Образовательное частное учреждение высшего образования
«МОСКОВСКИЙ УНИВЕРСИТЕТ ИМЕНИ А.С. ГРИБОЕДОВА»
(ИМПЭ им. А.С. Грибоедова)

ИНСТИТУТ МЕЖДУНАРОДНОЙ ЭКОНОМИКИ, ЛИДЕРСТВА И МЕНЕДЖМЕНТА

УТВЕРЖДАЮ
Директор института
международной экономики,
лидерства и менеджмента
_____ А.А. Панарин
«23» декабря 2024г.

Рабочая программа дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Специальность
38.05.02 Таможенное дело

Специализация:
Таможенные платежи и валютный контроль

Квалификация (степень):
специалист таможенного дела

Формы обучения:
очная, заочная

Москва

Рабочая программа дисциплины «Информационная безопасность и защита информации». По специальности 38.05.02 Таможенное дело, специализация «Таможенные платежи и валютный контроль» / О.А. Левичев – М.: ИМПЭ им. А.С. Грибоедова

Рабочая программа дисциплины составлена на основании требований Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 38.05.02 «Таможенное дело», утвержденного приказом Министерства науки и высшего образования Российской Федерации от 25 ноября 2020 г. № 1453 и Профессионального стандарта «Специалист по внешнеэкономической деятельности» от «17» июня 2019 г. № 409н (зарегистрирован Министерством юстиции Российской Федерации «11» июля 2019 г., регистрационный № 55208).

Разработчики:	О.А. Левичев, к.в.н., доцент
Ответственный рецензент:	М.К. Чистякова, кандидат экономических наук, доцент, декан экономического факультета ОАНО ВО «Московский психолого-социального университета»
	(Ф.И.О., уч. степень, уч. звание, должность)

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры аудита, финансов и кредита «23» декабря 2024, протокол № 4

Заведующий кафедрой _____/Т. В. Новикова, к. э. н., доцент

Согласовано от Библиотеки _____/О.Е. Стёпкина/

Раздел 1. Цель и задачи освоения дисциплины

Целью освоения дисциплины «Информационная безопасность и защита информации» является формирование у студентов знаний и умений в области обеспечения информационной безопасности, способностей к решению задач по защите информации от несанкционированного доступа, модификации, копирования и уничтожения.

Задачи дисциплины:

- изучение основных понятий и терминов в области информационной безопасности;
- ознакомление с методами и средствами защиты информации;
- анализ угроз и рисков информационной безопасности;
- разработка мер по предотвращению и ликвидации последствий нарушений информационной безопасности;
- проектирование систем защиты информации.

Раздел 2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
УК-10	**Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности**	**ИУК-10.1** Знает способы профилактики коррупции и формирования нетерпимого отношения к ней.
		ИУК-10.2 Предупреждает коррупционные риски в профессиональной деятельности; исключает вмешательство в свою профессиональную деятельность в случаях склонения к коррупционным правонарушениям

Раздел 3. Место дисциплины в структуре образовательной программы специалитета

Дисциплина «Информационная безопасность и защита информации» изучается в 5 семестре очной и заочной форм обучения, относится к Блоку Б.1 «Дисциплины (модули)», «Обязательная часть» образовательной программы по специальности 38.05.02 Таможенное дело (уровень специалитет), специализация: «Таможенные платежи и валютный контроль».

Раздел 4. Объем (трудоемкость) дисциплины (общая, по видам учебной работы, видам промежуточной аттестации)

Трудоемкость дисциплины и виды учебной работы на очной форме обучения

з.е.	Итого	Лекции	Практические занятия	Курсовое проектирование	Самостоятельная работа	Текущий контроль	Контроль, промежуточная аттестация
5 семестр							
3	108	16	32		56		4 Зачет

на заочной форме обучения

з.е.	Итого	Лекции	Практические занятия	Курсовое проектирование	Самостоятельная работа	Текущий контроль	Контроль, промежуточная аттестация
5 семестр							

3	108	2	8		94		4 Зачет

Тематический план дисциплины

Очная форма обучения

Разделы / Темы	Лекции	Практические занятия	Самостоятельная работа	Текущий контроль	Контроль, промежуточная аттестация	Всего часов
5 семестр						
Тема 1. Борьба с угрозами несанкционированного доступа к информации	6	12	20			38
Тема 2. Борьба с вирусным заражением информации.	4	10	18			32
Тема 3. Организационно-правовое обеспечение информационной безопасности	6	10	18			34
Зачет					4	4
Итого по дисциплине	16	32	56		4	108

на заочной форме обучения

Разделы / Темы	Лекции	Практические занятия	Самостоятельная работа	Текущий контроль	Контроль, промежуточная аттестация	Всего часов
5 семестр						
Тема 1. Борьба с угрозами несанкционированного доступа к информации	2	4	32			38
Тема 2. Борьба с вирусным заражением информации.		2	32			34
Тема 3. Организационно-правовое обеспечение информационной безопасности		2	30			32
Зачет					4	4
Итого по дисциплине	2	8	94		4	108

Структура и содержание дисциплины

Наименование раздела/ темы дисциплины	**Содержание дисциплины**
Тема 1. Борьба с угрозами несанкционированного доступа к информации	Актуальность проблемы обеспечение безопасности информации. Основные понятия безопасности: конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации. Угрозы информационной безопасности: классификация, источники возникновения и пути реализации. Определение требований к уровню обеспечения информационной безопасности. Стандарты в области

	информационной безопасности. Виды мер обеспечения информационной безопасности: законодательные, морально-этические, организационные, технические, программно-математические. Специфические приемы управления техническими средствами. Методы защиты от копирования. Защита программ в оперативной памяти. Защита ПК от вредоносных закладок. Защита информации в ПК. Основные принципы построения систем защиты информации. Основные защитные механизмы: идентификацию и аутентификацию. Классификацию атак, модели и результаты атак. Этапы реализации атак. Обнаружение атак. Противодействия атакам. Анализ риска.
Тема 2. Борьба с вирусным заражением информации.	Проблемы вирусного заражения и структура современных вирусов. Компьютерный вирус: понятие, пути распространения, проявление действия вируса. Структура современных вирусов: модели поведения вирусов; деструктивные действия вируса; разрушение программы защиты или изменение состояния программной среды; воздействия на программно-аппаратные средства защиты информации. Взлом парольной системы. Программы-шпионы. Программы-сканеры. Классификация антивирусных программ. Программы-детекторы. Программы-доктора. Программы-ревизоры. Программы-фильтры. Профилактика заражения вирусом.
Тема 3. Организационно-правовое обеспечение информационной безопасности	Международные, российские и отраслевые правовые документы. Опыт законодательного регулирования информатизации в России и за рубежом. Концепция правового обеспечения информационной безопасности РФ. Стандарты и нормативно-методические документы в области обеспечения информационной безопасности. Международные правовые акты по защите информации. Компьютерные преступления.

Занятия семинарского типа
(Практические занятия)

Общие рекомендации по подготовке к практическим занятиям. При подготовке к работе во время проведения занятий практического типа следует обратить внимание на следующие моменты: на процесс предварительной подготовки, на работу во время занятия, обработку полученных результатов, исправление полученных замечаний. Предварительная подготовка к учебному занятию практического типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач занятия.

Работа во время проведения занятия практического типа включает несколько моментов: а) консультирование обучающихся преподавателями с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем задач; б) самостоятельное выполнение заданий согласно обозначенной учебной программой тематики.

Тема 1. «Борьба с угрозами несанкционированного доступа к информации»

Вопросы и/или задания

1. Требования к уровню обеспечения информационной безопасности.
2. Стандарты в области информационной безопасности.
3. Виды мер обеспечения информационной безопасности.

Тема 2. «Борьба с вирусным заражением информации»

Вопросы и/или задания

1. Структура современных вирусов.
2. Взлом парольной системы.
3. Классификация антивирусных программ.

Тема 3. «Организационно-правовое обеспечение информационной безопасности»

Вопросы и/или задания

1. Концепция правового обеспечения информационной безопасности РФ.
2. Стандарты в области обеспечения информационной безопасности.
3. Международные правовые акты по защите информации.

Раздел 5. Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

Наряду с чтением лекций и проведением практических занятий неотъемлемым элементом учебного процесса является *самостоятельная работа.* При самостоятельной работе достигается конкретное усвоение учебного материала, развиваются теоретические способности, столь важные для успешной подготовки и защиты выпускной работы. Формы самостоятельной работы, обучаемых могут быть разнообразными. Самостоятельная работа включает: изучение литературы, веб-ресурсов, оценку, обсуждение и рецензирование публикуемых статей; ответы на контрольные вопросы; решение задач; самотестирование. Выполнение всех видов самостоятельной работы увязывается с изучением конкретных тем.

Типовые задания для самостоятельной работы и примерная тематика курсовых работ (проектов), предусмотренных учебным планом, представлены в фонде оценочных средств по дисциплине.

5.1. Индивидуальные задания для курсовых работ

Курсовая работа позволяет выявить степень владения базовыми знаниями, умениями необходимыми для обучения, и определить уровень владения новым материалом. Рекомендации по подготовке, оформлению и защите курсовой работы (курсового проекта), предусмотренной учебным планом, изложены в Методических указаниях по соответствующей дисциплине

5.1.1. Примерная тематика курсовых работ (проектов)

Курсовая работа не предусмотрена учебным планом.

Раздел 6. Оценочные и методические материалы по образовательной программе (фонд оценочных средств) для проведения текущего контроля успеваемости и промежуточной аттестации

В процессе освоения учебной дисциплины для оценивания сформированности требуемых компетенций используются оценочные материалы (фонды оценочных средств).

Типовые тестовые задания, типовые практические задания, типовые задания для контрольных работ, материалы для оценки результатов промежуточной аттестации и материалы для диагностической работы представлены в фонде оценочных средств по дисциплине.

6.1. Материалы для оценки результатов промежуточной аттестации

Перечень вопросов для подготовки к промежуточной аттестации (Зачет)

1. Требования к уровню обеспечения информационной безопасности.
2. Стандарты в области информационной безопасности.
3. Виды мер обеспечения информационной безопасности
4. Структура современных вирусов.
5. Взлом парольной системы.
6. Классификация антивирусных программ

7. Концепция правового обеспечения информационной безопасности РФ.
8. Стандарты в области обеспечения информационной безопасности.
9. Международные правовые акты по защите информации.
10. Анализ защищённости web-приложения на основе моделирования сетевых атак.
11. Блок защиты информации каналов управления автоматизированной системы спутниковой связи.
12. Комплексное обеспечение информационной безопасности при реализации угрозы попытки доступа в удалённую систему.
13. Концепция политики безопасности и систем контроля доступа для локальных вычислительных сетей.
14. Модель системы управления информационной безопасностью в условиях неопределённости воздействия.
15. Обеспечение безопасности транзакций с использованием банковских карт.
16. Организация информационной безопасности электронного архива оплаты платёжных документов населением.
17. Оценка эффективности средств и методов защиты информации на предприятии.
18. Построение типовой модели угроз безопасности информации кредитной организации.
19. Применение DLP-систем как инструмента обеспечения информационной безопасности компании.
20. Разработка защищённой информационной структуры для бюджетного медицинского учреждения.
21. Разработка и внедрение системы информационной безопасности в транспортной компании.
22. Разработка методики защиты информации от целевого фишинга в автоматизированной системе предприятия.
23. Разработка программы для повышения информационной безопасности в коммерческом банке.
24. Разработка регламента проведения аудита информационной безопасности государственного бюджетного учреждения.
25. Разработка средств защиты от утечек сеансов VPN мобильных пользователей.
26. Система защиты персональных данных на предприятии.
27. Система обеспечения защиты информации в переговорной комнате.
28. Управление рисками информационной безопасности в организации.
29. Внедрение системы мониторинга и анализа событий информационной безопасности.
30. Использование криптографических методов для защиты информации.
31. Тестирование и оценка эффективности систем защиты информации.
32. Управление инцидентами информационной безопасности и реагирование на них.

Краткая характеристика ответов (ключи):

1. **Требования к уровню обеспечения информационной безопасности** определяются на основе анализа ценности защищаемой информации и оценки потенциальных рисков. Они формируются с учётом законодательства РФ, в частности, законов «О государственной тайне», «О персональных данных» и «О коммерческой тайне». Требования регламентируют создание комплексной системы защиты, охватывающей организационные, технические и правовые меры. Ключевым принципом является непрерывность защиты и её адекватность актуальным угрозам.

2. **Стандарты в области информационной безопасности** служат основой для построения надёжных систем защиты и обеспечивают методологическое единство. В России базовым является ГОСТ Р ИСО/МЭК 27001, описывающий требования к системе менеджмента информационной безопасности (СУИБ). Для специфических отраслей, например, банковской сферы, применяются дополнительные стандарты (например, ГОСТ Р 57580). Международные стандарты, такие как серия ISO/IEC 27000, гармонизируют подходы к безопасности на глобальном уровне.

3. **Виды мер обеспечения информационной безопасности** традиционно делятся на три основные группы. **Правовые меры** включают законодательство и нормативные акты, устанавливающие ответственность за нарушения. **Организационные меры** — это внутренние политики, регламенты, правила доступа и обучение персонала. **Технические (программно-аппаратные) меры** представляют собой конкретные инструменты: межсетевые экраны, антивирусы, системы шифрования и средства обнаружения вторжений.

4. **Структура современных вирусов** эволюционировала от простых самораспространяющихся кодов до сложных программных комплексов. Как правило, вредоносное ПО состоит из **инсталлятора**, который проникает в систему, **полезной нагрузки** (payload), выполняющей деструктивные или шпионские действия, и **механизмов маскировки** и самозащиты от антивирусов. Современные угрозы часто используют модульную архитектуру и могут получать команды с удалённых серверов управления.

5. **Взлом парольной системы** — это процесс получения несанкционированного доступа к учётной записи путём обхода аутентификации. Основные методы включают **брутфорс** (перебор всех возможных комбинаций), **словарную атаку** (перебор слов из готовых списков) и **социальную инженерию** (обман пользователя с целью выведать пароль). Также используются уязвимости в программном обеспечении для перехвата хешей паролей или их сброса.

6. **Классификация антивирусных программ** может проводиться по нескольким критериям. По **режиму работы** они делятся на **сканеры** (проверяют файлы по запросу или расписанию) и **мониторы** (постоянно отслеживают активность в реальном времени). По **методу обнаружения** выделяют **сигнатурный анализ** (сравнение с базой известных вирусов) и **эвристический анализ** (поиск подозрительного поведения, характерного для вредоносного ПО).

7. **Концепция правового обеспечения информационной безопасности РФ** представляет собой совокупность законодательных актов, регулирующих отношения в этой сфере. Основу составляют Конституция РФ, а также федеральные законы: № 149-ФЗ «Об информации...», № 152-ФЗ «О персональных данных», № 98-ФЗ «О коммерческой тайне». Эта правовая база устанавливает права и обязанности субъектов, а также ответственность за правонарушения.

8. **Стандарты в области обеспечения информационной безопасности** (дублирует п.2). См. ответ на вопрос №2.

9. **Международные правовые акты по защите информации** играют ключевую роль в регулировании глобального информационного пространства. К ним относятся *Конвенция Совета Европы о киберпреступности* (*Будапештская конвенция*), которая устанавливает стандарты для национального законодательства, и различные соглашения в рамках *ООН* и *ВТО*, касающиеся защиты интеллектуальной собственности и электронной торговли.

10. **Анализ защищённости web-приложения на основе моделирования сетевых атак** — это процесс имитации действий злоумышленника для выявления уязвимостей. Специалисты по безопасности (пентестеры) используют те же инструменты и методики, что и хакеры, чтобы проверить устойчивость приложения к таким атакам, как *SQL-инъекции*, *XSS* и *CSRF*. Результатом является отчёт с описанием найденных уязвимостей и рекомендациями по их устранению.

11. **Блок защиты информации каналов управления автоматизированной системы спутниковой связи** предназначен для обеспечения конфиденциальности, целостности и доступности команд, передаваемых между наземным сегментом и космическим аппаратом. Он включает в себя аппаратные модули шифрования, системы аутентификации узлов сети и средства контроля целостности передаваемых пакетов данных для предотвращения перехвата управления или подмены команд.

12. **Комплексное обеспечение информационной безопасности при реализации угрозы попытки доступа в удалённую систему** требует эшелонированной обороны. На внешнем рубеже используются межсетевые экраны (*firewall*) для фильтрации трафика. Далее система обнаружения/предотвращения вторжений (*IDS/IPS*) анализирует попытки проникновения. Для самого доступа применяется строгая аутентификация, а действия пользователя внутри системы протоколируются для последующего аудита.

13. **Концепция политики безопасности и систем контроля доступа для локальных вычислительных сетей (ЛВС)** определяет правила, по которым субъекты (пользователи) получают доступ к объектам (файлам, папкам, устройствам). Основой является модель управления доступом: *дискреционная* (владелец ресурса сам назначает права), *мандатная* (доступ на основе меток конфиденциальности) или *ролевая* (права назначаются ролям, а роли — пользователям).

14. **Модель системы управления информационной безопасностью в условиях неопределённости воздействия** учитывает, что невозможно предсказать все угрозы со стопроцентной точностью. Такие модели строятся на принципах риск-менеджмента: выявляются активы, оцениваются вероятности реализации угроз и возможный ущерб, после чего для наиболее критичных рисков выбираются адекватные и экономически оправданные меры защиты.

15. **Обеспечение безопасности транзакций с использованием банковских карт** достигается за счёт многоуровневой защиты. Ключевую роль играет стандарт *PCI DSS*, обязывающий банки и магазины соблюдать строгие меры безопасности. Для каждой операции используются технологии *3D-Secure* (*Verified by Visa, Mastercard ID Check*), а данные карты передаются в зашифрованном виде с использованием протокола *TLS*.

16. **Организация информационной безопасности электронного архива оплаты платёжных документов населением** направлена на защиту финансовых данных граждан и обеспечение их неизменности. Система должна обеспечивать строгий контроль доступа на основе ролей, шифрование данных как при хранении, так и при передаче, а также ведение неизменяемых логов всех операций для возможности аудита и расследования инцидентов.

17. **Оценка эффективности средств и методов защиты информации на предприятии** проводится для определения их адекватности текущим угрозам и рентабельности вложений в безопасность. Оценка включает анализ ключевых показателей эффективности (*KPI*), таких как среднее время обнаружения и реагирования на инциденты, а также проведение имитационных атак (*пентестов*) для проверки реальной устойчивости систем.

18. **Построение типовой модели угроз безопасности информации кредитной организации** является обязательным этапом создания системы защиты согласно требованиям регулятора (*ЦБ РФ*). Модель включает классификацию активов (базы данных, транзакционные системы), идентификацию потенциальных нарушителей (внешние хакеры, инсайдеры) и описание векторов атак (фишинг, *DDoS*, взлом приложений).

19. **Применение DLP-систем как инструмента обеспечения информационной безопасности компании** (*Data Loss/Leak Prevention*) направлено на предотвращение утечек конфиденциальной информации за пределы корпоративного контура. Система анализирует исходящий трафик (почта, мессенджеры, веб-формы) и действия сотрудников на рабочих станциях, блокируя передачу файлов, содержащих ключевые слова или относящихся к защищаемым категориям.

20. **Разработка защищённой информационной структуры для бюджетного медицинского учреждения** требует особого внимания к защите персональных данных пациентов и врачебной тайны. Система должна соответствовать требованиям *ФЗ-152 «О персональных данных»*, что подразумевает внедрение средств защиты от несанкционированного

доступа, шифрование баз данных и строгий аудит всех действий пользователей с медицинской информацией.

21. **Разработка и внедрение системы информационной безопасности в транспортной компании** имеет свою специфику, связанную с защитой не только офисных данных, но и систем управления логистикой (*TMS*), GPS/ГЛОНАСС-мониторингом автопарка. Ключевыми задачами являются защита от взлома систем навигации для предотвращения угонов и обеспечение целостности данных о грузах и маршрутах перевозки.

22. **Разработка методики защиты информации от целевого фишинга в автоматизированной системе предприятия** должна быть комплексной, так как технические средства не всегда эффективны против социальной инженерии. Методика включает внедрение современных почтовых фильтров, использование систем многофакторной аутентификации (*MFA*) для доступа к критичным ресурсам и, что самое важное, регулярное обучение сотрудников распознаванию фишинговых писем.

23. **Разработка программы для повышения информационной безопасности в коммерческом банке** — это стратегическая задача, так как банк является одной из главных целей для киберпреступников. Программа должна включать внедрение передовых средств защиты (*SIEM, WAF, EDR*), регулярный анализ защищённости приложений и создание собственного центра мониторинга и реагирования на инциденты (*SOC*).

24. **Разработка регламента проведения аудита информационной безопасности государственного бюджетного учреждения** формализует процесс проверки соответствия системы защиты установленным нормам (например, требованиям ФСТЭК). Регламент определяет цели, объекты, периодичность аудита, методику оценки рисков и форму отчёта с выводами о состоянии ИБ и планом устранения выявленных недостатков.

25. **Разработка средств защиты от утечек сеансов VPN мобильных пользователей** актуальна в условиях удалённой работы. Такие средства включают внедрение систем многофакторной аутентификации (*MFA*) при подключении к VPN-шлюзу, использование агентов контроля состояния конечного устройства (*NAC/EDR*) перед предоставлением доступа и шифрование трафика по протоколам *IPsec* или *SSL/TLS* с проверкой сертификатов.

26. **Система защиты персональных данных на предприятии** строится в соответствии с требованиями законодательства (*ФЗ-152*) и нормативных актов регуляторов (*ФСТЭК, ФСБ*). Она включает определение уровней защищённости персональных данных (УЗ), внедрение технических (межсетевые экраны, СЗИ от НСД) и организационных мер (приказы, инструкции, назначение ответственных), а также применение средств криптографической защиты при необходимости.

27. **Система обеспечения защиты информации в переговорной комнате («чистая комната»)** предназначена для предотвращения утечки акустической и визуальной информации во время конфиденциальных встреч. Она включает комплекс мер: экранирование стен для блокировки радиосигналов (*Wi-Fi, GSM*), системы виброакустической зашумления для защиты от прослушивания через стёкла и стены, а также генераторы электромагнитного шума.

28. **Управление рисками информационной безопасности в организации** — это циклический процесс, являющийся ядром современной стратегии ИБ. Он включает идентификацию активов и угроз, оценку вероятности и ущерба от реализации рисков, выбор стратегии обработки (снижение, принятие, уклонение) и внедрение контролей для их минимизации с последующим мониторингом.

29. **Внедрение системы мониторинга и анализа событий информационной безопасности (*SIEM*)** позволяет собирать логи со всего сетевого оборудования, серверов и приложений в единое хранилище для корреляционного анализа в реальном времени. Это даёт возможность

выявлять сложные атаки на ранней стадии по косвенным признакам, оперативно реагировать на инциденты и проводить ретроспективный анализ для расследования причин сбоев или взломов.

30.**Использование криптографических методов для защиты информации** обеспечивает её конфиденциальность (шифрование), целостность (хеширование) и подлинность (электронная подпись). В зависимости от задач применяются симметричные алгоритмы (быстрое шифрование больших объёмов данных) или асимметричные (безопасный обмен ключами, цифровая подпись), которые являются фундаментом для построения защищённых каналов связи.

31.**Тестирование и оценка эффективности систем защиты информации** проводятся для проверки их реальной работоспособности против актуальных угроз. Это достигается через проведение тестов на проникновение (*пентестов*), когда специалисты имитируют действия хакеров, а также через анализ защищённости кода приложений (*SAST/DAST*) и проверку конфигураций оборудования на соответствие лучшим практикам.

32.**Управление инцидентами информационной безопасности и реагирование на них** — это процесс минимизации ущерба от уже произошедшего взлома или сбоя. Он регламентируется заранее разработанным планом реагирования (*IRP*), который определяет роли сотрудников, порядок локализации угрозы (например, отключение заражённого сервера), восстановления систем из резервных копий и извлечения уроков для предотвращения подобных инцидентов в будущем.

6.2. Оценивание ответов на вопросы и выполнения заданий промежуточной аттестации
При оценке знаний учитывается уровень сформированности компетенций:
1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

Шкала оценивания на экзамене, зачете с оценкой

Оценка	Критерии выставления оценки
Отлично	Обучающийся должен: - продемонстрировать глубокое и прочное усвоение знаний программного материала; - исчерпывающе, последовательно, грамотно и логически стройно изложить теоретический материал; - правильно формулировать определения; - продемонстрировать умения самостоятельной работы с литературой; - уметь сделать выводы по излагаемому материалу.
Хорошо	Обучающийся должен: - продемонстрировать достаточно полное знание программного материала; - продемонстрировать знание основных теоретических понятий; - достаточно последовательно, грамотно и логически стройно излагать материал; - продемонстрировать умение ориентироваться в литературе; - уметь сделать достаточно обоснованные выводы по излагаемому материалу.
Удовлетворительно	Обучающийся должен: - продемонстрировать общее знание изучаемого материала; - показать общее владение понятийным аппаратом дисциплины;

	- уметь строить ответ в соответствии со структурой излагаемого вопроса; - знать основную рекомендуемую программой учебную литературу.
Неудовлетворительно	Обучающийся демонстрирует: - незнание значительной части программного материала; - не владение понятийным аппаратом дисциплины; - существенные ошибки при изложении учебного материала; - неумение строить ответ в соответствии со структурой излагаемого вопроса; - неумение делать выводы по излагаемому материалу.

Шкала оценивания на зачете

Оценка	**Критерии выставления оценки**
«Зачтено»	Обучающийся должен: уметь строить ответ в соответствии со структурой излагаемого вопроса; продемонстрировать прочное, достаточно полное усвоение знаний программного материала; продемонстрировать знание основных теоретических понятий; правильно формулировать определения; последовательно, грамотно и логически стройно изложить теоретический материал; продемонстрировать умения самостоятельной работы с литературой; уметь сделать достаточно обоснованные выводы по излагаемому материалу.
«Не зачтено»	Обучающийся демонстрирует: незнание значительной части программного материала; не владение понятийным аппаратом дисциплины; существенные ошибки при изложении учебного материала; неумение строить ответ в соответствии со структурой излагаемого вопроса; неумение делать выводы по излагаемому материалу.

Методические материалы, определяющие процедуру оценивания сформированных компетенций в соответствии с ООП

Качество знаний характеризуется способностью обучающегося точно, структурированно и уместно воспроизводить информацию, полученную в процессе освоения дисциплины, в том виде, в котором она была изложена в учебном издании или преподавателем.

Умения, как правило, формируются на занятиях семинарского типа. Задания, направленные на оценку умений, в значительной степени требуют от обучающегося проявления стереотипности мышления, т.е. способности выполнить работу по образцам, с которыми он работал в процессе обучения. Преподаватель же оценивает своевременность и правильность выполнения задания.

Навыки можно трактовать как автоматизированные умения, развитые и закрепленные осознанным самостоятельным трудом. Навыки формируются при самостоятельном выполнении обучающимися практико-ориентированных заданий, моделирующих решение им производственных и социокультурных задач в соответствующей области профессиональной деятельности, как правило, при выполнении домашних заданий, курсовых проектов (работ), научно-исследовательских работ, прохождении практик, при работе индивидуально или в составе группы и т.д.

Устный опрос – это процедура, организованная как специальная беседа преподавателя с группой обучающихся (фронтальный опрос) или с отдельными обучающимися (индивидуальный опрос) с целью оценки сформированности у них основных понятий и усвоения учебного материала. Устный опрос может использоваться как вид контроля и метод оценивания формируемых компетенций (как и качества их формирования) в рамках самых

разных форм контроля, таких как: собеседование, коллоквиум, зачет, экзамен по дисциплине. Устный опрос (УО) позволяет оценить знания и кругозор обучающегося, умение логически построить ответ, владение монологической речью и иные коммуникативные навыки. УО обладает большими возможностями воспитательного воздействия преподавателя. Воспитательная функция УО имеет ряд важных аспектов: профессионально-этический и нравственный аспекты, дидактический (систематизация материала при ответе, лучшее запоминание материала при интеллектуальной концентрации), эмоциональный (радость от успешного прохождения собеседования) и др. Обучающая функция УО состоит в выявлении деталей, которые по каким-то причинам оказались недостаточно осмысленными в ходе учебных занятий и при подготовке к зачёту или экзамену. УО обладает также мотивирующей функцией: правильно организованные собеседование, коллоквиум, зачёт и экзамен могут стимулировать учебную деятельность студента, его участие в научной работе.

Тесты являются простейшей формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин. Тест может предоставлять возможность выбора из перечня ответов (один или несколько правильных ответов).

Семинарские занятия. Основное назначение семинарских занятий по дисциплине – обеспечить глубокое усвоение обучающимися материалов лекций, прививать навыки самостоятельной работы с литературой, воспитывать умение находить оптимальные решения в условиях изменяющихся отношений, формировать современное профессиональное мышление обучающихся. На семинарских занятиях преподаватель проверяет выполнение самостоятельных заданий и качество усвоения знаний, умений, определяет уровень сформированности компетенций.

Раздел 7. Методические указания для обучающихся по основанию дисциплины

Освоение обучающимся учебной дисциплины предполагает изучение материалов дисциплины на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме лекций, семинаров и практических занятий. Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся.

Для успешного освоения учебной дисциплины и достижения поставленных целей необходимо внимательно ознакомиться с настоящей рабочей программы учебной дисциплины. Следует обратить внимание на список основной и дополнительной литературы, которая имеется в электронной библиотечной системе Университета. Эта информация необходима для самостоятельной работы обучающегося.

При подготовке к аудиторным занятиям необходимо помнить особенности каждой формы его проведения.

Подготовка к учебному занятию лекционного типа. С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку: знакомит с новым учебным материалом; разъясняет учебные элементы, трудные для понимания; систематизирует учебный материал; ориентирует в учебном процессе.

С этой целью: внимательно прочитайте материал предыдущей лекции; ознакомьтесь с учебным материалом по учебнику и учебным пособиям с темой прочитанной лекции; внесите дополнения к полученным ранее знаниям по теме лекции на полях лекционной тетради; запишите возможные вопросы, которые вы зададите лектору на лекции по материалу изученной лекции; постарайтесь уяснить место изучаемой темы в своей подготовке; узнайте тему предстоящей лекции (по тематическому плану, по информации лектора) и запишите информацию, которой вы владеете по данному вопросу

Предварительная подготовка к учебному занятию семинарского типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач занятия.

Самостоятельная работа. Для более углубленного изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темы. При выполнении заданий по возможности используйте наглядное представление материала.

Подготовка к зачету, экзамену. К зачету, экзамену необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить учебную дисциплину в период зачетно-экзаменационной сессии, как правило, приносят не слишком удовлетворительные результаты. При подготовке к зачету обратите внимание на защиту практических заданий на основе теоретического материала. При подготовке к экзамену по теоретической части выделите в вопросе главное, существенное (понятия, признаки, классификации и пр.), приведите примеры, иллюстрирующие теоретические положения.

Раздел 8. Учебно-методическое и информационное обеспечение дисциплины

Основная литература

1. Мирошников А.И. Основы информационной безопасности и защита информации: учебное пособие / Мирошников А.И., Сысоев А.С. — Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2022. — 107 с. — ISBN 978-5-00175-160-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/128718.html

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 3-е изд. — Саратов: Профобразование, 2024. — 702 с. — ISBN 978-5-4488-0070-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/145912.html

3. Мартынов, А. П. Информационная безопасность и защита информации: учебное пособие / А. П. Мартынов, И. А. Мартынова, А. А. Русаков. — 2-е изд. — Москва: Ай Пи Ар Медиа, 2026. — 130 с. — ISBN 978-5-4497-2349-9. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/155918.html

Дополнительная литература

1. Информационная безопасность и защита информации: учебно-методический комплекс / составители С. А. Омарова, К. А. Искакова, Н. А. Тойганбаева. — Алматы: Нур-Принт, 2012. — 98 с. — ISBN 9965-756-05-8. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/67055.html
2. Прохорова, О. В. Информационная безопасность и защита информации: учебник / О. В. Прохорова. — Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — 113 с. — ISBN 978-5-9585-0603-3. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/43183.html/
3. Бахаров, Л. Е. Информационная безопасность и защита информации: сборник тестов / Л. Е. Бахаров. — Москва: Издательский Дом МИСиС, 2015. — 43 с. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/98858.html

8.1. Требования к материально-техническому и учебно-методическому обеспечению программы специалитета

8.1.1. Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой специалитета, оснащенные оборудованием и техническими средствами обучения, состав которых определяется в рабочих программах дисциплин

(модулей).

В Университете имеются специализированные аудитории для проведения занятий по информационным технологиям.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде Университета.

Электронная информационно-образовательная среда Университета включает:

1. Официальный сайт Университета (https://www.iile.ru/)
2. Электронная информационно-образовательная среда «1С: Университет» договор от 10.09.2018 г. №ПРКТ-18281 (бессрочно)
3. Программы для ЭВМ. Система дистанционного обучения «Mirapolis» - Лицензионный договор №107/06/24-к от 27.06.2024 (Спецификация к Лицензионному договору №107/06/24-к от 27.06.2024, срок действия с 02.07.2025 по 01.07.2026 г.) https://impe.lms.mirapolis.ru/mira/
4. Программа для ЭВМ. Виртуальная комната «Mirapolis» - Лицензионный договор №107/06/24-к от 27.06.2024 (Спецификация к Лицензионному договору №107/06/24-к от 27.06.2024, срок действия с 02.07.2025 по 01.07.2026 г.) https://impe.lms.mirapolis.ru/mira/
5. Система тестирования INDIGO лицензионное соглашение (Договор от 07.11.2018 г. №Д-54792, дополнительное соглашение № Д-5479/6 о пролонгации договора до 01.06.2026г.) http://212.48.35.211:85/

8.1.2. Университет обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства (состав определяется в рабочих программах дисциплин (модулей) и подлежит обновлению при необходимости).

Перечень лицензионного программного обеспечения, в том числе отечественного производства:

1. Операционная система «Атлант» - Atlant Academ от 24.01.2024 г. (бессрочно)
2. Антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition договор-оферта № Tr000941765 от 16.10.2025 г.

8.1.3. Обучающимся обеспечен доступ (удаленный доступ) к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочих программах дисциплин (модулей) и обновляется при необходимости, но не реже одного раз в год.

Перечень современных профессиональных баз данных и информационных справочных систем:

1. Информационно-поисковая система «Консультант Плюс» - Договор №МИ-ВИП-79717-56/2022 (бессрочно)
2. Электронно-библиотечная система IPRsmart лицензионный договор от 01.09.2024 г. №11652/24С (срок действия до 31.08.2027 г.) https://www.iprbookshop.ru/
3. Научная электронная библиотека eLIBRARY лицензионный договор SCIENC INDEX № SIO -3079/2026 от 30.01.2026 г. (срок действия до 29.01.2027г.) https://elibrary.ru

8.1.4. Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Раздел 9. Материально-техническое обеспечение образовательного процесса

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и	Оборудование: специализированная мебель (мебель аудиторная (столы, стулья, доска аудиторная навесная), стол преподавателя, стул

индивидуальных консультаций, текущего контроля и промежуточной аттестации	преподавателя. Технические средства обучения: персональный компьютер; мультимедийное оборудование (проектор, экран).
Помещение для самостоятельной работы	Специализированная мебель (столы, стулья), персональные компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета

ЛИСТ ИЗМЕНЕНИЙ

Актуализированы в 2024 году (решение Ученого совета 26.12.2024г., протокол №3):

- Перечень основной и дополнительной литературы;
- Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;
- Комплект лицензионного программного обеспечения.

Актуализированы в 2025 году (решение Ученого совета 23.12.2025г., протокол №3):

- Перечень основной и дополнительной литературы;
- Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;
- Комплект лицензионного программного обеспечения.