МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Информационная безопасность»

Направление подготовки: 38.03.05 Бизнес-информатика

Направленность (профиль) программы бакалавриата
«Электронный бизнес»

*в том числе **оценочные материалы***
для проведения текущего контроля успеваемости
и промежуточной аттестации обучающихся по дисциплине

ОДОБРЕНО
Ученым советом ЧУВО «ВШП»
Протокол заседания
№01-02/24 от 22 апреля 2024 г.

УТВЕРЖДАЮ
Ректор ЧУВО «ВШП»
«22» апреля 2024 г.
Ректор Аллабян М.Г.

Тверь, 2024

Документ подписан электронной цифровой подписью VSHP EDS GEN 1, уникальный ключ документа:
66DF-A294-58C5-EQVC
Организация: ЧУВО «ВШП», ИНН: 6903013604
Дата подписания: 12.06.2024 19:32 MSK
Подписал: Аллабян М. Г.

Рабочая программа учебной дисциплины Информационная безопасность, как обязательного компонента основной профессиональной образовательной программы высшего образования — программы бакалавриата по направлению подготовки 38.03.05. Бизнес-информатика (направленность (профиль) «Электронный бизнес»), одобренной на заседании Учёного совета образовательной организации, утверждённой ректором Частного образовательного учреждения высшего образования «Высшая школа предпринимательства» 22.04.2024, разработана в соответствии с профессиональным стандартом «Менеджер по информационным технологиям», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 30 августа 2021 г. № 588н, и профессиональным стандартом «Специалист по информационным системам», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 18 ноября 2014 г. № 896н, с учётом рабочей программы воспитания, календарного плана воспитательной работы образовательной организации на 2024/2025 учебный год, утверждённых ректором образовательной организации 22.04.2024.

Образовательная деятельность в форме практической подготовки организована Частным образовательным учреждением высшего образования «Высшая школа предпринимательства» при реализации учебной дисциплины Информационная безопасность (контактная работа педагогического работника с обучающимся (бакалавром) при проведении практических занятий по дисциплине), обязательного компонента основной профессиональной образовательной программы высшего образования — программы бакалавриата по направлению подготовки 38.03.05. Бизнес-информатика (направленность (профиль) «Электронный бизнес»), форма обучения — очная), одобренной на заседании Учёного совета образовательной организации, утверждённой ректором Частного образовательного учреждения высшего образования «Высшая школа предпринимательства» 22.04.24, в условиях выполнения обучающимися (бакалаврами) определённых видов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по профилю соответствующей основной образовательной программы высшего образования.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Информационная безопасность» является формирование у обучающихся общекультурных и профессиональных компетенций в процессе изучения различных аспектов защиты информации для последующего применения в учебной и практической деятельности.

Задачи дисциплины:

- систематизация, формализация и расширение знаний по основным положениям теории информации, информационной безопасности и стандартами шифрования;
- изучение математических основ защиты информации; а также методов, средств и инструментов шифрования, применяемых в сфере информационных технологий и бизнеса;
- дать студенту достаточно прочные представления о информационной безопасности, включая аппаратную часть и математическое обеспечение;
- привитие навыков работы с методами шифрования и криптоанализа;
- формирование современной культуры программирования.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП БАКАЛАВРИАТА

Дисциплина **«Информационная безопасность»** относится к вариативной части Блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы — программы бакалавриата по направлению подготовки 38.03.05 Бизнес-информатика направленность (профиль) «Электронный бизнес».

№ п/	Номер/ индекс компе-тенции	Содержание компетенции (или ее части)	В результате изучения дисциплины обучающиеся должны:		
			Знать:	Уметь:	Владеть (навыками):
1	ОПК-1	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	математические принципы, лежащие в основе криптографических моделей; теорию простых чисел и модульной арифметики	уметь использовать алгоритмические модели и языки программирования для разработки алгоритмов шифрования; уметь выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач	владеть алгоритмическими языками для разработки прикладных алгоритмов шифрования; владеть навыками решения задач криптоанализа и шифрования; Приемами обнаружения сетевых проникновений

2	ПК-9	организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия	Основные принципы административно-правовой защиты информации	Быстро реагировать на различные угрозы информационной безопасности уметь применять современные технологии создания брандмауэров и IDS-комплексов	Применения, установки и настройки антивирусных систем и систем распознавания угроз и атак; Навыками работы по обнаружению и защите от DDOS-атак

2.1. Для изучения дисциплины необходимы следующие знания, умения, навыки, формируемые предшествующими дисциплинами:

- *Математический анализ;*
- *Теория вероятностей и математическая статистика;*
- *Программирование*

2.2. Перечень последующих дисциплин, для которых необходимы знания, умения, навыки, формируемые данной дисциплиной:

- *Цифровые ресурсы предприятия;*
- *Администрирование цифровой инфраструктуры предприятия.*
- *Государственная итоговая аттестация.*

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

Изучение данной дисциплины направлено на формирование у обучающихся следующих общепрофессиональных (ОПК) и профессиональных (ПК) компетенций:

КАРТА КОМПЕТЕНЦИЙ ДИСЦИПЛИНЫ					
НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ: Информационная безопасность					
Цель дисциплины	формирование у обучающихся общепрофессиональных и профессиональных компетенций в процессе изучения бизнес-информатики и цифровой экономики для последующего применения в учебной и практической деятельности				
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие					
Общепрофессиональные компетенции					
ИНДЕКС	**ФОРМУЛИРОВКА**	**Перечень компонентов**	**Технологии формирования**	**Форма оценочного средства**	**Уровни освоения компетенций**
ОПК-1	способностью решать стандартные	**Знать** математические принципы, лежащие в основе криптографических моделей; теорию простых чисел и модульной	Путем проведения лекционных, лабораторных	Тестирование Вопросы	**Пороговый** Способен решать стандартные задачи

	задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	арифметики; **уметь** использовать алгоритмические модели и языки программирования для разработки алгоритмов шифрования; уметь выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач; **владеть** алгоритмическими языками для разработки прикладных алгоритмов шифрования; владеть навыками решения задач криптоанализа и шифрования; Приемами обнаружения сетевых проникновений;	занятий, применения новых образовательных технологий организации самостоятельной работы студентов		информационной безопасности **Повышенный** Способен решать задач криптографии повышенной сложности
Профессиональные компетенции					
ПК-9	организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия	**Знать** основные принципы административно-правовой защиты информации **Уметь** быстро реагировать на различные угрозы информационной безопасности уметь применять современные технологии создания брандмауэров и IDS-комплексов; **Владеть навыками п**рименения, установки и настройки антивирусных систем и систем распознавания угроз и атак; Навыками работы по обнаружению и защите от DDOS-атак	Путем проведения лекционных, лабораторных занятий, применения новых образовательных технологий ,организации самостоятельной работы студентов	Тестирование Вопросы	**Пороговый** Способен решать стандартные задачи **Повышенный** Способен быстро решать задачи определения взлома и атак злоумышленников повышенной

					сложности

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Форма обучения	Курс/ семестр	Аудиторные занятия/контактная работа, час.				СР, час.	Форма аттестации
		Л	П	Пром.атт	конс		
очная	4/7	36	36	18	1	89	Зачёт с оценкой

Условные обозначения:
Л — лекционные занятия
П — практические занятия
СР — самостоятельная работа обучающегося
Пром.атт — промежуточная аттестация
Конс — консультации

Вид учебной работы	Всего часов
Контактная работа	**72**
Лекционные занятия (Лек)	36
Практические занятия (Пр)	36
Иная контактная работа, в том числе:	**19**
консультации по курсовой работе (проекту), контрольным работам (РГР)	
контактная работа на аттестацию (сдача зачета, зачета с оценкой; защита курсовой работы (проекта); сдача контрольных работ (РГР))	18
контактная работа на аттестацию в сессию (консультация перед зачетом)	1
Часы на контроль	**18**
Самостоятельная работа (СР)	**89**
Общая трудоемкость дисциплины (модуля)	
часы:	**180**
зачетные единицы:	**5**

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО РАЗДЕЛАМ (ТЕМАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

5.1 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ семестра	№ раздела	Наименование раздела дисциплины	Содержание раздела в дидактических единицах

7	1	**Основные составляющие информационной безопасности**	Основные понятия информационной безопасности. Классификация угроз. Классификация средств защиты информации. Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности
	2	**Криптографические способы защиты информации**	Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Простые числа. Квадратичное сравнение. Криптографическая система RSA. Криптосистемы. Простые криптосистемы. Шифрование методом замены (подстановки). Многоалфавитная подстановка. Многоалфавитная одноконтурная обыкновенная подстановка. Таблицы Вижинера**.** Многоалфавитная одноконтурная монофоническая подстановка. Мно-алфавитная многоконтурная подстановка. Шифрование методом перестановки. Простая перестановка. Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard. Режимы работы алгоритма DES. Алгоритм шифрования данных IDEA. Общая схема алгоритма IDEA
7	3	**Антивирусная защита**	Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ. Основы работы антивирусных программ: Сигнатурный и эвристический анализ. Тестирование работы антивируса. Классификация антивирусов. Режимы рабо- ты антивирусов. Антивирусные комплексы

	4	**Сетевая безопасность**	Защита информации в локальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты. Уровень защиты рабочих станций и сетевых серверов. Уровень защиты почты. Уровень защиты шлюзов. Централизованное управление антивирусной защитой. Логическая сеть. Схема сбора статистики в системе антивирусной защиты. Управление ключами шифрования и безопасность сети. Целостность сообщения и установление подлинности сообщения. Криптографические хэш-функции. Цифровая подпись. Установление подлинности объекта. Управление ключами. Безопасность на прикладном уровне: PGP и S/MIME. Безопасность на транспортном уровне: SSL и TLS. Безопасность на сетевом уровне: IP SEC. Брандмауэры. Определение типов брандмауэров. Разработка конфигурации межсетевого экрана. Построение набора правил межсетевого экрана. Система обнаружения вторжений (IDS). Узловые IDS. Анализаторы журналов. Датчики признаков. Анализаторы системных вызовов. Анализаторы поведения приложений. Контроллеры целостности файлов. Сетевые IDS. Установка IDS. Определение целей применения IDS. Управление IDS

5.2 Разделы, темы дисциплины и виды занятий

ЛЕКЦИОННЫЕ ЗАНЯТИЯ И САМОСТОЯТЕЛЬНАЯ РАБОТА

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в ак. часах)		Индикаторы достижения компетенций
		занятия лекционного типа	самостоятельная работа	
1.	Основные составляющие информационной безопасности	9	22	ОПК-1.1 УК-9.1
2.	Криптографические способы защиты информации	9	23	
3.	Антивирусная защита	9	22	
4.	Сетевая безопасность	9	22	
	Итого	**36**	**89**	

ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

№ раздела	Наименование раздела дисциплины	Содержание раздела в дидактических единицах	Объем (час.)
1	**Основные составляющие информационной безопасности**	Основные понятия информационной безопасности. Классификация угроз. Классификация средств защиты информации. Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты.	9

		Программные и программно-аппаратные методы и средства обеспечения информационной безопасности	
2	**Криптографические способы защиты информации**	Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Простые числа. Квадратичное сравнение. Криптографическая система RSA. Криптосистемы. Простые криптосистемы. Шифрование методом замены (подстановки). Многоалфавитная подстановка. Многоалфавитная одноконтурная обыкновенная подстановка. Таблицы Вижинера**.** Многоалфавитная одноконтурная монофоническая подстановка. Мно-алфавитная многоконтурная подстановка. Шифрование методом перестановки. Простая перестановка. Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard. Режимы работы алгоритма DES. Алгоритм шифрования данных IDEA. Общая схема алгоритма IDEA	9
3	**Антивирусная защита**	Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ. Основы работы антивирусных программ: Сигнатурный и эвристический анализ. Тестирование работы антивируса. Классификация антивирусов. Режимы рабо-ты антивирусов. Антивирусные комплексы	9

4	**Сетевая безопасность**	Защита информации в локальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты. Уровень защиты рабочих станций и сетевых серверов. Уровень защиты почты. Уровень защиты шлюзов. Централизованное управление антивирусной защитой. Логическая сеть. Схема сбора статистики в системе антивирусной защиты. Управление ключами шифрования и безопасность сети. Целостность сообщения и установление подлинности сообщения. Криптографические хэш-функции. Цифровая подпись. Установление подлинности объекта. Управление ключами. Безопасность на прикладном уровне: PGP и S/MIME. Безопасность на транспортном уровне: SSL и TLS. Безопасность на сетевом уровне: IP SEC. Брандмауэры. Определение типов брандмауэров. Разработка конфигурации межсетевого экрана. Построение набора правил межсетевого экрана. Система обнаружения вторжений (IDS). Узловые IDS. Анализаторы журналов. Датчики признаков. Анализаторы системных вызовов. Анализаторы поведения приложений. Контроллеры целостности файлов. Сетевые IDS. Установка IDS. Определение целей применения IDS. Управление IDS	9
	Итого		**36**

6. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТА

Темы рефератов

1. Информация - фактор существования и развития общества. Основные формы проявления информации, её свойства как объекта безопасности.
2. Понятие безопасности и её составляющие. Безопасность информации.
3. Обеспечение информационной безопасности: содержание и структура понятия.
4. Национальные интересы в информационной сфере.
5. Источники и содержание угроз в информационной сфере.
6. Соотношение понятий «информационная безопасность» и «национальная безопасность»
7. Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности.
8. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.
9. Система обеспечения информационной безопасности.
10. Обеспечение информационной безопасности Российской Федерации.
11. Понятие информационной войны. Проблемы информационной войны.
12. Информационное оружие и его классификация.

13. Цели информационной войны, её составные части и средства её ведения. Объекты воздействия в информационной войне.

14. Уровни ведения информационной войны. Информационные операции. Психологические операции.

15. Уровни ведения информационной войны. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети.

16. Основные положения государственной информационной политики Российской Федерации.

17. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.

18. Виды защищаемой информации в сфере государственного и муниципального управления.

19. Обеспечение информационной безопасности организации.

20. Характеристика эффективных стандартов по безопасности.

21. Требования к полноте эффективных стандартов по безопасности.

22. Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере.

23. Информация - фактор существования и развития общества.

24. Обеспечение информационной безопасности: содержание и структура понятия.

25. Система обеспечения информационной безопасности. Обеспечение информационной безопасности организации.

26. Обеспечение информационной безопасности Российской Федерации.

27. Международная нормативная база обеспечения безопасности. Федеральная нормативная база обеспечения безопасности

28. Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти.

29. Административный уровень обеспечения информационной безопасности.

30. Организационные структуры системы обеспечения информационной безопасности предприятия (организации).

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Тестовые задания для текущего контроля успеваемости

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

1. Разработка аппаратных средств обеспечения правовых данных
2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий
3. Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

1. Хищение жестких дисков, подключение к сети, инсайдерство
2. Перехват данных, хищение данных, изменение архитектуры системы
3. Хищение данных, подкуп системных администраторов, нарушение регламента

работы

3) Виды информационной безопасности:
1. Персональная, корпоративная, государственная
2. Клиентская, серверная, сетевая
3. Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
1. несанкционированного доступа, воздействия в сети
2. инсайдерства в организации
3. чрезвычайных ситуаций

5) Основные объекты информационной безопасности:
1. Компьютерные сети, базы данных
2. Информационные системы, психологическое состояние пользователей
3. Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:
1. Искажение, уменьшение объема, перекодировка информации
2. Техническое вмешательство, выведение из строя оборудования сети
3. Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:
1. Экономической эффективности системы безопасности
2. Многоплатформенной реализации системы
3. Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:
1. руководители, менеджеры, администраторы компаний
2. органы права, государства, бизнеса
3. сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:
1. Установление регламента, аудит системы, выявление рисков
2. Установка новых офисных приложений, смена хостинг -компании
3. Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:
1. Неоправданных ограничений при работе в сети (системе)
2. Рисков безопасности сети, системы
3. Презумпции секретности

11) Принципом политики информационной безопасности является принцип:
1. Невозможности миновать защитные средства сети (системы)
2. Усиления основного звена сети, системы
3. Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

1. Усиления защищенности самого незащищенного звена сети (системы)
2. Перехода в безопасное состояние работы сети, системы
3. Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

1. Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
2. Одноуровневой защиты сети, системы
3. Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

1. Компьютерный сбой
2. Логические закладки («мины»)
3. Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

1. Прочитать приложение, если оно не содержит ничего ценного – удалить
2. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
3. Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

1. Секретность ключа определена секретностью открытого сообщения
2. Секретность информации определена скоростью передачи данных
3. Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

1. Электронно-цифровой преобразователь
2. Электронно-цифровая подпись
3. Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

1. Покупка нелицензионного ПО
2. Ошибки эксплуатации и неумышленного изменения режима работы системы
3. Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

1. Распределенный доступ клиент, отказ оборудования
2. Моральный износ сети, инсайдерство
3. Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:

1. Слабый трафик, информационный обман, вирусы в интернет
2. Вирусы в сети, логические мины (закладки), информационный перехват
3. Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:

1. Потерей данных в системе
2. Изменением формы информации
3. Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

1. Целостность
2. Доступность
3. Актуальность

23) Угроза информационной системе (компьютерной сети) – это:

1. Вероятное событие
2. Детерминированное (всегда определенное) событие
3. Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

1. Регламентированной
2. Правовой
3. Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

1. Программные, технические, организационные, технологические
2. Серверные, клиентские, спутниковые, наземные
3. Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

1. Владелец сети
2. Администратор сети
3. Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

1. Руководств, требований обеспечения необходимого уровня безопасности
2. Инструкций, алгоритмов поведения пользователя в сети
3. Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

1. Аудит, анализ затрат на проведение защитных мер
2. Аудит, анализ безопасности
3. Аудит, анализ уязвимостей, риск-ситуаций

Вопросы для промежуточной аттестации по дисциплине:

1. Роль информации в современном мире. Понятие о защищаемой информации.
2. Теория информационной безопасности. Основные направления.
3. Обеспечение ИБ и направления защиты.
4. Требования к системе и политике ИБ.

5. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.

6. Доктрина информационной безопасности РФ.

7. Защита государственной тайны в РФ.

8. Защита коммерческой тайны в РФ.

9. Защита персональных данных в РФ.

10. Защита служебной и профессиональной тайны в РФ.

11. Процедуры сертификации и аттестации в РФ.

12. Понятие о защищаемой информации. Свойства информации.

13. Угрозы информации. Классификация угроз.

14. Угрозы нарушения конфиденциальности информации. Особенности и примеры реализации угроз.

15. Угрозы нарушения целостности информации. Особенности и примеры реализации угроз.

16. Угроза нарушения доступности информации. Особенности и примеры реализации угрозы.

17. Источники угроз. Классификация источников угроз.

18. Идентификация и аутентификация. Использование парольной защиты. Недостатки парольной защиты.

19. Понятие электронной подписи.

20. Организационные меры обеспечения информационной безопасности. Служба безопасности предприятия.

21. Организация внутри объектового режима предприятия. Организация охраны.

22. Криптографические меры обеспечения информационной безопасности. Классификация криптографических алгоритмов.

23. Программно-аппаратные защиты информации. Межсетевые экраны, их функции и назначения.

24. Программно-аппаратные защиты информации. Антивирусные средства, их функции и назначения.

25. Особенности защиты беспроводных и мобильных подключений.

26. Симметричное и ассиметричное шифрование.

27. Принципы симметричного шифрования.

28. Односторонние функции и их применение.

29. Простейшие методы ассиметричного шифрования.

30. Метод RSA.

31. Электронная подпись и ее применение.

Оценка устного (письменного) ответа студента на экзамене:

- оценка **«отлично»** выставляется студенту, если он владеет понятийным аппаратом, демонстрирует глубину и полное овладение содержанием учебного материала, в котором легко ориентируется;
- оценка **«хорошо»** выставляется студенту, за умение грамотно излагать материал, но при этом содержание и форма ответа могут иметь отдельные неточности;
- оценка **«удовлетворительно»** выставляется, если студент обнаруживает знания и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности в определении понятий, не умеет доказательно обосновывать свои суждения;
- оценка **«неудовлетворительно»** выставляется, если студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определении понятий, искажает их смысл.

8. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники и учебные пособия, иная учебная литература, специальные технические средства обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

а) для слабовидящих:

- на промежуточной аттестации присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);
- задания для выполнения, а также инструкция о порядке проведения промежуточной аттестации оформляются увеличенным шрифтом;
- задания для выполнения на промежуточной аттестации зачитываются ассистентом;
- письменные задания выполняются на бумаге, надиктовываются ассистенту;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- студенту для выполнения задания при необходимости предоставляется увеличивающее устройство;

в) для глухих и слабослышащих:

- на промежуточной аттестации присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);
- промежуточная аттестация проводится в письменной форме;
- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости поступающим предоставляется звукоусиливающая аппаратура индивидуального пользования;
- по желанию студента промежуточная аттестация может проводиться в письменной форме;

д) для лиц с нарушениями опорно-двигательного аппарата (тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
- по желанию студента промежуточная аттестация проводится в устной форме.

Примечание:

а) Для обучающегося (бакалавра), осваивающего учебную дисциплину, обязательный компонент основной профессиональной образовательной программы высшего образования — программы бакалавриата по направлению подготовки **38.03.05. Бизнес-информатика** (направленность (профиль) «Электронный бизнес»), форма обучения — очная), одобренной на заседании Учёного совета образовательной организации, утверждённой ректором Частного образовательного учреждения высшего образования «Высшая школа предпринимательства» 22.04.24, **по индивидуальному учебному плану** (*при наличии факта зачисления в образовательную организацию такого обучающегося (бакалавра)*), **Институт:**

- разрабатывает, согласовывает с участниками образовательных отношений и утверждает в установленном порядке согласно соответствующему локальному нормативному акту **индивидуальный учебный план** конкретного обучающегося (бакалавра) (*учебный план, обеспечивающий освоение конкретной основной образовательной программы высшего образования на основе индивидуализации её содержания с учётом особенностей и образовательных потребностей конкретного обучающегося (бакалавра)*);
- устанавливает для конкретного обучающегося (бакалавра) по индивидуальному учебному плану **одинаковые дидактические единицы** — элементы содержания учебного материала, изложенного в виде утверждённой в установленном образовательной организацией порядке согласно соответствующему локальному нормативному акту рабочей программы учебной дисциплины, обязательного компонента разработанной и реализуемой Институтом основной

профессиональной образовательной программы высшего образования — программы бакалавриата по направлению подготовки **38.03.05. Бизнес-информатика** (направленность (профиль) «Электронный бизнес»), форма обучения — очная), как и для обучающего (бакалавра), осваивающего основную образовательную программу высшего образования в учебной группе;
- определяет в индивидуальном учебном плане конкретного обучающегося (бакалавра) **объём учебной дисциплины** с указанием количества академических часов/ ЗЕТ, выделенных на его контактную работу (групповую и (или) индивидуальную работу) с руководящими и (или) научно-педагогическими работниками, реализующими основную образовательную программу высшего образования;
- определяет в индивидуальном учебном плане конкретного обучающегося (бакалавра) количество академических часов/ ЗЕТ по учебной дисциплине, выделенных на его самостоятельную работу (*при необходимости*).

б) Для обучающегося (бакалавра) с ограниченными возможностями здоровья и инвалида, осваивающего учебную дисциплину, обязательный компонент основной профессиональной образовательной программы высшего образования — программы бакалавриата по направлению подготовки **38.03.05. Бизнес-информатика** (направленность (профиль) «Электронный бизнес»), форма обучения — очная), одобренной на заседании Учёного совета образовательной организации, утверждённой ректором Частного образовательного учреждения высшего образования «Высшая школа предпринимательства» 22.04.24, (*при наличии факта зачисления в образовательную организацию такого обучающегося (бакалавра) с учётом конкретной (конкретных) нозологии (нозологий)*), **Институт:**
- разрабатывает, согласовывает с участниками образовательных отношений и утверждает в установленном порядке согласно соответствующему локальному нормативному акту **индивидуальный учебный план** конкретного обучающегося (бакалавра) с ограниченными возможностями здоровья/ инвалида (*при наличии факта зачисления в образовательную организацию такого обучающегося (бакалавра) с учётом конкретной (конкретных) нозологии (нозологий)*) (*учебный план, обеспечивающий освоение конкретной основной образовательной программы высшего образования на основе индивидуализации её содержания с учётом особенностей и образовательных потребностей конкретного обучающегося (бакалавра)*);
- устанавливает для конкретного обучающегося (бакалавра) с ограниченными возможностями здоровья содержание образования (**одинаковые дидактические единицы** — элементы содержания учебного материала, как и для обучающего (бакалавра), осваивающего основную образовательную программу высшего образования в учебной группе) и условия организации обучения, изложенного в виде утверждённой в установленном Институтом порядке согласно соответствующему локальному нормативному акту рабочей программы учебной дисциплины, обязательного компонента разработанной и реализуемой им адаптированной основной профессиональной образовательной программы высшего образования - программы бакалавриата по направлению подготовки **38.03.05. Бизнес-информатика** (направленность (профиль) «Электронный бизнес»), форма обучения — очная), а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида (для конкретного обучающегося (бакалавра) с ограниченными возможностями здоровья/ инвалида (*при наличии факта зачисления в образовательную организацию такого обучающегося (бакалавра) с учётом конкретной (конкретных) нозологии (нозологий)*);
- определяет в индивидуальном учебном плане конкретного обучающегося бакалавра) с ограниченными возможностями здоровья/ инвалида (*при наличии факта зачисления такого обучающегося (бакалавра) с учётом конкретной (конкретных) нозологии (нозологий)*) **объём учебной дисциплины** с указанием количества академических часов/ ЗЕТ, выделенных на его контактную работу (групповую и (или) индивидуальную работу) с руководящими и (или) научно-педагогическими работниками, реализующими основную образовательную программу высшего образования;
- определяет в индивидуальном учебном плане конкретного обучающегося (бакалавра) с ограниченными возможностями здоровья/ инвалида (*при наличии факта зачисления в образовательную организацию такого обучающегося (бакалавра) с учётом конкретной*

(конкретных) нозологии (нозологий)) количество академических часов/ ЗЕТ по учебной дисциплине, выделенных на его самостоятельную работу (*при необходимости*).

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Конеев, И. Информационная безопасность предприятия [Текст] / И.Конеев, А.Беляев. – СПб. : БХВ-Петербург, 2003. – 752с.

2. Штарьков, Ю. М. Универсальное кодирование: Теория и алгоритмы [Электронный ресурс] / Ю. М. Штарьков. – М. : Физматлит, 2013. – 280 с. –Режим доступа: http://biblioclub.ru/index.php?page=book&id=275569

Дополнительная литература:

1. Нестеров, С. А. Информационная безопасность [Электронный ресурс]: учебник и практикум для академического бакалавриата / С. А. Нестеров. —Москва : Издательство Юрайт, 2019. — 321 с. — Режим доступа: https://www.biblio-online.ru/bcode/434171

2. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс] : учебное пособие / Ю.Н. Загинайлов. – М. ; Берлин : Директ-Медиа, 2015. – 253 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=276557

3. Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О. В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=438331

9.2 Используемое программное обеспечение (*комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства*):

1. Microsoft Windows 10 (подписка MSDN 700593597, подписка DreamSparkPremium, 19.06.19) Adobe Acrobat Reader https://acrobat.adobe.com/ru/ru/acrobat/pdfreader.html
2. Microsoft office 2010 (Лицензия № 49487295 от 19.12.2011) OpenOffice https://www.openoffice.org/ru/
3. Консультант Плюс PTC Mathcad Express https://www.mathcad.com/ru

9.3 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Ватолин, Д. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео [Электронный ресурс] / Д. Ватолин [и др.]. – М.: ДИАЛОГМИФИ, 2002. – 384 с. – Режим доступа: http://www.compression.ru/book, свободный (дата обращения: 30.08.2019).
2. Сэломон, Д. Сжатие данных, изображения и звука [Электронный ресурс] / Д. Сэломон. – М.: Техносфера, 2004. – 367 с. – Режим доступа: http://da.kalinin.ru/books/salmon.pdf, свободный
3. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека. – Режим доступа: http://elibrary.ru/defaultx.asp, свободный
4. Единая коллекция цифровых образовательных ресурсов [Электронный ресурс] :

федеральный портал. – Режим доступа: http://school-collection.edu.ru/, свободный

5. Единое окно доступа к образовательным ресурсам [Электронный ресурс] : федеральный портал. – Режим доступа: http://window.edu.ru/, свободный

6. Интернет Университет Информационных технологий. [Электронный ресурс] : сайт. – Режим доступа: http://www.intuit.ru/, свободный

7. Портал естественных наук. [Электронный ресурс] : сайт. – Режим доступа: http://e-science11.ru, свободный

8. Российский общеобразовательный портал [Электронный ресурс] : образовательный портал. – Режим доступа: http://www.school.edu.ru/, свободный

9. Сервер Информационных Технологий [Электронный ресурс] : сайт. –Режим доступа: http://citforum.ru/, свободный

9.4 Базы данных, информационно-справочные и поисковые системы

1. Европейская цифровая библиотека Europeana: http://www.europeana.eu/portal
2. КонсультантПлюс: справочно-поисковая система [Электронный ресурс]. - http://www.consultant.ru
3. Информационно-издательский центр по геологии и недропользованию Министерства природных ресурсов и экологии Российской Федерации - ООО "ГЕОИНФОРММАРК": http://www.geoinform.ru
4. Информационно-аналитический центр «Минерал»: http://www.mineral.ru
5. Мировая цифровая библиотека: http://wdl.org/ru
6. Научная электронная библиотека «Scopus»: https://www.scopus.com
7. Научная электронная библиотека ScienceDirect: http://www.sciencedirect.com
8. Научная электронная библиотека «eLIBRARY»: https://elibrary.ru
9. Портал «Гуманитарное образование» http://www.humanities.edu.ru
10. Федеральный портал «Российское образование» http://www.edu.ru
11. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» http://school-collection.edu.ru
12. Поисковые системы Yandex, Rambler, Yahoo и др.
13. Электронно-библиотечная система издательского центра «Лань»: https://e.lanbook.com/books
14. Электронная библиотека Российской Государственной Библиотеки (РГБ): http://elibrary.rsl.ru
15. Электронная библиотека учебников: http://studentam.net
16. Электронно-библиотечная система «ЭБС ЮРАЙТ»: http://www.biblio-online.ru.
17. Электронная библиотечная система «Национальный цифровой ресурс «Руконт»»: http://rucont.ru
18. Электронно-библиотечная система http://www.sciteclibrary.ru

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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

Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно- наглядных пособий и используемого программного обеспечения	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
Специализированная многофункциональная учебная аудитория для проведения учебных занятий лекционного типа, групповых и индивидуальны	170001, Россия, город Тверь, улица Спартака, дом 26а

консультаций, текущего контроля промежуточной аттестации, в том числе, дл организации практической подготовк обучающийся, с перечнем основно оборудования (аудитория № 309): Столы для обучающихся; Стулья для обучающихся; Стол педагогического работника; Стул педагогического работника; Компьютер с возможностью подключения сети «Интернет» и обеспечением доступа электронную информационно-образовательну среду лицензиата; Интерактивная доска; Проектор	
Специализированная многофункциональная учебная аудитория дл проведения учебных занятий семинарско типа, групповых и индивидуальны консультаций, текущего контроля промежуточной аттестации, в том числе, дл организации практической подготовк обучающийся, с перечнем основно оборудования (аудитория № 308): Столы для обучающихся; Стулья для обучающихся; Стол педагогического работника; Стул педагогического работника; Компьютеры с возможностью подключения сети «Интернет» и обеспечением доступа электронную информационно-образовательну среду лицензиата; Интерактивная доска; Проектор; Сканер; Принтер	170001, Россия, город Тверь, улица Спартака, дом 26а