МИНОБРНАУКИ РОССИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г. ШУХОВА»

(БГТУ им. В.Г. Шухова)

СОГЛАСОВАНО
Директор института заочного образования
_____ С.Е. Спесивцева
«25» 05 2021 г.

УТВЕРЖДАЮ
Директор института
_____ Ю.А. Дорошенко
«25» 05 2021 г.

РАБОЧАЯ ПРОГРАММА
дисциплины (модуля)

Информационная безопасность

направление подготовки
38.03.05 Бизнес-информатика

Направленность программы (профиль):
Технологическое предпринимательство

Квалификация
Бакалавр

Форма обучения
заочная

Институт экономики и менеджмента

Кафедра экономики и организации производства

Белгород – 2021

Рабочая программа составлена на основании требований:

Федерального государственного образовательного стандарта высшего образования по направлению подготовки 38.03.05 Бизнес-информатика - бакалавриат, утвержден Приказом Министерства науки и высшего образования Российской Федерации от 29 июля 2020 г. № 838, введенного в действие в 2021 году

- учебного плана, утвержденного ученым советом БГТУ им. В. Г. Шухова в 2021 году

Составитель: к.э.н., доц. (А.А. Рябов)

Рабочая программа согласована с выпускающей кафедрой
экономика и организация производства

Заведующий кафедрой (Селиверстов Ю.И.)

«13» 05 2021 г.

Рабочая программа обсуждена на заседании кафедры
экономики и организации производства
(наименование кафедры)

«13» 05 2021 г., протокол № 8

Заведующий кафедрой д.э.н., профессор (Ю.И. Селиверстов)

Рабочая программа одобрена методической комиссией института
института экономики и менеджмента

«18» 05 2021 г., протокол № 9

Председатель к.э.н., доц. Л.И. Журавлева

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Наименование показателя оценивания результата обучения по дисциплине
ПК-2 Способен выполнять работы по сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы	ПК-2.6. Проводит аудит безопасности информационных систем, использует современные методики защиты информации	**Знания:** - этапов проектирования систем, комплексов, средства и технологий обеспечения информационной безопасности. **Умения:** – формировать требования к проектированию систем, комплексов, средства и технологий обеспечения информационной безопасности. **Навыки:** - разработки систем, комплексов, средства и технологий обеспечения информационной безопасности с учетом особенностей объектов защиты.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1. Компетенция ПК-2 Способен выполнять работы по сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы**.**

Данная компетенция формируется следующими дисциплинами:

Стадия	Наименования дисциплины
1.	Моделирование бизнес-процессов
2.	Электронная коммерция
3.	Экономика и эффективность информационных систем
4.	Информационная безопасность
5.	Управление проектами в сфере ИКТ
6.	Управление стоимостью компании
7.	Человеко-машинное взаимодействие
8.	Организационное обеспечение ИТ-услуг
9.	Регламентация ИТ-услуг и процессов
10.	Информационные системы управления производственной компанией

3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 5 зач. единиц, 180 часов.

Дисциплина реализуется в рамках практической подготовки:

Форма промежуточной аттестации экзамен.

Вид учебной работы	Всего часов	Семестр № 8	Семестр № 9
Общая трудоемкость дисциплины, час	180	2	178
Контактная работа (аудиторные занятия), в т.ч.:	10	2	8
лекции	4	2	2
лабораторные	4		4
практические			
групповые консультации в период теоретического обучения и промежуточной аттестации	2		2
Самостоятельная работа студентов, включая индивидуальные и групповые консультации, в том числе:	170		170
Курсовой проект			
Курсовая работа			
Расчетно-графическое задание	18		18
Индивидуальное домашнее задание			
Самостоятельная работа на подготовку к аудиторным занятиям (лекции, лабораторные занятия)	116		116
Экзамен	36		36

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Наименование тем, их содержание и объем

Курс 4 Семестр 8,9

№ п/п	Наименование раздела (модуля)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа
1	2	3	4	5	6
1	**Предмет, методология и понятийный аппарат курса.** Предмет информационной безопасности. Концепция информационной безопасности, важность и ценность информации, модели информационной безопасности, физические и программные каналы утечки информации, закладки и вирусы как средства атаки на информационные системы, парольная защита, аутентификация,	0,5		0,5	20

	разграничение прав доступа, способы закрытия информации и их значение. Аппаратные и программно-аппаратные средства защиты информационной безопасности.				
2	**Разрушающие программные воздействия и средства несанкционированного доступа (НСД).** Технологии защиты от НСД. Защита операционных систем. Безопасность компьютерной сети. Закрытие информации шифрованием, финансовые применения и протоколы.	0,5		0,5	20
3	**Инфраструктура открытых ключей. Защищенные протоколы.** Краткая история развития криптологии. Основные понятия и определения. Подстановочные и перестановочные шифры. Американский стандарт шифрования DES: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости. Отечественный стандарт шифрования данных ГОСТ 28147-89: алгоритм, скорость работы на различных платформах, режимы пользования. Асимметричные системы шифрования (системы с открытым ключом).	0,5		0,5	20
4	**Межсетевые экраны, классы их защищенности.** Политика безопасности и стратегия создания брандмауэра. Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты.	0,5		0,5	20
5	**Обнаружение атак в глобальных сетях.** Виртуальные сети и прозрачные сетевые службы. Построение защищенных ВЧС. Многоуровневая защита информации в компьютерных системах и сетях.	0,5		0,5	20
6	**Информационная безопасность банковских систем и систем электронной коммерции.** Общие сведения об электронной цифровой подписи (ЭЦП). Алгоритм ЭЦП в симметричной криптосистеме. Алгоритм ЭЦП в асимметричной криптосистеме. Проблема обмена открытыми ключами при ЭЦП. Сложные математические задачи и алгоритмы ЭЦП с открытыми ключами. Алгоритм DSA. Алгоритм ГОСТ Р34.10–94. Стандарт ЭЦП Р34.10–2001.	1		1	16

	ВСЕГО	**4**		**4**	**116**

4.2. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	К-во часов	К-во часов СРС
семестр №9				
1	Разрушающие программные воздействия и средства несанкционированного доступа (НСД)	Комплексная система обеспечения информационной безопасности.	1	4
2	Инфраструктура открытых ключей. Защищенные протоколы.	Современные приложения криптографии	0,25	2
		Изучение ППП систем криптографической защиты информации, классическая криптография и распределение ключей	0,25	1
		Практическое применение криптографии с открытым ключом. Пакет PGP	0,25	1
3	Межсетевые экраны, классы их защищенности.	Методы аутентификации	0,25	4
4	Обнаружение атак в глобальных сетях	Основные технологии построения защищенных ЭИС	1	4
5	Информационная безопасность банковских систем и систем электронной коммерции	Федеральный закон «Об электронной цифровой подписи». Электронная цифровая подпись (ЭЦП)	0,5	2
		Криптосистема операционной системы Windows. CryptoAPI: шифрование и дешифрование в CryptoAPI, ЭЦП в проектах на CryptoAPI	0,5	2
		ИТОГО:	4	20

4.3. Содержание расчетно-графического задания, индивидуальных домашних заданий.

Учебным планом предусмотрено расчетно-графическое задание (РГЗ).

Успешное выполнение РГЗ во многом зависит от четкого соблюдения установленных сроков и последовательного выполнения отдельных этапов работы:

1. Выбор темы не позднее, чем за 1 месяц до сдачи работы

2. Подбор научной литературы

3. Написание и представление преподавателю работы не позднее, чем за 7 дней до ее сдачи.

Оформление работы

Текстовый материал в работе должен быть изложен согласно правилам оформления студенческих работ.

Объем индивидуального задания 15-25 стр.

Структура и содержание РГЗ

Структура работы состоит из следующих частей:

- Введение
- Раздел 1. Теоретические основы изучаемой проблемы
- Раздел 2. Анализ рассматриваемой проблемы на конкретном примере
- Заключение
- Список литературы

В работе следует отразить вопросы, касающиеся рассматриваемой проблемы, в соответствии с приведенным ниже содержанием.

Введение. Во вступительной части рассматриваются основные тенденции изучения и развития проблемы, обосновывается актуальность проблемы, а также формируются цель и задачи работы.

Раздел 1. Теоретические основы изучения проблемы. В данном разделе, прежде всего, необходимо охарактеризовать объект и предмет исследования. Затем оценить степень изученности данной проблемы в научной литературе и привести различные точки зрения по данному вопросу. В процессе изучения имеющихся литературных источников по исследуемой проблеме очень важно найти сходство и различия точек зрения разных авторов, дать их анализ и обосновать свою позицию по данному вопросу.

Раздел 2. Анализ рассматриваемой проблемы на конкретном примере

При выполнении этой части работы студенты должны провести анализ состояния дел по данному вопросу, дать характеристику имеющимся особенностям и высказать свое мнение для их корректировки в случае необходимости.

Заключение

В заключении должны быть приведены основные выводы, вытекающие из результатов проведенного исследования.

Порядок выбора темы

Выбор темы определяется в соответствии со следующей схемой.

Номер темы ИДЗ выбирается в зависимости от номера фамилии студента в журнале группы.

Порядок проверки и защиты ТГЗ

Задание представляется преподавателю на проверку не позднее, чем за 7 дней до ее сдачи.

Ознакомившись с работой, преподаватель принимает решение о форме ее приема. Задание либо зачитывается, либо назначается время сдачи.

Замечания о необходимости доработок содержания оформляются преподавателем на титульном листе. Защита предполагает краткий доклад по ключевым вопросам.

Если работа не представлена в срок, то ее сдача производится комиссии, назначаемой зав. кафедрой.

Темы РГЗ

1. Доктрина информационной безопасности РФ.
2. Информационное обеспечение государственной политики РФ.
3. Развитие современных информационных технологий.
4. Угрозы информационной безопасности РФ.
5. Информационно-психологическое оружие.
6. Информациоино-психологическая война.
7. Защита информационных ресурсов от несанкционированного доступа.
8. Информационный терроризм.
9. Международное сотрудничество РФ в области защиты информации.
10. Государственная тайна.
11. Служебная тайна.
12. Коммерческая тайна.
13. Персональные данные.
14. Личная тайна.
15. Семейная тайна.
16. Тайна ЗАГСа.
17. Врачебная (медицинская) тайна.
18. Тайна вероисповедания.
19. Тайна исповеди.
20. Адвокатская тайна.
21. Тайна следствия.
22. Судебная тайна.
23. Тайна нотариата.
24. Налоговая тайна.
25. Банковская тайна.
26. Журналистская тайна (тайна СМИ).
27. Авторское право.

4.4. Содержание курсового проекта/работы

Не предусмотрено учебным планом.

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5.1. Реализация компетенций

1. Компетенция ПК-2. Способен выполнять работы по сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы**.**

Наименование индикатора достижения компетенции	Используемые средства оценивания
ПК-2.6. Проводит аудит безопасности информационных систем, использует современные методики защиты информации	экзамен, защита РГЗ, лабораторные работы, собеседование

5.2. Типовые контрольные задания для промежуточной аттестации

Перечень контрольных вопросов (типовых заданий) для экзамена

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1	Предмет, методология и понятийный аппарат курса.	1.Место информационной безопасности экономических систем в национальной безопасности страны. Информационная безопасность в условиях функционирования в России глобальных сетей. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Международные стандарты информационного обмена. 2.Основные положения теории информационной безопасности информационных систем. Конфиденциальность. Целостность. Доступность. 3.Основные положения теории информационной безопасности информационных систем. Объект и субъект доступа. Средство работы с информацией. Несанкционированный доступ к информации. 4.Основные положения теории информационной безопасности информационных систем. Идентификация. Аутентификация. 5.Основные положения теории информационной безопасности информационных систем. Принципы распределения прав и ответственности. 6.Модели безопасности и их применение. Модели доступа. Решетчатая модель. Модель Белл-ЛаПадула. Модель безопасности. 7.Модели безопасности и их применение. Модели доступа. Модель Биба. Модель Гогена-Мезигера. Модель безопасности. 8.Модели безопасности и их применение. Модели доступа. Модель Сазерленда. Модель Кларка-Вильсона. Модель безопасности. 9.Модели безопасности и их применение. Модели доступа. Обязательное управление доступом и переназначаемое управление доступом Доступ по правилам и доступ по ролям. Модель безопасности. 10.Таксономия (классификация) нарушений информационной безопасности вычислительной системы

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		и причины, обуславливающие их существование. Три вида возможных нарушений информационной системы. Нарушения конфиденциальности. 11.Таксономия (классификация) нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Три вида возможных нарушений информационной системы. Изменения в системе. 12.Таксономия (классификация) нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Три вида возможных нарушений информационной системы. Утрата работоспособности или производительности.
2	Разрушающие программные воздействия и средства несанкционированного доступа (НСД)	13.Анализ способов нарушений информационной безопасности. Виды противников или "нарушителей". Источники и мотивы нарушений. Непреднамеренные действия сотрудников. 14.Анализ способов нарушений информационной безопасности. Виды противников или "нарушителей". Источники и мотивы нарушений. Преднамеренные действия сотрудников. 15.Анализ способов нарушений информационной безопасности. Виды противников или "нарушителей". Источники и мотивы нарушений. Действия сторонних лиц криминального характера. 16.Понятие угрозы. Классификация угроз информационной безопасности. Угрозы, не зависящие от человека. 17.Понятие угрозы. Классификация угроз информационной безопасности. Искусственные угрозы. 18.Понятие угрозы. Классификация угроз информационной безопасности. Угрозы информационной безопасности от использования специальных средств. 19.Атака. Локальная и удаленная атака. Хакер. Кракер. Фрикер. 20.Типовая атака на систему. 21.Локальные атаки. Социальная инженерия. 22.Закладки в аппаратном обеспечении. 23.Преодоление ограничений доступа на уровне firmware. 24.Получение доступа на этапе загрузки ОС.
3	Инфраструктура открытых ключей. Защищенные протоколы.	25. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи. Исторические пример. Шифр Цезаря. Привести пример. 26. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи. Исторические пример. Квадрат Полибия (тюремная азбука). Привести пример. 27. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи. Исторические пример. Квадрат Кардано. Привести

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		пример. 28. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи. Исторические примеры. Таблица Виженера. Многоалфавитная замена. Привести пример. 29. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи. Исторические примеры. Шифрование по книге. Привести пример. 30. Методы криптографии. Практически стойкий шифр. Абсолютная стойкость шифра. Атака на основе шифротекста, на основе известного открытого текста, на основе выбранного открытого текста. Надежный шифр. 31. Методы криптографии. Поточное шифрование. Исключающее ИЛИ (сложение по модулю 2). 32. Методы криптографии. Линейные регистры сдвига. Привести пример. 33. Методы криптографии. Блочное шифрование. 34. Методы криптографии. Симметричное шифрование (шифрование на секретном ключе). Асимметричное шифрование (шифрование на открытом ключе). 35. Методы криптографии. Электронная цифровая подпись. 36.Методы криптографии. Хэш-функция в электронной цифровой подписи.
4	Межсетевые экраны, классы их защищенности.	37.Защита. Использование защищенных компьютерных систем. Механизмы защиты. Нормативно-правовые, морально-этические, организационные и физические (технические) средства защиты. 38.Основные технологии построения защищенных ЭИС. Контроль жизненного цикла программного обеспечения с точки зрения информационной безопасности. Мероприятия, осуществляемые при создании ИС. Сертификация программного обеспечения. 39.Основные технологии построения защищенных ЭИС. Контроль жизненного цикла программного обеспечения с точки зрения информационной безопасности. Мероприятия, осуществляемые в процессе эксплуатации ИС. 40.Концепция информационной безопасности. Концепция информационной безопасности предприятия. Управления рисками. Политика информационной безопасности. 41.Защита. Механизмы защиты. Физические средства защиты. 42.Аппаратно-программные средства защиты. Системы идентификации и аутентификации пользователей. Системы шифрования дисковых данных. 43.Аппаратно-программные средства защиты. Системы аутентификации электронных данных.

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		44.Аппаратно-программные средства защиты. Средства управления криптографическими ключами.
5	Обнаружение атак в глобальных сетях	45.Атаки на средства аутентификации. Биометрические средства аутентификации. 46.Атаки на средства аутентификации. Токены. 47.Атаки на средства аутентификации. Пароли. Способы хранения паролей Системной политики паролей 48.Атаки на средства аутентификации. Пароли. Имитация системного приглашения Атака на слабость паролей. 49.Атаки класса "повышение привилегий". 50.Постороннее программное обеспечение. 51.Удаленные атаки. Зловредные программы. 52.Понятия о видах вирусов. 53.Удаленные атаки. Атаки на отказ в обслуживании. Маскировка. 54.Удаленные атаки. Атаки на маршрутизацию. Переполнение буфера. 55.Удаленные атаки. Атаки на севрверы: *CGI* и *HTTP*. Атаки на клиентов: *ActiveX, Java*. 56.Удаленные атаки. Атаки на поток данных. Активные атаки. Атака повтором. 57.Атака "злоумышленник-посредник". Атаки на основе сетевой маршрутизации. Перехват сессии.
6	Информационная безопасность банковских систем и систем электронной коммерции	58.Информационная безопасность при подключении к Internet. Межсетевые экраны. 59.Информационная безопасность при подключении к Internet. Управляемые коммутаторы. 60.Информационная безопасность при подключении к Internet. Сетевые фильтры. 61.Информационная безопасность при подключении к Internet. Шлюзы сеансового уровня. Посредники прикладного уровня. 62.Информационная безопасность при подключении к Internet. Инспекторы состояния.

5.3. Типовые контрольные задания (материалы) для текущего контроля в семестре

Текущий контроль в семестре осуществляется в форме выполнения и защиты лабораторных работ, а также собеседования. Собеседование проводится в форме ответов на заданные вопросы.

Лабораторные работы. В лабораторном практикуме по дисциплине представлен перечень лабораторных работ, обозначены цель и задачи, необходимые теоретические и методические указания работе, рассмотрен практический пример, даны варианты выполнения и перечень контрольных вопросов.

Защита лабораторных работ возможна после проверки правильности выполнения задания, оформления отчета. Защита проводится в форме

собеседования преподавателя со студентом по теме лабораторной работы. Примерный перечень контрольных вопросов для защиты лабораторных работ представлен в таблице.

№ п/п	Тема лабораторной работы	Содержание вопросов (типовых заданий)
1	Лабораторная работа №1 Комплексная система обеспечения информационной безопасности.	1.Анализ способов нарушений информационной безопасности. Виды противников или "нарушителей". Источники и мотивы нарушений. Непреднамеренные действия сотрудников. 2.Анализ способов нарушений информационной безопасности. Виды противников или "нарушителей". Источники и мотивы нарушений. Преднамеренные действия сотрудников. 3.Анализ способов нарушений информационной безопасности. Виды противников или "нарушителей". Источники и мотивы нарушений. Действия сторонних лиц криминального характера. 4.Понятие угрозы. Классификация угроз информационной безопасности. Угрозы, не зависящие от человека. 5.Понятие угрозы. Классификация угроз информационной безопасности. Искусственные угрозы. 6.Понятие угрозы. Классификация угроз информационной безопасности. Угрозы информационной безопасности от использования специальных средств. 7.Атака. Локальная и удаленная атака. Хакер. Кракер. Фрикер. 8.Типовая атака на систему. 9.Локальные атаки. Социальная инженерия. 10.Закладки в аппаратном обеспечении. 11.Преодоление ограничений доступа на уровне firmware. 12.Получение доступа на этапе загрузки ОС.
2	Лабораторная работа №2 Изучение программных продуктов и систем криптографической защиты информации, классическая криптография и распределение ключей	1. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи. Исторические пример. Шифр Цезаря. Привести пример. 2. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи. Исторические пример. Квадрат Полибия (тюремная азбука). Привести пример. 3. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи. Исторические пример. Квадрат Кардано. Привести пример. 4. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи. Исторические примеры. Таблица Виженера. Многоалфавитная замена. Привести пример. 5. Методы криптографии. Основные принципы

№ п/п	Тема лабораторной работы	Содержание вопросов (типовых заданий)
		криптографии. Шифрование. История тайнописи. Исторические примеры. Шифрование по книге. Привести пример.
3	Лабораторная работа №3 Практическое применение криптографии с открытым ключом. Пакет PGP	1. Методы криптографии. Практически стойкий шифр. Абсолютная стойкость шифра. Атака на основе шифротекста, на основе известного открытого текста, на основе выбранного открытого текста. Надежный шифр. 2. Методы криптографии. Поточное шифрование. Исключающее ИЛИ (сложение по модулю 2). 3. Методы криптографии. Линейные регистры сдвига. Привести пример. 4. Методы криптографии. Блочное шифрование. 5. Методы криптографии. Симметричное шифрование (шифрование на секретном ключе). Асимметричное шифрование (шифрование на открытом ключе). 6. Методы криптографии. Электронная цифровая подпись. 7. Методы криптографии. Хэш-функция в электронной цифровой подписи.
4	Лабораторная работа №4 Межсетевые экраны, классы их защищенности.	1. Защита. Использование защищенных компьютерных систем. Механизмы защиты. Нормативно-правовые, морально-этические, организационные и физические (технические) средства защиты. 2. Основные технологии построения защищенных ЭИС. Контроль жизненного цикла программного обеспечения с точки зрения информационной безопасности. Мероприятия, осуществляемые при создании ИС. Сертификация программного обеспечения. 3. Основные технологии построения защищенных ЭИС. 4. Контроль жизненного цикла программного обеспечения с точки зрения информационной безопасности. Мероприятия, осуществляемые в процессе эксплуатации ИС. 5. Концепция информационной безопасности. Концепция информационной безопасности предприятия. Управления рисками. Политика информационной безопасности. 6. Защита. Механизмы защиты. Физические средства защиты. 7. Аппаратно-программные средства защиты. Системы идентификации и аутентификации пользователей. Системы шифрования дисковых данных.

№ п/п	Тема лабораторной работы	Содержание вопросов (типовых заданий)
		8. Аппаратно-программные средства защиты. Системы аутентификации электронных данных. 9. Аппаратно-программные средства защиты. Средства управления криптографическими ключами.
5	Лабораторная работа №5 Основные технологии построения защищенных ЭИС	1. Атаки на средства аутентификации. Биометрические средства аутентификации. 2. Атаки на средства аутентификации. Токены. 3. Атаки на средства аутентификации. Пароли. Способы хранения паролей Системной политики паролей 4. Атаки на средства аутентификации. Пароли. Имитация системного приглашения Атака на слабость паролей. 5. Атаки класса "повышение привилегий". 6. Постороннее программное обеспечение. 7. Удаленные атаки. Зловредные программы. 8. Понятия о видах вирусов. 9. Удаленные атаки. Атаки на отказ в обслуживании. Маскировка. 10. Удаленные атаки. Атаки на маршрутизацию. Переполнение буфера. 11. Удаленные атаки. Атаки на севрверы: CGI и HTTP. Атаки на клиентов: ActiveX, Java. 12. Удаленные атаки. Атаки на поток данных. Активные атаки. Атака повтором. 13. Атака "злоумышленник-посредник". Атаки на основе сетевой маршрутизации. Перехват сессии.
6	Лабораторная работа №6 Информационная безопасность банковских систем и систем электронной коммерции	1. Информационная безопасность при подключении к Internet. Межсетевые экраны. 2. Информационная безопасность при подключении к Internet. Управляемые коммутаторы. 3. Информационная безопасность при подключении к Internet. Сетевые фильтры. 4. Информационная безопасность при подключении к Internet. Шлюзы сеансового уровня. Посредники прикладного уровня. 5. Информационная безопасность при подключении к Internet. Инспекторы состояния.

5.4. Описание критериев оценивания компетенций и шкалы оценивания

При промежуточной аттестации в форме экзамена, используется следующая шкала оценивания: 2 – неудовлетворительно, 3 – удовлетворительно, 4 – хорошо, 5 – отлично.

Критериями оценивания достижений показателей являются:

Наименование	Критерий оценивания

показателя оценивания результата обучения по дисциплине	
ПК-2 Способен выполнять работы по сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы ПК-2.6. Проводит аудит безопасности информационных систем, использует современные методики защиты информации	
Знания	Знание этапов проектирования систем, комплексов, средства и технологий обеспечения информационной безопасности.
	Объем освоенного материала.
	Полнота ответов на вопросы.
Умения	Формировать требования к проектированию систем, комплексов, средства и технологий обеспечения информационной безопасности. Сравнение, сопоставление, обобщение материала и формулировка выводов.
Навыки	Разработки систем, комплексов, средства и технологий обеспечения информационной безопасности с учетом особенностей объектов защиты. Анализ результатов решенных задач.

Оценка преподавателем выставляется интегрально с учетом всех показателей и критериев оценивания.

Оценка сформированности компетенций по показателю *Знания*.

Критерий	Уровень освоения и оценка			
	2	3	4	5
ПК-2 Способен выполнять работы по сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы ПК-2.6. Проводит аудит безопасности информационных систем, использует современные методики защиты информации				
Знание этапов проектирования систем, комплексов, средства и технологий обеспечения информационной безопасности.	Не знает этапов проектирования систем, комплексов, средства и технологий обеспечения информационной безопасности	Знает этапы проектирования систем, комплексов, средства и технологий обеспечения информационной безопасности, но допускает неточности формулировок	Знает этапы проектирования систем, комплексов, средства и технологий обеспечения информационной безопасности	Знает этапы проектирования систем, комплексов, средства и технологий обеспечения информационной безопасности, может корректно сформулировать их самостоятельно
Объем освоенного материала	Не знает значительной части материала дисциплины	Знает только основной материал дисциплины, не усвоил его деталей	Знает материал дисциплины в достаточном объеме	Обладает твердым и полным знанием материала дисциплины, владеет дополнительными знаниями
Полнота ответов на вопросы	Не дает ответы на большинство вопросов	Дает неполные ответы на все вопросы	Дает ответы на вопросы, но не все - полные	Дает полные, развернутые ответы на поставленные вопросы, делает самостоятельные выводы

Оценка сформированности компетенций по показателю *Умения*.

Критерий	Уровень освоения и оценка			
	2	3	4	5
ПК-2 Способен выполнять работы по сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы ПК-2.6. Проводит аудит безопасности информационных систем, использует современные методики защиты информации				
Формировать требования к проектированию систем, комплексов, средства и технологий обеспечения информационной безопасности	Не умеет формировать требования к проектированию систем, комплексов, средства и технологий обеспечения информационной безопасности	Умеет формировать требования к проектированию систем, комплексов, средства и технологий обеспечения информационной безопасности, но допускает ошибки	Умеет формировать требования к проектированию систем, комплексов, средства и технологий обеспечения информационной безопасности	Умеет правильно формировать требования к проектированию систем, комплексов, средства и технологий обеспечения информационной безопасности, грамотно и самостоятельно делать выводы
Сравнение, сопоставление, обобщение материала и формулировка выводов	Не может сравнивать, сопоставлять, обобщать материал и делать выводы	Может сравнивать, сопоставлять, обобщать материал и делать выводы, но допускает ошибки	Может сравнивать, сопоставлять, обобщать материал и делать выводы	Может правильно сравнивать, сопоставлять, обобщать материал и самостоятельно делать выводы

Оценка сформированности компетенций по показателю *Навыки.*

Критерий	Уровень освоения и оценка			
	2	3	4	5
ПК-2 Способен выполнять работы по сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы ПК-2.6. Проводит аудит безопасности информационных систем, использует современные методики защиты информации				
Разработки систем, комплексов, средства и технологий обеспечения информационной безопасности с учетом особенностей объектов защиты.	Не имеет навыков разработки систем, комплексов, средства и технологий обеспечения информационной безопасности с учетом особенностей объектов защиты.	Имеет недостаточные навыки разработки систем, комплексов, средства и технологий обеспечения информационной безопасности с учетом особенностей объектов защиты.	Разрабатывает системы, комплексы, средства и технологии обеспечения информационной безопасности с учетом особенностей объектов защиты, но допускает неточности	Правильно и самостоятельно разрабатывает системы, комплексы, средства и технологии обеспечения информационной безопасности с учетом особенностей объектов защиты
Анализ результатов решенных задач	Не владеет навыки анализа результатов решенных задач	Неуверенно владеет навыками анализа результатов решенных задач	Владеет навыками анализа результатов решенных задач, но допускает неточности	В полной мере владеет навыками анализа решенных выполненных задач

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

6.1. Материально-техническое обеспечение

№	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы

	Учебная аудитория для проведения лекционных и практических занятий, консультаций, текущего контроля, промежуточной аттестации.	Специализированная мебель; мультимедийный проектор, переносной экран, ноутбук
	Методический кабинет для самостоятельной работы	Специализированная мебель; мультимедийный проектор, переносной экран, ноутбук
	Читальный зал библиотеки для самостоятельной работы	Специализированная мебель; компьютерная техника, подключенная к сети «Интернет», имеющая доступ в электронную информационно-образовательную среду

6.2. Перечень лицензионного и свободно распространяемого программного обеспечения

№	Перечень лицензионного программного обеспечения.	Реквизиты подтверждающего документа
1.	Microsoft Windows 10 Корпоративная	Соглашение Microsoft Open Value Subscription V6328633. Соглашение действительно с 02.10.2017 по 31.10.2023). Договор поставки ПО 0326100004117000038-0003147-01 от 06.10.2017
2.	Microsoft Office Professional Plus 2016	Соглашение Microsoft Open Value Subscription V6328633. Соглашение действительно с 02.10.2017 по 31.10.2023
3.	Kaspersky Endpoint Security «Стандартный Russian Edition»	Сублицензионный договор № 102 от 24.05.2018. Срок действия лицензии до 19.08.2020 Гражданско-правовой Договор (Контракт) № 27782 «Поставка продления права пользования (лицензии) Kaspersky Endpoint Security от 03.06.2020. Срок действия лицензии 19.08.2022г.
4.	Google Chrome	Свободно распространяемое ПО согласно условиям лицензионного соглашения
5.	Mozilla Firefox	Свободно распространяемое ПО согласно условиям лицензионного соглашения

6.3. Перечень учебных изданий и учебно-методических материалов

1. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 с.— Режим доступа: http://www.iprbookshop.ru/33430.html.
2. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.html.
3. Калмыков И.А. Криптографические методы защиты информации [Электронный ресурс]: лабораторный практикум/ Калмыков И.А., Науменко Д.О., Гиш Т.А.— Электрон. Текстовые данные.— Ставрополь:

СевероКавказский федеральный университет, 2015.— 109 с.— Режим доступа: http://www.iprbookshop.ru/63099.html.
4. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс]: лабораторный практикум/ М.А. Лапина [и др.].— Электрон. текстовые данные.— Ставрополь: СевероКавказский федеральный университет, 2016.— 242 с.— Режим доступа: http://www.iprbookshop.ru/62945.html.
5. Нестеров С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Нестеров С.А.— Электрон. текстовые данные.— СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014.— 322 с.— Режим доступа: http://www.iprbookshop.ru/43960.html.
6. Основы информационной безопасности: опорный конспект / Е.А. Рыбакова. - СПб.: Изд-во СЗТУ, 2016. - 49 с.
7. Пашинцев В.П. Нестандартные методы защиты информации [Электронный ресурс]: лабораторный практикум/ Пашинцев В.П., Ляхов А.В.— Электрон. Текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2016.— 196 с.— Режим доступа: http://www.iprbookshop.ru/63217.html. 15
8. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс]/ Петров А.А.— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 446 с.— Режим доступа: http://www.iprbookshop.ru/63800.html.
9. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. Текстовые данные.— Саратов: Профобразование, 2017.— 544 с.— Режим доступа: http://www.iprbookshop.ru/63592.html.

6.4. Перечень интернет-ресурсов, профессиональных баз данных, информационно-справочных систем

1. eLIBRARY.RU - научная электронная библиотека [сайт]. – URL: https://elibrary.ru
2. Научно-техническая библиотека БГТУ им. В.Г. Шухова: [сайт]. – URL: http://ntb.bstu.ru
3. Официальный интернет-портал правовой информации: [сайт]. – URL: http://pravo.gov.ru
4. СПС КонсультантПлюс: [сайт]. – URL: http://www.consultant.ru
5. http://www.promo.s-director.ru/ – сайт журнала «Директор по безопасности»
6. http://college.ru/UDP/texts/ – учебный курс «Защита информации»;
7. http://www.mirash.ru/doki11.html - нормативная база по защите информации;
8. http://tk.plexor.ru/web-links/info/38-zakon.html - нормативные документы по защите информации.
9. http://www.inattack.ru/ - антивирусное программное обеспечение

10. http://securityvulns.ru/ - нормативные документы по защите информации
11. http://www.glossary.ru/cgi-bin/gl_sch2.cgi?RIt(uwsg.outtg9!hlnuvgxtuxy
12. http://www.gosecure.ru/ - сайт форматов ЭЦП
13. http://z-oleg.com/ - антивирусное программное обеспечение
14. http://www.aladdin.ru/ - сайт производителя средств защиты информации