Код формируемой компетенции	Этапы формирования компетенций в процессе освоения образовательной программы		
	Начальный	Основной	Заключительный
ОПК-2	Основы информационных технологий Пакеты прикладных	Информационная безопасность Интеллектуальные информационные системы	Преддипломная практика Подготовка к процедуре защиты и защита выпускной квалификационной работы

	программ для профессиональной деятельности Ознакомительная практика	Иностранный язык в профессиональной деятельности Основы научных исследований Технологическая практика Научно-исследовательская работа	
ПК-4	Биотехнология пищевых продуктов Разработка программных приложений Основы алгоритмизации и программирования Пакеты прикладных программ для профессиональной деятельности Основы информационных технологий	Оборудование и системы биотехнологических процессов на пищевых производствах Инженерная энзимология Технология ферментных препаратов Информационная безопасность Интеллектуальные информационные системы	Преддипломная практика Подготовка к процедуре защиты и защита выпускной квалификационной работы

3. Планируемые результаты освоения образовательной программы по дисциплине, выраженные через компетенции и индикаторы их достижений, описание шкал оценивания

ОПК-2 - Способен осуществлять поиск, хранение, обработку и анализ профессиональной информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий, включая проведение расчетов и моделирование, с учетом основных требований информационной безопасности	
Индикаторы	Формулировка индикатора
ОПК-2.1	Знает процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); современные инструментальные среды, программно-технические платформы и программные средства, в том числе системы искусственного интеллекта, используемые для решения задач профессиональной деятельности, и принципы их работы
ОПК-2.2	Умеет выбирать и использовать современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы и программные средства для решения задач профессиональной деятельности; анализировать профессиональные задачи, выбирать и использовать подходящие информационные технологии
ОПК-2.3	Владеет навыками работы с данными с помощью информационных технологий; навыками применения современных информационно-

	коммуникационных и интеллектуальных технологий, инструментальных сред, программно-технических платформ и программных средств для решения задач профессиональной деятельности
ПК-4 Способен управлять биотехнологическими процессами и технологическим оборудованием на предприятиях пищевой промышленности для обеспечения качества и безопасности продуктов питания в соответствии с действующими нормативами	
ПК-4.4	Использует основы организационного и технологического обеспечения процесса разработки прикладного программного обеспечения

Для оценки сформированности соответствующих компетенций по дисциплине при проведении итоговой аттестации в форме экзамена применяется следующая шкала оценивания:

Шкала оценивания:

№	Критерии оценивания	Шкала оценивания			
		неудовлетворительно	**удовлетворительно**	**хорошо**	**отлично**
		Описание показателя			
1	Уровень усвоения обучающимся теоретических знаний иумение использовать ихдля решения профессиональных задач	Низкий уровень усвоения материала. Продемонстрировано незнание значительной части программного материала	Представлены знания только основного материала, но не усвоены его деталей	Твердое знание материала	Высокий уровень усвоения материала, продемонстрировано умение тесно увязывать теорию с практикой
2	Правильность решения практического задания с использованием вычислительной техники и современных информационных технологий	Обучающийся с неуверенно, большими затруднениями выполняет практические работы	Обучающийся испытывает затруднения при выполнении практических работ	Обучающийся правильно применяет теоретические положения прирешении практических вопросов и задач, владеет необходимым и навыками и приемами их выполнения	Обучающийся свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий,
3	Логичность, обоснованность, четкость ответа на вопросы	Существенные ошибки, нет ответовна дополнительные уточняющие вопросы	Неточности в ответах, недостаточно правильные формулировки, нарушения логической	Грамотное и по существу изложение теоретического материала, недопуская существенных	Исчерпывающе последовательно,четко и логически стройно излагается

			последовательности в изложении программного материала.	неточностей в ответе на вопрос	теоретический материал
4	Работа в течение семестра, наличие задолженности по текущему контролю успеваемости.	Имеются многочисленные пропуски занятий, задолженность по текущему контролю знаний	Имеются пропуски занятий, частичная задолженность по текущему контролю знаний	Активная работа, задолженность отсутствует	Активная работа, задолженность отсутствует

4. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Примерный перечень вопросов для подготовки к экзамену:

1. Государственная политика в сфере обеспечения безопасности. Концепция национальной безопасности РФ.
2. Государственная политика в сфере обеспечения информационной безопасности. Доктрина информационной безопасности РФ.
3. Методы обеспечения информационной безопасности России.
4. Источники угроз информационной безопасности России.
5. Виды угроз информационной безопасности России.
6. Правовые методы обеспечения информационной безопасности России.
7. Права человека и информационная безопасность.
8. Ответственность за посягательство на информацию в сфере экономической деятельности.
9. Нормативно-правовые акты РФ по защите государственной тайны. Основные положения закона «О государственной тайне».
10. Роль ФАПСИ, ФСБ, ФСТЭК в обеспечении информационной безопасности России.
11. Определения ТСПИ и ТКУИ.
12. Способы перехвата информации передаваемой ТСПИ.
13. Достоинства и недостатки акустических закладок, в зависимости от их принадлежности к определённому классу (классификация акустических закладок)
14. Методы выявления акустических закладок, в зависимости от класса
15. Шифр Цезаря, простой биграммной замены, самоключ Вижинера, квадраты Кардано.

16. Определение понятий код, номенклатор, открытый текст, шифры замены и перестановки, много- и одно- алфавитные шифры замены, криптоанализ, криптология.
17. Роль Джованни Порта, Этьена Базери, Блеза Виженера, Кергоффса, Клода Шенона, Уитфилда Диффи и Мартина Хеллмана в становлении крптографии.
18. Что означает формулировка числа a и b сравнимы по модулю N
19. Множество значений оператора mod N(т.е. понимать, что это за множество)
20. Какие свойства определяют группы и кольца
21. Образующая группы
22. Циклическая группа
23. Поле
24. Функция Эйлера и как вычислить её значение
25. Формулировка Малой теоремы Ферма
26. Алгоритм Евклида
27. Расширенный алгоритм Евклида
28. Формулировка китайской теоремы об остатках
29. Тест Ферма
30. Псевдопростые числа по определённому основанию
31. Решето Эратосфена
32. Теорема Котельникова-Найквиста
33. Принципы проводной передачи данных
34. Принципы беспроводной передачи данных
35. Симметричный алгоритм шифрования
36. Рассеивание и полнота
37. Режимы шифрования
38. Определение длинны излучающей антенны
39. Высокочастотное навязывание и методы защиты от него
40. Сеть Фейстеля и SP-блоки
41. Вычислительно необратимые функции
42. Какие существуют атаки на алгоритмы шифрования
43. Запас криптостойкости
44. Понятие раунда шифрования
45. Понятие открытого и закрытого ключа
46. Что такое ассиметричное шифрование, и в каких областях оно используется
47. Алгоритм RSA
48. Виды и способы защиты от XSS атак
49. Виды и способы защиты от CSRF атак

50. Произведение Монтгомери

51. Каким образом осуществляется настройка стандартных средств обеспечения информационной безопасности систем SAP (стойкость и время действия паролей, длительность сессий, параметры SSO и др.).

52. Каким образом осуществляется настройка типовых расширенных средств обеспечения информационной безопасности систем SAP (SAPCRYPTOLIB, Audit, GRC).

53. Аудит ролей и полномочий SAP (R/3, BW, Enterprise Portal, BusinessObjects), проектирование и корректировка ролевых моделей.

54. ИТ-аудит корпоративных информационных систем в части информационной безопасности.

Тестовые задания
по дисциплине «Информационная безопасность»
для промежуточной аттестации в форме экзамена

1. 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 направ-лениям от воздействия

В) нет правильного ответа

2. Защита информации – это..

А) комплекс мероприятий, направленных на обеспечение информационной безопасности.

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей

В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?

А) от компьютеров

Б) от поддерживающей инфраструктуры

В) от информации

4. Основные составляющие информационной безопасности:

А) целостность

Б) достоверность

В) конфиденциальность

5. Доступность – это…

А) возможность за приемлемое время получить требуемую информационную услугу.

Б) логическая независимость

В) нет правильного ответа

6. Целостность – это..

А) целостность информации

Б) непротиворечивость информации

В) защищенность от разрушения

7. Конфиденциальность – это..

А) защита от несанкционированного доступа к информации

Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

В) описание процедур

8. Для чего создаются информационные системы?

А) получения определенных информационных услуг

Б) обработки информации

В) все ответы правильные

9. Целостность можно подразделить:

А) статическую

Б) динамичную

В) структурную

10. Где применяются средства контроля динамической целостности?

А) анализе потока финансовых сообщений

Б) обработке данных

В) при выявлении кражи, дублирования отдельных сообщений

11. Какие трудности возникают в информационных системах при конфиденциальности?

А) сведения о технических каналах утечки информации являются закрытыми

Б) на пути пользовательской криптографии стоят многочисленные технические проблемы

В) все ответы правильные

12. Угроза – это…

А) потенциальная возможность определенным образом нарушить информационную безопасность

Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных

В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

13. Атака – это…

А) попытка реализации угрозы

Б) потенциальная возможность определенным образом нарушить информационную безопасность

В) программы, предназначенные для поиска необходимых программ.

14. Источник угрозы – это..

А) потенциальный злоумышленник

Б) злоумышленник

В) нет правильного ответа

15. Окно опасности – это…

А) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.

Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области

В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

16. Какие события должны произойти за время существования окна опасности?

А) должно стать известно о средствах использования пробелов в защите.

Б) должны быть выпущены соответствующие заплаты.

В) заплаты должны быть установлены в защищаемой И.С.

17. Угрозы можно классифицировать по нескольким критериям:

А) по спектру И.Б.

Б) по способу осуществления

В) по компонентам И.С

18. Основными источниками внутренних отказов являются:

А) отступление от установленных правил эксплуатации

Б) разрушение данных

В) все ответы правильные

19. Основными источниками внутренних отказов являются:

А) ошибки при конфигурировании системы

Б) отказы программного или аппаратного обеспечения

В) выход системы из штатного режима эксплуатации

20. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

А) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности

Б) обрабатывать большой объем программной информации

В) нет правильного ответа

21. Какие существуют грани вредоносного П.О.?

А) вредоносная функция

Б) внешнее представление

В) способ распространения

22. По механизму распространения П.О. различают:

А) вирусы

Б) черви

В) все ответы правильные

23. Вирус – это…

А) код обладающий способностью к распространению путем внедрения в другие программы

Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов

В) небольшая программа для выполнения определенной задачи

24. Черви – это…

А) код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения

Б) код обладающий способностью к распространению путем внедрения в другие программы

В) программа действий над объектом или его свойствами

25. Конфиденциальную информацию можно разделить:

А) предметную

Б) служебную

В) глобальную

26. Природа происхождения угроз:

А) случайные

Б) преднамеренные

В) природные

27. Предпосылки появления угроз:

А) объективные

Б) субъективные

В) преднамеренные

28. К какому виду угроз относится присвоение чужого права?

А) нарушение права собственности

Б) нарушение содержания

В) внешняя среда

29. Отказ, ошибки, сбой – это:

А) случайные угрозы

Б) преднамеренные угрозы

В) природные угрозы

30. Отказ - это…

А) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

Б) некоторая последовательность действий, необходимых для выполнения конкретного задания

В) структура, определяющая последовательность выполнения и взаимосвязи процессов

31. Сбой – это…

А) такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент

Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния

В) объект-метод

32. Побочное влияние – это…

А) негативное воздействие на систему в целом или отдельные элементы

Б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент

В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

33. СЗИ (система защиты информации) делится:

А) ресурсы автоматизированных систем

Б) организационно-правовое обеспечение

В) человеческий компонент

34. Что относится к человеческому компоненту СЗИ?

А) системные порты

Б) администрация

В) программное обеспечение

35. Что относится к ресурсам А.С. СЗИ?

А) лингвистическое обеспечение

Б) техническое обеспечение

В) все ответы правильные

36. По уровню обеспеченной защиты все системы делят:

А) сильной защиты

Б) особой защиты

В) слабой защиты

37. По активности реагирования СЗИ системы делят:

А) пассивные

Б) активные

В) полупассивные

38. Правовое обеспечение безопасности информации – это…

А) совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации

Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных

В) нет правильного ответа

39. Правовое обеспечение безопасности информации делится:

А) международно-правовые нормы

Б) национально-правовые нормы

В) все ответы правильные

40. Информацию с ограниченным доступом делят:

А) государственную тайну

Б) конфиденциальную информацию

В) достоверную информацию

41. Что относится к государственной тайне?

А) сведения, защищаемые государством в области военной, экономической … деятельности

Б) документированная информация

В) нет правильного ответа

42. Вредоносная программа - это…

А) программа, специально разработанная для нарушения нормального функционирования систем

Б) упорядочение абстракций, расположение их по уровням

В) процесс разделения элементов абстракции, которые образуют ее структуру и поведение

43. Что относится к организационным мероприятиям:

А) хранение документов

Б) проведение тестирования средств защиты информации

В) пропускной режим

44. Какие средства используется на инженерных и технических мероприятиях в защите информации:

А) аппаратные

Б) криптографические

В) физические

45. Программные средства – это…

А) специальные программы и системы защиты информации в информационных системах различного назначения

Б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла

В) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

46. Криптографические средства – это…

А) средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования

Б) специальные программы и системы защиты информации в информационных системах различного назначения

В) механизм, позволяющий получить новый класс на основе существующего

5. Методические материалы, определяющие процедуры оценивания опыта деятельности, характеризующих этапы формирования компетенций.

Процедура оценивания знаний, умений и навыков при проведении промежуточной аттестации по дисциплине «Информационная безопасность» проводится в форме экзамена.

Порядок организации и проведения промежуточной аттестации обучающегося, форма проведения, процедура сдачи экзамена, сроки и иные вопросы определены Положением о порядке организации и проведения текущего контроля успеваемости и промежуточной аттестации обучающихся.

Процедура оценивания знаний, умений и навыков при проведении теоретической части экзамена проводится путем письменного или компьютерного тестирования обучающихся:

- обучающемуся выдается вариант письменного или компьютерного теста (система Moodle) с учетом определенного уровня сложности (низкого, базового или продвинутого);
- в определенное время (в среднем 2 минуты на 1 тестовое задание)

обучающийся отвечает на вопросы теста, в котором представлены все изучаемые темы дисциплины;

- по результатам ответов на тестовые задания выставляется оценка согласно установленной шкале оценивания.

Для подготовки к экзамену рекомендуется использовать лекционный и практический материал по дисциплине, литературные источники, рекомендованные в рабочей программе дисциплины.

Приложение 2

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости по дисциплине
«Информационная безопасность»

Направление подготовки специальности 19.03.01 Биотехнология
Направленность (профиль) программы «Пищевая биотехнология»
Квалификация бакалавр

1. Описание назначения фонда оценочных средств

Настоящий фонд оценочных средств (ФОС) входит в состав рабочей программы дисциплины **«Информационная безопасность»** и предназначен для оценки планируемых результатов обучения - сформированности индикаторов достижения компетенций и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения дисциплины.

2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы:

Общепрофессиональные компетенции:

- Способен осуществлять поиск, хранение, обработку и анализ профессиональной информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий, включая проведение расчетов и моделирование, с учетом основных требований информационной безопасности (ОПК-2);

Профессиональные компетенции:

- Способен управлять биотехнологическими процессами и технологическим оборудованием на предприятиях пищевой промышленности для обеспечения качества и безопасности продуктов питания в соответствии с действующими нормативами (ПК-4).

3. Банк оценочных средств

Для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения дисциплины «Информационная безопасность» используются следующие оценочные средства:

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства
1	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося

Пример тестовых заданий по дисциплине «Информационная безопасность»:

1. 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 направ-лениям от воздействия

В) нет правильного ответа

2. Защита информации – это..

А) комплекс мероприятий, направленных на обеспечение информационной безопасности.

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей

В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?

А) от компьютеров

Б) от поддерживающей инфраструктуры

В) от информации

4. Основные составляющие информационной безопасности:

А) целостность

Б) достоверность

В) конфиденциальность

5. Доступность – это…

А) возможность за приемлемое время получить требуемую информационную услугу.

Б) логическая независимость

В) нет правильного ответа

6. Целостность – это..

А) целостность информации

Б) непротиворечивость информации

В) защищенность от разрушения

7. Конфиденциальность – это..

А) защита от несанкционированного доступа к информации

Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

В) описание процедур

8. Для чего создаются информационные системы?

А) получения определенных информационных услуг

Б) обработки информации

В) все ответы правильные

9. Целостность можно подразделить:

А) статическую

Б) динамичную

В) структурную

10. Где применяются средства контроля динамической целостности?

А) анализе потока финансовых сообщений

Б) обработке данных

В) при выявлении кражи, дублирования отдельных сообщений

11. Какие трудности возникают в информационных системах при конфиденциальности?

А) сведения о технических каналах утечки информации являются закрытыми

Б) на пути пользовательской криптографии стоят многочисленные технические проблемы

В) все ответы правильные

12. Угроза – это…

А) потенциальная возможность определенным образом нарушить информационную безопасность

Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных

В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

13. Атака – это…

А) попытка реализации угрозы

Б) потенциальная возможность определенным образом нарушить информационную безопасность

В) программы, предназначенные для поиска необходимых программ.

14. Источник угрозы – это..

А) потенциальный злоумышленник

Б) злоумышленник

В) нет правильного ответа

15. Окно опасности – это…

А) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.

Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области

В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

Методические материалы, определяющие процедуру оценивания

Процедура оценивания знаний, умений и навыков студентов при проведении текущего контроля:

- оценка знаний, умений и навыков студентов осуществляется по результатам постоянного контроля выполнения индивидуальных заданий и ответам на задаваемые вопросы по темам разделов;
- время на выполнение заданий определяется графиком самостоятельнойработы обучающихся.

Приложение 3

ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)
«Информационная безопасность»

Наименование специальных помещений	Оснащенность специальных помещений
Учебная аудитория для проведения занятий лекционного типа	Д-304 Доска, рабочее место преподавателя, комплект столов и стульев для обучающихся, комплект мультимедийного оборудования с экраном. Список ПО: Windows, Microsoft Office, Kaspersky Antivirus и свободно распространяемое программное обеспечение
Учебная аудитория для занятий семинарского типа	Д-116 Доска, рабочее место преподавателя, комплект столов и стульев для обучающихся, комплект мультимедийного оборудования с экраном, 10 персональных компьютеров, принтер. Список ПО: Windows, Microsoft Office, Kaspersky Antivirus, Directum, Гарант Аэро, Консультант Плюс, Программный комплекс «Компьютерная деловая игра «БИЗНЕС-КУРС: Корпорация Плюс. Версия 4», KonSi SWOT – Analysis, KonSi Anketter, KonSi Сегментирование и рынки, Project Expert 7 версия Tutorial, 1С Предприятие 7.7, 8.3 с конфигурациями и свободно распространяемое программное обеспечение
Учебная аудитория для групповых и индивидуальных консультаций	Д-116 Доска, рабочее место преподавателя, комплект столов и стульев для обучающихся, комплект мультимедийного оборудования с экраном, 10 персональных компьютеров, принтер. Список ПО: Windows, Microsoft Office, Kaspersky Antivirus, Directum, Гарант Аэро, Консультант Плюс, Программный комплекс «Компьютерная деловая игра «БИЗНЕС-КУРС: Корпорация Плюс. Версия 4», KonSi SWOT – Analysis, KonSi Anketter, KonSi Сегментирование и рынки, Project Expert 7 версия Tutorial, 1С Предприятие 7.7, 8.3 с конфигурациями и свободно распространяемое программное обеспечение
Учебная аудитория для текущего контроля и промежуточной аттестации	Д-116 Доска, рабочее место преподавателя, комплект столов и стульев для обучающихся, комплект мультимедийного оборудования с экраном, 10 персональных компьютеров, принтер. Список ПО: Windows, Microsoft Office, Kaspersky Antivirus, Directum, Гарант Аэро, Консультант Плюс, Программный комплекс «Компьютерная деловая игра «БИЗНЕС-КУРС: Корпорация Плюс. Версия 4», KonSi SWOT – Analysis, KonSi Anketter, KonSi Сегментирование и рынки, Project Expert 7 версия Tutorial, 1С Предприятие 7.7, 8.3 с конфигурациями и свободно распространяемое программное обеспечение
Помещение для самостоятельной работы	Б-202 Рабочее место администратора, компьютерная мебель, компьютер администратора, 5 персональных компьютеров, 3 принтера, видеоувеличитель. Список ПО: Windows, Microsoft Office, Kaspersky Antivirus и свободно распространяемое программное обеспечение

	С возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации

Приложение 4

Перечень
периодических изданий, рекомендуемый по дисциплине
«Информационная безопасность»

Наименование	Наличие доступа
Информационная безопасность/журнал [Электронный ресурс]	Режим доступа: https://www.itsec.ru/?__hstc=93476674.7091d70750d1a218e3c6fe03f7b17a41.1669819088385.1669819088385.1669819088385.1&__hssc=93476674.1.1669819088386&__hsfp=3033540334
SecurityLab.ru by Positive Technologies [Электронный ресурс]	Режим доступа: https://www.securitylab.ru/