ФГБОУ ВО «УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»
СИБАЙСКИЙ ИНСТИТУТ (ФИЛИАЛ) УУНиТ
ЕСТЕСТВЕННО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Утверждено:
на заседании кафедры
протокол № 11 от «31» мая 2023 г.

Зав. кафедрой _____/Гумеров И.С.

Согласовано:
Председатель УМК естественно-математического факультета

_____ /Ильбулова Г.Р.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

(наименование дисциплины)

Обязательная часть

(обязательная часть или часть, формируемая участниками образовательных отношений, факультатив)

программа бакалавриата

Направление подготовки
01.03.02 Прикладная математика и информатика
(указывается код и наименование направления подготовки)

Направленность (профиль) подготовки
Прикладная математика и информационные технологии
(указывается наименование направленности (профиля) подготовки)

Квалификация
бакалавр
(указывается квалификация)

Разработчик (составитель)
Доцент кафедры, к.ф.-м.н. / Хисаметдинов Ф.З.
(должность, ученая степень, ученое звание)

Для приема: 2023 г.

Сибай 2023 г.

Составитель: Хисаметдинов Ф.З.

Рабочая программа дисциплины утверждена на заседании кафедры прикладной математики и информационных технологий, протокол № 11 от «31» мая 2023 г.

И.о. заведующего кафедрой _____ / Гумеров И.С./

Дополнения и изменения, внесенную в рабочую программу дисциплины

_____

_____

утверждены на заседании кафедры

протокол №__ от «___»_____20__г.

Заведующий кафедрой_____/_____/

Дополнения и изменения, внесенную в рабочую программу дисциплины

_____

_____

утверждены на заседании кафедры

протокол №__ от «___»_____20__г.

Заведующий кафедрой_____/_____/

Дополнения и изменения, внесенную в рабочую программу дисциплины

_____

_____

утверждены на заседании кафедры

протокол №__ от «___»_____20__г.

Заведующий кафедрой_____/_____/

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций
2. Цель и место дисциплины в структуре образовательной программы
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)
4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине

4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины

6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

В результате освоения образовательной программы обучающийся должен овладеть компетнциями:

ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

По итогам освоения дисциплины обучающийся должен достичь следующих результатов обучения:

Формируемая компетенция (с указанием кода)	**Код и наименование индикатора достижения компетенции**	**Результаты обучения по дисциплине**
ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-4.1 Знает основные существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности. ОПК-4.2 Умеет использовать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности. ОПК-4.3 Имеет навыки применения существующих информационно-коммуникационные технологий для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.	Обладает фундаментальными знаниями по математическим моделям для решения прикладных задач Умеет использовать аппарат математических моделей при решении задач в профессиональной деятельности. Имеет навыки применения и модификации математических моделей при решении задач в профессиональной деятельности. Знает основные существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности. Умеет использовать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности. Имеет навыки применения существующих информационно-коммуникационные технологий для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.

УК-8 способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций.

Формируемая компетенция (с указанием кода)	**Код и наименование индикатора достижения компетенции**	**Результаты обучения по дисциплине**
УК-8 способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	УК-8.1 Знать методы создания и поддержки безопасных условий жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций УК-8.2 Уметь создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций УК-8.3 Владеть навыками создания и поддержки безопасных условий жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	Знает способы создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций. Умеет использовать способы создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций. Имеет навыки применения способов создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций.

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» относится к *обязательной* части.

Дисциплина изучается на *3 курсе* очной (6 *семестр)* и на *4 курсе* очно-заочной (8 *семестр)* форм обучения.

Дисциплина «Информационная безопасность» является дисциплиной по выбору вариативной части. Теоретический и практический материал изучаемых тем может использоваться во многих разделах прикладной информатики.

Информация является одним из наиболее ценных ресурсов любой компании, поэтому обеспечение защиты информации является одной из важнейших и приоритетных задач. Безопасность информационной системы - это свойство, заключающее в способности системы обеспечить ее нормальное функционирование, то есть обеспечить целостность и секретность информации. Для обеспечения целостности и конфиденциальности информации необходимо обеспечить защиту информации от случайного уничтожения или несанкционированного доступа к ней.

Для успешного усвоения дисциплины «Информационная безопасность» необходимо иметь хороший уровень подготовки по дисциплинам «Основы информатики», «Введение в специальность» и «Архитектура компьютеров».

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении № 1.

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине

Код и формулировка компетенции: **ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности**

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	«Не зачтено»	«Зачтено»
ОПК-4.1 Знает основные существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности. ОПК-4.2 Умеет использовать существующие информационно-коммуникационные технологии для решения за-	Знает основные существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности. Умеет использовать существующие информационно-коммуникационные технологии для решения задач	Не знает основные существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности. Не умеет использовать существующие информаци-	Знает хорошо основные существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности. Умеет на хорошем уровне использо-

дач в области профессиональной деятельности с учетом требований информационной безопасности. ОПК-4.3 Имеет навыки применения существующих информационно-коммуникационные технологий для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.	в области профессиональной деятельности с учетом требований информационной безопасности. Имеет навыки применения существующих информационно-коммуникационные технологий для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.	онно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности. Не имеет навыков применения существующих информационно-коммуникационные технологий для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.	вать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности. Имеет стабильные навыки применения существующих информационно-коммуникационные технологий для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.

УК-8 способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
УК-8.1 Знать методы создания и поддержки безопасных условий жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	Знать методы создания и поддержки безопасных условий жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	Не знает методы создания и поддержки безопасных условий жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	Знает методы создания и поддержки безопасных условий жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций
УК-8.2 Уметь создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	Уметь создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	Не умеет создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	Умеет создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций

УК-8.3 Владеть навыками создания и поддержки безопасных условий жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	Владеть навыками создания и поддержки безопасных условий жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	Не владеет навыками создания и поддержки безопасных условий жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	Владеет навыками создания и поддержки безопасных условий жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (*для экзамена:* текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10; *для зачета:* текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
не зачтено – от 0 до 59 рейтинговых баллов).

4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине.

Код и формулировка компетенции: **ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности**

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**
ОПК-4.1 Знает основные существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности. ОПК-4.2 Умеет использовать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.	Знает основные существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности. Умеет использовать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности. Имеет навыки применения существующих информационно-коммуникационные технологий для решения задач в	Индивидуальный, групповой опрос; тестирование; письменные ответы на вопросы; устный опрос (вопросы для самоконтроля); лабораторные работы; контрольные работы; собеседование; доклад; сообщение; задача; практическое задание; реферат; тесты; коллоквиум; отчет (по практикам, научно-исследовательской работе студентов и т.п.); научный доклад по теме НИРС; кейс-задача; комплексное практическое задание, проект; творческие задания (выступления, презентации,

ОПК-4.3 Имеет навыки применения существующих информационно-коммуникационные технологий для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.	области профессиональной деятельности с учетом требований информационной безопасности.	подготовка кроссворда и пр.);эссе; статья; ситуационные задачи и тесты; круглый стол; диспут; дискуссия; мозговой штурм; деловые, ролевые игры; рабочая тетрадь; тренинги; компьютерные симуляции, тренажеры; задания с использованием интерактивной доски и т.д.

Код и формулировка компетенции: **УК-8 способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций**.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**
УК-8.1 Знать методы создания и поддержки безопасных условий жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	Знает методы создания и поддержки безопасных условий жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	Индивидуальный, групповой опрос; тестирование; письменные ответы на вопросы; устный опрос (вопросы для самоконтроля); лабораторные работы; контрольные работы; собеседование; доклад; сообщение; задача; практическое задание; реферат; тесты; коллоквиум; отчет (по практикам, научно-исследовательской работе студентов и т.п.); научный доклад по теме НИРС; кейс-задача; комплексное практическое задание, проект; творческие задания (выступления, презентации, подготовка кроссворда и пр.);эссе; статья; ситуационные задачи и тесты; круглый стол; диспут; дискуссия; мозговой штурм; деловые, ролевые игры; рабочая тетрадь; тренинги; компьютерные симуляции, тренажеры; задания с использованием интерактивной доски и т.д.
УК-8.2 Уметь создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	Умеет создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	
УК-8.3 Владеть навыками создания и поддержки безопасных условий жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	Владеет навыками создания и поддержки безопасных условий жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций	

Критериями оценивания при *модульно-рейтинговой системе* являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (*для экзамена:* текущий контроль – максимум 70 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10)
Шкалы оценивания:

Рейтинг-план дисциплины

Рейтинг–план дисциплины представлен в приложении 2.

Вопросы к зачету по дисциплине

1. Что понимается под «Информационной безопасностью»? Назовите основные методы обеспечения информационной безопасности и дайте их краткую характеристику.
2. Приведите классификацию угроз ИБ с примерами.
3. Эшелонированная модель системы защиты. Назовите ее компоненты. Почему они расположены именно в таком порядке, поясните каждый компонент.
4. Организационные меры и физическая безопасность. Идентификация и аутентификация.
5. Парольные системы аутентификации. Их особенности.
6. Оценка стойкости парольных систем. Методы хранения и передачи паролей.
7. Дискреционное и мандатное разграничение доступа. Особенности.
8. Криптография для обеспечения безопасности и конфиденциальности информации.
9. Защита внешнего периметра. 4 класса межсетевых экранов.
10. Системы обнаружения вторжений. Принцип работы.
11. Протоколирование и аудит.
12. Принципы обеспечения целостности
13. Криптография для обеспечения целостности. Цифровая подпись, криптографические хеш-функции, коды проверки подлинности.
14. Системы защиты от угроз нарушения доступности информации.

Тест по дисциплине
«Информационная безопасность»

Пример заданий для тестового контроля уровня усвоения учебного материала

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. По каким компонентам классифицируется угрозы доступности:

А) отказ пользователей
Б) отказ поддерживающей инфраструктуры
В) ошибка в программе

19. Основными источниками внутренних отказов являются:

А) отступление от установленных правил эксплуатации
Б) разрушение данных
В) все ответы правильные

20. Основными источниками внутренних отказов являются:

А) ошибки при конфигурировании системы

Б) отказы программного или аппаратного обеспечения
В) выход системы из штатного режима эксплуатации

21. 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

22. Какие существуют грани вредоносного П.О.?

А) вредоносная функция
Б) внешнее представление
В) способ распространения

23. По механизму распространения П.О. различают:

А) вирусы
Б) черви
В) все ответы правильные

24. 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

25. 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

26. Конфиденциальную информацию можно разделить:

А) предметную
Б) служебную
В) глобальную

27. Природа происхождения угроз:

А) случайные
Б) преднамеренные
В) природные

28. Предпосылки появления угроз:

А) объективные

Б) субъективные
В) преднамеренные

29. К какому виду угроз относится присвоение чужого права?

А) нарушение права собственности
Б) нарушение содержания
В) внешняя среда

30. Отказ, ошибки, сбой – это:

А) случайные угрозы
Б) преднамеренные угрозы
В) природные угрозы

31. 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

32. Ошибка – это…

А) неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния
Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
В) негативное воздействие на программу

33. 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

34. 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

35. СЗИ (система защиты информации) делится:

А) ресурсы автоматизированных систем
Б) организационно-правовое обеспечение
В) человеческий компонент

36. Что относится к человеческому компоненту СЗИ?

А) системные порты
Б) администрация
В) программное обеспечение

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

А) лингвистическое обеспечение
Б) техническое обеспечение
В) все ответы правильные

38. По уровню обеспеченной защиты все системы делят:

А) сильной защиты
Б) особой защиты
В) слабой защиты

39. По активности реагирования СЗИ системы делят:

А) пассивные
Б) активные
В) полупассивные

40. 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

41. Правовое обеспечение безопасности информации делится:

А) международно-правовые нормы
Б) национально-правовые нормы
В) все ответы правильные

42. Информацию с ограниченным доступом делят:

А) государственную тайну
Б) конфиденциальную информацию
В) достоверную информацию

43. Что относится к государственной тайне?

А) сведения, защищаемые государством в области военной, экономической … деятельности
Б) документированная информация
В) нет правильного ответа

44. 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

45. Основополагающие документы для обеспечения безопасности внутри организации:

А) трудовой договор сотрудников
Б) должностные обязанности руководителей
В) коллективный договор

46. К организационно - административному обеспечению информации относится:

А) взаимоотношения исполнителей
Б) подбор персонала
В) регламентация производственной деятельности

47. Что относится к организационным мероприятиям:

А) хранение документов
Б) проведение тестирования средств защиты информации
В) пропускной режим

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

А) аппаратные
Б) криптографические
В) физические

49. 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

50. 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

Критерии оценки для студентов очной формы обучения (в баллах):

Процент правильных ответов	Количество баллов

95 - 100 %	10
85 - 94 %	9
75 - 84%	8
65 - 74%	7
55 - 64%	6
45 – 54%	5
менее 45%	0

Критерии оценки для студентов заочной (очно-заочной) формы обучения:

80 - 100 %	Отлично
60 - 79 %	Хорошо
40 - 59%	Удовлетворительно
менее 40%	Неудовлетворительно

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1 . Бабаш, А. В. Информационная безопасность : лабораторный практикум : учеб. пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников .— 2-е изд., стер .— М. : Кнорус, 2013 .— 136 с + 1 диск .
2. Стащук П. В. Краткое введение в операционные системы: учеб. пособие/ П.В. Стащук; Российская академия образования; Московский психолого-социальный институт. - М.: Флинта, 2008. - 128 с.

Дополнительная литература:

3. Загинайлов Ю.Н. Основы информационной безопасности: курс визуальных лекций. — М.: Берлин: Директ-Медиа, 2015. — 105 с. Режим доступа: http://biblioclub.ru/index.php?page=book_red&id=362895
4. Беломойцев Д. Е. , Волосатова Т. М. , Родионов С. В. Основные методы криптографической обработки данных: учебное пособие. — М.: Издательство МГТУ им. Н.Э. Баумана, 2014. — 80 с. Режим доступа: http://biblioclub.ru/index.php?page=book_red&id=258552

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины

1) http://www.mccme.ru - сайт Московского центра непрерывного образования;
2) http://www.etudes.ru – научно-популярный сайт по математике;
3) http://www.mathedu.ru – сайт «Математическое образование: прошлое и настоящее»;
4) http://www.math.ru.
5) www.lib.bashedu.ru – сайт библиотеки БашГУ;
6) «Электронный читальный зал» (ЭБС «Библиотех»);

7) ЭБС «Университетская библиотека online» - www.biblioclub.ru;
8) ЭБС изд-ва «Лань» - www.e.lanbook.com;
9) http://www.exponenta.ru –образовательный математический сайт;

6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
1	**2**	**3**
Аудитория 201	Лекции	Демонстрационное оборудование: доска, проектор – 1 шт., переносной экран – 1 шт. Специализированная мебель: столы, стулья (28 посадочных мест).
Аудитория 201	Практические занятия	Демонстрационное доска, проектор – 1 шт., переносной экран – 1 шт. Специализированная мебель: столы, стулья (28 посадочных мест).

Перечень специальных помещений и используемого лицензионного программного обеспечения представлен в справке о материально-техническом обеспечении ОП ВО по направлению подготовки 01.03.02 Прикладная математика и информатика (http://www.sibsu.ru/sveden/education).

Приложение № 1

ФГБОУ ВО «УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»
СИБАЙСКИЙ ИНСТИТУТ (ФИЛИАЛ) УУНиТ
ЕСТЕСТВЕННО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины Информационная безопасность на 6 семестр

очная форма обучения

Виды работ	**Объем**
Общая трудоемкость дисциплины (ЗЕТ / часов)	2 / 72
Учебных часов на контактную работу с преподавателем:	
Лекций	12
практических/ семинарских	
лабораторных	12
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	47,8
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	

Форма(ы) контроля:
Зачет 6 семестр

№ п/п	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР	ЛР	СР			
1	2	3	4	5	6	7	8	9
1.	Основы защиты информации	4		4	12	1-4	– проработка лекций и работа с литературой по теме; – дополнительное изучение отдельных тем;	– опрос по теории;
2.	Правовые основы защиты информации	2		2	12	1-4	– проработка лекций и работа с литературой по теме; – решение задач; – дополнительное изучение отдельных тем;	– опрос (тестирование) по теории; – контрольная работа;
3.	Криптографические средства защиты информации	4		4	12	1-4	– проработка лекций и работа с литературой по теме; – решение задач; – дополнительное изучение отдельных тем;	– опрос (тестирование) по теории; – контрольная работа;
4.	Защита информационных и операционных систем	2		2	11,8	1-4	– проработка лекций и работа с литературой по теме; – решение задач; – дополнительное изучение отдельных тем;	– опрос (тестирование) по теории; – контрольная работа;
	Всего часов:	12		12	47,8			

ФГБОУ ВО «УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»
СИБАЙСКИЙ ИНСТИТУТ (ФИЛИАЛ) УУНиТ
ЕСТЕСТВЕННО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины Информационная безопасность на 6 семестр

очно-заочная форма обучения

Виды работ	Объем
Общая трудоемкость дисциплины (ЗЕТ / часов)	2 / 72
Учебных часов на контактную работу с преподавателем:	
Лекций	6
практических/ семинарских	
лабораторных	6
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	
Учебных часов на самостоятельную работу обучающихся (СР)	60
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	

Форма(ы) контроля:
Зачет 8 семестр

№ п/п	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР	ЛР	СР			
1	2	3	4	5	6	7	8	9
1.	Основы защиты информации	1		1	14	1-4	– проработка лекций и работа с литературой по теме; – дополнительное изучение отдельных тем;	– опрос по теории;
2.	Правовые основы защиты информации	1		1	14	1-4	– проработка лекций и работа с литературой по теме; – решение задач; – дополнительное изучение отдельных тем;	– опрос (тестирование) по теории; – контрольная работа;
3.	Криптографические средства защиты информации	2		2	16	1-4	– проработка лекций и работа с литературой по теме; – решение задач; – дополнительное изучение отдельных тем;	– опрос (тестирование) по теории; – контрольная работа;
4.	Защита информационных и операционных систем	2		2	16	1-4	– проработка лекций и работа с литературой по теме; – решение задач; – дополнительное изучение отдельных тем;	– опрос (тестирование) по теории; – контрольная работа;
	Всего часов:	6		6	60			

Приложение № 2

Рейтинг-план дисциплины

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1 (Разделы 1. 2 по РПД)				
Текущий контроль			12	20
1. Работа на занятиях	2	15	12	20
Рубежный контроль				
1.Контрольная работа	3	5	10	15
Модуль 2 (Разделы 3, 4 по РПД)				
Текущий контроль			13	20
1. Работа на занятиях	4	5	13	20
Рубежный контроль				
1.Контрольная работа	3	5	10	15
Поощрительные баллы				
1. Выполнение заданий повышенной трудности	2	5	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
Посещение лекционных и практ. занятий			-7	0
Итоговый контроль				
1.Экзамен			0	30
ИТОГО			**45**	**110**