МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Луганский государственный университет имени Владимира Даля»

Институт управления и государственной службы
Кафедра производственного менеджмента

УТВЕРЖДАЮ:
Директор института
_____ Р.Г.Харьковский
(подпись)
«__» _____ 2023 года

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Обеспечение информационной безопасности»

По направлению подготовки 38.05.01 Экономическая безопасность
Специализация: Экономика и организация производства на режимных объектах

Луганск – 2023

Лист согласования РПУД

Рабочая программа учебной дисциплины «Обеспечение информационной безопасности» по направлению подготовки 38.05.01 Экономическая безопасность, специализация «Экономика и организация производства на режимных объектах» – 29 с.

Рабочая программа учебной дисциплины «Обеспечение информационной безопасности» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 38.05.01 Экономическая безопасность (утвержденный приказом Министерства образования и науки Российской Федерации от 12 августа 2020 г. № 970).

СОСТАВИТЕЛЬ:

кандидат экон. наук, доц. Галицкий А.И.

Рабочая программа дисциплины утверждена на заседании кафедры производственного менеджмента «21» 03 2023 г., протокол № 11.

Заведующий кафедрой
производственного менеджмента _____ Родионов А.В.

Переутверждена: «___» _____20___ г., протокол № _____

Директор института
управления и государственной службы _____ Харьковский Р.Г.

Рекомендована на заседании учебно-методической комиссии института управления и государственной службы «12» 04 2023 г., протокол № 8.

Председатель учебно-методической
комиссии института _____ Резник А.А.

Структура и содержание дисциплины

1. Цели и задачи дисциплины, ее место в учебном процессе

Цель изучения дисциплины заключаются в формировании у студентов комплексных знаний и навыков в области обеспечения информационной безопасности.

Предметом изучения дисциплины являются методические основы теории обеспечения информационной безопасности.

Задачи изучения дисциплины:

- освоить систему обеспечения информационной безопасности предприятия.
- сформировать навыки прогнозирования развития предприятия в сфере обеспечения информационной безопасности.
- овладеть методами обеспечения информационной безопасности.
- выработать способность к комплексному анализу и принятию управленческих решений в сфере обеспечения информационной безопасности.

2. Место дисциплины в структуре ООП ВО. Требования к результатам освоения содержания дисциплины

Дисциплина «Обеспечение информационной безопасности» (Б1.В.19).

Содержание дисциплины является логическим продолжением содержания дисциплин: «Оценка рисков экономической безопасности и антикризисное управление», «Обеспечение экономической безопасности, прогнозирование и планирование деятельности предприятия», «Оценка экономических угроз на предприятиях» «Документирование управленческой деятельности в системе экономической безопасности». Служит основой для освоения дисциплин направления подготовки 38.05.01 Экономическая безопасность: «Экономика и организация производства на режимных объектах».

3. Требования к результатам освоения содержания дисциплины

Код и наименование компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине)	Перечень планируемых результатов
ПК-7. Способен применять теоретические знания и методы исследования для решения профессиональных задач в области экономики,	**ПК-7.1:** Способен проводить анализ и диагностику рисков и угроз информационной безопасности предприятия **ПК-7.2** Способен разрабатывать	**Знать:** Теоретические основы экономической безопасности предприятия Методологию анализа, диагностики и оценки рисков информационной

управления и обеспечения безопасности предприятия	прогнозы развития предприятия и его системы информационной безопасности с учетом выявленных рисков **ПК-7.3:** Способен разрабатывать планы и мероприятия по обеспечению информационной безопасности предприятия	безопасности предприятия. **Уметь:** Выявлять и анализировать конкретные риски и угрозы информационной безопасности. Уметь разрабатывать проекты планов и мероприятий по обеспечению информационной безопасности. **Владеть:** Навыками проведения комплексного анализа экономического состояния предприятия и его системы безопасности.

4. Структура и содержание дисциплины

4.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов (зач. ед.)**	
	Очная форма	**Заочная форма**
Общая учебная нагрузка (всего)	**288 (8 зач. ед)**	**288 (8 зач. ед)**
Обязательная аудиторная учебная нагрузка (всего) в том числе:	**126**	**40**
Лекции	54	20
Семинарские занятия	-	-
Практические занятия	72	20
Лабораторные работы	0	0
Другие формы и методы организации образовательного процесса	-	-
Самостоятельная работа студента (всего)	162	248
Итоговая аттестация	Экзамен/зачет	Экзамен/зачет

4.2. Содержание разделов дисциплины

1. Введение в информационную безопасность. Основные понятия и угрозы

Дается определение информационной безопасности, рассматривается классическая триада — Конфиденциальность, Целостность, Доступность. Описываются основные виды угроз, уязвимостей и атак, а также современный ландшафт киберпреступности.

2. Криптография как фундамент защиты информации

Рассматриваются базовые принципы криптографии: симметричное и асимметричное шифрование, хэш-функции и электронная цифровая подпись (ЭЦП). На

примерах разбирается, как эти механизмы обеспечивают конфиденциальность, целостность и аутентификацию данных.

3. Защита от вредоносного программного обеспечения и сетевые атаки

Анализируются различные типы вредоносных программ (вирусы, черви, трояны) и методы защиты от них. Изучаются распространенные сетевые атаки, такие как DDoS, MITM-атаки и сканирование портов, а также принципы работы межсетевых экранов (файрволов) и систем обнаружения вторжений (IDS).

4. Управление доступом и аутентификация

Изучаются основные модели управления доступом: дискреционная, мандатная и ролевая. Подробно разбираются современные методы аутентификации: многофакторная аутентификация (MFA), биометрия и протоколы единого входа (Single Sign-On).

5. Безопасность операционных систем и приложений

Рассматриваются встроенные механизмы безопасности в современных ОС (Windows, Linux). Изучаются распространенные уязвимости на уровне приложений, такие как SQL-инъекции и XSS, а также методологии безопасной разработки программного обеспечения (DevSecOps).

6. Организационные и правовые аспекты ИБ. Политики безопасности

Освещаются вопросы создания и внедрения организационных мер защиты: политики информационной безопасности, регламенты и инструкции для сотрудников. Рассматривается базовое правовое поле, включая регуляторные требования и стандарты.

7. Основы безопасности беспроводных сетей и мобильных устройств

Анализируются специфические угрозы для беспроводных технологий (Wi-Fi, Bluetooth) и мобильных платформ. Изучаются методы защиты: безопасная настройка точек доступа, использование VPN, управление мобильными устройствами (MDM) и безопасность интернета вещей (IoT).

8.Инцидент-менеджмент и обеспечение непрерывности бизнеса

Рассматривается жизненный цикл управления инцидентами информационной безопасности: от обнаружения и анализа до ликвидации последствий. Изучаются принципы обеспечения непрерывности бизнеса и аварийного восстановления после киберинцидентов (DRP).

4.3. Лекции

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
1	Введение в информационную безопасность. Основные понятия и угрозы	8	
2	Криптография как фундамент защиты информации	6	
3	Защита от вредоносного программного обеспечения и сетевые атаки	6	
4	Управление доступом и аутентификация	8	
5	Безопасность операционных систем и приложений	8	
6	Организационные и правовые аспекты ИБ. Политики безопасности	6	
7.	Основы безопасности беспроводных сетей и мобильных устройств	6	
8.	Инцидент-менеджмент и обеспечение непрерывности бизнеса	6	
Итого:		54	

4.4. Практические (семинарские) занятия

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
1	Введение в информационную безопасность. Основные понятия и угрозы	9	
2	Криптография как фундамент защиты информации	9	
3	Защита от вредоносного программного обеспечения и сетевые атаки	9	
4	Управление доступом и аутентификация	9	
5	Безопасность операционных систем и приложений	9	
6	Организационные и правовые аспекты ИБ. Политики безопасности	9	
7.	Основы безопасности беспроводных сетей и мобильных устройств	9	
8.	Инцидент-менеджмент и обеспечение непрерывности бизнеса	9	
Итого:		72	

4.5. Самостоятельная работа студентов

№ п/п	Название темы	Объем часов	
		Очная форма	Заочная форма
1	Введение в информационную безопасность. Основные понятия и угрозы	20	
2	Криптография как фундамент защиты информации	22	
3	Защита от вредоносного программного обеспечения и сетевые атаки	20	
4	Управление доступом и аутентификация	20	
5	Безопасность операционных систем и приложений	20	
6	Организационные и правовые аспекты ИБ. Политики безопасности	20	
7.	Основы безопасности беспроводных сетей и мобильных устройств	20	
8.	Инцидент-менеджмент и обеспечение непрерывности бизнеса	20	
Итого:		162	

4.6. Курсовые работы/проекты –учебный план дисциплины не предусматривает курсовую работу

5. Образовательные технологии

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

- традиционные объяснительно-иллюстративные технологии, которые обеспечивают доступность учебного материала для большинства студентов, системность, отработанность организационных форм и привычных методов, относительно малые затраты времени;
- технологии проблемного обучения, направленные на развитие познавательной активности, творческой самостоятельности студентов и предполагающие последовательное и целенаправленное выдвижение перед студентом познавательных задач, разрешение которых позволяет студентам активно усваивать знания (используются поисковые методы; постановка познавательных задач);
- технологии развивающего обучения, позволяющие ориентировать учебный процесс на потенциальные возможности студентов, их реализацию и развитие;
- технологии концентрированного обучения, суть которых состоит в создании максимально близкой к естественным психологическим особенностям человеческого восприятия структуры учебного процесса и которые дают возможность глубокого и системного изучения содержания учебных дисциплин за счет объединения занятий в тематические блоки;
- технологии модульного обучения, дающие возможность обеспечения гибкости процесса обучения, адаптации его к индивидуальным потребностям и особенностям обучающихся (применяются, как правило, при самостоятельном обучении студентов по индивидуальному учебному плану);
- технологии дифференцированного обучения, обеспечивающие возможность создания оптимальных условий для развития интересов и способностей студентов, в том числе и студентов с особыми образовательными потребностями, что позволяет реализовать в культурно-образовательном пространстве университета идею создания равных возможностей для получения образования
- технологии активного (контекстного) обучения, с помощью которых осуществляется моделирование предметного, проблемного и социального содержания будущей профессиональной деятельности студентов (используются активные и интерактивные методы обучения) и т.д.

Максимальная эффективность педагогического процесса достигается путем конструирования оптимального комплекса педагогических технологий и (или) их элементов на личностно-ориентированной, деятельностной, диалогической основе и использования необходимых современных средств обучения.

а) Основная литература:

Ветошкин, Д. И. Информационная безопасность: учебное пособие / Д. И. Ветошкин. — Москва : Юрайт, 2023. — 255 с. — ISBN 978-5-534-16027-6.

Гафнер, В. В. Информационная безопасность: учебное пособие для вузов / В. В. Гафнер, О. Э. Багдасарян. — 2-е изд., перераб. и доп. — Москва : Юрайт, 2022. — 336 с. — ISBN 978-5-534-14636-2.

Шеметев, А. А. Информационная безопасность предприятия: учебное

пособие / А. А. Шеметев. — 2-е изд., перераб. и доп. — Москва : Форум, 2020. — 320 с. — ISBN 978-5-00091-687-9.

Яковлев, А. В. Информационная безопасность и защита информации: учебное пособие / А. В. Яковлев, В. А. Королев. — Москва : КноРус, 2022. — 286 с. — ISBN 978-5-406-09084-7.

б) Дополнительная литература:

Белов, Е. Б. Основы информационной безопасности: учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков. — 2-е изд., испр. и доп. — Москва : Юрайт, 2022. — 237 с. — ISBN 978-5-534-14629-4.

Вус, М. А. Криптография: учебное пособие для вузов / М. А. Вус, А. Н. Тихонов, К. С. Горбунов. — Москва : Юрайт, 2023. — 199 с. — ISBN 978-5-534-15534-0.

Лапонина, О. Р. Криптографические основы безопасности: учебник для вузов / О. Р. Лапонина. — 3-е изд., испр. и доп. — Москва : Юрайт, 2022. — 251 с. — ISBN 978-5-534-14630-0.

Платонов, В. В. Информационная безопасность. Правовые основы: учебное пособие / В. В. Платонов, К. А. Лагутин. — Москва : ИНФРА-М, 2023. — 198 с. — (Высшее образование). — ISBN 978-5-16-017735-0.

Скиба, В. И. Защита информации в экономических информационных системах: учебное пособие / В. И. Скиба, А. В. Сенашова. — Москва : КноРус, 2021. — 196 с. — ISBN 978-5-406-08395-5.

Щербаков, А. Ю. Современная компьютерная безопасность. Криптографические методы защиты: учебное пособие / А. Ю. Щербаков. — Москва : КноРус, 2021. — 262 с. — ISBN 978-5-406-07898-2.

в) Методические указания:

г) Интернет-ресурсы:

Bank of Russia — Official website [сайт]. – URL: https://www.cbr.ru (для анализа угроз финансовой кибербезопасности и методических рекомендаций).

eLIBRARY.RU — Scientific Digital Library [сайт]. – URL: https://elibrary.ru (для поиска научных статей и монографий).

FSTEC of Russia — Federal Service for Technical and Export Control [сайт]. – URL: https://fstec.ru (для работы с официальными документами, требованиями и методиками по защите информации).

IS "ConsultantPlus" — Reference and Legal System [сайт]. – URL: http://www.consultant.ru (для работы с законодательной базой в сфере ИБ).

Official Internet portal of legal information [сайт]. – URL: http://pravo.gov.ru (для доступа к официальным текстам законов).

RU-CERT — National Computer Incident Response and Coordination Center [сайт]. – URL: https://www.cert.ru (для анализа актуальных киберугроз и инцидентов).

SecurityLab.ru — Информационно-аналитический портал [сайт]. – URL: https://www.securitylab.ru (для изучения новостей, обзоров уязвимостей и вирусов).

д) Материально-техническое и программное обеспечение дисциплины

Освоение дисциплины «Обеспечение информационной безопасности» предполагает использование академических аудиторий, соответствующих действующим санитарным и противопожарным правилам и нормам.

Прочее: рабочее место преподавателя, оснащенное компьютером с доступом в Интернет и проектором. Для проведения лабораторных работ необходимы компьютерные классы, оснащенные ПК с установленным специализированным программным обеспечением (например, виртуальные машины VMware/VirtualBox для моделирования атак и защиты, средства анализа защищенности, криптографические утилиты, межсетевые экраны).

7. Программное обеспечение:

Функциональное назначение	**Бесплатное программное обеспечение**	**Ссылки**
Офисный пакет	Libre Office 6.3.1	https://www.libreoffice.org/ https://ru.wikipedia.org/wiki/LibreOffice
Операционная система	UBUNTU 19.04	https://ubuntu.com/ https://ru.wikipedia.org/wiki/Ubuntu
Браузер	Firefox Mozilla	http://www.mozilla.org/ru/firefox/fx
Браузер	Opera	http://www.opera.com
Почтовый клиент	Mozilla Thunderbird	http://www.mozilla.org/ru/thunderbird
Файл-менеджер	Far Manager	http://www.farmanager.com/download.php
Архиватор	7Zip	http://www.7-zip.org/
Графический редактор	GIMP (GNU Image Manipulation Program)	http://www.gimp.org/ http://gimp.ru/viewpage.php?page_id=8 http://ru.wikipedia.org/wiki/GIMP
Редактор PDF	PDFCreator	http://www.pdfforge.org/pdfcreator
Аудиоплейер	VLC	http://www.videolan.org/vlc/

8. Оценочные средства по дисциплине

Паспорт
оценочных средств по учебной дисциплине
«Обеспечение информационной безопасности»

Описание уровней сформированности и критериев оценивания компетенций на этапах их формирования в ходе изучения дисциплины

Этап	Код компетенции	Уровни сформированности компетенции	Критерии оценивания компетенции
Начальный	**ПК-7.** Способен применять теоретические знания и методы исследования для решения профессиональных задач в области экономики, управления и обеспечения безопасности предприятия	**Пороговый**	**знать:** Теоретические основы экономической безопасности предприятия Методологию анализа, диагностики и оценки рисков информационной безопасности предприятия.
Основной		**Базовый**	**уметь:** Выявлять и анализировать конкретные риски и угрозы информационной безопасности. Уметь разрабатывать проекты планов и мероприятий по обеспечению информационной безопасности.
Заключительный		**Высокий**	Навыками проведения комплексного анализа экономического состояния предприятия и его системы безопасности.

Перечень компетенций (элементов компетенций), формируемых в результате освоения учебной дисциплины.

№ п/п	Код компетенции	Формулировка контролируемой компетенции	Индикаторы достижений компетенции (по дисциплине)	Темы учебной дисциплины	Этапы формирования (семестр зучения)
1	**ПК-7.**	Способен применять теоретические знания и методы исследования для решения профессиональных	**ПК-7.1:** Способен проводить анализ и диагностику рисков и угроз информационной безопасности	***Тема 1.*** ***Тема 2*** ***Тема 3*** ***Тема 4.***	1

		задач в области экономики, управления и обеспечения безопасности предприятия	предприятия		
			ПК-7.2: Способен разрабатывать прогнозы развития предприятия и его системы информационной безопасности с учетом выявленных рисков **ПК-7.3:** Способен разрабатывать планы и мероприятия по обеспечению информационной безопасности предприятия	***Тема 5*** ***Тема 6*** ***Тема 7*** ***Тема 8.***	

Показатели и критерии оценивания компетенций, описание шкал оценивания

№ п/п	Код компетенции	Индикаторы достижений компетенции	Планируемые результаты обучения по дисциплине	Контролируемые темы учебной дисциплины	Наименование оценочного средства
1.	**ПК - 7** Способен применять теоретические знания и методы исследования для решения профессиональных задач в области экономики, управления и обеспечения безопасности предприятия	**ПК-7.3:** Способен разрабатывать планы и мероприятия по обеспечению информационной безопасности предприятия	Знать: Принципы управления системами защиты информации Методы мониторинга и аудита информационной безопасности Уметь: Администрировать комплексные системы защиты информации Проводить контроль эффективности мер безопасности Владеть: Навыками управления средствами защиты информации Методами анализа журналов событий и расследования инцидентов	***Тема 1.*** ***Тема 2*** ***Тема 3*** ***Тема 4.***	Контрольные вопросы и задания, тестовые задания, разноуровневые задания

		ПК-7.2 Способен разрабатывать прогнозы развития предприятия и его системы информационной безопасности с учетом выявленных рисков	Знать: Методологии анализа рисков информационной безопасности Принципы разработки организационно-распорядительной документации по ИБ Уметь: Проводить оценку рисков и разрабатывать меры защиты Формировать политики и процедуры информационной безопасности Владеть: Навыками разработки регламентов и инструкций по ИБ Методами управления инцидентами информационной безопасности		
		ПК – 7.1 Способен проводить анализ и диагностику рисков и угроз информационной безопасности предприятия	Знать: Основные понятия, угрозы и принципы обеспечения информационной безопасности. Законодательные и нормативные требования в области защиты информации. Уметь: Анализировать угрозы и уязвимости информационных систем. Применять основные методы и средства защиты информации. Владеть: Навыками работы с системами защиты информации (межсетевые экраны, антивирусы). Методами криптографической защиты и управления доступом.	***Тема 5.*** ***Тема 6*** ***Тема 7*** ***Тема 8***	Контрольные вопросы и задания, тестовые задания, разноуровневые задания

1.Типовые тестовые задания

(пороговый уровень)

1. Информационная безопасность: основные понятия

Какое определение верно характеризует понятие "информационная безопасность"?

а) Состояние защищенности информации от внутренних и внешних угроз

б) Система хранения данных

в) Метод шифрования сообщений

2. Угрозы информационной безопасности

К внешним угросам ИБ относится:

а) Хакерская атака из интернета

б) Ошибка сотрудника при работе с данными

в) Неисправность оборудования

3. Методы защиты информации

Антивирусное ПО используется для:

а) Обнаружения и блокировки вредоносных программ

б) Шифрования конфиденциальных данных

в) Резервного копирования информации

4. Криптографические методы

Шифрование необходимо для:

а) Обеспечения конфиденциальности информации

б) Ускорения передачи данных

в) Сжатия файлов

5. Управление доступом

Многофакторная аутентификация предполагает:

а) Использование двух и более способов подтверждения личности

б) Автоматический вход в систему

в) Единый пароль для всех сервисов

6. Защита сетей

Межсетевой экран (файрвол) предназначен для:

а) Контроля и фильтрации сетевого трафика

б) Повышения скорости интернета

в) Организации беспроводной сети

7. Инциденты информационной безопасности

При обнаружении утечки данных необходимо:

а) Немедленно начать расследование и блокировать угрозу

б) Увеличить скорость интернета
в) Переустановить операционную систему

8. Политика безопасности
Локальные нормативные акты в области ИБ включают:
а) Положение о защите персональных данных
б) График отпусков сотрудников
в) Штатное расписание

9. Оценка эффективности защиты
Аудит информационной безопасности проводится для:
а) Проверки соответствия системы защиты установленным требованиям
б) Повышения зарплаты сотрудникам
в) Увеличения объема хранимых данных

10. Управление рисками ИБ
Оценка рисков информационной безопасности включает:
а) Анализ вероятности и последствий угроз
б) Расчет заработной платы
в) Планирование корпоративных мероприятий

11. Резервное копирование
Цель резервного копирования данных:
а) Восстановление информации после сбоев
б) Увеличение производительности системы
в) Сокращение затрат на оборудование

12. Правовые основы ИБ
Федеральный закон "О персональных данных" регулирует:
а) Порядок обработки и защиты персональных данных
б) Правила построения компьютерных сетей
в) Нормы разработки программного обеспечения

13. Защита от социальной инженерии
К мерам защиты от социальной инженерии относится:
а) Обучение сотрудников правилам безопасности
б) Установка более мощных серверов
в) Увеличение объема оперативной памяти

14. Мониторинг ИБ
Система обнаружения вторжений предназначена для:
а) Выявления попыток несанкционированного доступа
б) Контроля рабочего времени сотрудников
в) Автоматизации бухгалтерского учета

15. Аутентификация и авторизация
Разграничение прав доступа пользователей необходимо для:
а) Ограничения доступа к информации по принципу минимальных привилегий
б) Ускорения работы системы
в) Упрощения администрирования

16. Если антивирусная программа не обновлялась 6 месяцев, это означает:
а) Система уязвима для новых угроз
б) Защита усилена
в) Производительность системы повышена

17. Внедрение системы шифрования данных привело к:
а) Повышению конфиденциальности информации
б) Увеличению скорости передачи данных
в) Сокращению затрат на оборудование

18. При оценке уязвимости информационной системы:
а) Анализируются возможные векторы атак
б) Рассчитывается стоимость оборудования
в) Определяется график отпусков сотрудников

19. Системы мониторинга ИБ
SIEM-система позволяет:
а) Агрегировать и анализировать события безопасности
б) Автоматизировать только учет оборудования
в) Проводить только антивирусную проверку

20. План восстановления после сбоев
К мерам по обеспечению непрерывности бизнеса относится:
а) Регулярное резервное копирование критически важных данных
б) Увеличение количества сотрудников
в) Сокращение бюджета на ИТ-инфраструктуру

21. Анализ защищенности
Пентест (тестирование на проникновение) - это:
а) Проверка системы на уязвимости путем моделирования атак
б) Оптимизация баз данных
в) Настройка сетевого оборудования

22. При использовании слабых паролей безопасность системы:
а) Снижается
б) Повышается
в) Не изменяется

23. Мониторинг информационной безопасности предполагает:
а) Постоянный контроль событий и инцидентов ИБ
б) Ежегодную инвентаризацию оборудования
в) Разработку дизайна сайта компании

24. При обнаружении вредоносного ПО необходимо:
а) Изолировать зараженную систему и начать лечение
б) Увеличить объем жесткого диска
в) Изменить цветовую схему интерфейса

25. Система показателей эффективности ИБ включает:
а) Количество обнаруженных и нейтрализованных инцидентов
б) Количество сотрудников в отделе
в) Стоимость офисной мебели

При использовании формы текущего контроля «Тестирование» студентам могут предлагаются задания на бумажном носителе.

Критерии и шкала оценивания по оценочному средству «Тесты»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Тесты выполнены на высоком уровне (правильные ответы даны на 90-100% тестов)
4	Тесты выполнены на среднем уровне (правильные ответы даны на 75-89% тестов)
3	Тесты выполнены на низком уровне (правильные ответы даны на 50-74% тестов)
2	Тесты выполнены на неудовлетворительном уровне (правильные ответы даны менее чем на 50% тестов)

2.Разноуровневые задания (базовый уровень)

1.Сущность и основные компоненты системы информационной безопасности современной организации

2.Классификация угроз информационной безопасности: внутренние и внешние источники рисков

3.Методы анализа рисков информационной безопасности и оценки уязвимостей

4.Криптографические методы защиты информации: основные принципы и области применения

5.Прогнозирование киберугроз и разработка сценариев реагирования на инциденты
6.Разработство политики информационной безопасности и регламентирующих документов
7.Организация системы управления информационной безопасностью на предприятии
8.Защита персональных данных и обеспечение соответствия требованиям законодательства
9.Анализ и управление рисками в системе информационной безопасности
10.Роль внутреннего аудита и контроля в системе обеспечения информационной безопасности
11.Обеспечение информационной безопасности в облачных средах и мобильных технологиях
12.Планирование мероприятий по восстановлению после киберинцидентов
13.Оценка эффективности и мониторинг системы защиты информации
14.Нормативно-правовая база обеспечения информационной безопасности в РФ
15.Зарубежный опыт построения систем информационной безопасности
16.Обеспечение безопасности веб-приложений и интернет-ресурсов организации
17.Методы защиты от социальной инженерии и кибермошенничества
18.Информационная безопасность в цепочках поставок и партнерских отношениях
19.Корпоративная культура как элемент системы информационной безопасности
20.Комплексный кейс: разработка концепции информационной безопасности для предприятия конкретной отрасли

Задачи
(высокий уровень)

Задача 1. Выбор системы защиты информации
Ситуация:
Предприятие выбирает между двумя системами защиты:
Система А: Стоимость 500 тыс. руб., базовый функционал, защита от известных угроз.
Система Б: Стоимость 1,5 млн руб., включает AI-анализ угроз, защиту от нулевых атак, автоматическое реагирование.
Задание:
Какую систему выберете для банковского сектора? Для стартапа? Обоснуйте.
Оцените риски внедрения каждой системы (ложные срабатывания, сложность интеграции).
Предложите меры для снижения стоимости Системы Б (лизинг, поэтапное внедрение).

Задача 2. Кризисное управление ИБ-инцидентами
Ситуация:
Обнаружена масштабная утечка данных. Необходимо в течение 24 часов:
Локализовать угрозу;
Уведомить регуляторов;
Сохранить репутацию.
Задание:
Разработайте пошаговый план действий (блокировка учетных записей, анализ логов).
Какие ресурсы нельзя сокращать при ликвидации инцидента? (например, команда цифровой криминалистики).
Рассчитайте потенциальные убытки при задержке реагирования на 2 часа (штрафы, потеря клиентов).

Задача 3. Управление уязвимостями
Ситуация:
Хакеры exploited уязвимость в устаревшем ПО, что привело к простою производства.
Задание:
Разработайте план экстренного обновления систем.
Какие превентивные меры needed? (регулярный патч-менеджмент, пентесты).
Рассчитайте стоимость простоя (200 тыс. руб./час) vs стоимость регулярных обновлений (50 тыс. руб./мес).

Задача 4. Инвестиции в ИБ-инфраструктуру
Ситуация:
Годные потери от кибератак — 5 млн руб. Внедрение SIEM-системы за 3 млн руб. снизит ущерб на 70%.
Задание:
Рассчитайте ROI и срок окупаемости.

Оцените нематериальные выгоды (соответствие стандартам, доверие клиентов).
Докажите руководству необходимость инвестиций с учетом роста киберугроз.

Задача 5. Защита цепочки поставок
Ситуация:
Второстепенный поставщик ПО стал источником атаки на вашу сеть.
Задание:
Проведите оценку рисков всех поставщиков (проверка сертификатов, аудит).
Разработайте требования к кибербезопасности для партнеров.
Рассчитайте экономию от предотвращения инцидента vs затраты на аудит поставщиков.

Задача 6. Сценарное планирование киберугроз
Ситуация:
Появились данные о новой уязвимости в облачной инфраструктуре.
Задание:
Разработайте 3 сценария:
Пессимистичный: полный компромат критической инфраструктуры.
Реалистичный: частичный простой систем.
Оптимистичный: локализованная атака.
Определите индикаторы реализации каждого сценария (сканирование портов, подозрительные авторизации).
Предложите превентивные меры для каждого сценария.

Задача 7. Восстановление после атаки
Ситуация:
Ransomware зашифровало базы данных. Резервные копии не обновлялись 3 дня.
Задание:
Составьте план восстановления (отключение сетей, использование бэкапов, перевыпуск сертификатов).
Оцените убытки от потери данных за 3 дня (1 млн руб./день).
Предложите улучшения для политики резервного копирования и процедур DRP.

Критерии и шкала оценивания по оценочному средству
«разноуровневые задания »

Шкала оценивания (интервал баллов)	Критерии оценивания
5	Обучающийся полностью и правильно выполнил задание. Показал отличные знания, умения и владения навыками применения их при решении задач в рамках усвоенного учебного материала. Работа оформлена аккуратно в соответствии с предъявляемыми требованиями

4	Обучающийся выполнил задание с небольшими неточностями. Показал хорошие знания, умения и владения навыками применения их при решении задач в рамках освоенного учебного материала. Есть недостатки в оформлении работы
3	Обучающийся выполнил задание с существенными неточностями. Показал удовлетворительные знания, умения и владения навыками применения их при решении задач
2	Обучающийся выполнил задание неправильно. При выполнении обучающийся продемонстрировал недостаточный уровень знаний, умений и владения ими при решении задач в рамках усвоенного учебного материала

Методические рекомендации:

На основе изучения основных теоретических положений следует сформулировать собственное обоснованное мнение по проблемам и возможным путям их решения в данной области управления (в зависимости от конкретной постановки вопроса).

3. Контрольные вопросы

(базовый уровень)

1.Дайте определение информационной безопасности организации.
2.Назовите основные объекты и субъекты защиты в системе информационной безопасности.
3.Перечислите ключевые компоненты триады CIA (конфиденциальность, целостность, доступность).
4.В чем различие между внутренними и внешними угрозами информационной безопасности? Приведите примеры.
5.Что понимается под «приемлемым уровнем риска» в контексте информационной безопасности?
6.Опишите алгоритм проведения оценки рисков информационной безопасности.
7.Какие методы используются для качественной и количественной оценки рисков ИБ?
8.Что такое модель угроз и как она применяется для оценки защищенности информации?
9.Какие технические средства защиты информации используются для обеспечения конфиденциальности данных?
10.Что представляет собой система индикаторов компрометации (IoC) и как она используется?
11.Как проводится оценка уязвимостей информационных систем предприятия?
12.Какова роль политик безопасности в системе управления информационной безопасностью?
13.Назовите основные этапы разработки политики информационной безопасности.

14.Что такое система менеджмента информационной безопасности (СМИБ) и каковы этапы ее внедрения?
15.Какие исходные данные необходимы для построения модели угроз информационной системы?
16.Как оценивается эффективность применяемых средств защиты информации?
17.Какие виды планов разрабатываются в системе управления информационной безопасностью?
18.Назовите основные разделы плана обеспечения непрерывности бизнеса (BCP).
19.Что включается в структуру плана реагирования на инциденты информационной безопасности?
20.Как осуществляется планирование мероприятий по защите персональных данных?
21.Каковы принципы организации системы управления доступом?
22.Опишите типовую организационную структуру службы информационной безопасности на предприятии.
23.Какие подразделения обычно вовлекаются в обеспечение информационной безопасности?
24.Как осуществляется распределение ролей и ответственности в системе управления ИБ?
25.Какие методы повышения осведомленности персонала в области ИБ наиболее эффективны?
26.Какова роль высшего руководства в построении системы информационной безопасности?
27.Как организован мониторинг событий информационной безопасности?
28.Какие показатели (KPI) используются для оценки эффективности системы защиты информации?
29.Как проводится аудит системы информационной безопасности?
30.Что такое Security Operations Center (SOC) и каковы его функции?
31.Как осуществляется совершенствование системы защиты на основе результатов мониторинга?
32.Раскройте содержание криптографических методов защиты информации.
33.Что включает в себя система защиты от утечек конфиденциальной информации (DLP)?
34.Назовите основные цели и инструменты обеспечения безопасности сетей.
35.В чем заключаются особенности обеспечения безопасности облачных сервисов?
36.Как обеспечивается безопасность мобильных устройств и приложений?
37.Какую роль в обеспечении ИБ играют системы обнаружения и предотвращения вторжений (IDS/IPS)?
38.Каковы основные источники финансирования мероприятий по обеспечению информационной безопасности?
39.Как нормативно-правовая база регулирует вопросы информационной безопасности в РФ?

40.Опишите порядок действий при обнаружении инцидента информационной безопасности.
41.Как оцениваются операционные риски в системе информационной безопасности?
42.Каковы особенности обеспечения ИБ для распределенных и филиальных сетей?
43.Как интегрируется система управления рисками ИБ в общую систему риск-менеджмента организации?
44.Разработайте примерный план мероприятий по восстановлению работоспособности ИТ-инфраструктуры после кибератаки.

Критерии и шкала оценивания по оценочному средству «Контрольные вопросы»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Студент в полном объеме осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, владеет профильным понятийным (категориальным) аппаратом и т.п.)
4	Студент в целом осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, допустив некоторые неточности и т.п.)
3	Студент допустил существенные неточности, изложил материал с ошибками, не владеет в достаточной степени профильным категориальным аппаратом и т.п.)
2	Раскрытие вопроса представлено на неудовлетворительном уровне или не представлено (студент не готов, не выполнил задание и т.п.)

Тематика контрольных работ:
(базовый уровень)

1.Современные подходы к построению системы информационной безопасности организации
2.Классификация угроз информационной безопасности: анализ внутренних и внешних факторов риска
3.Методы диагностики и оценки рисков в системе управления информационной безопасностью
4.Роль и место криптографической защиты в общей системе информационной безопасности предприятия
5.Защита персональных данных как ключевой элемент обеспечения информационной безопасности
6.Кадровая безопасность: методы предотвращения инсайдерских угроз и формирования культуры ИБ
7.Организационная структура службы информационной безопасности на современном предприятии

8.Разработка и реализация политик информационной безопасности организации

9.Прогнозирование киберугроз и планирование мероприятий по обеспечению безопасности

10.Мониторинг и контроль в системе управления информационной безопасностью

11.Управление инцидентами информационной безопасности: планирование и реализация мероприятий

12.Оценка эффективности системы защиты информации на предприятии

13.Нормативно-правовое обеспечение информационной безопасности в Российской Федерации

14.Управление рисками в системе обеспечения информационной безопасности

15.Защита от утечек конфиденциальной информации (DLP-системы)

16.Обеспечение информационной безопасности в условиях цифровой трансформации бизнеса

17.Взаимосвязь корпоративной культуры и уровня информационной безопасности

18.Особенности обеспечения информационной безопасности в различных отраслях экономики

19.Стратегическое планирование как инструмент обеспечения информационной безопасности

20.Анализ и управление уязвимостями в системе информационной безопасности

21.Обеспечение безопасности облачных технологий и сервисов

22.Политика управления доступом в системе информационной безопасности организации

23.Бюджетирование и управление затратами в системе обеспечения информационной безопасности

24.Зарубежный опыт построения систем информационной безопасности предприятий

25.Комплексный анализ системы информационной безопасности организации (на примере конкретного предприятия)

26.Обеспечение безопасности мобильных устройств и приложений в корпоративной среде

27.Методы и средства защиты информации в сетях передачи данных

28.Организация безопасного удаленного доступа к корпоративным ресурсам

29.Аутсорсинг в области информационной безопасности: преимущества и риски

30.Формирование программы осведомленности сотрудников в области информационной безопасности

Критерии и шкала оценивания по оценочному средству «Контрольная работа»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Контрольная работа выполнена на высоком уровне (правильные ответы даны на 90-100% вопросов/задач)
4	Контрольная работа выполнена на среднем уровне (правильные ответы даны на 75-89% вопросов/задач)
3	Контрольная работа выполнена на низком уровне (правильные ответы даны на 50-74% вопросов/задач)
2	Контрольная работа выполнена на неудовлетворительном уровне (правильные ответы даны менее чем на 50%)

Вопросы к экзамену

1.Раскройте сущность и основные компоненты системы информационной безопасности организации.
2.Опишите классификацию угроз информационной безопасности (внутренние, внешние, комбинированные). Приведите примеры.
3.Каковы цели и задачи анализа рисков информационной безопасности (в контексте профессиональных компетенций)?
4.Охарактеризуйте методы качественной и количественной оценки рисков информационной безопасности.
5.Как применяется модель STRIDE для классификации угроз информационной безопасности?
6.Назовите ключевые показатели эффективности (KPI) системы информационной безопасности и их целевые значения.
7.В чем заключается роль и методы прогнозирования киберугроз в системе управления информационной безопасностью?
8.Опишите процесс и инструменты сценарного планирования для прогнозирования инцидентов информационной безопасности.
9.Каковы основные принципы и этапы разработки политик информационной безопасности?
10.Что включается в содержание раздела «Обеспечение информационной безопасности» в стратегии развития организации?
11.Назовите виды и структуру планов реагирования на инциденты информационной безопасности.
12.Каковы основные задачи и функции службы информационной безопасности на предприятии.
13.Раскройте содержание компетенции постановки задач исполнителям применительно к организации работ по обеспечению информационной безопасности.
14.Какие методы мотивации и координации исполнителей наиболее эффективны в системе управления информационной безопасностью?
15.Как организован мониторинг и контроль выполнения планов

обеспечения информационной безопасности?
16.Какие показатели эффективности (KPI) используются для оценки системы защиты информации?
17.Раскройте содержание и механизмы обеспечения криптографической защиты информации.
18.Что включает в себя система управления уязвимостями и каковы основные этапы ее организации?
19.Опишите инструменты и методы обеспечения безопасности персонала для минимизации инсайдерских угроз.
20.Как обеспечивается соответствие требованиям регуляторов в области информационной безопасности?
21.Каковы современные вызовы и угрозы информационной безопасности в условиях цифровой трансформации?
22.Как интегрируется система управления рисками ИБ в общую систему управления организацией?
23.В чем особенности обеспечения информационной безопасности распределенных и облачных инфраструктур?
24.Какова роль внутреннего аудита в системе обеспечения информационной безопасности?
25.Опишите порядок действий при обнаружении инцидента информационной безопасности.
26.Каковы источники и механизмы финансирования мероприятий по обеспечению информационной безопасности?
27.Как оцениваются операционные риски и включаются в общую систему управления рисками ИБ?
28.В чем заключается роль стратегического планирования в предупреждении угроз информационной безопасности?
29.Опишите алгоритм проведения аудита системы информационной безопасности.
30.Каковы особенности обеспечения информационной безопасности для организаций малого и среднего бизнеса?

Вопросы к зачету

1.Дайте определение информационной безопасности (ИБ). Назовите и раскройте основные свойства (атрибуты) защищенности информации.
2.Что такое политика информационной безопасности? Опишите ее структуру и основные виды (общеорганизационная, тематическая, политика конкретной системы).
3.Раскройте содержание базовых принципов обеспечения информационной безопасности (например, принцип минимальных привилегий, принцип разделения обязанностей, "защита в глубину").
4.Что представляет собой модель угроз и модель нарушителя? Как они используются при построении системы защиты информации?

5. Опишите основные этапы процесса управления рисками информационной безопасности.
6. Назовите и охарактеризуйте качественные и количественные методы оценки рисков ИБ.
7. Какие основные российские законы и нормативные акты регулируют область информационной безопасности? (Например, ФЗ-152 "О персональных данных", ФЗ-187 "О безопасности КИИ", приказы ФСТЭК России).
8. Что такое система классификации информации? Приведите пример такой системы и мер защиты для каждого уровня классификации.
9. Раскройте суть организационных мер обеспечения ИБ. Какие документы и процедуры к ним относятся?
10. Опишите основные методы и средства управления доступом: DAC, MAC, RBAC. В чем их ключевые различия?
11. Что такое инцидент информационной безопасности? Опишите основные этапы управления инцидентами (обнаружение, реагирование, восстановление, анализ).
12. Дайте определение криптографии. В чем разница между симметричными и асимметричными криптосистемами? Приведите примеры алгоритмов.
13. Что такое электронная цифровая подпись (ЭЦП)? Опишите принцип ее работы и области применения.
14. Для чего предназначены межсетевые экраны (firewalls)? Какие типы МЭ существуют (пакетные, шлюзы сеансового уровня, прикладного уровня)?
15. Что такое системы обнаружения и предотвращения вторжений (IDS/IPS)? В чем их ключевое различие?
16. Опишите принципы работы и типы систем защиты от утечек информации (DLP-системы).
17. Назовите основные угрозы безопасности в сетях передачи данных. Какие меры защиты можно применить на сетевом уровне?
18. Что такое виртуальные частные сети (VPN)? Опишите их основные типы и принципы работы.
19. Перечислите основные уязвимости веб-приложений (например, по списку OWASP Top 10). Как можно защититься от атак типа "SQL-инъекция" или "Межсайтовый скриптинг (XSS)"?
20. В чем заключаются особенности обеспечения безопасности облачных сервисов (модели ответственности "разделенная ответственность")?
21. Каковы основные этапы "закалки" (hardening) операционной системы?
22. Что такое средства защиты от вредоносного программного обеспечения? Классифицируйте основные типы вредоносных программ.
23. Опишите цели и задачи управления уязвимостями. Что такое система управления уязвимостями и как она работает?
24. Какие инженерно-технические меры защиты информации вы знаете? (Физическая безопасность, защита от утечки по каналам ПЭМИН).
25. Что такое стандарты информационной безопасности (ISO 27000, PCI DSS)? Какова их роль в построении системы ИБ в организации?

Критерии и шкала оценивания по оценочному средству «Экзамен»

Шкала оценивания (интервал баллов)	Критерий оценивания
отлично (5)	Студент глубоко и в полном объёме владеет программным материалом. Грамотно, исчерпывающе и логично его излагает в устной или письменной форме. При этом знает рекомендованную литературу, проявляет творческий подход в ответах на вопросы и правильно обосновывает принятые решения, хорошо владеет умениями и навыками при выполнении практических задач.
хорошо (4)	Студент знает программный материал, грамотно и по сути излагает его в устной или письменной форме, допуская незначительные неточности в утверждениях, трактовках, определениях и категориях или незначительное количество ошибок. При этом владеет необходимыми умениями и навыками при выполнении практических задач.
удовлетворительно (3)	Студент знает только основной программный материал, допускает неточности, недостаточно чёткие формулировки, непоследовательность в ответах, излагаемых в устной или письменной форме. При этом недостаточно владеет умениями и навыками при выполнении практических задач. Допускает до 30% ошибок в излагаемых ответах.
неудовлетворительно (2)	Студент не знает значительной части программного материала. При этом допускает принципиальные ошибки в доказательствах, в трактовке понятий и категорий, проявляет низкую культуру знаний, не владеет основными умениями и навыками при выполнении практических задач. Студент отказывается от ответов на дополнительные вопросы

Форма листа изменений и дополнений, внесенных в ФОС

Лист изменений и дополнений

№ п/п	Виды дополнений и изменений	Дата и номер протокола заседания кафедры (кафедр), на котором были рассмотрены и одобрены изменения и дополнения	Подпись (с расшифровкой) заведующего кафедрой (заведующих кафедрами)