ФГБОУ ВО «УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИИ»
СИБАЙСКИЙ ИНСТИТУТ (ФИЛИАЛ)
ФАКУЛЬТЕТ ЭКОНОМИКИ И ПРАВА

Актуализировано:
на заседании кафедры
протокол № 12 от «21» июня 2023 г.

Зав. Кафедрой / Якшимбетова Г.И..

Согласовано:
Председатель УМК факультета

Янтилина Н.Т.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина: **Информационная безопасность**

(наименование дисциплины)

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

программа бакалавриата

Направление подготовки:
38.03.01 ЭКОНОМИКА
(указывается код и наименование направления подготовки (специальности))

Направленность (профиль) подготовки:
«Бухгалтерский учет, анализ и аудит»
(указывается наименование направленности (профиля) подготовки)

Квалификация:
Бакалавр

Разработчик (составитель)
К.ф-м.н, доцент _____/ Хисаметдинов Ф.З.
(должность, ученая степень, ученое звание)

Для приема: 2023г.

Сибай 2023 г.

Составитель:

Рабочая программа дисциплины *утверждена* на заседании кафедры протокол от «31» августа 2021 г. № 1

Заведующий кафедрой _____/ Ситнова И.А.

Рабочая программа дисциплины актуализирована на заседании кафедры экономики и менеджмента протокол от «22» июня 2022 г. № 11

Заведующий кафедрой _____/ Якшимбетова Г.И./

Рабочая программа дисциплины актуализирована на заседании кафедры экономики и менеджмента протокол от «21» июня 2023 г. № 12

Заведующий кафедрой _____/ Якшимбетова Г.И./

Дополнения и изменения, внесенные в рабочую программу дисциплины_____
утверждены на заседании кафедры, протокол № ____ от «____» _____ 20____ г.

Заведующий кафедрой _____/ _____/

Дополнения и изменения, внесенные в рабочую программу дисциплины_____
утверждены на заседании кафедры, протокол № ____ от «____» _____ 20____ г.

Заведующий кафедрой _____/ _____/

Дополнения и изменения, внесенные 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 компетенцийс 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

По итогам освоения дисциплины обучающийся должен достичь следующих результатов обучения:

Категория (группа) компетенций	Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
Профессиональные компетенции	*ПК-1. Способен проводить финансовый анализ, бюджетирование и управление денежными потоками*	*ПК-1.1.* ***Знает*** *теоретические аспекты проведения финансового анализа, бюджетирования и управления денежными потоками; типовые методики проведения финансового анализа, бюджетирования и управления денежными потоками; особенности применения методик проведения финансового анализа, бюджетирования и управления денежными потоками*	***Знает:*** *теоретические аспекты проведения финансового анализа, бюджетирования и управления денежными потоками; типовые методики проведения финансового анализа, бюджетирования и управления денежными потоками; особенности применения методик проведения финансового анализа, бюджетирования и управления денежными потоками*
		ПК-1.2. ***Умеет*** *демонстрировать способность проведения финансового анализа, бюджетирования и управления денежными потоками*	***Умеет:*** *демонстрировать способность проведения финансового анализа, бюджетирования и управления денежными потоками*
		ПК-1.3. ***Владеет*** *навыками проведения финансового анализа, бюджетирования и управления денежными потоками*	***Владеет*** *навыками проведения финансового анализа, бюджетирования и управления денежными потоками*

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «*Информационная безопасность*» относится к части, формируемой участниками образовательных отношений.

Дисциплина изучается на **4** курсе в **7** семестре.

Цель дисциплины: формирование у студентов системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.

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 **ПК-1 Способен проводить финансовый анализ, бюджетирование и управление денежными потоками (зачет)**

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		Зачтено	Не зачтено
ПК-1.1. ***Знает*** *теоретические аспекты проведения финансового анализа, бюджетирования и управления денежными потоками; типовые методики проведения финансового анализа, бюджетирования и управления денежными потоками; особенности применения методик проведения финансового анализа, бюджетирования и управления денежными потоками*	***Знает:*** *теоретические аспекты проведения финансового анализа, бюджетирования и управления денежными потоками; типовые методики проведения финансового анализа, бюджетирования и управления денежными потоками; особенности применения методик проведения финансового анализа, бюджетирования и управления денежными потоками*	Знает	Не знает
ПК-1.2. ***Умеет*** *демонстрировать способность проведения финансового анализа, бюджетирования и управления денежными потоками*	***Умеет:*** *демонстрировать способность проведения финансового анализа, бюджетирования и управления денежными потоками*	Умеет	Не умеет
ПК-1.3. ***Владеет*** *навыками проведения финансового анализа, бюджетирования и управления денежными потоками*	***Владеет*** *навыками проведения финансового анализа, бюджетирования и управления денежными потоками*	Владеет	Не владеет

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 наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**
ПК-1.1. ***Знает*** *теоретические аспекты проведения финансового анализа, бюджетирования и управления денежными потоками; типовые методики проведения финансового анализа, бюджетирования и управления денежными потоками; особенности применения методик проведения финансового анализа, бюджетирования и управления денежными потоками*	***Знает:*** *нормативно-правовую базу расчета и анализа экономических показателей результатов деятельности организации; типовые методики расчета и анализа экономических показателей результатов деятельности организации; особенности применения методик расчета и анализа экономических показателей результатов деятельности организации*	устный опрос, проверка заданий в рабочей тетради, тестирование, решение задач, письменные ответы на вопросы, проверка конспектов научной и учебной литературы, контрольная работа, написание статьи
ПК-1.2. ***Умеет*** *демонстрировать способность проведения финансового анализа, бюджетирования и управления денежными потоками*	***Умеет:*** *демонстрировать способность расчета и анализа экономических показателей результатов деятельности организации*	устный опрос, проверка заданий в рабочей тетради, тестирование, решение задач, письменные ответы на вопросы, проверка конспектов научной и учебной литературы, контрольная работа, написание статьи

ПК-1.3. ***Владеет** навыками проведения финансового анализа, бюджетирования и управления денежными потоками*	***Владеет**:* *навыками расчета и анализа экономических показателей результатов деятельности организации;* *современным инструментарием, техническими средствами, информационными технологиями расчета и анализа экономических показателей результатов деятельности организации*	устный опрос, проверка заданий в рабочей тетради, тестирование, решение задач, письменные ответы на вопросы, проверка конспектов научной и учебной литературы, контрольная работа, написание статьи

Критерии оценивания:

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 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).

Шкалы оценивания:

для зачета:

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

РЕЙТИНГ-ПЛАН ДИСЦИПЛИНЫ

Информационная безопасность
(название дисциплины согласно рабочему учебному плану)

Направление **Экономика**
Направленность (профиль) подготовки **«Бухгалтерский учет, анализ и аудит»**
курс 4, семестр 7

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1				
Текущий контроль			**10**	**20**
1. Аудиторная работа	2	2	4	6
2. Выполнение самостоятельных работ	4	2	6	8
Рубежный контроль			**10**	**20**
1. Защита лабораторных работ		1	**10**	**20**
Модуль 2				
Текущий контроль			**10**	**14**
1. Аудиторная работа	3	2	6	6
2. Выполнение самостоятельных работ	4	2	4	8
Рубежный контроль			**10**	**20**
1. Защита лабораторных работ		1	**10**	**20**
Поощрительные баллы				
Выполнение заданий повышенной трудности	5	2	0	**10**
Посещаемость (баллы вычитываются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение лабораторных занятий			0	-10

Итоговый контроль				
Зачет				
ИТОГО			**60**	**110**

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ЗАЧЕТА

1. Классификация средств защиты информации и программного обеспечения от несанкционированного доступа и копирования.
2. Активные и пассивные методы защиты программного обеспечения.
3. Средства и методы защиты дисков от несанкционированного доступа и копирования.
4. Способы создания ключевых носителей информации.
5. Привязка программных средств к конкретному компьютеру.
6. Критерии выбора системы защиты.
7. Технические устройства защиты информации и программного обеспечения.
8. Принципы действия электронных ключей.
9. Место информационной безопасности в национальной безопасности РФ.
10. Цели и задачи обеспечения информационной безопасности.
11. Составляющие информационной безопасности.
12. Правовые, организационные, технические, программно-аппаратные и криптографические методы обеспечения информационной безопасности.
13. Виды и источники угроз информационной безопасности РФ.
14. Структура государственной системы обеспечения информационной безопасности РФ.
15. Применение патентования и норм авторского права при защите программных продуктов.
16. Основные положения Закона об охране программ для ЭВМ и баз данных.
17. Критерий надежности шифрования.
18. Основные криптографические приемы.
19. Блочное шифрование.
20. Схема поточного шифрования.
21. Использование генераторов псевдослучайных чисел для шифрования.
22. Шифрование с открытым ключом.
23. Идентификация электронной подписи.
24. Хеширование данных.
25. Стандарты шифрования данных.
26. Основы симметричного шифрования данных.
27. Блочное и поточное шифрование данных.
28. Асимметричная криптография и электронная цифровая подпись.
29. Криптосистемы. Системы управления ключами, сертификация ключей.
30. Сжатие данных как способ кодирования.
31. Кодирование Хаффмена.
32. Адаптивное сжатие по Хаффмену.
33. Арифметическое кодирование.
34. Алгоритм сжатия Lempel-Ziv-Welch.
35. Организация систем защиты информации от несанкционированного доступа.
36. Идентификация и установление подлинности.
37. Установление подлинности пользователя, файла, вычислительной системы.
38. Выбор пароля.
39. Установление полномочий.
40. Матрица установления полномочий.
41. Иерархические системы установления полномочий.
42. Системы регистрации пользователей, событий, используемых ресурсов.
43. Компьютерное пиратство.
44. Компьютерные вирусы.

45. Вирусы, заражающие загрузочные сектора.
46. Файловые вирусы.
47. Загрузочно-файловые вирусы.
48. Полиморфные вирусы.
49. Организационные и программные способы борьбы с вирусным заражением программного обеспечения.
50. Защита информации в компьютерных сетях.
51. Классификация удаленных атак.
52. Методы защиты от них.
53. Технологии VPN.
54. Шифрование данных на сетевом уровне.
55. Применение технологий шифрования данных совместно с межсетевыми экранами.
56. Защищенные протоколы прикладных уровней.
57. Межсетевые экраны.
58. Модель безопасности современной операционной системы.

Критерии оценки (в баллах):

20-30 баллов выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание функциональных возможностей, терминологии, основных элементов, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок;

10-19 баллов выставляется студенту, если при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос. Студент не решил задачу или при решении допущены грубые ошибки;

0-9 баллов выставляется студенту, если он отказался от ответа или не смог ответить на вопросы билета, ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний при выполнении практических заданий. Студент не смог ответить ни на один дополнительный вопрос.

Критерии оценки (для очно-заочной и заочной форм обучения):

«**Зачтено**» выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности. При выполнении практической части работы допущены несущественные ошибки;

«Не зачтено» выставляется студенту, если ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Студент не смог ответить ни на один дополнительный вопрос.

ПЛАНЫ СЕМИНАРСКИХ ЗАНЯТИЙ

ВОПРОСЫ ДЛЯ АУДИТОРНОЙ РАБОТЫ

1) Основы защиты информации. Классификация средств защиты информации и программного обеспечения от несанкционированного доступа и копирования: средства собственной защиты, средства защиты в составе вычислительной системы, средства защиты

с запросом информации. Активные и пассивные методы защиты программного обеспечения. Средства и методы защиты дисков от несанкционированного доступа и копирования. Способы создания ключевых носителей информации. Привязка программных средств к конкретному компьютеру. Критерии выбора системы защиты. Технические устройства защиты информации и программного обеспечения. Принципы действия электронных ключей.

2) Правовые основы защиты информации. Место информационной безопасности в национальной безопасности РФ. Цели и задачи обеспечения информационной безопасности. Составляющие информационной безопасности. Правовые, организационные, технические, программно-аппаратные и криптографические методы обеспечения информационной безопасности. Виды и источники угроз информационной безопасности РФ. Структура государственной системы обеспечения информационной безопасности РФ. Применение патентования и норм авторского права при защите программных продуктов. Основные положения Закона об охране программ для ЭВМ и баз данных.

3) Криптографические средства защиты информации. Основы криптографии. Критерий надежности шифрования. Основные криптографические приемы. Блочное шифрование. Схема поточного шифрования. Использование генераторов псевдослучайных чисел для шифрования. Шифрование с открытым ключом. Идентификация электронной подписи. Хеширование данных. Стандарты шифрования данных. Основы симметричного шифрования данных. Блочное и поточное шифрование данных. Асимметричная криптография и электронная цифровая подпись. Криптосистемы. Системы управления ключами, сертификация ключей. Сжатие данных как способ кодирования. Кодирование Хаффмена. Адаптивное сжатие по Хаффмену. Арифметическое кодирование. Алгоритм сжатия Lempel-Ziv-Welch.

4) Защита информационных и операционных систем. Организация систем защиты информации от несанкционированного доступа. Идентификация и установление подлинности. Установление подлинности пользователя, файла, вычислительной системы. Выбор пароля. Установление полномочий. Матрица установления полномочий. Иерархические системы установления полномочий. Системы регистрации пользователей, событий, используемых ресурсов. Компьютерное пиратство. Компьютерные вирусы. Вирусы, заражающие загрузочные сектора. Файловые вирусы. Загрузочно-файловые вирусы. Полиморфные вирусы. Организационные и программные способы борьбы с вирусным заражением программного обеспечения. Защита информации в компьютерных сетях. Классификация удаленных атак. Методы защиты от них. Технологии VPN. Шифрование данных на сетевом уровне. Применение технологий шифрования данных совместно с межсетевыми экранами. Защищенные протоколы прикладных уровней. Межсетевые экраны. Модель безопасности современной операционной системы.

ТЕСТОВЫЕ ЗАДАНИЯ
«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 (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

Количество баллов	Критерии оценивания на вопросы для аудиторной работы
2	При ответе студент демонстрирует свободное владение заявленной проблемой, умение грамотно использовать физический понятийный аппарат в рамках рассматриваемого вопроса, не использует конспект семинарского занятия как план при ответе.
1	При ответе на вопрос студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Имеются принципиальные ошибки в логике построения ответа на вопрос.
0	Дан в целом неверный ответ

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. Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета,

2016. - 74 с. : схем., табл., ил. - Библиогр. в кн. - ISBN 978-5-9275-2364-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=493175.

Дополнительная литература:

1. Поляк-Брагинский, А. Локальная сеть. Самое необходимое. / А. Поляк-Брагинский .— 2-е изд.— СПб. : БХВ-Петербург, 2011 .— 576 с.
2. 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
3. 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. Университетская библиотека онлайн. http//www.biblioclub.ru
2. Электронно- библиотечная система «Лань». http//www.e.lanbok.com
3. Российская научная электронная библиотека, интегрированная с Российским индексом научного цитирования (РИНЦ). http//www.elibrary.ru

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 320	Лекции	Демонстрационное оборудование: доска, проектор – 1 шт., переносной экран – 1 шт. Специализированная мебель: столы, стулья (26 посадочных мест).
Аудитория 322	Практические занятия	Демонстрационное оборудование: доска, проектор – 1 шт., переносной экран – 1 шт. Специализированная мебель: столы, стулья (26 посадочных мест).

Приложение 1

ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
СИБАЙСКИЙ ИНСТИТУТ (ФИЛИАЛ)
ФАКУЛЬТЕТ ЭКОНОМИКИ И ПРАВА

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Информационная безопасность** на **1** семестр
(наименование дисциплины)

ОЧНАЯ
форма обучения

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	2 / 72
Учебных часов на контактную работу с преподавателем:	36
лекций	18
практических/ семинарских	18
лабораторных	-
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
из них, предусмотренные на выполнение курсовой работы/курсового проекта	-
Учебных часов на самостоятельную работу обучающихся (СР)	35,8
из них, предусмотренные на выполнение курсовой работы/курсового проекта	-
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	-

Форма (ы) контроля:

зачет – 7семестр

№ 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	КСР	ЛР	СРС			
1	2	3	4	5	6	7	8	9
1.	Основы защиты информации	4	4		9	1-2 / 1-3	Изучение доп. материала	самостоятельная работа, лабораторная работа
2.	Правовые основы защиты информации	4	4		9	1-2 / 1-3	Изучение доп. материала	самостоятельная работа, лабораторная работа
3.	Криптографические средства защиты информации	4	4		9	1-2 / 1-3	Изучение доп. материала	самостоятельная работа, лабораторная работа
4.	Защита информационных и операционных систем	6	6		8,8	1-2 / 1-3	Изучение доп. материала	самостоятельная работа, лабораторная работа
	Всего	**18**	**18**		**35,8**			
	ФКР				**0,2**			
	Итого	**18**	**18**		**36**			

ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
СИБАЙСКИЙ ИНСТИТУТ (ФИЛИАЛ)
ФАКУЛЬТЕТ ЭКОНОМИКИ И ПРАВА

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Информационная безопасность** на **1** семестр
(наименование дисциплины)

ОЧНО-ЗАОЧНАЯ
форма обучения

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	
Учебных часов на контактную работу с преподавателем:	
лекций	
практических/ семинарских	
лабораторных	
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	
из них, предусмотренные на выполнение курсовой работы/курсового проекта	
Учебных часов на самостоятельную работу обучающихся (СР)	
из них, предусмотренные на выполнение курсовой работы/курсового проекта	
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	

Форма (ы) контроля:

зачет – 7 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	КСР	ЛР	СРС			
1	2	3	4	5	6	7	8	9
1.	Основы защиты информации					1-2 / 1-3	Изучение доп. материала	самостоятельная работа, лабораторная работа
2.	Правовые основы защиты информации					1-2 / 1-3	Изучение доп. материала	самостоятельная работа, лабораторная работа
3.	Криптографические средства защиты информации					1-2 / 1-3	Изучение доп. материала	самостоятельная работа, лабораторная работа
4.	Защита информационных и операционных систем					1-2 / 1-3	Изучение доп. материала	самостоятельная работа, лабораторная работа
	Всего							
	ФКР							
	Итого							

ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
СИБАЙСКИЙ ИНСТИТУТ (ФИЛИАЛ)
ФАКУЛЬТЕТ ЭКОНОМИКИ И ПРАВА

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Информационная безопасность** на **1** семестр
(наименование дисциплины)

ЗАОЧНАЯ
форма обучения

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	
Учебных часов на контактную работу с преподавателем:	
лекций	
практических/ семинарских	
лабораторных	
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	
из них, предусмотренные на выполнение курсовой работы/курсового проекта	
Учебных часов на самостоятельную работу обучающихся (СР)	
из них, предусмотренные на выполнение курсовой работы/курсового проекта	
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	

Форма (ы) контроля:

зачет – 7семестр

№ 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	КСР	ЛР	СРС			
1	2	3	4	5	6	7	8	9
1.	Основы защиты информации					1-2 / 1-3	Изучение доп. материала	самостоятельная работа, лабораторная работа
2.	Правовые основы защиты информации					1-2 / 1-3	Изучение доп. материала	самостоятельная работа, лабораторная работа
3.	Криптографические средства защиты информации					1-2 / 1-3	Изучение доп. материала	самостоятельная работа, лабораторная работа
4.	Защита информационных и операционных систем					1-2 / 1-3	Изучение доп. материала	самостоятельная работа, лабораторная работа
	Всего							
	ФКР							
	Итого							