Частное учреждение высшего образования
«Высшая школа предпринимательства (институт)»
(ЧУВО «ВШП»)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.ДЭ.03.01 «Информационная безопасность бизнеса»

Направление подготовки: 09.04.03 Прикладная информатика

Направленность (профиль) программы магистратуры
«Информационные технологии в управлении и бизнесе»

ОДОБРЕНО
Ученым советом ЧУВО «ВШП»
Протокол заседания
№01-02/24 от 30 августа 2024 г.

УТВЕРЖДАЮ
Ректор ЧУВО «ВШП»
«30» августа 2024 г.
Аллабян М.Г.

Документ подписан электронной цифровой подписью
VSHP EDS GEN 1, уникальный ключ документа:

8F30-29EE-EB2F-GNI5

Организация: ЧУВО “ВШП”, ИНН 6903013604
Дата подписания: 30.08.2024
Подписал: Аллабян М.Г.

Тверь, 2024

Рабочая программа учебной дисциплины **Б1.В.ДЭ.03.01 Информационная безопасность бизнеса**, обязательного компонента основной профессиональной образовательной программы высшего образования - программы магистратуры по направлению подготовки **09.04.03 Прикладная информатика** направленность (профиль) «**Информационные технологии в управлении и бизнесе**», направлена на обеспечение у обучающегося способности осуществлять профессиональную деятельность в соответствующей области и сферах профессиональной деятельности, в том числе на их практическую подготовку с учётом рабочей программы воспитания и календарного плана воспитательной работы Частном учреждении высшего образования «**Высшая школа предпринимательства (институт)**» *(далее — **ЧУВО «ВШП»)***.

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения программы магистратуры обучающийся должен овладеть следующими результатами обучения по дисциплине:

Код	Результаты освоения ООП (Содержание компетенций)	Индикаторы достижения	Перечень планируемых результатов обучения по дисциплине
ПК -5	Способен планировать аналитические работы в ИТ-проекте с использованием международных стандартов	ПК-5.1 Обладает знаниями по основам финансового планирования; теории систем и системного анализа; методики описания и моделирования бизнес-процессов; современные подходы и стандарты автоматизации организации; основы информационной безопасности в организации.	**Знать:** современные подходы и стандарты автоматизации организации (например, CRM, RP, ERP…, ITIL, ITSM); технологию документирования процессов создания информационных систем на стадиях жизненного цикла программного обеспечения
		ПК-5.2 Демонстрирует умение анализировать исходную документацию и планировать аналитические работы на основе оценки качества надежности и информационной безопасности ИС	**Уметь:** применять международные (ISO), государственные (ГОСТ)и производственные стандарты при разработке автоматизированных информационных систем; планирования работ по определению первоначальных требований заказчика к ИС и возможности их реализации в ИС

2. Распределение часов дисциплины по семестрам

ОФО

Семестр (курс)	3 семестр (2)
Виды деятельности	
лекционные занятия	10
лабораторные занятия	10
практические занятия/ семинарские занятия	-
руководство курсовой работой	-
клинические практические занятия (практическая подготовка)	-
контактная работа на выполнение курсового проекта	-
практическая подготовка	-
консультация перед экзаменом	-

самостоятельная работа	88
промежуточная аттестация	-
общая трудоемкость	108

3. Структура, тематический план и содержание учебной дисциплины

	лекционные занятия	**лабораторные занятия**	**самостоятельная работа**	**формы текущего контроля**
	О Ф О	О Ф О	О Ф О	
Раздел: Раздел 1. Обеспечение информационной безопасности бизнеса	4	4	40	тест по итогам занятия доклад / конференция / реферат устный опрос / собеседование
Тема раздела: Тема 1. Информационная сущность и безопасность бизнеса. Информационные характеристики бизнеса. Основные понятия и определения. Информационная безопасность (ИБ) информационной системы и ее составляющие. Информационная безопасность ИС в процессе эксплуатации прикладных ИС. Комплексный подход к защите информации на предприятии. Виды информации. Состав защищаемой информации. Виды угроз информационным объектам предприятия Классификация угроз информационной безопасности бизнеса. Влияние специфики деятельности предприятия на определение состава элементов защищаемого объекта. Правовая среда бизнеса и ее свойства. Учредительная и лицензионная база организации ***Тема раздела: Тема 2 Характеристика методов и средств обеспечения информационной безопасности*** Каналы и методы несанкционированного доступа к информации. Определение источников дестабилизирующего воздействия на информацию. Определение причин и условий дестабилизирующего воздействия на информацию Выявление каналов доступа к информации. Соотношение между каналами и источниками на информацию. Методы оценки качества, надежности и информационной безопасности ИС. ИКТ и вычислительное оборудование как инструментарий автоматизации и информатизации прикладных задач ИБ Криптографические методы защиты данных. Организационные средства защиты данных. Законодательные средства защиты данных. Морально-этические средства защиты данных. Защита информации в компьютерных сетях. Защита информации при проведении совещаний и переговоров. Защита информации при работе с посетителями.			
Раздел: Раздел 2. Управление информационной безопасностью бизнеса	6	6	48	тест по итогам занятия доклад / конференция / реферат устный опрос / собеседование

Тема раздела: Тема 3. Разработка политики безопасности предприятия и подготовка персонала Основные понятия политики ИБ. Структура политики безопасности. Базовая политика ИБ. Процедуры ИБ. Специализированные политики ИБ. Разработка политики безопасности предприятия. Анализ требований бизнеса. Оценка рисков. Подбор и подготовка персонала для работы в новых условиях. Особенности работы с персоналом, владеющим конфиденциальной информацией. Собеседование с кандидатами на должность. Доступ персонала к конфиденциальным сведениям и базам данных. Мотивация. Разработка кодекса корпоративного поведения. Риск-ориентированный подход к обеспечению ИБ. Использование передовых методов оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС. Проблема персонала в задачах обеспечения информационной безопасности бизнеса. Формализованное представление угроз ИБ от персонала ***Тема раздела: Тема 4. Система управления информационной безопасностью*** Построение системы управления информационной безопасностью (СУИБ). Планирование затрат на ИБ. Понятие СУИБ. Этапы разработки СУИБ и состав работ. Факторы, влияющие на выбор состава СУИБ. Использование информационных сервисов для автоматизации прикладных и информационных процессов управления ИБ Порядок разработки и внедрения документов нормативно-методического обеспечения СЗИ. Аудит безопасности. Оценка информационной безопасности бизнеса. Проблема измерения и оценивания информационной безопасности бизнеса. Управление идентификационными данными и доступом. Противодействие угрозам ИБ от персонала. .Принципы и алгоритмы принятия решений в нестандартных ситуациях. Расследование инцидентов. Виды чрезвычайных ситуаций. Подготовка мероприятий на случай возникновения ЧС.				
Итого часов	**10**	**10**	**88**	

4. Формы текущего контроля

- доклад / конференция / реферат (шкала: значение от 0 до 15, количество: 1)

раздел дисциплины: Раздел 1. Обеспечение информационной безопасности бизнеса

Примерное задание:

1. Законодательство РФ в области защиты коммерческой тайны.
2. Виды искусственных преднамеренных угроз ИБ предприятия.
3. Определение объектов информационной защиты.
4. Задачи правоохранительных органов в обеспечении информационной безопасности бизнеса
5. Перспективы развития технологий в сфере безопасности данных.
6. Деловая разведка как канал получения информации.
7. Характеристика каналов доступа
8. Характеристика потенциальных нарушителей.
9. Технология работы с электронной подписью.
10. Системы обнаружения вторжений.

- тест по итогам занятия (шкала: значение от 0 до 15, количество: 1)

раздел дисциплины: Раздел 1. Обеспечение информационной безопасности бизнеса

Примерное задание:

1. В систему обеспечения ИБ входят: *

процессы контроля ИБ

процессы управления ИБ
процессы ЗИ

2. Меры обеспечения ИБ предназначены для реализации*
процессов системы ЗИ
процессов системы управления ИБ

3. Процессы обеспечения ИБ - это:*
Вид вспомогательных процессов, реализующих поддержку (обеспечение) процессов основной деятельности организации
Вид процессов основной деятельности организации

4. Как определен риск в соответствии с Федеральным законом № 184-ФЗ «О техническом регулировании»?
согласованные виды деятельности по руководству и управлению организацией в отношении рисков ИБ
вероятность причинения вреда с учетом его тяжести

5. Оценивание риска ИБ – это:*
сравнение достигаемого уровня риска с уровнем допустимого риска (риск-аппетит)
целостный процесс анализа и оценки значимости риска ИБ

6. Обработка риска ИБ – это: *
действия, направленные на уменьшение (модификация), перенос, уход (избежание) от риска ИБ
действие, направленное изменение уровня риска в соответствии с требованиями нормативных документов, относящихся к обеспечению ИБ
7. Методика оценки риска ИБ может быть:*
Количественной
Вербальной
аналитической

8. Политика обеспечения ИБ объекта может быть оформлена:*
одним документом
совокупностью документов
отчетом к проекту на систему обеспечения ИБ

9. Как может быть определена корпоративная политика обеспечения ИБ?
Это документация, определяющая высокоуровневые цели, содержание и основные направления и устанавливающая правила, процедуры, практические приемы и руководящие принципы обеспечения ИБ организации, которыми она руководствуется в своей деятельности
Это локальный нормативный документ, определяющий требования безопасности, систему мер, либо порядок действий, а также ответственность сотрудников организации и механизмы контроля для определенной области обеспечения ИБ

10. Как может быть определена частная политика обеспечения ИБ? *
Это документация, определяющая высокоуровневые цели, содержание и основные направления и устанавливающая правила, процедуры, практические приемы и руководящие принципы обеспечения

ИБ организации, которыми она руководствуется в своей деятельности
Это документ, содержащий совокупность требований и правил по ИБ для объекта ИБ, выработанных в соответствии с требованиями руководящих и нормативных документов в целях противодействия заданному множеству угроз ИБ, с учетом ценности защищаемой информационной сферы
Это локальный нормативный документ, определяющий требования безопасности, систему мер, либо порядок действий, а также ответственность сотрудников организации и механизмы контроля для определенной области обеспечения ИБ

- устный опрос / собеседование (шкала: значение от 0 до 10, количество: 5)
раздел дисциплины: Раздел 1. Обеспечение информационной безопасности бизнеса
Примерное задание:
1. Какие вы знаете источники дестабилизирующего воздействия на информацию?
2. Определите результаты дестабилизирующего воздействия на информацию в зависимости от его вида и способа.
3. Выявление каналов доступа к информации.
4. Методы получения несанкционированного доступа к информации
5. Канал доступа к информации и его связь с и источником воздействия на информацию.
6. ИКТ и вычислительное оборудование как инструментарий автоматизации и информатизации прикладных задач ИБ..
7. Методы оценки качества, надежности и информационной безопасности ИС.
8. Какие задачи решаются с помощью криптографических методов?
9. Законодательная база защиты информации.
10. Защита информации при работе с посетителями.
11. Политика ИБ предприятия и ее структура
12. Политика ИБ: уровни и процедуры.
13. Что включает базовая политика ИБ?
14. Анализ рисков. Риск-ориентированный подход к обеспечению ИБ.
15. Проблема персонала в задачах обеспечения информационной безопасности бизнеса .

- доклад / конференция / реферат (шкала: значение от 0 до 15, количество: 1)
раздел дисциплины: Раздел 2. Управление информационной безопасностью бизнеса
Примерное задание:
1.Обзор методик и программных средств для анализа и управления рисками
2. Персональная ответственность топ-менеджера за сохранность корпоративных и клиентских данных
3. Основные информационные риски в работе топ-менеджера.
4. Методология реагирования на инциденты.
5. Методы борьбы с инсайдерами.
6. Подсистема защиты корпоративной информации от вредоносных программ.
7. Контроль функционирования СУИБ.
8. Состав сотрудников, обеспечивающих функционирование СУИБ.
9. Аудит ИБ предприятия.
10. Обзор современных стандартов и методологий по управлению ИБ.

- тест по итогам занятия (шкала: значение от 0 до 15, количество: 1)

раздел дисциплины: Раздел 2. Управление информационной безопасностью бизнеса

Примерное задание:

1. Меры защиты информации предназначены для реализации*
процессов системы ЗИ
процессов системы управления ИБ

2. Какой процесс не входит в систему защиты информации (ЗИ)?
защита персональных данных
защита от вредоносного кода
контроль целостности и защищенности информационной инфраструктуры
обеспечение защиты вычислительных сетей
обеспечение ЗИ при управлении доступом

3. Какие процессы системы ЗИ не имеют подпроцессы?*
предотвращение утечек информации
управление инцидентами ИБ

4. Система управления обеспечением ИБ (СУОИБ). Результат реализации меры «описание объекта»?
Описание инфраструктуры объекта
Описание процессов объекта и связи их с процессами организации
Описание активов объекта

5. В процессную модель организации включают:*
Основные (бизнес) процессы
Вспомогательные процессы (по видам обеспечения)
Вспомогательные процессы (автоматизация отдельных процессов организации)
Процессы аудита деятельности организации
Процессы мониторинга деятельности организации

6. Система управления обеспечением ИБ (СУОИБ). Этапы идентификации активов объекта:
Определить перечень активов объекта
Определить перечень активов объекта в контексте бизнес-процессов организации
Определить уязвимости активов
7. К активам объекта можно отнести:*
Информационные активы
ИТ-сервисы
Нематериальные активы
Объект в целом как часть организации
Организацию в целом

8. Цель реализации меры обеспечения ИБ «Анализ угроз ИБ»? *
Сформировать перечень актуальных угроз ИБ
Описать угрозы ИБ

9. Какие меры могут быть использованы при анализе угроз ИБ?
Оценка риска ИБ
Оценивание риска ИБ

Обработка риска ИБ

10.Какой базовый подход используется при анализе угроз ИБ объекта?
Экспертный подход
Процессный подход

11.Какая угроза ИБ признается актуальной?*
Уровень риска ИБ, относящийся к этой угрозе, будет превышать риск-аппетит
Уровень риска ИБ, относящийся к этой угрозе, будет равен риск-аппетиту
Уровень риска ИБ, относящийся к этой угрозе, будет меньше риск-аппетита

12.Какими категориями оперирует вербальная методика оценки риска?
степень возможной реализации угрозы ИБ
степень тяжести последствий от угрозы ИБ
вероятность реализации угрозы ИБ
ущерб от реализации угрозы ИБ

13.Может ли сотрудник организации быть внутренним нарушителем?*
НЕТ (всегда)
ДА, если он имеет санкционированный доступ к активу, на который направлена конкретная угроза ИБ
ДА (всегда)
НЕТ, если он не имеет санкционированный доступ к активу, на который направлена конкретная угроза ИБ

14.Обработка рисков связана с:*
выбором процессов защиты информации
выборов мер защиты информации, реализующие процессы защиты информации
выбором методов защиты информации

15.Что должен содержать реестр рисков в отношении к конкретной угрозе?
величину начального риска ИБ
величину остаточного риска ИБ
величину принятого риска

- устный опрос / собеседование (шкала: значение от 0 до 10, количество: 5)
раздел дисциплины: Раздел 2. Управление информационной безопасностью бизнеса
Примерное задание:
1. Понятие СУИБ. Модели, которые входят в состав архитектуры СУИБ.
2. Разработка технико-экономического обоснования СУИБ.
3. Модель системы автоматизированного проектирования СУИБ
4. Какие требования предъявляются к технологии управления СЗИ?
5. Расследование инцидентов.
6. Управление идентификационными данными и доступом
7. Чрезвычайные ситуации (ЧС) и их классификация.
8. Принципы и алгоритмы принятия решений в нестандартных ситуациях.
9. Использование информационных сервисов для автоматизации прикладных и информационных

процессов управления ИБ.
10. Аудит безопасности. Оценка информационной безопасности бизнеса. Проблема измерения и оценивания информационной безопасности бизнеса.
11. Формализованное представление угроз ИБ от персонала.
12. Проблема персонала в задачах обеспечения информационной безопасности бизнеса.
13. Мотивация. Разработка кодекса корпоративного поведения.
14. В чем заключается нормативное обеспечение СЗИ?
15. Использование передовых методов оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС.

5. Формы промежуточной аттестации

- зачет - 2 курс, 3 семестр (шкала: значение от 0 до 20)

Примерное задание:

• Вопросы к зачету

блок 1

1. Информационные характеристики бизнеса: основные понятия и определения .
2. Информационная безопасность ИС в процессе эксплуатации прикладных ИС .
3. Виды информации. Конфиденциальная информация .
4. Виды угроз информационным объектам предприятия .
5. Какими факторами определяется состав угроз защищаемой информации?
6. Комплексный подход к защите информации на предприятии
7. Признаки классификации угрозы ИБ
8. Влияние специфики деятельности предприятия на определение состава элементов защищаемого объекта
9. Правовая среда бизнеса и ее свойства.
10. Учредительная и лицензионная база организации .
11. Состав защищаемой информации.
12. Какие вы знаете источники дестабилизирующего воздействия на информацию?
13. Определите результаты дестабилизирующего воздействия на информацию в зависимости от его вида и способа.
14. Выявление каналов доступа к информации.
15. Методы получения несанкционированного доступа к информации .
16. Канал доступа к информации и его связь с и источником воздействия на информацию.
17. ИКТ и вычислительное оборудование как инструментарий автоматизации и информатизации прикладных задач ИБ .
18. Методы оценки качества, надежности и информационной безопасности ИС .
19. Какие задачи решаются с помощью криптографических методов?
20. Охарактеризуйте программные атаки на доступность.
21. Законодательная база защиты информации .
22. Защита информации при работе с посетителями .
23. Электронная подпись и ее назначение.
24. Вредоносное программное обеспечение .
25. Криптографические системы и их применение в защите информации .

блок 2

1. Политика ИБ предприятия и ее структура .

2. Политика ИБ: уровни и процедуры.
3. Какие разделы должна содержать документально оформленная политика безопасности? .
4. Что включает базовая политика ИБ? .
5. Приведите примеры специализированных политик ИБ с описанием их особенностей .
6. Основные этапы разработки политики ИБ.
7. Анализ рисков. Риск-ориентированный подход к обеспечению ИБ.
8. Проблема персонала в задачах обеспечения информационной безопасности бизнеса.
9. Формализованное представление угроз ИБ от персонала.
10. Проблема персонала в задачах обеспечения информационной безопасности бизнеса .
11. Мотивация. Разработка кодекса корпоративного поведения.
12. В чем заключается нормативное обеспечение СЗИ?
13. Использование передовых методов оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС.
14. Понятие СУИБ. Модели, которые входят в состав архитектуры СУИБ.
15. Разработка технико-экономического обоснования СУИБ.
16. Модель системы автоматизированного проектирования СУИБ .
17. Какие требования предъявляются к технологии управления СЗИ?
18. Расследование инцидентов .
19. Управление идентификационными данными и доступом .
20. Чрезвычайные ситуации (ЧС) и их классификация.
21. Принципы и алгоритмы принятия решений в нестандартных ситуациях .
22. Использование информационных сервисов для автоматизации прикладных и информационных процессов управления ИБ.
23. Аудит безопасности. Оценка информационной безопасности бизнеса.
24. Проблема измерения и оценивания информационной безопасности бизнеса.
25. Факторы, влияющие на выбор состава СУИБ.

блок 3
Примеры заданий к зачету
1. Что именно необходимо отнести к «коммерческой тайне» для Вашего предприятия? Приведите несколько примеров .
2. Составьте перечень угроз информационной безопасности (не менее 5) для рекламного агентства .
3. Назовите объекты, которые необходимо защищать от угроз информационной безопасности для финансового учреждения.

Критерии оценивания:

18-20 баллов: Обучающийся, достигающий должного уровня:
- даёт полный, глубокий, выстроенный логично по содержанию вопроса ответ, используя различные источники информации, не требующий дополнений
- доказательно иллюстрирует основные теоретические положения практическими примерами;
- способен глубоко анализировать теоретический и практический материал, обобщать его, самостоятельно делать выводы, вести диалог и высказывать свою точку зрения.

14-17 баллов: Обучающийся на должном уровне:
- раскрывает учебный материал: даёт содержательно полный ответ, требующий незначительных дополнений и уточнений, которые он может сделать самостоятельно после наводящих вопросов преподавателя;
- демонстрирует учебные умения и навыки в области решения практико-ориентированных задач;

- владеет способами анализа, сравнения, обобщения и обоснования выбора методов решения практико-ориентированных задач.

11-13 баллов: Достигнутый уровень оценки результатов обучения обучающегося показывает:
- знания имеют фрагментарный характер, отличаются поверхностью и малой содержательностью; студент раскрывает содержание вопроса, но не глубоко, бессистемно, с некоторыми неточностями;
- слабо, недостаточно аргументированно может обосновать связь теории с практикой;
- способен понимать и интерпретировать основной теоретический материал по дисциплине.

0-10 баллов: Результаты обучения обучающегося свидетельствуют:
- об усвоении им некоторых элементарных знаний, но студент не владеет понятийным аппаратом изучаемой образовательной области (учебной дисциплины);
- не умеет установить связь теории с практикой;
- не владеет способами решения практико-ориентированных задач.

6. Балльная система оценивания по дисциплине

ОФО

Семестр (Курс) - 3 (2)			
Форма текущего контроля	**Раздел дисциплины**	**Максимальный балл**	**Максимальный приведенный балл**
доклад / конференция / реферат	Раздел 1. Обеспечение информационной безопасности бизнеса	15	
доклад / конференция / реферат	Раздел 2. Управление информационной безопасностью бизнеса	15	
тест по итогам занятия	Раздел 1. Обеспечение информационной безопасности бизнеса	15	
тест по итогам занятия	Раздел 2. Управление информационной безопасностью бизнеса	15	
устный опрос / собеседование	Раздел 1. Обеспечение информационной безопасности бизнеса	50	
устный опрос / собеседование	Раздел 2. Управление информационной безопасностью бизнеса	50	
Максимальный текущий балл		160	80
Промежуточная аттестация		зачет	
Максимальный аттестационный балл		20	20

Общий балл по дисциплине	180	100

Общий балл по дисциплине за семестр складывается из результатов, полученных по формам текущего контроля в течение семестра и аттестационного балла.
Оценка успеваемости по дисциплине в семестре пересчитывается по приведенной 100-балльной шкале независимо от шкалы, определенной преподавателем.
Перевод баллов из 100-балльной шкалы в числовой и буквенный эквивалент:
- для зачета:

Сумма баллов	Отметка
51-100	Зачтено
0-50	Не зачтено

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины. Электронно-библиотечные системы

Основная литература

1. Горбенко, А. О., Безопасность электронного бизнеса : учебное пособие / А. О. Горбенко, А. В. Горбенко. — Москва : КноРус, 2024. — 225 с. — ISBN 978-5-406-11953-2. — URL: https://book.ru/book/950426 — Текст : электронный.
2. Николаев Н.С., Управление информационной безопасностью [Электронный ресурс] : учебник / Н.С. Николаев. - М. : КноРус, 2021. - 188 с. - ISBN 978-5-406-07325-4. - Режим доступа: https://book.ru/book/939841

Дополнительная литература

1. Мельников В.П., Информационная безопасность [Электронный ресурс] : учебник / В.П. Мельников, А.И. Куприянов, Т.Ю. Васильева. - М. : КноРус, 2023. - 371 с. - ISBN 978-5-406-11960-0. - Режим доступа: https://book.ru/book/950148
2. Бабаш А.В., Информационная безопасность. Лабораторный практикум + еПриложение [Электронный ресурс] : учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М. : КноРус, 2023. - 131 с. - ISBN 978-5-406-11731-6. - Режим доступа: https://book.ru/book/949452

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Обучающимся (магистрам) обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам (*подлежащим обновлению при необходимости*), а именно:

1. КонсультантПлюс: справочно-поисковая система [Электронный ресурс]. - http://www.consultant.ru
2. Мировая цифровая библиотека: http://wdl.org/ru
3. Научная электронная библиотека «Scopus»: https://www.scopus.com
4. Научная электронная библиотека ScienceDirect: http://www.sciencedirect.com
5. Научная электронная библиотека «eLIBRARY»: https://elibrary.ru

6. Портал «Гуманитарное образование» http://www.humanities.edu.ru
7. Федеральный портал «Российское образование» http://www.edu.ru
8. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» http://school-collection.edu.ru
9. Поисковые системы Yandex, Rambler и др.
10. Электронная библиотека Российской Государственной Библиотеки (РГБ): http://elibrary.rsl.ru
11. Электронно-библиотечная система http://www.sciteclibrary.ru

9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Помещения для проведения всех видов работы, предусмотренных учебным планом, укомплектованы необходимым оборудованием и техническими средствами обучения.

Наименование оборудованных учебных кабинетов, объектов для проведения практических занятий, объектов физической культуры и спорта с перечнем основного оборудования	**Адрес (местоположение) учебных кабинетов, объектов для проведения практических занятий, объектов физической культуры и спорта** (с указанием площади и номера помещения в соответствии с документами бюро технической инвентаризации)	**Собственность или оперативное управление, хозяйственное ведение, аренда (субаренда), безвозмездное пользование, практическая подготовка**	**Полное наименование собственника (арендодателя, ссудодателя) объекта недвижимого имущества**	**Документ – основание возникновения права** (реквизиты и срок действия)
Специализированная многофункциональная учебная аудитория для проведения учебных занятий лекционного и семинарского типов, групповых и индивидуальных консультаций, текущего контроля и промежуточной	170001, Тверская область, г. Тверь, ул. Спартака, д. 26а (39,2 кв.м., 1 этаж, помещение № 3)	Безвозмездное пользование	Богачев Сергей Александрович	Договор безвозмездного пользования недвижимым имуществом № 01-18/Н от 01.11.2020 с приложениями №№ 1-3; срок действия договора: с 01.11.2020 по 30.09.2025

аттестации, в том числе, для организации практической подготовки обучающийся, с перечнем основного оборудования (аудитория № 3): Столы для обучающихся; Стулья для обучающихся; Стол педагогического работника; Стул педагогического работника; Компьютер с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду лицензиата; Интерактивная доска; Проектор				
Специализированная многофункциональная учебная аудитория для проведения учебных занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, в том числе, для организации практической	170001, Тверская область, г. Тверь, ул. Спартака, д. 26а (31,1 кв.м., 2 этаж, помещение № 27)	Безвозмездное пользование	Богачев Сергей Александрович	Договор безвозмездного пользования недвижимым имуществом № 01-18/Н от 01.11.2020 с приложениями №№ 1-3; срок действия договора: с 01.11.2020 по 30.09.2025

подготовки обучающийся, с перечнем основного оборудования (аудитория № 27) Компьютерные столы для обучающихся; Стулья для обучающихся; Стол педагогического работника; Стул педагогического работника; Компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду лицензиата; Интерактивная доска; Проектор Сканер; Принтер				
Специализированная многофункциональная учебная аудитория для проведения учебных занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, в том числе, для организации практической подготовки	170001, Тверская область, г. Тверь, ул. Спартака, д. 26а (31,4 кв.м., 2 этаж, помещение № 16)	Безвозмездное пользование	Богачев Сергей Александрович	Договор безвозмездного пользования недвижимым имуществом № 01-18/Н от 01.11.2020 с приложениями №№ 1-3; срок действия договора: с 01.11.2020 по 30.09.2025

обучающийся, с перечнем основного оборудования (аудитория № 16) Компьютерные столы для обучающихся; Стулья для обучающихся; Стол педагогического работника; Стул педагогического работника; Компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду лицензиата; Интерактивная доска; Проектор Сканер; Принтер				
Помещение для самостоятельной работы обучающихся с перечнем основного оборудования (аудитория № 22): Столы для обучающихся; Стулья для обучающихся; Компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-о	170001, Тверская область, г. Тверь, ул. Спартака, д. 26а (19,3 кв.м., 2 этаж, помещение № 22)	Безвозмездное пользование	Богачев Сергей Александрович	Договор безвозмездного пользования недвижимым имуществом № 01-18/Н от 01.11.2020 с приложениями №№ 1-3; срок действия договора: с 01.11.2020 по 30.09.2025

бразовательную среду лицензиата; Ноутбуки с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-о бразовательную среду лицензиата; Принтер; Сканер				
Помещение для самостоятельной работы обучающихся с перечнем основного оборудования (аудитория № 14): Столы для обучающихся; Стулья для обучающихся; Компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-о бразовательную среду лицензиата; Ноутбуки с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-о бразовательную среду лицензиата; Принтер; Сканер	170001, Тверская область, г. Тверь, ул. Спартака, д. 26а (22,5 кв.м., 1 этаж, помещение № 14)	Безвозмездное пользование	Богачев Сергей Александрович	Договор безвозмездног о пользования недвижимым имуществом № 01-18/Н от 01.11.2020 с приложениям и №№ 1-3; срок действия договора: с 01.11.2020 по 30.09.2025
Помещение для самостоятельной	170001, Тверская	Безвозмездное пользование	Богачев Сергей Александрович	Договор безвозмездног

работы обучающихся с перечнем основного оборудования (аудитория № 31): Столы для обучающихся; Стулья для обучающихся; Компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду лицензиата; Ноутбуки с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду лицензиата; Принтер; Сканер	область, г. Тверь, ул. Спартака, д. 26а (20,3 кв.м., 2 этаж, помещение № 31)			о пользования недвижимым имуществом № 01-18/Н от 01.11.2020 с приложениям и №№ 1-3; срок действия договора: с 01.11.2020 по 30.09.2025

10. Образовательные технологии

Наименование образовательной технологии	Краткая характеристика
Дифференцированное обучение	Технология обучения, целью которой является создание оптимальных условий для выявления задатков, развития интересов и способностей обучающихся через разделение на группы, подразумевает наличие разных уровней учебных требований к группам в овладении ими содержанием образования.

11. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся созданы фонды оценочных средств, адаптированные для инвалидов и лиц с

ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе. Форма проведения текущей аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При тестировании для слабовидящих студентов используются фонды оценочных средств с укрупненным шрифтом. На экзамен приглашается сопровождающий, который обеспечивает техническое сопровождение студенту. При необходимости студенту-инвалиду предоставляется дополнительное время для подготовки ответа на экзамене (или зачете). Обучающиеся с ограниченными возможностями здоровья и обучающиеся инвалиды обеспечиваются печатными и электронными образовательными ресурсами (программы, учебники, учебные пособия материалы для самостоятельной работы и т.д.) в формах, адаптированных к ограничениям их здоровья и восприятия информации:

1) для инвалидов и лиц с ограниченными возможностями здоровья **по зрению:**

- **для слепых:** задания для выполнения на семинарах и практических занятиях оформляются рельефно-точечным шрифтом Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом; письменные задания выполняются на бумаге рельефно-точечным шрифтом Брайля или на компьютере со специализированным программным обеспечением для слепых либо надиктовываются ассистенту; обучающимся для выполнения задания при необходимости предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;
- **для слабовидящих:** обеспечивается индивидуальное равномерное освещение не менее 300 люкс; обучающимся для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; задания для выполнения заданий оформляются увеличенным шрифтом;

2) для инвалидов и лиц с ограниченными возможностями здоровья **по слуху:**

- **для глухих и слабослышащих:** обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования; предоставляются услуги сурдопереводчика;
- **для слепоглухих** допускается присутствие ассистента, оказывающего услуги тифлосурдопереводчика (помимо требований, выполняемых соответственно для слепых и глухих);

3) для лиц с тяжелыми нарушениями речи, глухих, слабослышащих лекции и семинары, проводимые в устной форме, проводятся в письменной форме;

4) для инвалидов и лиц с ограниченными возможностями здоровья, **имеющих нарушения опорно-двигательного аппарата:**

- для лиц с нарушениями опорно-двигательного аппарата, нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей: письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту; выполнение заданий (тестов, контрольных работ), проводимые в письменной форме, проводятся в устной форме путем опроса, беседы с обучающимся.

Частное учреждение высшего образования
«Высшая школа предпринимательства (институт)»
(ЧУВО «ВШП»)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
по дисциплине
Б1.В.ДЭ.03.01 «Информационная безопасность бизнеса»

Направление подготовки: 09.04.03 Прикладная информатика

Направленность (профиль) программы магистратуры
«Информационные технологии в управлении и бизнесе»

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения программы магистратуры обучающийся должен овладеть следующими результатами обучения по дисциплине (модулю):

Код	Результаты освоения ООП (Содержание компетенций)	Индикаторы достижения	Перечень планируемых результатов обучения по дисциплине
ПК-5	Способен планировать аналитические работы в ИТ-проекте с использованием международных стандартов	ПК-5.1 Обладает знаниями по основам финансового планирования; теории систем и системного анализа; методики описания и моделирования бизнес-процессов; современные подходы и стандарты автоматизации организации; основы информационной безопасности в организации.	**Знать:** современные подходы и стандарты автоматизации организации (например, CRM, RP, ERP…, ITIL, ITSM); технологию документирования процессов создания информационных систем на стадиях жизненного цикла программного обеспечения П.П1 П.П2 П.П3 П.П4 П.П5 П.П6 П.П7 П.ТВ1 П.ТВ2 П.ТВ3 П.ТВ4 П.ТВ5 П.ТВ6 П.ТВ7 П.ТВ8 П.ТВ9 П.ТВ10 П.ТВ11 П.ТВ12 П.ТВ13 П.ТВ14 П.ТВ15 П.ТВ16 П.ТВ17 П.ТВ18 П.ТВ19 П.ТВ20 П.ТВ21 П.ТВ22 П.Т1 П.Т2 П.Т3 П.Т4

				Т.Д1_1 Т.Д2_1 Т.Д3_1 Т.Д4_1 Т.Д5_1 Т.Т1_1 Т.Т2_1 Т.Т3_1 Т.У1_1 Т.У2_1 Т.У3_1 Т.У4_1 Т.У5_1 Т.У6_1 Т.У7_1 Т.У8_1 Т.У9_1 Т.У10_1 Т.У11_1 Т.У12_1 Т.У13_1 Т.У14_1 Т.У15_1 Т.У16_1 Т.Д1_2 Т.Д2_2 Т.Д3_2 Т.Д4_2 Т.Д5_2 Т.У1_2
		ПК-5.2 Демонстрирует умение анализировать исходную документацию и планировать аналитические работы на основе оценки качества надежности и информационной безопасности ИС	**Уметь:** применять международные (ISO), государственные (ГОСТ)и производственные стандарты при разработке автоматизированных информационных систем; планирования работ по определению первоначальных требований заказчика к ИС и возможности их реализации в ИС	П.П1 П.П2 П.П3 П.П4 П.П5 П.П6 П.П7 П.ТВ1 П.ТВ2 П.ТВ3

			П.ТВ5 П.ТВ6 П.ТВ7 П.ТВ8 П.ТВ9 П.ТВ10 П.ТВ11 П.ТВ12 П.ТВ13 П.ТВ14 П.ТВ15 П.ТВ16 П.ТВ17 П.ТВ18 П.ТВ19 П.ТВ20 П.ТВ21 П.ТВ22 Т.У1_1 Т.У4_1 Т.У5_1 Т.У6_1 Т.У9_1 Т.Д1_2 Т.Д2_2 Т.Д4_2 Т.Т1_2

Контрольные задания. Текущая аттестация

доклад / конференция / реферат - Раздел 1. Обеспечение информационной безопасности бизнеса	**Номер задания**
Виды искусственных непреднамеренных угроз ИБ предприятия.	Т.Д1_1
Законодательство РФ в области защиты коммерческой тайны.	Т.Д2_1
Определение объектов информационной защиты.	Т.Д3_1
Задачи правоохранительных органов в обеспечении информационной безопасности бизнеса.	Т.Д4_1
Перспективы развития технологий в сфере безопасности данных.	Т.Д5_1

тест по итогам занятия - Раздел 1. Обеспечение информационной безопасности бизнеса	**Варианты ответов**	**Номер задания**
Что не является административными мерами, относящимися к процедурам действий в аварийных ситуациях?	**1** Системы выявления вторжений 2 Обучение и повышение осведомленности 3 Тренировки и проверки 4 Делегирование обязанностей.	Т.Т1_1
Политика безопасности строится на основе …	1 изучения политики безопасности родственных организаций **2** анализа рисков 3 общих представлений об информационной системы организации 4 требований к персоналу организации	Т.Т2_1
В каких единицах измеряется риск?	**1** в уровнях 2 в процентах 3 в стоимостном выражении 4 во временном выражении	Т.Т3_1

устный опрос / собеседование - Раздел 1. Обеспечение информационной безопасности бизнеса	**Номер задания**
Деловая разведка как канал получения информации.	Т.У1_1
Характеристика каналов доступа	Т.У2_1
Характеристика потенциальных нарушителей.	Т.У3_1
Технология работы с электронной подписью.	Т.У4_1
Системы обнаружения вторжений.	Т.У5_1
Персональная ответственность топ-менеджера за сохранность корпоративных и клиентских данных	Т.У6_1
Основные информационные риски в работе топ-менеджера	Т.У7_1
Обзор методик и программных средств для анализа и управления рисками	Т.У8_1

Методология реагирования на инциденты	Т.У9_1
Понятие СУИБ. Модели, которые входят в состав архитектуры СУИБ.	Т.У10_1
Разработка технико-экономического обоснования СУИБ.	Т.У11_1
1. Дайте определение следующему понятию: несанкционированный доступ к данным.	Т.У12_1
В каких правовых документах идет речь о государственной тайне? Приведите выдержку из документа с нужным определением.	Т.У13_1
Дайте определение следующему понятию: идентификация	Т.У14_1
В каких правовых документах идет речь о коммерческой тайне? Приведите выдержку из документа с нужным определением.	Т.У15_1
1. Дайте определение следующему понятию: анализ рисков. 2. В каких правовых документах идет речь о защите информации. Приведите выдержку из документа с нужным определением	Т.У16_1

доклад / конференция / реферат - Раздел 2. Управление информационной безопасностью бизнеса	**Номер задания**
Подсистема защиты корпоративной информации от вредоносных программ.	Т.Д1_2
Контроль функционирования СУИБ	Т.Д2_2
Состав сотрудников, обеспечивающих функционирование СУИБ	Т.Д3_2
Аудит ИБ предприятия.	Т.Д4_2
Обзор современных стандартов и методологий по управлению ИБ	Т.Д5_2

тест по итогам занятия - Раздел 2. Управление информационной безопасностью бизнеса	**Варианты ответов**	**Номер задания**
1.Естественные угрозы безопасности информации вызваны: деятельностью человека; ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения; воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека корыстными устремлениями злоумышленников; ошибками при действиях персонала. 2. Искусственные угрозы безопасности информации вызваны: деятельностью человека ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека корыстными устремлениями злоумышленников ошибками при действиях персонала 3. К основным непреднамеренным искусственным угрозам АСОИ относится: физическое разрушение системы путем взрыва, поджога и т.п.; перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;		Т.Т1_2

изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.; чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы 4. К основным преднамеренным искусственным угрозам АСОИ относится: игнорирование организационных ограничений (установленных правил) при работе в системе пересылка данных по ошибочному адресу абонента неправомерное отключение оборудования или изменение режимов работы устройств и программ хищение носителей информации Тема 2. Характеристика методов и средств обеспечения информационной безопасности 1.Федеральным законом, определяющим правовые условия использования ЭЦП в электронных документах является: №184-ФЗ «О техническом регулировании» №149-ФЗ «Об информации, информационных технологиях и о защите информации» Гражданский кодекс РФ №63-ФЗ «Об электронной подписи» Закон РФ «О безопасности» №2446-1 №152-ФЗ «О персональных данных»2. 2. Решение каких задач информационной безопасности обеспечивает ЭЦП, как реквизит электронного документа (выберите все правильные ответы): Целостность конфиденциальность неотказуемость аутентичность 3.Какой из перечисленных алгоритмов шифрования разрешено использовать в органах государственной власти РФ: DES ГОСТ 28147-89 RSA ГОСТ Р 34.10-2001 4.Криптографические средства – это...? регламентация правил использования, обработки и передачи информации ограниченного доступа средства защиты с помощью преобразования информации (шифрование) средства, в которых программные и аппаратные части полностью взаимосвязаны. 5.Что используется для создания цифровой подписи? Закрытый ключ получателя Открытый ключ отправителя Закрытый ключ отправителя Открытый ключ получателя 6. Шифрование информации это: процесс сбора, накопления, обработки, хранения, распределения и поиска информации преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа		

получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё. 7.Атака, которая использует недостатки алгоритмов удаленного поиска (DNS (Internet)…): подмена доверенного объекта или субъекта распределенной вычислительной сети ложный объект распределенной вычислительной сети анализ сетевого трафика отказ в обслуживании; удаленный контроль над станцией в сети. Тестовые задания 1.Что не является административными мерами, относящимися к процедурам действий в аварийных ситуациях? Системы выявления вторжений Обучение и повышение осведомленности Тренировки и проверки Делегирование обязанностей. 2. Политика безопасности строится на основе … изучения политики безопасности родственных организаций анализа рисков общих представлений об информационной системы организации требований к персоналу организации 3.В каких единицах измеряется риск? в уровнях в процентах в стоимостном выражении во временном выражении 4.Анализ информационных рисков предназначен для: убеждения руководства компании в необходимости вложений в систему обеспечения информационной безопасности и для инструментальной проверки защищенности информационной системы получения стоимостной оценки вероятного финансового ущерба от реализации угроз, направленных на информационную систему компании и для оценки возможности реализации угроз оценки технического уровня защищенности оценки существующего уровня защищенности информационной системы и формирования оптимального бюджета на информационную безопасность оценки технического уровня защищенности информационной системы 5.Аудит информационной безопасности в том числе должен включать в себя (выберите наиболее полный ответ из перечисленных): оценку стоимости ресурсов и информации анализ и классификацию угроз безопасности согласно модели нарушителя анализ информационных рисков для оценки вероятного ущерба и инструментальную проверку защищенности для определения возможности реализации угроз оценку зависимости компании от внешних связей и тесты на проникновение 6.В число целей политики информационной безопасности верхнего уровня входят … обеспечение конфиденциальности почтовых сообщений регулярное обновление антивирусных баз		

классификация ресурсов по степени важности с точки зрения ИБ решение сформировать или пересмотреть комплексную программу информационной безопасности		

устный опрос / собеседование - Раздел 2. Управление информационной безопасностью бизнеса	**Номер задания**
1. Понятие СУИБ. Модели, которые входят в состав архитектуры СУИБ. 2. Разработка технико-экономического обоснования СУИБ. 3. Модель системы автоматизированного проектирования СУИБ 4. Какие требования предъявляются к технологии управления СЗИ? 5. Расследование инцидентов. 6. Управление идентификационными данными и доступом 7. Чрезвычайные ситуации (ЧС) и их классификация. 8. Принципы и алгоритмы принятия решений в нестандартных ситуациях. 9. Использование информационных сервисов для автоматизации прикладных и информационных процессов управления ИБ. 10. Аудит безопасности. Оценка информационной безопасности бизнеса. Проблема измерения и оценивания информационной безопасности бизнеса. Формализованное представление угроз ИБ от персонала. 11. Проблема персонала в задачах обеспечения информационной безопасности бизнеса. 12. Мотивация. Разработка кодекса корпоративного поведения. 13. В чем заключается нормативное обеспечение СЗИ? 14. Использование передовых методов оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС.	Т.У1_2

Контрольные задания. Промежуточная аттестация

Зачет. Практическое задание	**Номер задания**
Создать ключи посредством утилиты «Kleopatra».	П.П1
Шифровать и дешифровать текст на жестком диске.	П.П2
Проверить достоверности полученных ключей.	П.П3
Шифровать текст и передача криптограммы.	П.П4
Принять и дешифровать криптограммы.	П.П5
Создать сообщение, заверенноеэлектронной подписью.	П.П6
Создать зашифрованные сообщения, заверенные электронной подписью.	П.П7

Зачет. Теоретический вопрос	**Номер задания**
Информационные характеристики бизнеса: основные понятия и определения .	П.ТВ1
Информационная безопасность ИС в процессе эксплуатации прикладных ИС .	П.ТВ2
Виды информации. Конфиденциальная информация .	П.ТВ3
Виды угроз информационным объектам предприятия .	П.ТВ4

Какими факторами определяется состав угроз защищаемой информации?	П.ТВ5
Комплексный подход к защите информации на предприятии	П.ТВ6
Признаки классификации угрозы ИБ	П.ТВ7
Влияние специфики деятельности предприятия на определение состава элементов защищаемого объекта	П.ТВ8
Правовая среда бизнеса и ее свойства	П.ТВ9
Учредительная и лицензионная база организации	П.ТВ10
Состав защищаемой информации	П.ТВ11
Какие вы знаете источники дестабилизирующего воздействия на информацию?	П.ТВ12
Определите результаты дестабилизирующего воздействия на информацию в зависимости от его вида и способа .	П.ТВ13
Выявление каналов доступа к информации .	П.ТВ14
Методы получения несанкционированного доступа к информации .	П.ТВ15
Канал доступа к информации и его связь с и источником воздействия на информацию .	П.ТВ16
Методы оценки качества, надежности и информационной безопасности ИС .	П.ТВ17
Защита информации при работе с посетителями .	П.ТВ18
Криптографические системы и их применение в защите информации .	П.ТВ19
Вредоносное программное обеспечение .	П.ТВ20
Электронная подпись и ее назначение .	П.ТВ21
Политика ИБ: уровни и процедуры .	П.ТВ22

Зачет. Тестовый вопрос	**Варианты ответов**	**Номер задания**
Федеральным законом, определяющим правовые условия использования ЭЦП в электронных документах является:	1 №184-ФЗ «О техническом регулировании» 2 №149-ФЗ «Об информации, информационных технологиях и о защите информации» 3 Гражданский кодекс РФ 4 №63-ФЗ «Об электронной подписи» 5 Закон РФ «О безопасности» №2446-1 **6** № 1-ФЗ "Об электронной цифровой подписи"	П.Т1
Естественные угрозы безопасности информации вызваны:	1 деятельностью человека;	П.Т2

	2 ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения; 3 воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека **4** корыстными устремлениями злоумышленников; 5 ошибками при действиях персонала.	
Искусственные угрозы безопасности информации вызваны:	1 деятельностью человека 2 ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения 3 воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека **4** корыстными устремлениями злоумышленников 5 ошибками при действиях персонала	П.Т3
Что используется для создания цифровой подписи?	1 Закрытый ключ получателя 2 Открытый ключ отправителя 3 Закрытый ключ отправителя 4 Открытый ключ получателя	П.Т4

Балльная система оценивания по дисциплине

ОФО

Семестр (Курс) - 3 (2)			
Форма текущего контроля	**Раздел дисциплины**	**Максимальный балл**	**Максимальный приведенный балл**
доклад / конференция / реферат	Раздел 1. Обеспечение информационной безопасности бизнеса	15	
доклад / конференция / реферат	Раздел 2. Управление информационной безопасностью бизнеса	15	

тест по итогам занятия	Раздел 1. Обеспечение информационной безопасности бизнеса	15	
тест по итогам занятия	Раздел 2. Управление информационной безопасностью бизнеса	15	
устный опрос / собеседование	Раздел 1. Обеспечение информационной безопасности бизнеса	50	
устный опрос / собеседование	Раздел 2. Управление информационной безопасностью бизнеса	50	
Максимальный текущий балл		160	80
Промежуточная аттестация		зачет	
Максимальный аттестационный балл		20	20
Критерии оценивания		18-20 баллов: Обучающийся, достигающий должного уровня: - даёт полный, глубокий, выстроенный логично по содержанию вопроса ответ, используя различные источники информации, не требующий дополнений - доказательно иллюстрирует основные теоретические положения практическими примерами; - способен глубоко анализировать теоретический и практический материал, обобщать его, самостоятельно делать выводы, вести диалог и высказывать свою точку зрения. 14-17 баллов: Обучающийся на должном уровне: - раскрывает учебный материал: даёт содержательно полный ответ, требующий незначительных дополнений и уточнений, которые он может сделать самостоятельно после наводящих вопросов преподавателя; - демонстрирует учебные умения и навыки в области решения практико-ориентированных задач; - владеет способами анализа, сравнения, обобщения и обоснования выбора методов решения практико-ориентированных задач. 11-13 баллов: Достигнутый уровень оценки результатов обучения обучающегося показывает: - знания имеют фрагментарный характер, отличаются поверхностью и малой содержательностью; студент раскрывает содержание вопроса, но не глубоко, бессистемно, с некоторыми неточностями; - слабо, недостаточно аргументированно может обосновать связь теории с практикой; - способен понимать и интерпретировать основной теоретический материал по дисциплине.	

	0-10 баллов: Результаты обучения обучающегося свидетельствуют: - об усвоении им некоторых элементарных знаний, но студент не владеет понятийным аппаратом изучаемой образовательной области (учебной дисциплины); - не умеет установить связь теории с практикой; - не владеет способами решения практико-ориентированных задач.	
Общий балл по дисциплине	180	100

Общий балл по дисциплине за семестр складывается из результатов, полученных по формам текущего контроля в течение семестра и аттестационного балла.

Оценка успеваемости по дисциплине в семестре пересчитывается по приведенной 100-балльной шкале независимо от шкалы, определенной преподавателем.

Перевод баллов из 100-балльной шкалы в числовой и буквенный эквивалент:

- для зачета:

Сумма баллов	Отметка
51-100	Зачтено
0-50	Не зачтено

Список используемых сокращений

Текущая аттестация

Тип задания	**Сокращение**
внеаудиторное чтение	Т.В
доклад / конференция / реферат	Т.Д
индивидуальное задание (перевод / презентация / план урока / тезаурус / глоссарий / сценарий деловой игры / алгоритм задачи / программа / конспектирование научной литературы)	Т.И
итоговая лабораторная работа	Т.ЛР
кейс	Т.КС
коллоквиум	Т.К
контрольная работа	Т.КР
лабораторная работа	Т.Л
отчет (по научно-исследовательской работе / практике)	Т.О
письменная работа	Т.ПР

практическая работа	Т.П
расчетно-графическая работа	Т.РГ
семестровая работа	Т.СР
ситуационная задача / ситуационное задание / проект	Т.СЗ
творческая работа	Т.ТР
тест по итогам занятия	Т.Т
устный опрос / собеседование	Т.У
эссе	Т.Э

Промежуточная аттестация

Тип задания	**Сокращение**
Практическое задание	П.П
Теоретический вопрос	П.ТВ
Тестовый вопрос	П.Т