

Министерство науки и высшего образования
Российской Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Донецкий государственный университет»

Факультет математики и информационных технологий
Кафедра информационных систем управления



УТВЕРЖДАЮ
проректор

«29» марта 2024 г.

МП

П.А. Машаров

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Укрупненная группа направлений подготовки	38.00.00 Экономика и управление
Программа высшего образования	Программа специалитета
Специальность	38.05.01 Экономическая безопасность
Специализация	Экономико-правовое обеспечение экономической безопасности
Квалификация	Экономист
Форма обучения	Очная, заочная

Рабочая программа адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины **«Информационная безопасность»** для обучающихся по направлению подготовки 38.05.01 Экономическая безопасность (специализация: Экономико-правовое обеспечение экономической безопасности), составлена на основании составлена на основании Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 38.05.01 Экономическая безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 14 апреля 2021 г. № 293 (с изм. и доп.), Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 06 апреля 2021 г. № 245 (с изм. и доп.), в соответствии с учебным планом, утвержденным Ученым советом ФГБОУ ВО «ДонГУ» для набора 2024 года.

Разработчик:
доцент кафедры информационных
систем управления
канд. экон. наук, доцент

А. М. Гизатулин

Рабочая программа одобрена на заседании кафедры информационных систем управления
Протокол от 22.03.2024 г. № 6а

Заведующий кафедрой

Н. Ш. Пономаренко

СОГЛАСОВАНО:

Декан экономического факультета
28.03.2024 г.

Ю. Н. Полшков

Учебно-методическая комиссия экономического факультета
Протокол от 27.03.2024 г. № 7
Председатель

Е. Н. Стрелина

Руководитель основной профессиональной образовательной программы,
д-р экон. наук, проф.
26.03.2024 г.

В. В. Краснова

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Требования к предварительной подготовке обучающихся, предшествующие и сопутствующие дисциплины, на которых основывается изучение данной:

дисциплины программы бакалавриата: «Информационные технологии и инструменты программирования в экономике», «Экономическая безопасность», «Управление рисками», «Экономическая разведка».

1.2. Дисциплины, курсовые работы и практики, для которых освоение данной дисциплины необходимо как предшествующее:

производственная практика: преддипломная; выпускная квалификационная работа.

2. ОПИСАНИЕ ДИСЦИПЛИНЫ

2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	38.05.01 Экономическая безопасность (Специализация: Экономико-правовое обеспечение экономической безопасности)
Шифр и название в соответствии с учебным планом	Б1.Б.М6.20 «Информационная безопасность»
Часть образовательной программы	Базовая часть
Количество зачетных единиц / всего часов	2 / 72

2.2. Распределение часов по формам и периодам обучения

Форма обучения	курс	семестр	Общее количество часов					Форма контроля
			лекционных	лабораторных	практических	самостоятельной работы + контроль	всего	
Очная	5	9	17	-	17	38	72	Зачет
Заочная	5	9	4	-	2	66	72	Зачет

3. ЦЕЛИ ДИСЦИПЛИНЫ

Цель изучения дисциплины «Информационная безопасность» – формирование у будущего специалиста в сфере экономической безопасности знаний, умений и навыков, позволяющих принимать решения в сфере информационной безопасности.

4. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ КОМПОНЕНТА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ, ИХ ИНДИКАТОРЫ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

4.1. Компетенции

ОПК-6. Способен использовать современные информационные технологии и программные средства при решении профессиональных задач.

ПК-4. Способен планировать, организовывать и контролировать текущие и перспективные мероприятия по обеспечению экономической безопасности в организации, управлять рисками организации, руководить службами и подразделениями экономической безопасности предприятий и организаций.

4.2. Индикаторы компетенций

Компетенции	Индикаторы	Результаты обучения
ОПК-6. Способен использовать современные информационные технологии и программные средства при решении профессиональных задач	ОПК-6.И-2. Применяет современные информационные технологии и программные средства для решения профессиональных задач	ОПК-6. И-2. У-1. <i>Умеет</i> использовать современные информационные технологии и программные средства для решения профессиональных задач
	ОПК-6.И-3. Демонстрирует способность анализировать угрозы информационной безопасности и обеспечивать защиту электронного документооборота	ОПК-6. И-3. З-1. <i>Знает</i> основные понятия и методику анализа угроз информационной безопасности
		ОПК-6. И-3. З-2. <i>Знает</i> концепцию электронного документооборота
		ОПК-6. И-3. З-3. <i>Знает</i> особенности защиты электронного документооборота
		ОПК-6. И-3. У-1. <i>Умеет</i> анализировать угрозы информационной безопасности
		ОПК-6. И-3. У-2. <i>Умеет</i> выбирать средства защиты баз данных
		ОПК-6. И-3. У-3. <i>Умеет</i> выбирать средства защиты системы электронного документооборота
ПК-4. Способен планировать, организовывать и контролировать текущие и перспективные мероприятия по обеспечению экономической безопасности в организации, управлять рисками организации, руководить службами и подразделениями экономической безопасности предприятий и организаций	ПК-4. И-5. Демонстрирует способность разрабатывать политику информационной безопасности	ПК-4.И-5. З-1. <i>Знает</i> методику разработки политики информационной безопасности
		ПК-4.И-5. З-2. <i>Знает</i> методику разработки специализированных политик информационной безопасности
		ПК-4.И-5. У-1. <i>Умеет</i> разрабатывать политику информационной безопасности
		ПК-4.И-5. У-2. <i>Умеет</i> разрабатывать специализированные политики информационной безопасности

5. ПРОГРАММА ДИСЦИПЛИНЫ

Темы	Краткое содержание темы
Содержательный модуль 1. Политика информационной безопасности	
Тема 1. Основные понятия и анализ угроз информационной безопасности	1.1. Основные понятия защиты информации и информационной безопасности 1.2. Анализ угроз информационной безопасности 1.3. Способы обеспечения безопасности информационных систем
Тема 2. Политика информационной безопасности	2.1. Политика информационной безопасности 2.2. Уровни политики безопасности 2.3. Структура политики безопасности организации 2.4. Базовая политика безопасности 2.5. Специализированные политики безопасности 2.6. Политика допустимого использования. 2.7. Политика удаленного доступа. 2.8. Процедуры безопасности 2.9. Процедура реагирования на события. 2.10. Процедура управления конфигурацией. 2.11. Разработка политики безопасности организации 2.12. Организация информационной безопасности банка
Тема 3. Криптографическая защита информации	3.1. Основные понятия криптографической защиты информации. 3.2. Классификация криптографических алгоритмов. 3.3. Электронная цифровая подпись. 3.4. Основные процедуры цифровой подписи. 3.5. Алгоритм цифровой подписи ГОСТ Р 34.10-94 3.6. Алгоритм цифровой подписи ECDSA. 3.7. Стандарт цифровой подписи ГОСТ Р 34.10-2001. 3.8. Управление криптоключами.
Содержательный модуль 2. Защита электронного документооборота	
Тема 4. Идентификация, аутентификация и управление доступом	4.1. Аутентификация, авторизация и администрирование действий пользователей. 4.2. Аутентификация на основе многоразовых паролей. 4.3. Аутентификация на основе одноразовых паролей. 4.4. Идея строгой аутентификация. 4.5. Строгая двухфакторная аутентификация. 4.6. Применение смарт-карт. 4.7. Применение USB-токенов. 4.8. Особенности использования PIN-кода. 4.9. Криптографические протоколы строгой аутентификации. 4.10. Биометрическая аутентификация пользователя. 4.11. Управление доступом по схеме однократного входа с авторизацией Single Sign-On. 4.12. Простая система однократного входа Single Sign-On. 4.13. Системы однократного входа Web SSO. 4.14. SSO-продукты уровня предприятия.
Тема 5. Защита электронного документооборота	5.1. Концепция электронного документооборота. 5.2. Особенности защиты электронного документооборота. 5.2.1. Угрозы для СЭД 5.2.2. Средства защиты СЭД 5.3. Защита баз данных

Темы	Краткое содержание темы
	5.3.1. Основные типы угроз 5.3.2. Методы и средства защиты СУБД 5.3.3. Средства защиты СУБД Microsoft Access 5.3.4. Средства защиты СУБД Oracle 5.3.5. Защищенный доступ к базам данных 5.4. Защита корпоративного почтового документооборота 5.5. Защита системы электронного документооборота DIRECTUM 5.5.1. Функциональные возможности системы DIRECTUM 5.5.2. Архитектура системы DIRECTUM 5.5.3. Управление электронными документами в системе DIRECTUM

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

6.1. Форма обучения – очная, курс – 5, семестр – 9.

Наименования содержательных модулей и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
Содержательный модуль 1. Политика информационной безопасности					
Тема 1. Основные понятия и анализ угроз информационной безопасности	3		3	8	14
Тема2. Политика информационной безопасности	4		4	8	16
Тема3. Криптографическая защита информации	2		2	8	12
Итого по содержательному модулю 1	9		9	24	42
Содержательный модуль 2. Защита электронного документооборота					
Тема 4. Идентификация, аутентификация и управление доступом	4		4	7	15
Тема 5. Защита электронного документооборота	4		4	7	15
Итого по содержательному модулю 2	8		8	14	30
Всего по компоненту ОПОП	17		17	38	72

6.2. Форма обучения – очно-заочная, курс – 5, семестр – 9

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
Содержательный модуль 1. Политика информационной безопасности					
Тема 1. Основные понятия и анализ угроз информационной безопасности	0,5		0,4	13,1	14
Тема2. Политика информационной безопасности	1		0,4	14,6	16
Тема3. Криптографическая защита информации	0,5		0,4	11,1	12
Итого по содержательному модулю 1	2	0	1,2	38,8	42
Содержательный модуль 2. Защита электронного документооборота					
Тема 4. Идентификация, аутентификация и управление доступом	1		0,4	13,6	15
Тема 5. Защита электронного документооборота	1		0,4	13,6	15
Итого по содержательному модулю 2	2	0	0,8	27,2	30
Всего по компоненту ОПОП	4	0	2	66	72

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (СРЕДСТВА) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Контрольные вопросы

СОДЕРЖАТЕЛЬНЫЙ МОДУЛЬ 1 ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Сформулируйте понятие информационной безопасности ИС.
2. Объясните понятия целостности, конфиденциальности и доступности информации.
3. Объясните понятия идентификации, аутентификации и авторизации пользователя. Как они взаимосвязаны?
4. Укажите отличия санкционированного доступа от несанкционированного доступа к информации.
5. Сформулируйте определение политики безопасности.
6. Сформулируйте особенности избирательной и полномочной политики безопасности.
7. Объясните понятие «угроза безопасности ИС».
8. Укажите основные признаки классификации возможных угроз безопасности ИС.
9. Каковы основные виды угроз безопасности ИС по цели и степени воздействия?
10. Дайте краткую характеристику угроз безопасности, обозначаемых терминами: «троянский конь», «вирус», «червь»?
11. Перечислите и дайте краткую характеристику основных методов реализации угроз информационной безопасности.
12. Объясните суть комплексного подхода к обеспечению информационной безопасности ИС.
13. Объясните понятие «политика безопасности организации».
14. Какие разделы должна содержать документально оформленная политика безопасности?
15. Какие проблемы решает верхний уровень политики безопасности?
16. Какие задачи решает средний уровень политики безопасности?
17. Каковы особенности нижнего уровня политики безопасности?
18. Сформулируйте обязанности руководителей подразделений, администраторов и пользователей при реализации политики безопасности.
19. Опишите структуру политики безопасности организации.
20. Что представляют собой специализированные политики безопасности?
21. Приведите несколько примеров специализированных политик безопасности с описанием их особенностей.
22. Что представляют собой процедуры безопасности?
23. Приведите несколько примеров процедур безопасности с описанием их особенностей.
24. Сформулируйте основные этапы разработки политики безопасности организации.
25. Что такое криптография?
26. Дайте определения следующих понятий: криптограмма, криптоалгоритм, криптосистема.
27. В чем состоит коренное различие симметричных и асимметричных криптосистем?
28. Охарактеризуйте четыре основных режима работы блочного алгоритма.
29. Расскажите о способах комбинирования блочных алгоритмов для получения алгоритмов с более длинным ключом, сравните их между собой.

30. Каковы основные характеристики и режимы работы отечественного стандарта шифрования данных?
31. Сформулируйте концепцию криптосистемы с открытым ключом?
32. Дайте определение однонаправленной функции. Приведите примеры однонаправленных функций.
33. Каковы особенности однонаправленных функций с «потайным ходом»?
34. На чем основывается надежность криптоалгоритма шифрования RSA?
35. Опишите две основные процедуры, осуществляемые системой электронной цифровой подписи для подтверждения подлинности электронного документа.
36. Опишите отечественный стандарт цифровой подписи, укажите его преимущества по сравнению с алгоритмом цифровой подписи DSA.
37. Каково назначение хэш-функции и каким требованиям должна удовлетворять качественная хэш- функция?
38. Каким образом комбинированный метод шифрования позволяет сочетать достоинства асимметричных и симметричных криптосистем? Опишите протокол реализации комбинированного метода шифрования.
39. Опишите работу алгоритма Диффи - Хэлла. Укажите достоинства этого алгоритма.
40. Каково назначение инфраструктуры открытых ключей PKI? Опишите функционирование инфраструктуры PKI.

СОДЕРЖАТЕЛЬНЫЙ МОДУЛЬ 2

ЗАЩИТА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

1. Дайте определения понятий: идентификация, аутентификация, авторизация, администрирование. Что понимают под решением задач AAA?
2. Какие задачи решает подсистема управления идентификацией и доступом IAM (Identity and Access Management)?
3. На какие категории можно разделить процессы аутентификации в зависимости от сущностей, предъявляемых пользователем для подтверждения своей подлинности?
4. Перечислите основные атаки на протоколы аутентификации.
5. Опишите метод аутентификации на основе многофакторных паролей. Каковы недостатки этого метода?
6. Опишите метод аутентификации на основе одноразовых паролей. Каковы его достоинства и недостатки?
7. Сформулируйте принцип строгой аутентификации. Опишите типы процедур строгой аутентификации.
8. Объясните назначение PIN-кода и особенности его использования.
9. Объясните принцип работы двухфакторной аутентификации. Какие внешние носители информации используются для двухфакторной аутентификации пользователей? Каковы достоинства этого метода аутентификации?
10. Опишите функциональность и характеристики смарт-карт и USB-токенов.
11. Опишите методы биометрической аутентификации пользователя. Что означают коэффициент ошибочных отказов и коэффициент ошибочных подтверждений?
12. Поясните принцип управления доступом по схеме однократного входа с авторизацией Single Sign-On.
13. Укажите преимущества электронного документооборота по сравнению с бумажным документооборотом. Укажите различия между понятиями «система электронного документооборота» (СЭД) и ECM (Enterprise Content Management).
14. Охарактеризуйте базовые составляющие системы электронного документооборота.
15. Опишите функциональность подсистемы автоматизации управления потоками работ (Workflow).

16. Укажите особенности построения и функционирования системы распределенного электронного документооборота.
17. Назовите угрозы информационной безопасности для СЭД и охарактеризуйте источники этих угроз.
18. Какие функции должны быть реализованы средствами защиты информации СЭД?
19. Назовите основные угрозы информационной безопасности баз данных. Укажите методы и средства защиты СУБД.
20. Определите понятие «RAID-массив». Поясните особенности применения RAID-массивов в СУБД.
21. Сравните возможности средств защиты СУБД Microsoft Access и СУБД Oracle.
22. Охарактеризуйте методы и средства защиты корпоративного почтового документооборота.
23. Опишите функциональные возможности и архитектуру системы электронного документооборота DIRECTUM.
24. Охарактеризуйте приемы и методы защиты, реализованные в системе DIRECTUM.

7.2. Темы докладов (рефератов)

Не предусмотрены программой дисциплины

7.3. Темы письменных работ (типы задач)

Контрольная работа проводится в виде тестирования на платформе Moodle Центра дистанционного образования экономического факультета ФГБОУ ВО «ДонГУ».

Тестирование включает 20 тестовых заданий по темам 1-3.

Время выполнения – 30 минут.

Пример тестового задания приведен ниже.

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

Разработка аппаратных средств обеспечения правовых данных

Разработка и установка во всех компьютерных правовых сетях журналов учета действий

Разработка и конкретизация правовых нормативных актов обеспечения безопасности

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

Хищение жестких дисков, подключение к сети, инсайдерство

Перехват данных, хищение данных, изменение архитектуры системы

Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

Персональная, корпоративная, государственная

Клиентская, серверная, сетевая

Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
несанкционированного доступа, воздействия в сети

инсайдерства в организации
чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

Компьютерные сети, базы данных

Информационные системы, психологическое состояние пользователей

Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

Искажение, уменьшение объема, перекодировка информации

Техническое вмешательство, выведение из строя оборудования сети

Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

Экономической эффективности системы безопасности

Многоплатформенной реализации системы

Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

руководители, менеджеры, администраторы компаний

органы права, государства, бизнеса

сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

Установление регламента, аудит системы, выявление рисков

Установка новых офисных приложений, смена хостинг-компаний

Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:

Неоправданных ограничений при работе в сети (системе)

Рисков безопасности сети, системы

Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

Невозможности миновать защитные средства сети (системы)

Усиления основного звена сети, системы

Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

Усиления защищенности самого незащищенного звена сети (системы)

Перехода в безопасное состояние работы сети, системы

Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

Разделения доступа (обязанностей, привилегий) клиентам сети (системы)

Одноуровневой защиты сети, системы

Совместимых, однотипных программно-технических средств сети, системы

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

Компьютерный сбой

Логические закладки («мины»)

Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:
Прочитать приложение, если оно не содержит ничего ценного – удалить
Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:
Секретность ключа определена секретностью открытого сообщения
Секретность информации определена скоростью передачи данных
Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:
Электронно-цифровой преобразователь
Электронно-цифровая подпись
Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

Покупка нелегального ПО
Ошибки эксплуатации и неумышленного изменения режима работы системы
Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

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

20) Наиболее распространены средства воздействия на сеть офиса:

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

Критерии оценивания модульной контрольной работы

Вид задания	Количество баллов
1 тестовое задание	0,25
Количество тестов	20
Всего	5

Самостоятельная работа по дисциплине «Информационная безопасность» выполняется в виде практических работ и максимально оценивается в 78 баллов.

8. РАСПРЕДЕЛЕНИЕ БАЛЛОВ, КОТОРЫЕ ПОЛУЧАЮТ ОБУЧАЮЩИЕСЯ

Общая оценка знаний обучающихся по дисциплине проводится по 100-балльной шкале исходя из максимума, приведенного в таблице ниже. Организационно-учебная работа в аудитории оценивается на основе таких критериев как посещаемость занятий, своевременное и качественное выполнение домашних заданий, активность во время проведения лекционных и практических занятий (участие в обсуждении текущего и пройденного материала, решение задач и т.п.).

Содержательные модули	Виды работ	Баллы
Содержательный модуль 1	Организационно-учебная работа студента в аудитории	9
	Модульная контрольная работа	5
	Итого	14
Содержательный модуль 2	Организационно-учебная работа студента в аудитории	8
	Итого	8
Самостоятельная работа (практические работы по вариантам)		78
Всего		100

Соответствие баллов оценке

Количество баллов из 100	ECTS	Оценка по пятибалльной шкале	
		Экзамен, дифференцированный зачет	Зачет
90-100	A	отлично	зачтено
80-89	B	хорошо	зачтено
75-79	C		зачтено
70-74	D	удовлетворительно	зачтено
60-69	E		зачтено
35-59	FX	неудовлетворительно	не зачтено
0-34	F		не зачтено

9. ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- 1) для слепых и слабовидящих:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
 - письменные задания оформляются увеличенным шрифтом.
- 2) для глухих и слабослышащих:
 - лекции оформляются в виде электронного документа;
 - письменные задания выполняются на компьютере в письменной форме;
 - экзамен проводится в письменной форме на компьютере; возможно проведение в форме тестирования.
- 3) для лиц с нарушениями опорно-двигательного аппарата:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - письменные задания выполняются на компьютере;
 - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- 1) для слепых и слабовидящих:
 - в печатной форме увеличенным шрифтом;
 - в форме электронного документа;
- 2) для глухих и слабослышащих:
 - в печатной форме;
 - в форме электронного документа.
- 3) для обучающихся с нарушениями опорно-двигательного аппарата:
 - в печатной форме;
 - в форме электронного документа.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия проводятся в 7-м и 5-м корпусах ДонГУ (г. Донецк, ул. Челюскинцев, 186; 189б). Для проведения лабораторных занятий требуется аудитория, оборудованная меловой или маркерной доской, мультимедийный проектор и экран, ноутбук, комплект учебной мебели для студентов, рабочее место преподавателя, выход в Интернет – проводной или с использованием Wi-Fi.

Для самостоятельной работы используются текстовые и электронные ресурсы Научной библиотеки университета и других электронных библиотечных баз данных, учебно-методическое обеспечение, представленное в учебно-методическом кабинете 7-го корпуса (ауд. 103).

Обучающиеся имеют возможность использовать учебные материалы по дисциплине, размещенные на платформе Moodle Центра дистанционного образования экономического факультета «ДонГУ». При изучении дисциплины применяются электронное обучение и дистанционные образовательные технологии.

С использованием ресурсов платформы дистанционного образования осуществляется текущий контроль знаний обучающихся на основе тестирования и проверки результатов самостоятельной работы.

Дистанционный курс «Информационная безопасность» для студентов специальности 38.05.01 Экономическая безопасность, специализации «Экономико-правовое обеспечение экономической безопасности» доступен по ссылке: disk.yandex.ru/d/-TPUFYbaCDPhsw

11. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

11.1. Основная литература

1. Бондаренко, И. С. Информационная безопасность : учебник / И. С. Бондаренко. — Москва : МИСИС, 2023. — 254 с.
2. Капгер, И. В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь : ПНИПУ, 2023. — 91 с.
3. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 324 с.
4. Ярочкин, В. И. Информационная безопасность : учебник / В. И. Ярочкин. — 5-е изд. — Москва : Академический Проект, 2020. — 544 с.

11.2. Дополнительная литература

1. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г. Милославская. — М.: ГЛТ, 2017. — 536 с.
2. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2018. — 558 с.
3. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. — М.: Форум, 2016. — 432 с.
4. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. — М.: АРТА, 2016. — 296 с.
5. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. — М.: МГИУ, 2017. — 277 с.
6. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2017. — 336 с.
7. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. — М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2017. — 416 с.
8. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. — М.: ДМК, 2017. — 702 с.
9. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. — М.: Акад. Проект, 2018. — 544 с.
10. Ярочкин, В.И. Информационная безопасность. 5-е изд. / В.И. Ярочкин. — М.: Академический проект, 2016. — 544 с.

12. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Базелюк Никита Григорьевич, Степанов Алексей Владимирович. Методы управления информационной безопасностью в организации // Евразийский Союз Ученых. 2015. №4-13 (13). URL: <https://cyberleninka.ru/article/n/metody-upravleniya-informatsionnoy-bezopasnostyu-v-organizatsii> (дата обращения: 01.09.2023).
2. Евглевская Наталья Валерьевна. Модуль принятия решений по управлению информационной безопасностью в информационно-коммуникационной сети // Научные технологии в космических исследованиях Земли. 2020. №6. URL: <https://cyberleninka.ru/article/n/modul-prinyatiya-resheniy-po-upravleniyu-informatsionnoy-bezopasnostyu-v-informatsionno-kommunikatsionnoy-seti> (дата обращения: 01.09.2023).
3. Земцов И.В. О ситуационном подходе к управлению информационной безопасностью // Актуальные проблемы авиации и космонавтики. 2016. №12. URL: <https://cyberleninka.ru/article/n/o-situatsionnom-podhode-k-upravleniyu-informatsionnoy-bezopasnostyu> (дата обращения: 01.09.2023).
4. Козунова Светлана Сергеевна Система управления информационной безопасностью предприятия // Евразийский Союз Ученых. 2016. №7-2 (28). URL: <https://cyberleninka.ru/article/n/sistema-upravleniya-informatsionnoy-bezopasnostyu-predpriyatiya> (дата обращения: 01.09.2023).
5. Л. В. Фомченкова, А. В. Леонов Модель управления информационной безопасностью // Экономика и бизнес: теория и практика. 2019. №12-3. URL: <https://cyberleninka.ru/article/n/model-upravleniya-informatsionnoy-bezopasnostyu> (дата обращения: 01.09.2023).
6. Национальная электронная библиотека (НЭБ): федеральная государственная информационная система / Министерство Культуры РФ; Российская государственная библиотека. — Москва, 2019- . — URL: <https://rusneb.ru/> (дата обращения: 01.09.2023). — Режим доступа: свободный, подписка. Необходима установка программного обеспечения. — Текст: электронный.

7. eLIBRARY.RU: научная электронная библиотека: сайт. – Москва, 2000- . – URL: <https://elibrary.ru> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

8. Научная электронная библиотека «КиберЛенинка»: сайт / Ассоциация «Открытая наука». – Москва, 2014. – URL: <https://cyberleninka.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный. – Текст: электронный.

9. Электронно-библиотечная система «Лань»: [сайт]. – URL: <https://e.lanbook.com> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

10. ЭБС Юрайт: электронная библиотечная система: сайт. – Москва, 2013. – URL: <https://biblio-online.ru> (дата обращения 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

11. Электронно-библиотечная система ДонГУ: сайт / ФГБОУ ВО «ДонГУ». – Донецк, 2016- . – URL: <http://library.donnu.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный. – Текст: электронный.

12. Электронный каталог Научной библиотеки ДонГУ: раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://library.donnu.ru/catalog/> (дата обращения: 01.09.2023). – Режим доступа: поиск свободный, электронные документы – для пользователей ДонГУ.

13. Электронный архив ДонГУ: раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://repo.donnu.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный.

13. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДонГУ № 46484614)
2. Microsoft Office (корпоративная лицензия ДонГУ № 46472919)
3. Microsoft Visual Studio (лицензия программы Dream Spark для высших учебных заведений)
4. Антивирус Касперского, Adobe Acrobat Reader, xPDF (лицензии GPL, Apache, BSD для свободного программного обеспечения).