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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.ДЭ.03.02 «Технология обеспечения информационной безопасности»

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.
Ректор _____ 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.03.02 Технология обеспечения информационной безопасности**, 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 информационных систем	4	4	44	тест по итогам занятия доклад / конференция / реферат устный опрос / собеседование
Тема раздела: Тема 1. Обеспечение информационной безопасности на всех уровнях. 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. Правовая база и международные стандарты информационной безопасности ИС в процессе эксплуатации. ***Тема раздела: Тема 2 Технологии 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.			
Раздел: Раздел 2. Управление информационной безопасностью информационных систем	6	6	44	доклад / конференция / реферат устный опрос / собеседование
Тема раздела: Тема 3. Разработка политики безопасности ИС предприятия Основные понятия политики ИБ. Структура политики безопасности. Базовая политика ИБ. Процедуры ИБ. Специализированные политики ИБ. Разработка политики безопасности предприятия. Анализ требований бизнеса. Оценка рисков. Риск-ориентированный подход к обеспечению ИБ. Использование передовых методов оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС.				

Тема раздела: Тема 4. Система управления информационной безопасностью ИС 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. Проблема измерения и оценивания информационной безопасности ИС. Управление идентификационными данными и доступом..Принципы и алгоритмы принятия решений в нестандартных ситуациях. Расследование инцидентов.				
Итого часов	**10**	**10**	**88**	

4. Формы текущего контроля

- тест по итогам занятия (шкала: значение от 0 до 20, количество: 1)

Примерное задание:

Тестовые задания

1.Естественные 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.

2. 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

3. К основным непреднамеренным искусственным угрозам АСОИ относится:

1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
5. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы

4. К основным преднамеренным искусственным угрозам АСОИ относится:

1. игнорирование организационных ограничений (установленных правил) при работе в системе
2. пересылка данных по ошибочному адресу абонента
3. неправомерное отключение оборудования или изменение режимов работы устройств и программ

4. хищение носителей информации

1.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. №152-ФЗ «О персональных данных»2.
2. Решение каких задач информационной безопасности обеспечивает ЭЦП, как реквизит электронного документа (выберите все правильные ответы):
1. Целостность
2. конфиденциальность
3. неотказуемость
4. аутентичность
3.Какой из перечисленных алгоритмов шифрования разрешено использовать в органах государственной власти РФ:
1. DES
2. ГОСТ 28147-89
3. RSA
4. ГОСТ Р 34.10-2001
4.Криптографические средства – это...?
1. регламентация правил использования, обработки и передачи информации ограниченного доступа
2. средства защиты с помощью преобразования информации (шифрование)
3. средства, в которых программные и аппаратные части полностью взаимосвязаны.
5.Что используется для создания цифровой подписи?
4. Закрытый ключ получателя
5. Открытый ключ отправителя
6. Закрытый ключ отправителя
7. Открытый ключ получателя
6. Шифрование информации это:
1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.
7.Атака, которая использует недостатки алгоритмов удаленного поиска (DNS (Internet)…):
1. подмена доверенного объекта или субъекта распределенной вычислительной сети
2. ложный объект распределенной вычислительной сети
3. анализ сетевого трафика
4. отказ в обслуживании;

5. удаленный контроль над станцией в сети.

1.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.
2. Политика безопасности строится на основе …
1. изучения политики безопасности родственных организаций
2. анализа рисков
3. общих представлений об информационной системе организации
4. требований к персоналу организации
3.В каких единицах измеряется риск?
1. в уровнях
2. в процентах
3. в стоимостном выражении
4. во временном выражении
4.Анализ информационных рисков предназначен для:
1. убеждения руководства компании в необходимости вложений в систему обеспечения информационной безопасности и для инструментальной проверки защищенности информационной системы
2. получения стоимостной оценки вероятного финансового ущерба от реализации угроз, направленных на информационную систему компании и для оценки возможности реализации угроз оценки технического уровня защищенности
3. оценки существующего уровня защищенности информационной системы и формирования оптимального бюджета на информационную безопасность
4. оценки технического уровня защищенности информационной системы
5.Аудит информационной безопасности в том числе должен включать в себя (выберите наиболее полный ответ из перечисленных):
1. оценку стоимости ресурсов и информации
2. анализ и классификацию угроз безопасности согласно модели нарушителя
3. анализ информационных рисков для оценки вероятного ущерба и инструментальную проверку защищенности для определения возможности реализации угроз
4. оценку зависимости компании от внешних связей и тесты на проникновение
6.В число целей политики информационной безопасности верхнего уровня входят …
1. обеспечение конфиденциальности почтовых сообщений
2. регулярное обновление антивирусных баз
3. классификация ресурсов по степени важности с точки зрения ИБ
4. решение сформировать или пересмотреть комплексную программу информационной безопасности

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

Примерное задание:

1. Виды искусственных непреднамеренных угроз ИБ предприятия.
2. Законодательство РФ в области защиты коммерческой тайны.

3. Виды искусственных преднамеренных угроз ИБ предприятия.
4. Определение объектов информационной защиты.
5. Перспективы развития технологий в сфере безопасности данных.
1. Характеристика потенциальных нарушителей.
2. Технология работы с электронной подписью.
3. Характеристика атак через Интернет
4. Системы обнаружения вторжений.

1. Роль стандартов ИБ
2. Программный комплекс ГРИФ для анализа и управления рисками
3. Обзор методик и программных средств для анализа и управления рисками
4. Персональная ответственность топ-менеджера за сохранность корпоративных и клиентских данных
5. Методология реагирования на инциденты

1. Защита удаленного доступа.
2. Структура СЗИ в корпоративной ИС.
3. Подсистема управления криптографическими ключами
4. Аудит ИБ предприятия.
5. Обзор современных стандартов и методологий по управлению ИБ

- устный опрос / собеседование (шкала: значение от 0 до 15, количество: 1)

Примерное задание:

1. Информационная безопасность ИС в процессе эксплуатации прикладных ИС.
2. Виды информации. Конфиденциальная информация.
3. Виды угроз информационным объектам предприятия.
4. Комплексный подход к защите информации на предприятии.
5. Признаки классификации угрозы ИБ.
6. Правовая база ИБ.
7. Состав защищаемой информации.

1. Какие вы знаете источники дестабилизирующего воздействия на информацию?
2. Выявление каналов доступа к информации.
3. Методы получения несанкционированного доступа к информации
4. Канал доступа к информации и его связь с и источником воздействия на информацию.
5. Методы оценки качества, надежности и информационной безопасности ИС.
6. Какие задачи решаются с помощью криптографических методов?
7. Законодательная база защиты информации.
1. Политика ИБ предприятия и ее структура
2. Политика ИБ: уровни и процедуры.
3. Анализ рисков. Риск-ориентированный подход к обеспечению ИБ.
4. В чем заключается нормативное обеспечение СЗИ?
5. Использование передовых методов оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС.
1. Понятие СУИБ. Модели, которые входят в состав архитектуры СУИБ.

2. Разработка технико-экономического обоснования СУИБ.
3. Модель системы автоматизированного проектирования СУИБ
4. Расследование инцидентов.
5. Управление идентификационными данными и доступом
6. Чрезвычайные ситуации (ЧС) и их классификация.
7. Принципы и алгоритмы принятия решений в нестандартных ситуациях.
8. Аудит безопасности. Оценка информационной безопасности бизнеса. Проблема измерения и оценивания информационной безопасности бизнеса.

5. Формы промежуточной аттестации

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

Примерное задание:

• Вопросы к зачету

блок 1

1. Информационная безопасность ИС в процессе эксплуатации прикладных ИС .
2. Виды информации. Конфиденциальная информация .
3. Понятие коммерческой тайны .
4. Виды угроз информационным объектам предприятия .
5. Комплексный подход к защите информации на предприятии .
6. Признаки классификации угрозы ИБ .
7. Внутренние угрозы ИБ.
8. Внешние угрозы ИБ .
9. Правовая база ИБ .
10. Нормативная база защиты информации .
11. Организационные средства защиты данных .
12. Международные стандарты информационной безопасности ИС в процессе эксплуатации.
13. Состав защищаемой информации .
14. Какие вы знаете источники дестабилизирующего воздействия на информацию?
15. Выявление каналов доступа к информации.
16. Методы получения несанкционированного доступа к информации.
17. Канал доступа к информации и его связь с и источником воздействия на информацию.
18. Методы оценки качества, надежности и информационной безопасности ИС
19. Какие задачи решаются с помощью криптографических методов?
20. Криптографические системы симметричного шифрования .
21. Криптографические системы асимметричного шифрования.
22. Составные криптографические системы .
23. Защита информации в компьютерных сетях .
24. Электронная подпись и ее назначение .
25. Вредоносное программное обеспечение .

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. В чем заключается нормативное обеспечение СЗИ?
9. Использование передовых методов оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС .
10. Понятие СУИБ. Модели, которые входят в состав архитектуры СУИБ.
11. Разработка технико-экономического обоснования СУИБ.
12. Модель системы автоматизированного проектирования СУИБ .
13. Какие требования предъявляются к технологии управления СЗИ?
14. Расследование инцидентов.
15. Управление идентификационными данными и доступом.
16. Чрезвычайные ситуации (ЧС) и их классификация .
17. Принципы и алгоритмы принятия решений в нестандартных ситуациях .
18. Использование информационных сервисов для автоматизации прикладных и информационных процессов управления ИБ .
19. Аудит безопасности. Оценка информационной безопасности бизнеса .
20. Проблема измерения и оценивания информационной безопасности ИС .
21. 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 информационных систем	15	
доклад / конференция / реферат	Раздел 2. Управление информационной безопасностью информационных систем	15	
тест по итогам занятия	Раздел 1. Обеспечение информационной безопасности информационных систем	20	
устный опрос / собеседование	Раздел 1. Обеспечение информационной безопасности информационных систем	15	
устный опрос / собеседование	Раздел 2. Управление информационной безопасностью информационных систем	15	
	Максимальный текущий балл	80	80
Промежуточная аттестация		зачет	
	Максимальный аттестационный балл	20	20
	Общий балл по дисциплине	100	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. 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

Дополнительная литература:

1. 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

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 аттестации, в том числе, для организации практической подготовки обучающийся, с перечнем основного оборудования (аудитория № 3): Столы для обучающихся; Стулья для обучающихся;	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

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 подготовки обучающийся, с перечнем основного оборудования (аудитория № 27) Компьютерные столы для обучающихся; Стулья для обучающихся; Стол педагогического работника;	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

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 обучающийся, с перечнем основного оборудования (аудитория № 16) Компьютерные столы для обучающихся; Стулья для обучающихся; Стол педагогического работника;	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

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-образовательную среду лицензиата; Ноутбуки с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду лицензиата; Принтер; Сканер	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

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-образовательную среду лицензиата; Ноутбуки с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную 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 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
Помещение для самостоятельной работы обучающихся с перечнем основного оборудования (аудитория № 31): Столы для обучающихся; Стулья для обучающихся; Компьютеры с возможностью подключения к сети «Интернет» и обеспечением	170001, Тверская область, г. Тверь, ул. Спартака, д. 26а (20,3 кв.м., 2 этаж, помещение № 31)	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

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				

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.03.02 «Технология обеспечения информационной безопасности»

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.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.ТВ23 П.ТВ24 П.ТВ25 П.Т1 П.Т2

				Т.Д1_1 Т.Д2_1 Т.Д3_1 Т.Д4_1 Т.Д5_1 Т.Д6_1 Т.Д7_1 Т.Д8_1 Т.Д9_1 Т.Д10_1 Т.Д11_1 Т.Д12_1 Т.Д13_1 Т.Д14_1 Т.Д15_1 Т.Д16_1 Т.Д17_1 Т.Д18_1 Т.Д19_1 Т.Д20_1 Т.Т1_1 Т.Т2_1 Т.Т3_1 Т.У1_1 Т.У2_1 Т.У3_1 Т.У4_1 Т.Д1_2 Т.Д2_2 Т.У1_2 Т.У2_2 Т.У3_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.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.ТВ23 П.ТВ24 П.ТВ25 Т.Д1_1 Т.Д2_1 Т.Д3_1 Т.Д4_1 Т.Д5_1 Т.Д6_1 Т.Д7_1 Т.Д8_1 Т.Д9_1 Т.Д10_1 Т.Д11_1 Т.Д12_1 Т.Д13_1 Т.Д14_1 Т.Д15_1 Т.Д16_1 Т.Д17_1 Т.Д18_1 Т.Д19_1 Т.Д20_1 Т.У1_1

			Т.У2_1 Т.У3_1 Т.У4_1 Т.Д1_2 Т.Д2_2 Т.У1_2 Т.У2_2 Т.У3_2

Контрольные задания. Текущая аттестация

доклад / конференция / реферат - Раздел 1. Обеспечение информационной безопасности информационных систем	**Номер задания**
1. Законодательство РФ в области защиты коммерческой тайны.	Т.Д1_1
Виды искусственных преднамеренных угроз ИБ предприятия.	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
Деловая разведка как канал получения информации.	Т.Д6_1
Характеристика каналов доступа	Т.Д7_1
Характеристика потенциальных нарушителей.	Т.Д8_1
Технология работы с электронной подписью.	Т.Д9_1
Системы обнаружения вторжений.	Т.Д10_1
Обзор методик и программных средств для анализа и управления рисками	Т.Д11_1
Персональная ответственность топ-менеджера за сохранность корпоративных и клиентских данных	Т.Д12_1
Основные информационные риски в работе топ-менеджера.	Т.Д13_1
Методология реагирования на инциденты.	Т.Д14_1
Методы борьбы с инсайдерами.	Т.Д15_1
Подсистема защиты корпоративной информации от вредоносных программ.	Т.Д16_1
Контроль функционирования СУИБ.	Т.Д17_1
Состав сотрудников, обеспечивающих функционирование СУИБ.	Т.Д18_1
Аудит ИБ предприятия.	Т.Д19_1
Обзор современных стандартов и методологий по управлению ИБ.	Т.Д20_1

тест по итогам занятия - Раздел 1. Обеспечение информационной безопасности информационных систем	**Варианты ответов**	**Номер задания**
Шифрование информации это:	1 процесс сбора, накопления, обработки, хранения, распределения и поиска информации 2 преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа 3 получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств 4 совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям 5 деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.	T.T1_1
Атака, которая использует недостатки алгоритмов удаленного поис¬ка (DNS (Internet)…):	1 подмена доверенного объекта или субъекта распределенной вычислительной сети 2 ложный объект распределенной вычислительной сети 3 анализ сетевого трафика 4 отказ в обслуживании; 5 удаленный контроль над станцией в сети.	T.T2_1
В каких единицах измеряется риск?	1 в уровнях 2 в процентах 3 в стоимостном выражении 4 во временном выражении	T.T3_1

устный опрос / собеседование - Раздел 1. Обеспечение информационной безопасности информационных систем	**Номер задания**

Информационные характеристики бизнеса: основные понятия и определения.	Т.У1_1
Правовая среда бизнеса и ее свойства.	Т.У2_1
Учредительная и лицензионная база организации.	Т.У3_1
Влияние специфики деятельности предприятия на определение состава элементов защищаемого объекта.	Т.У4_1

доклад / конференция / реферат - Раздел 2. Управление информационной безопасностью информационных систем	**Номер задания**
Виды искусственных непреднамеренных угроз ИБ предприятия.	Т.Д1_2
Законодательство РФ в области защиты коммерческой тайны.	Т.Д2_2

устный опрос / собеседование - Раздел 2. Управление информационной безопасностью информационных систем	**Номер задания**
Какие вы знаете источники дестабилизирующего воздействия на информацию	Т.У1_2
Методы получения несанкционированного доступа к информации Выявление каналов доступа к информации.	Т.У2_2
Какие задачи решаются с помощью криптографических методов? Законодательная база защиты информации.	Т.У3_2

Контрольные задания. Промежуточная аттестация

Зачет. Практическое задание	**Номер задания**
Дайте определение следующему понятию: несанкционированный доступ к данным.	П.П1
В каких правовых документах идет речь о государственной тайне? Приведите выдержку из документа с нужным определением.	П.П2
Дайте определение следующему понятию: идентификация	П.П3
В каких правовых документах идет речь о коммерческой тайне? Приведите выдержку из документа с нужным определением.	П.П4
Дайте определение следующему понятию: анализ рисков.	П.П5
В каких правовых документах идет речь о защите информации. Приведите выдержку из документа с нужным определением.	П.П6

Зачет. Теоретический вопрос	**Номер задания**
Информационная безопасность ИС в процессе эксплуатации прикладных ИС	П.ТВ1
Виды информации. Конфиденциальная информация.	П.ТВ2
Понятие коммерческой тайны.	П.ТВ3

Виды угроз информационным объектам предприятия.	П.ТВ4
Комплексный подход к защите информации на предприятии.	П.ТВ5
Признаки классификации угрозы ИБ.	П.ТВ6
Внутренние угрозы ИБ.	П.ТВ7
Внешние угрозы ИБ.	П.ТВ8
Правовая база ИБ.	П.ТВ9
Нормативная база защиты информации.	П.ТВ10
Организационные средства защиты данных.	П.ТВ11
Международные стандарты информационной безопасности ИС в процессе эксплуатации.	П.ТВ12
Состав защищаемой информации.	П.ТВ13
Какие вы знаете источники дестабилизирующего воздействия на информацию?	П.ТВ14
Выявление каналов доступа к информации.	П.ТВ15
Методы получения несанкционированного доступа к информации.	П.ТВ16
Канал доступа к информации и его связь с и источником воздействия на информацию.	П.ТВ17
Методы оценки качества, надежности и информационной безопасности ИС	П.ТВ18
Какие задачи решаются с помощью криптографических методов?	П.ТВ19
Криптографические системы симметричного шифрования..	П.ТВ20
Криптографические системы асимметричного шифрования..	П.ТВ21
Составные криптографические системы.	П.ТВ22
Защита информации в компьютерных сетях.	П.ТВ23
Электронная подпись и ее назначение .	П.ТВ24
Вредоносное программное обеспечение .	П.ТВ25

Зачет. Тестовый вопрос	**Варианты ответов**	**Номер задания**
Криптографические средства – это..?	1 регламентация правил использования, обработки и передачи информации ограниченного доступа 2 средства защиты с помощью преобразования информации (шифрование) 3 средства, в которых программные и аппаратные части полностью взаимосвязаны.	П.Т1
Что используется для создания		П.Т2

цифровой подписи?	1 Закрытый ключ получателя 2 Открытый ключ отправителя 3 Закрытый ключ отправителя 4 Открытый ключ получателя	

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 информационных систем	15	
доклад / конференция / реферат	Раздел 2. Управление информационной безопасностью информационных систем	15	
тест по итогам занятия	Раздел 1. Обеспечение информационной безопасности информационных систем	20	
устный опрос / собеседование	Раздел 1. Обеспечение информационной безопасности информационных систем	15	
устный опрос / собеседование	Раздел 2. Управление информационной безопасностью информационных систем	15	
Максимальный текущий балл		80	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	100	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