Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гриб Владислав Валерьевич
Должность: Ректор
Дата подписания: 06.11.2026 16:50:38
Уникальный программный ключ:
637517d24e103c3db032acf37e839d98ec1c5bb2f5eb89c29abfcd7f43985447

Образовательное частное учреждение высшего образования

«МОСКОВСКИЙ УНИВЕРСИТЕТ ИМЕНИ А.С. ГРИБОЕДОВА»

(ИМПЭ им. А.С. Грибоедова)

ФАКУЛЬТЕТ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
(МЕЖДУНАРОДНЫЙ ДИПЛОМАТИЧЕСКИЙ КОЛЛЕДЖ)

УТВЕРЖДАЮ
Директор Международного
дипломатического колледжа
_____ Н.И. Платонова
«16» февраля 2026г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Основы информационной безопасности

Специальность
09.02.11 Разработка и управление программным обеспечением

Квалификация выпускника:
Программист

на базе среднего общего образования

Форма обучения: очная

Москва

Рабочая программа дисциплины «Стандартизация, сертификация и техническое документоведение». Специальность 09.02.11 Разработка и управление программным обеспечением /– М.: ИМПЭ им. А. С. Грибоедова.

Рабочая программа учебного предмета составлена на основании Федерального государственного образовательного стандарта 09.02.11 Разработка и управление программным обеспечением, утвержденного приказом №138 от 24.02.2025 г. «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.11 Разработка и управление программным обеспечением».

Организация-разработчик:	Образовательное частное учреждение высшего образования «Московский университет имени А. С. Грибоедова»
Ответственный рецензент:	Е.В. Михалёва, к. ф.-м. н. исполнительный директор института информационных систем и инженерно-компьютерных технологий
	(Ф.И.О., уч. степень, уч. звание, должность)

Рабочая программа дисциплины рассмотрена и одобрена на заседании Международного дипломатического колледжа «16» февраля 2026 г., протокол №6

Директор Международного
дипломатического колледжа_____/Н.И. Платонова

Согласовано от Библиотеки_____/О. Е. Стёпкина

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

1.1. Область применения рабочей программы дисциплины

Рабочая программа дисциплины «Стандартизация, сертификация и техническое документоведение» является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности 09.02.11 Разработка и управление программным обеспечением.

1.2. Место дисциплины в структуре программы подготовки специалистов среднего звена

Дисциплина «Стандартизация, сертификация и техническое документоведение» является обязательной частью социально-гуманитарного цикла основной профессиональной образовательной программы в соответствии с ФГОС по специальности 09.02.11 Разработка и управление программным обеспечением.

Дисциплина «Стандартизация, сертификация и техническое документоведение» обеспечивает формирование общих компетенций по видам деятельности ФГОС по специальности 09.02.11 Разработка и управление программным обеспечением.

1.3. Цель и планируемые результаты освоения дисциплины

Обучающийся должен освоить следующие общие компетенции:

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности;

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках;

ПК 1.1. Проектировать базы данных;

ПК 1.4. Администрировать базы данных;

ПК 1.5. Защищать информацию в базе данных с использованием технологии защиты информации;

В рамках программы дисциплины обучающимися осваиваются умения и знания:

Код ПК, ОК	Умения	Знания

ОК 01. ОК 02. ОК 09. ПК 1.1 ПК 1.4 ПК 1.5	- распознавать задачу и/или проблему в профессиональном и/или социальном контексте, анализировать и выделять её составные части; - определять этапы решения задачи, составлять план действия, реализовывать составленный план, определять необходимые ресурсы; - выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; - владеть актуальными методами работы в профессиональной и смежных сферах; - оценивать результат и последствия своих действий (самостоятельно или с помощью наставника);	-актуальный профессиональный и социальный контекст, в котором приходится работать и жить; - структура плана для решения задач, алгоритмы выполнения работ в профессиональной и смежных областях; - основные источники информации и ресурсы для решения задач и/или проблем в профессиональном и/или социальном контексте; - методы работы в профессиональной и смежных сферах; - порядок оценки результатов решения задач профессиональной деятельности; − - основные положения теории баз данных, хранилищ данных, баз знаний;

	- определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации; - выделять наиболее значимое в перечне информации, структурировать получаемую информацию, оформлять результаты поиска; - оценивать практическую значимость результатов поиска; - применять средства информационных технологий для решения профессиональных задач; - использовать современное программное обеспечение в профессиональной деятельности; - использовать различные цифровые средства для решения профессиональных задач; - понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; - участвовать в диалогах на знакомые общие и профессиональные темы; - строить простые высказывания о себе и о своей профессиональной деятельности; - кратко обосновывать и объяснять свои действия (текущие и планируемые); - писать простые связные сообщения на знакомые или интересующие профессиональные темы; − анализировать предметную область и выделять основные сущности; − определять требования к базе данных; − разрабатывать концептуальную, логическую и физическую модели баз данных; − проектировать схему базы данных; − работать с современными	− основные принципы структуризации и нормализации базы данных; − основные принципы построения концептуальной, логической и физической модели данных; − методы описания схем баз данных в современных системах управления базами данных; − структуру данных систем управления базами данных, основные понятия и принципы проектирования баз данных; − структуру реляционной базы данных; − язык SQL и особенности его реализации в различных системах управления базами данных; − оптимизацию производительности баз данных принципы безопасности хранения данных; − архитектуру СУБД; − основные принципы администрирования баз данных; − методы мониторинга и оптимизации работы баз данных; − принципы резервного копирования и восстановления баз данных; − методы защиты баз данных от внешних угроз; − особенности работы с различными СУБД; – Язык SQL (Structured Query Language); − управление транзакциями и контроль целостности данных; − управление доступом и безопасностью баз данных; − резервное копирование и восстановление данных; – оптимизацию производительности баз данных; – работу с индексами и оптимизация запросов; – мониторинг и анализ

	casecредствами проектирования баз данных; − определять связи между таблицами; − определять типы данных для полей таблиц; − оформление документации на спроектированную базу данных; − разработки схемы базы данных, используя NoSQL модели данных, такие как документо-ориентированные, ключ-значение, колоночные и др; − установки и настройки СУБД; − создания и удаления баз данных; − восстановления баз данных; − резервного копирования баз данных; − создания пользователей и назначения прав доступа; − оптимизации запросов к базе данных; мониторинга и обслуживания NoSQL баз данных, включая резервное копирование и восстановление данных; − разрабатывать и внедрять системы защиты баз данных от несанкционированного доступа; – разрабатывать и внедрять системы резервного копирования и восстановления баз данных; − проводить аудит безопасности баз данных; − устанавливать и настраивать механизмы аутентификации и авторизации пользователей; – создавать и управлять ролями и правами доступа к данным; − шифровать данные и обеспечивать их конфиденциальность; – контролировать целостность данных и обнаруживать изменения; − использовать механизмы аудита для отслеживания доступа к данным; − использовать механизмы мониторинга	производительности; − принципы работы с реляционными базами данных; принципы работы с нереляционными базами данных; − методы защиты баз данных от несанкционированного доступа; − методы создания и восстановления резервных копий баз данных; – особенности работы с различными типами СУБД; − методы проведения аудита безопасности баз данных; – принципы криптографии и методов шифрования данных; − стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.; − методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных; − методы контроля доступа, включая создание ролей и групп пользователей, управление правами доступа и аудит доступа к данным; − методы обнаружения и предотвращения атак, включая защиту от SQL-инъекций, DoS/DDoS-атак и других угроз безопасности; − методы мониторинга и анализа журналов событий для обнаружения угроз безопасности и анализа производительности базы данных; − методы создания и управления защищенными соединениями с базой данных, включая VPN-туннели и SSLшифрование; − методы создания и управления бэкапами и резервными копиями данных, включая использование инкрементальных и дифференциальных бэкапов; – методы обеспечения безопасности базы данных при использовании облачных сервисов, включая защиту от

	для обнаружения угроз безопасности; − создавать и управлять защищенными соединениями с базой данных; − использовать механизмы защиты от SQL-инъекций и других видов атак; − создавать и управлять бэкапами и резервными копиями данных; − обеспечивать безопасность базы данных при использовании облачных сервисов.	утечки данных и управление доступом к облачным ресурсам; законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы

Вид учебной работы	**Объем часов (очная форма)**
Объем образовательной программы дисциплины	70
в том числе:	
лекции, уроки	22
практические занятия	26
курсовая работа (проект)	-
консультации	-
Самостоятельная работа	16
Промежуточная аттестация в форме дифференцированного зачета	6

2.2. Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов очной формы
1	2	3
Модуль 1. Основные концепции и методы информационной безопасности		**26**
Тема 1.1. Основы ИБ и криптографические методы защиты.	**Содержание учебного материала** Понятие информации, информационной безопасности. CIA-триада (Конфиденциальность, Целостность, Доступность). Классификация угроз и источников угроз. Основные законы РФ в сфере ИБ (152-ФЗ, 187-ФЗ). Стандарты и руководящие документы (ГОСТ Р ИСО/МЭК 27001). Ответственность за нарушение законодательства в области ИБ. Основные угрозы и уязвимости ПО. Принципы работы криптографии: симметричное/асимметричное шифрование (AES, RSA), хэш-функции (SHA), электронная подпись.	4
	Практические занятия Анализ требований законодательства РФ к ПО. Применение криптографических средств (OpenSSL/GnuPG).	6
	Самостоятельная работа обучающихся Работа над учебным материалом, ответы на контрольные вопросы. Систематическая проработка конспектов занятий, учебной и специальной литературы (по вопросам к параграфам, разделам учебных пособий, составленным преподавателем).	2
Тема 1.2. Защита программных систем на уровне ОС и сети.	**Содержание учебного материала** Глубокая классификация: вирусы (файловые, загрузочные), черви (сетевые), троянские программы, шпионское ПО (spyware), программы-вымогатели (ransomware), руткиты. Методы распространения и сокрытия. Жизненный цикл современной кибератаки. Анализ стека TCP/IP с точки зрения уязвимостей: IP-спуфинг, подмена ARP, атаки типа "отказ в обслуживании" (DoS/DDoS) на транспортном и прикладном уровнях, сниффинг трафика.	4
	Практические занятия Исследование отчетов о поведении вредоносного ПО. Настройка базового сетевого экрана (брандмауэра)	4

	Самостоятельная работа обучающихся Работа над учебным материалом, ответы на контрольные вопросы. Систематическая проработка конспектов занятий, учебной и специальной литературы (по вопросам к параграфам, разделам учебных пособий, составленным преподавателем).	6

Модуль 2. Документоведение		**42**
Тема 2.1. Обеспечение безопасности в разработке и управлении ПО и БД	**Содержание учебного материала** Дискреционное управление доступом (DAC). Матрица доступа. Ролевое управление доступом (RBAC). Принцип минимальных привилегий. Иерархия ролей, статические и динамические ограничения. Мандатное управление доступом (MAC). Модели БеллаЛаПадулы (конфиденциальность) и Бибы (целостность). Использование в госсекторе. SQL-инъекция. Механизм возникновения (смешение кода и данных). Процедуры аудита. Прозрачное шифрование данных (TDE) на уровне табличных пространств/файлов. Шифрование на уровне столбцов (CLE). Маскирование данных (Data Masking) для тестовых сред.	6
	Практические занятия Реализация модели ролевого доступа (RBAC) в учебной БД. Защита от SQL-инъекций и настройка прав доступа в СУБД.	8
	Самостоятельная работа обучающихся Работа над учебным материалом, ответы на контрольные вопросы. Систематическая проработка конспектов занятий, учебной и специальной литературы (по вопросам к параграфам, разделам учебных пособий, составленным преподавателем).	4
Тема 2.2 Безопасное программирование и управление уязвимостями.	**Содержание учебного материала** Уязвимости веб-приложений. Принципы безопасного кодирования (Secure Coding). Валидация, санация и экранирование всех входных данных. Принцип "явного разрешения" (whitelisting). Безопасная работа с памятью. Контекстно-зависимое экранирование выходных данных. Работа с базами уязвимостей CVE (Common Vulnerabilities and Exposures) и NVD (National Vulnerability Database). Формат описания CVE (идентификатор, описание, CVSS-метрика). Процесс ответа на инциденты безопасности.	8

	Практические занятия Поиск уязвимостей в коде с использованием средств статического анализа Анализ кода проекта и разработка рекомендаций по безопасности	8
	Самостоятельная работа обучающихся Работа над учебным материалом, ответы на контрольные вопросы. Систематическая проработка конспектов занятий, учебной и специальной литературы (по вопросам к параграфам, разделам учебных пособий, составленным преподавателем).	8
Промежуточная аттестация в виде дифференцированного зачета		**6**
Всего:		**70**

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация дисциплины производится в учебном кабинете, предназначенном для проведения теоретических и практических занятий.

Оборудование учебного кабинета: рабочие места обучающихся; рабочее место преподавателя; технические средства обучения: мультимедийный комплекс (проектор, экран), компьютер, колонки; оборудование: камера видеонаблюдения; доска меловая. Помещение для самостоятельной и воспитательной работы: столы, стулья, ПК обучающихся, программное обеспечение: 1С Предприятие, OnlyOffice (AGPLv3), GIMP (GNU GPL 3), Krita (GNU GPL 3), Inkscape (GNU GPL 3),
SciLab (CeCILL), Kaspersky Endpoint Security, Агент администрирования Kaspersky Security Center, Mozilla Firefox (MPL 2), Apache NetBeans IDE (Apache License 2), Notepadqq (GNU GPL 3), VSCodium (MIT), Mono Development IDE (MIT), PyCharm Community Edition (Apache License 2), Android Studio (Apache License 2), Python (Python Software Foundation License), Java (GNU GPL), Node.js (MIT), Git (GNU GPL 2), GitHub Desktop (No Copyright), UnityHub (Unity Companion License), FreeCAD (LGPL-2.0-or-later), Sweet Home 3D (GNU GPL 2+), draw.io (Apache License 2), DBeaver (Apache License 2), PostgreSQL (License (free and open-source)), MariaDB (GNU GPL), PSPP (GNU GPL 3), Wireshark (GNU GPL 2+),
Imunes (Creative Commons Attribution 4.0 International Public License), VirtualBox (GNU GPL 2), Apache (Apache License 2), Консультант+ (Коммерческая лицензия), OBS (GNU GPL).

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь электронные образовательные и информационные ресурсы, рекомендуемых для использования в образовательном процессе.

Основная учебная литература

1. Шестернинов, Е. Е. Индивидуальный проект. Шаг в профессию. Базовый уровень. Практикум: учебное пособие, разработанное в комплекте с учебником для образовательных организаций, реализующих образовательные программы среднего профессионального образования / Е. Е. Шестернинов. – 2-е изд., стер. - Москва: Просвещение, 2025. - 82 с. – (Учебник СПО). - ISBN 978-5-09-124912-5. - Текст: электронный. - URL: https://znanium.ru/catalog/product/2202038.

2. Козырь, Н. С. Анализ и оценка рисков информационной безопасности: учебник для среднего профессионального образования / Н. С. Козырь, В. Н. Хализев. — Москва: Издательство Юрайт, 2026. — 157 с. — (Профессиональное образование). — ISBN 978-5-
534-20645-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590435.

3. Информационные технологии в юридической деятельности: учебник и практикум для среднего профессионального образования / Т. М. Беляева, А. Т. Кудинов, Н. В. Пальянова, С. Г. Чубукова; ответственный редактор С. Г. Чубукова. — 4-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 338 с. — (Профессиональное образование). — ISBN 978-5-534-18966-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583745.

4. Илюшечкин, В. М. Основы использования и проектирования баз данных: учебник для среднего профессионального образования / В. М. Илюшечкин. — Москва: Издательство Юрайт, 2026. — 213 с. — (Профессиональное образование). — ISBN 978-5-534-01283-5. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/585059.

Дополнительная учебная литература

1. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва: Издательство Юрайт, 2026. — 352 с. — (Профессиональное образование). — ISBN 978-5-534-19384-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587457

2. Компьютерные сети: учебник и практикум для среднего профессионального образования / под научной редакцией А. М. Нечаева, А. Е. Трубина, А. Ю. Анисимова. — Москва: Издательство Юрайт, 2026. — 515 с. — (Профессиональное образование). — ISBN 978-5-534-21453-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590199 3. Внуков, А. А. Основы информационной безопасности: защита информации:
учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587458 4. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва:
Издательство Юрайт, 2026. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588246

Базы данных и/или Интернет-ресурсы

1. 1. https://pravo.gov.ru/ - Официальный интернет-портал правовой информации
2. https://fstec.ru/ - Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России)
3. https://vulnerabilities.securitylab.ru/ - База уязвимостей SecurityLab
4. https://www.ru-cert.ru/ - Национальный центр реагирования на компьютерные инциденты
5. https://www.garant.ru/ - Информационно-правовая система Гарант
6. https://www.consultant.ru/ - Справочная правовая система «КонсультантПлюс»

Официальные, справочно-библиографические и периодические издания

1. Информационные технологии и вычислительные системы: научный журнал / гл.
ред. Попков Ю.С.; учред. ФГУ «Федеральный исследовательский центр «Информатика и управление» РАН». - М., 2026

2. Экономика и математические методы: журнал / гл. ред. В.Л. Макаров / Российская Академия наук, Центральный экономико-математический институт, Институт проблем рынка - Российская академия наук, Москва, 2026

3. Экономический журнал Высшей школы экономики / Higher School of Economics Economic Journal: журнал / гл. ред. Е.Е. Гавриленков / Национальный исследовательский университет «Высшая школа экономики» - Издательский дом Высшей школы экономики, Москва, 2026

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Методы оценки
Перечень знаний, осваиваемых в рамках дисциплины		

-актуальный профессиональный и социальный контекст работы в сфере ИТ и ИБ, включая понимание современного ландшафта киберугроз. -структура и алгоритмы решения профессиональных задач в области защиты информации при разработке и управлении ПО. -основные источники информации и ресурсы для решения профессиональных задач; -методы работы в сфере информационной безопасности и смежных областях (администрирование, разработка). -порядок и критерии оценки результатов решения задач профессиональной деятельности; -основные принципы информационной безопасности: конфиденциальность, целостность, доступность (CIA-триада), аутентичность, неотказуемость; -принципы и методы криптографии: симметричное и асимметричное шифрование (AES, RSA), хэш-функции (SHA), электронная цифровая подпись; -стандарты и протоколы безопасности: SSL/TLS для защищенной передачи данных, принципы работы VPN, основы Kerberos; -законодательство и стандарты в области ИБ: Федеральные законы №152-ФЗ и №187-ФЗ, международные стандарты (ГОСТ Р ИСО/МЭК 27001, PCI	Ответы на вопросы на знание и понимание: 85 - 100% правильных ответов – «отлично» 69-84% правильных ответов – «хорошо» 51-68% правильных ответов – «удовлетворительно» 50% и менее – «неудовлетворительно»	Устный опрос. Тестирование по темам дисциплины. Практические занятия. Практические занятия по заполнению документов.

DSS, GDPR);		

-основные положения теории баз данных. -архитектура СУБД и принципы работы с реляционными базами данных. -основные понятия и принципы проектирования баз данных; -структура реляционной базы данных (таблицы, связи, ключи); -основные принципы структуризации и нормализации базы данных; -принципы построения концептуальной, логической и физической модели данных; -методы описания схем баз данных в современных СУБД. -язык SQL и особенности его реализации в различных СУБД; -управление транзакциями и контроль целостности данных. -принципы и методы оптимизации производительности баз данных: работа с индексами, оптимизация SQL-запросов. -методы мониторинга и анализа производительности СУБД. -основные принципы администрирования баз данных; -принципы и методы резервного копирования и восстановления баз данных); -особенности работы с различными типами и конкретными СУБД; -принципы безопасности хранения данных; -методы аутентификации и авторизации пользователей:		

механизмы на основе паролей, сертификатов, интеграция с системными аккаунтами; - язык SQL для управления безопасностью; -методы защиты баз данных от внешних угроз и		

несанкционированного доступа; -методы обнаружения и предотвращения атак, в частности, защита от SQLинъекций; -методы проведения аудита безопасности баз данных; -методы контроля и аудита доступа к данным: мониторинг и анализ журналов событий (логов) СУБД для обнаружения подозрительной активности и анализа действий пользователей; -методы создания и управления защищенными соединениями с БД, включая использование SSL/TLS для шифрования трафика между клиентом и сервером БД; -принципы криптографии и методы шифрования данных в БД: прозрачное шифрование, шифрование на уровне столбцов.		
Перечень умений, осваиваемых в рамках дисциплины		

-распознавать и анализировать задачи информационной безопасности в контексте разработки и эксплуатации ПО, выделять их составные части; -определять этапы решения задач ИБ, составлять план действий и реализовывать его, определяя необходимые ресурсы; выявлять и эффективно осуществлять поиск информации, необходимой для решения задач ИБ, используя специализированные источники; -владеть актуальными методами работы в сфере ИБ применительно к разработке ПО; -оценивать результат и последствия своих действий по настройке безопасности;	Ответы на вопросы на знание и понимание: выполнено полностью, без критических ошибок, обоснования корректны, оформление соответствует требованиям– «отлично» выполнено в целом верно, есть 1–2 некритичные ошибки или недочёта в оформлении – «хорошо» выполнено частично, есть ошибки в логике или оформлении, требуется доработка по замечаниям – «удовлетворительно» задание не выполнено или содержит существенные ошибки, отсутствуют ключевые элементы – «неудовлетворительно»	Проверка выполнения практических работ по темам модуля. Оценка оформленных документов по чеклисту качества. Защита практической работы и ответы на уточняющие вопросы. Проверка самостоятельной работы и мини-отчётов по источникам.

-применять средства информационных технологий для решения профессиональных задач в области ИБ; -использовать современное программное обеспечение в профессиональной деятельности. -использовать различные цифровые средства для решения задач обеспечения безопасности; понимать общий смысл технической документации, сообщений об ошибках и статей по основам информационной безопасности на английском языке; -участвовать в диалогах на знакомые профессиональные темы, связанные с безопасностью ПО и БД, используя базовую профессиональную лексику. -строить простые высказывания о своей профессиональной деятельности в области ИБ; -кратко обосновывать и объяснять свои действия по настройке параметров безопасности или выбору методов защиты; -писать простые связные сообщения на профессиональные темы; - определять требования к безопасности базы данных на этапе анализа предметной области. -проектировать схему базы данных с учетом требований целостности и безопасности. устанавливать и настраивать		

СУБД с учетом базовых требований безопасности; - создавать и удалять базы данных.; -разрабатывать и внедрять базовые системы защиты БД от		

несанкционированного доступа; -устанавливать и настраивать механизмы аутентификации и авторизации пользователей в СУБД; -создавать и управлять ролями и правами доступа к данным, таблицам и процедурам. - применять базовые методы шифрования данных; -использовать механизмы аудита СУБД для отслеживания доступа к данным и фиксации подозрительных событий; -использовать механизмы мониторинга для обнаружения аномальной активности, указывающей на потенциальные угрозы безопасности; -создавать и управлять защищенными соединениями с базой данных		

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения по учебной дисциплине

Темы для подготовки к промежуточной аттестации

1. Основные понятия информационной безопасности. Триада CIA (конфиденциальность, целостность, доступность). Дополнительные свойства (аутентичность, неотказуемость). Классификация угроз и уязвимостей.
2. Нормативно-правовое регулирование в области ИБ в РФ. Федеральный закон №152ФЗ «О персональных данных»: основные принципы и требования. Федеральный закон №187-ФЗ «О безопасности КИИ»: ключевые понятия.
3. Основы криптографии. Симметричное и асимметричное шифрование: принципы работы, области применения, примеры алгоритмов (AES, RSA). Криптографические хэш-функции: свойства и применение (целостность, хранение паролей).
4. Вредоносное программное обеспечение (Malware). Классификация (вирусы, черви, трояны, ransomware). Основные каналы распространения и методы защиты на уровне пользователя и организации.
5. Основы сетевой безопасности. Базовые сетевые угрозы: спуфинг, сниффинг, DoS/DDoS-атаки. Назначение и принципы работы межсетевых экранов (firewall). Понятие VPN.
6. Модели управления доступом. Дискреционная (DAC), ролевая (RBAC) и мандатная (MAC) модели доступа. Сравнительный анализ, достоинства и недостатки. Принцип минимальных привилегий.
7. Основные угрозы безопасности баз данных. SQL-инъекция: механизм, виды, последствия. Общие методы защиты от несанкционированного доступа к данным.
8. Администрирование безопасности в СУБД. Задачи администратора БД по обеспечению безопасности. Управление пользователями, ролями и привилегиями. Понятие аудита (логирования) событий безопасности.
9. Технологии защиты данных в базах данных. Шифрование данных: прозрачное (TDE) и на уровне столбцов. Маскирование и анонимизация данных. Резервное копирование как элемент обеспечения доступности.
10. Безопасное программирование (Secure Coding). Обзор OWASP Top 10 (на примере SQLi, XSS, уязвимых компонентов). Основные принципы: валидация входных данных, экранирование выходных данных, использование параметризованных запросов.
11. Инструменты анализа защищенности ПО. Статический (SAST) и динамический (DAST) анализ: цели, принципы работы, отличия. Назначение баз уязвимостей (CVE/NVD) в процессе разработки.
12. Обеспечение безопасности в облачных средах. Модель общей ответственности (Shared Responsibility Model) в облачных сервисах. Ключевые аспекты безопасности баз данных, развернутых в облаке.
13. Эволюция понятия «информационная безопасность»: от защиты данных к кибербезопасности и управлению рисками.
14. Атаки на конфиденциальность: методы перехвата информации (сниффинг, социальная инженерия, утечки данных).

15. Атаки на целостность: способы несанкционированного изменения данных (подмена, манипуляция пакетами, атаки «человек посередине»).
16. Атаки на доступность: отказ в обслуживании (DoS/DDoS) – виды, принципы работы, цели атакующих.
17. Уязвимости нулевого дня (Zero-day): определение, жизненный цикл, экономика и значение для безопасности ПО.
18. Стандарт PCI DSS: основные требования к безопасности данных держателей платежных карт.
19. Концепция «Защита в глубину» (Defense in Depth): принципы многоуровневой защиты информационной системы.
20. Криптостойкость: факторы, влияющие на стойкость шифрования, понятие о полном переборе и атаках по сторонним каналам.
21. Цифровая подпись и инфраструктура открытых ключей (PKI): принципы работы, составные части PKI (удостоверяющий центр, регистрационный центр).
22. Протокол SSL/TLS: назначение, этапы рукопожатия (handshake), значение сертификатов для аутентификации сервера.
23. Принципы работы сетевых сканеров (Nmap) и анализаторов трафика (Wireshark) с точки зрения безопасности.
24. Классификация межсетевых экранов (брандмауэров): эволюция от packet filter до UTM и NGFW.
25. Принципы обнаружения и предотвращения вторжений (IDS/IPS): сравнение сигнатурного и аномального анализа.
26. Модель киберубийства (Cyber Kill Chain) Lockheed Martin: этапы целенаправленной атаки и точки противодействия.
27. Социальная инженерия: основные техники (фишинг, претекстинг, вишинг), цели и методы защиты.
28. Принцип безопасных настроек по умолчанию (Secure by Default) для ПО и СУБД.
29. Жизненный цикл разработки защищённого ПО (Secure SDLC): основные этапы и внедрение практик безопасности на каждом из них.
30. Статический анализ безопасности приложений (SAST): методология, типы обнаруживаемых дефектов, преимущества и ограничения.
31. Динамический анализ безопасности приложений (DAST): методология «серого ящика», примеры инструментов.
32. OWASP Top 10 2021: подробный разбор уязвимостей «Небезопасная десериализация» и «Недостатки журналирования и мониторинга».
33. Аутентификация: многофакторная аутентификация (MFA), биометрия, основанные на рисках системы.
34. Управление сессиями: безопасные методы генерации, хранения и инвалидации идентификаторов сессий.
35. Контроль доступа на уровне функций и данных в веб-приложениях.
36. Безопасная обработка ошибок и исключений: почему сообщения об ошибках не должны раскрывать внутреннюю структуру системы.
37. Безопасная загрузка файлов: основные риски (подмена, XSS, RCE) и методы защиты.
38. Реляционная модель данных с точки зрения безопасности: как структура таблиц и связей влияет на политики доступа.

39. Встроенные механизмы безопасности в СУБД (на примере PostgreSQL/MySQL): объекты безопасности (роли, профили, политики).
40. Инъекции NoSQL: принцип работы, отличия от SQLi, методы предотвращения.
41. Шифрование «на лету» (Transparent Data Encryption – TDE): архитектура, защищаемые данные, влияние на производительность.
42. Маскирование данных.
43. Журналирование (аудит) в СУБД.
44. Модель общей ответственности в облаках: разграничение обязанностей по безопасности между провайдером и клиентом.
45. Концепция «Непрерывная безопасность» (DevSecOps): интеграция практик и инструментов безопасности в процесс непрерывной интеграции и поставки (CI/CD), автоматизация проверок безопасности.
46. Управление секретами (Secrets Management) в разработке: безопасное хранение и использование паролей, ключей API, токенов доступа в средах разработки, тестирования и производства (на примере HashiCorp Vault, AWS Secrets Manager).
47. Контейнеризация и безопасность.
48. Управление идентификацией и доступом (IAM) в распределенных системах и микросервисных архитектурах: вызовы централизованной аутентификации, использование токенов (JWT), сервис-аккаунтов.
49. Юридические и этические аспекты тестирования на проникновение: понятие «разрешенного взлома», правила взаимодействия, оформление договоров и отчетности.
50. Обеспечение безопасности API (Application Programming Interface).

Темы для самостоятельной работы обучающихся

1. Сравнительный анализ моделей информационной безопасности: триада CIA, модель Паркера (шесть элементов), модель DIE.
2. Методологии моделирования угроз (Threat Modeling): STRIDE, PASTA, OCTAVE. Сравнение областей применения.
3. Принципы и этапы процесса управления рисками информационной безопасности: идентификация, оценка, обработка, мониторинг.
4. Классификация и анализ современных социально-инженерных атак: целевой фишинг (spear phishing), бизнес-компрометация email (BEC), принципы защиты.
5. Теоретические основы атак типа «отказ в обслуживании» (DoS/DDoS): классификация по уровням OSI, механизмы усиления (amplification), стратегии смягчения.
6. Понятие «Атакующая поверхность» (Attack Surface): методы анализа и сокращения для веб-приложения.
7. Эволюция и сравнительный анализ алгоритмов симметричного шифрования: от DES к AES и современным режимам работы (GCM, XTS).
8. Криптографические протоколы для безопасного удаленного доступа: сравнительный анализ SSH и TLS с точки зрения архитектуры и применения.
9. Теоретические основы криптографии на эллиптических кривых (ECC): преимущества перед RSA, области применения.

10. Принципы работы и архитектура инфраструктуры открытых ключей (PKI): роль корневых и промежуточных центров сертификации, жизненный цикл сертификата.
11. Квантовые вычисления и их потенциальное влияние на современную криптографию (криптоапокалипсис). Постквантовая криптография: основные направления.
12. Принципы архитектуры Zero Trust (Нулевого доверия): основные постулаты, отличия от периметровой модели, ключевые компоненты.
13. Модели зрелости безопасной разработки (BSIMM, OpenSAMM): сравнительный анализ и принципы использования для оценки процессов.
14. Теоретические основы статического (SAST) и динамического (DAST) анализа безопасности кода: внутренние механизмы, виды обнаруживаемых паттернов уязвимостей.
15. Формальные методы верификации программного обеспечения: теория и применение для обеспечения безопасности критических систем.
16. Уязвимости цепочки поставок программного обеспечения (Software Supply Chain): типы атак (компрометация зависимостей, злонамеренные коммиты), принципы защиты (SBOM).
17. Мандатные модели контроля доступа: детальный разбор моделей Белла-ЛаПадулы (конфиденциальность) и Бибы (целостность), их применение в СУБД.
18. Теоретические основы гомоморфного шифрования: принципы работы, потенциальные применения для защиты данных в облаке и БД.
19. Концепции и методы обеспечения конфиденциальности данных: анонимизация, псевдонимизация, дифференциальная приватность (differential privacy).
20. Архитектура и принципы работы систем управления секретами (Secrets Management) в DevOps-средах.
21. Внутренние механизмы транзакций в СУБД (ACID) с точки зрения обеспечения целостности данных и их взаимосвязь с журналами транзакций (WAL).
22. Архитектура и принципы работы систем обнаружения и предотвращения вторжений (IDS/IPS) на основе сигнатур и аномального поведения.
23. Теоретические основы сегментации сети (Network Segmentation) и микросегментации: цели, методы реализации, влияние на безопасность.
24. Стандарты и протоколы безопасной маршрутизации: анализ уязвимостей протоколов (например, BGP) и методов их защиты (RPKI).
25. Фазы жизненного цикла обработки инцидента информационной безопасности (NIST SP 800-61): подготовка, обнаружение, анализ, сдерживание, ликвидация, восстановление, извлечение уроков.
26. Сравнительный анализ международных стандартов информационной безопасности: ISO/IEC 27001, NIST Cybersecurity Framework, CIS Controls.
27. Регуляторные требования к защите персональных данных: сравнительный анализ GDPR (ЕС) и 152-ФЗ (РФ).
28. Этические кодексы и принципы в сфере информационной безопасности и хакерской этики.
29. Теоретические основы безопасности интернета вещей (IoT): специфические угрозы, архитектурные уязвимости, подходы к защите.
30. Современные тренды и будущее ИБ: влияние искусственного интеллекта (AI) и машинного обучения (ML) на кибербезопасность (как для защиты, так и для атак).

Примерные варианты тестовых оценочных заданий (ТОЗ) для контрольного рубежа в рамках текущего контроля

Тестовое задание	Оцениваемые компетенции
ВОПРОСЫ ОТКРЫТОГО ТИПА	
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Совокупность правовых, организационных и технических мер, направленных на защиту информации от угроз, называется информационной _____. +: безопасностью	ПК 1.5.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Ключевой принцип обработки персональных данных, означающий, что оператор должен собирать только те данные, которые необходимы для заявленной цели, называется _____. +: ограничение обработки персональных данных	ОК 09.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Свойство информации, означающее, что она не должна быть изменена или уничтожена несанкционированно, — это _____. +: целостность	ОК 01.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Свойство безопасности, гарантирующее, что система или ресурсы доступны для использования авторизованными пользователями в любой момент времени, — это _____. +: доступность	ПК 1.4.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Криптографический алгоритм, использующий один и тот же ключ для шифрования и дешифрования, называется _____ шифрованием +: симметричным	ПК 1.5.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Стандарт шифрования, принятый в 2001 году как преемник DES, называется _____ +: Advanced Encryption Standard	ОК 02.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Модель управления доступом, где права назначаются не пользователям напрямую, а ролям, которые они занимают, называется _____. +: ролевым доступом	ПК 1.4.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Принцип информационной безопасности, согласно которому пользователь должен обладать минимальным набором привилегий, необходимым для выполнения своей работы, называется принципом _____. +: минимальных привилегий	ПК 1.5.

(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Одна из самых распространенных и опасных уязвимостей вебприложений, позволяющая внедрить произвольный SQL-код в запрос к базе данных, называется _____. +: SQL-инъекция	ПК 1.1.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Тип вредоносного программного обеспечения, которое блокирует доступ к данным или системе и требует выкуп за его восстановление, называется _____. +: программой-вымогателем	ОК 01.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Атака, целью которой является полное исчерпание ресурсов системы (канала связи, процессора, памяти) и приведение к отказу в обслуживании, называется _____ +: отказ в обслуживании	ОК 01.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Язык SQL, используемый для назначения и отзыва прав доступа пользователей и ролей к объектам базы данных, называется языком управления _____ +: доступом	ПК 1.4.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Процесс регулярного копирования данных для возможности их восстановления в случае утери или повреждения называется _____. +: резервное копирование	ПК 1.4.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ)	ПК 1.5.

Технология шифрования, при которой данные на диске (табличном пространстве, файлах данных) шифруются и дешифруются автоматически, прозрачно для приложения, называется _____ шифрованием +: прозрачным	
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Запись действий пользователей и системы в специальный журнал для последующего анализа и расследования инцидентов в СУБД называется _____ +: аудит	ПК 1.5.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Протокол, обеспечивающий защищенную передачу данных по сетям TCP/IP, на основе которого работает HTTPS, — это _____. +: TLS	ОК 09.

(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Программный или аппаратный барьер, контролирующий сетевой трафик между сегментами сети на основе заданных правил, называется _____. +: межсетевой экран	ОК 02.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Международный стандарт, описывающий требования к системе менеджмента информационной безопасности, — это _____. +: ГОСТ Р ИСО/МЭК 27001	ОК 09.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Процесс подтверждения подлинности пользователя или системы (например, с помощью логина и пароля) называется _____. +: аутентификация	ОК 01.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Общепризнанная база данных для публикации информации об уязвимостях программного обеспечения использует идентификаторы формата _____. +: CVE	ОК 02.
(ВПИСАТЬ ПРАВИЛЬНЫЙ ОТВЕТ) Процесс проверки исходного кода программы на наличие уязвимостей без его выполнения называется _____ анализом +: статическим	ПК 1.1.
ВОПРОСЫ ЗАКРЫТОГО ТИПА	
Какой федеральный закон Российской Федерации является основным, регулирующим обработку персональных данных операторами? -: 149-ФЗ «Об информации, информационных технологиях и о защите информации» +: 152-ФЗ «О персональных данных» -: 187-ФЗ «О безопасности критической информационной инфраструктуры» -: 98-ФЗ «О коммерческой тайне»	ОК 09.
Какой класс вредоносного программного обеспечения характеризуется способностью к саморепликации и распространению по сети без участия пользователя, эксплуатируя уязвимости в программном обеспечении?	ОК 01.

-: Вирус -: Троянская программа +: Сетевой червь -: Руткит	

Какая модель управления доступом предполагает, что права доступа к объекту назначаются его владельцем? -: Ролевая (RBAC) +: Дискреционная (DAC) -: Мандатная (MAC) -: Атрибутная (ABAC)	ПК 1.4.
Какой стандарт (алгоритм) является текущим мировым стандартом симметричного шифрования, рекомендованным для защиты конфиденциальной информации? -: DES (Data Encryption Standard) -: 3DES (Triple DES) -: RC4 (Rivest Cipher 4) +: AES (Advanced Encryption Standard)	ОК 02.
Что из перечисленного является ПРАВИЛЬНОЙ последовательностью этапов классического процесса управления рисками информационной безопасности? -: Обработка -> Идентификация -> Оценка -> Мониторинг +: Идентификация -> Оценка -> Обработка -> Мониторинг -: Оценка -> Мониторинг -> Идентификация -> Обработка -: Мониторинг -> Обработка -> Оценка -> Идентификация	ОК 01.
Основной целью какой фазы атаки по модели Cyber Kill Chain является закрепление злоумышленника в системе для длительного присутствия и достижения конечных целей? -: Разведка (Reconnaissance) -: Установка бэкдора (Installation) +: Закрепление (Establishment of Foothold) -: Выполнение целей (Actions on Objectives)	ОК 01.
Какой из перечисленных методов является НАИБОЛЕЕ эффективным для предотвращения атак типа SQL-инъекция на уровне прикладного кода? -: Валидация ввода на стороне клиента (в браузере) -: Экранирование специальных символов (например, кавычек) +: Использование параметризованных запросов (Prepared Statements) -: Частая смена паролей учетных записей БД	ПК 1.5.
Что из перечисленного является основной задачей системы DLP (Data Loss Prevention)? (ОК 01) -: Защита от сетевых атак типа DoS +: Предотвращение утечки конфиденциальной информации за пределы организации -: Шифрование данных на жестких дисках -: Обнаружение сетевых вторжений	ОК 01.

В рамках модели общей ответственности (Shared Responsibility Model) при использовании облачной услуги PaaS (Platform as a Service) за безопасность какой из перечисленных компонентов ОТВЕЧАЕТ КЛИЕНТ, а не провайдер? -: Физическая безопасность дата-центра -: Безопасность операционной системы и патчи для неё -: Безопасность сетевой инфраструктуры (маршрутизаторы, фаерволы)	ПК 1.5.
+: Безопасность прикладного кода и настройка прав доступа пользователей в приложении	

Шкала оценивания тестовых заданий

Данный вид контроля, рассчитан на выявление уровня усвоения теоретического и практического материала в рамках изучения дисциплин. Критерии оценивания теста: 1 вопрос = 1 балл.

Оценка «5»	30-27 Баллов
Оценка «4»	26-23 Баллов
Оценка «3»	22-18 Баллов
Оценка «2»	0-17 Баллов

ЛИСТ АКТУАЛИЗАЦИИ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Методические рекомендации при подготовке к теоретическим занятиям

Основными видами аудиторной работы обучающихся являются лекции.

В ходе теоретических занятий преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации и указания на самостоятельную работу.

В ходе теоретических занятий необходимо вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Контроль ведения конспекта лекций

1. Конспект лекций обучающегося должен вестись в отдельной тетради с количеством страниц, рекомендованном ведущим лектором. На обороте титульного листа тетрадь с конспектом лекций должна содержать подписи:

- фамилия и инициалы обучающегося;
- номер группы;
- ФИО ведущих учебный предмет преподавателей.

2. В начале каждой лекции обучающийся должен записать тему и перечень рассматриваемых вопросов, а также перечень рекомендуемой литературы (при условии, что они оговариваются лектором).

3. При записи содержания лекции следует применять минимум сокращений, желательно общеупотребимых. Обучающимся может быть разработана своя система сокращений, с выносом ее в конце конспекта для пояснения.

4. Табличный, графический, цифровой материал должен быть точно перенесен в конспект с доски (проектора) без искажений динамики зависимостей и обозначений формул, а также значений результатов расчетов.

5. Тетрадь с конспектом должна содержать полный объем прочитанного материала лекций по их количеству и полноте изложения, включая материал для самостоятельного изучения и конспектирования.

Записи должны быть сделаны аккуратным почерком, разборчиво.

Методические рекомендации при проведении практических занятий

Практические занятия необходимы для закрепления изученного теоретического материала, контроля преподавателем степени подготовленности обучающихся по изучаемым учебным предметом, дисциплине или профессиональному модулю.

Перед практическим занятием следует изучить конспект лекции и рекомендованную преподавателем литературу, обращая внимание на практическое применение теории и на методику решения типовых задач. Логическая связь теоретических и практических занятий заключается в том, что информация, полученная на теоретических занятиях, в процессе самостоятельной работы на практическом занятии осмысливается и перерабатывается, при помощи преподавателя анализируется, после чего усваивается.

Методические рекомендации обучающимся для самостоятельной работы

Самостоятельная работа - это планируемая работа обучающихся, выполняемая по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Самостоятельная работа выполняет ряд функций, среди которых особенно выделяются:

- ✓ развивающая (повышение культуры умственного труда, приобщение к творческим видам деятельности, обогащение интеллектуальных способностей, обучающихся);
- ✓ ориентирующая и стимулирующая (процессу обучения придается ускорение и мотивация);
- ✓ воспитательная (формируются и развиваются профессиональные качества специалиста);
- ✓ исследовательская (новый уровень профессионально-творческого мышления);
- ✓ информационно-обучающая (учебная деятельность обучающихся на аудиторных занятиях).

Целью самостоятельных занятий является самостоятельное более глубокое изучение обучающимися отдельных вопросов курса с использованием рекомендуемой дополнительной литературы и других информационных источников.

Задачами самостоятельной работы обучающихся являются:

- ✓ систематизация и закрепление полученных теоретических знаний и практических умений, обучающихся;
- ✓ углубление и расширение теоретических знаний;
- ✓ формирование умения использовать справочную литературу;
- ✓ развитие познавательных способностей и активности обучающихся:

творческой инициативы, самостоятельности, ответственности и организованности;

Внеаудиторная самостоятельная работа включает такие формы работы, как:

Индивидуальные занятия (домашние занятия):

- ✓ изучение программного материала дисциплины (работа с учебником и конспектом лекции);
- ✓ изучение рекомендуемых литературных источников;
- ✓ конспектирование источников;
- ✓ выполнение контрольных работ;
- ✓ работа со словарями и справочниками;

- ✓ использование аудио- и видеозаписи;
- ✓ работа с электронными информационными ресурсами и ресурсами Internet;
- ✓ составление плана и тезисов ответа на лекции;
- ✓ составление схем, таблиц, для систематизации учебного материала;
- ✓ выполнение тестовых заданий;
- ✓ решение задач;
- ✓ подготовка презентаций;
- ✓ ответы на контрольные вопросы;
- ✓ аннотирование, реферирование, рецензирование текста;
- ✓ написание эссе, тезисов, докладов, рефератов;
- ✓ составление глоссария, кроссворда по темам дисциплины; ✓ работа с компьютерными программами;
- ✓ подготовка к дифференцированному зачету.

Групповая самостоятельная работа обучающихся:

- ✓ подготовка к занятиям, проводимым с использованием активных форм обучения (круглые столы, деловые игры);
- ✓ анализ деловых ситуаций (мини-кейсов) и др; ✓ участие в Интернет - конференциях.

Получение консультаций для разъяснений по вопросам изучаемого учебного предмета.

Но наиболее часто при изучении учебного предмета используются следующие виды самостоятельной работы обучающихся:

- ✓ поиск (подбор) литературы (в том числе электронных источников информации) по заданной теме; ✓
- подготовка рефератов; ✓
- подготовка докладов.

Реферат - форма письменной работы. Как правило, реферат является самостоятельным библиографическим исследованием обучающегося, носящим описательно-аналитический характер. Объем реферата может достигать 10-15 страниц. Подготовка реферата подразумевает самостоятельное изучение обучающимся нескольких литературных источников (монографий, научных статей и т.д.) по теме, не рассматриваемой подробно на лекции, систематизацию материала и краткое его изложение. Цель написания реферата - привитие навыков краткого и лаконичного представления собранных материалов и фактов в соответствии с требованиями, предъявляемыми к научным отчетам, обзорам и статьям.

Работа обучающегося над рефератом включает следующие операции:

- ✓ уяснение сути темы (по её названию);
- ✓ выявление литературных источников по данной теме;
- ✓ ознакомление с содержанием источников, направленным на осмысление его внешней и внутренней структуры;
- ✓ работа над выделением главных смысловых компонентов текста (ключевых слов и предложений);
- ✓ отбор наиболее важных сведений из выделенных фрагментов;
- ✓ составление «связок» из отобранного материала в соответствии с логикой изложения фактов;
- ✓ написание реферата.

✓ Реферат в структурном отношении должен включать:

✓ заголовочную часть (введение);

✓ собственно, реферативную часть (изложение основных положений по плану с соответствующими названиями и нумерацией);

✓ заключительную часть (выводы);

✓ справочную часть (список использованной литературы); ✓ оглавление (содержание).

Текст реферата должен иметь связанное, цельное построение. Содержание реферата должна пронизывать главная идея, которая объединяет все информационные элементы источников, а также приводимые факты. При этом допускается сохранение отдельных структурных элементов оригинала. Однако не допустимо простое переписывание положение литературных источников. Язык должен быть кратким, ясным, доступным.

Оформление реферата должно быть выполнено машинописным способом в соответствии со следующими требованиями: **печатный шрифт** – Times New Roman, кегль (размер) 14; **листы бумаги** – формата А4, все страницы должны быть пронумерованы, с размером полей по 2 см; **междустрочный интервал** – полуторный; **абзац –** с отступом первой строки 1,25 см; **текст –** должен быть **выровнен по ширине** и **структурирован** по главам (разделам, параграфам), сопровождаться ссылками на источники при использовании прямых (в кавычках) цитат и фрагментов опубликованных текстов, т.е. на такое использование источников должно быть явным образом указано в сносках или за текстовом списке литературы в соответствии с требованиями ГОСТа.

Реферат оценивается исходя из следующих критериев:

✓ поставлена ли цель в работе;

✓ сумел ли обучающийся самостоятельно составить логический план к теме и реализовать его;

✓ каков научный уровень реферата;

✓ собран ли достаточный фактический материал;

✓ удалось ли раскрыть тему;

✓ показана ли связь рассматриваемой темы с современными проблемами науки и общества, со специальностью обучающегося;

✓ каков авторский вклад в систематизацию, структурирование материала, в составлении заключения;

✓ достигнута ли цель работы.

Тематика рефератов приводится в рамках тем лекционных занятий. Возможно написание реферата по теме, предложенной самим обучающимся (по согласованию с преподавателем). Реферат на занятиях (научно-практических конференциях) может быть представлен в виде доклада.

Реферат должен быть выполнен за один месяц до начала экзаменационной сессии. Обучающиеся, не представившие в установленный срок реферат, либо получившие оценку «неудовлетворительно», к сдаче экзамена не допускаются.

Углубленному изучению материала по отдельным разделам учебного предмета способствует подготовка обучающимися докладов. Доклад - это самостоятельная работа, анализирующая и обобщающая публикации по заданной тематике, предполагающая выработку и обоснование собственной позиции автора в отношении рассматриваемых вопросов. Подготовка доклада - достаточно кропотливый труд. Его написанию

предшествует изучение широкого круга экономических первоисточников, монографий, статей, обобщение личных наблюдений. Работа над докладом способствует развитию самостоятельного, творческого мышления, учит применять экономические знания на практике при анализе актуальных социальных и правовых проблем. Рекомендуемое время доклада - 10-12 минут.

Непременным условием закрепления теоретических и практических знаний, обучающихся является выполнение ими домашних заданий. Одним из основных видов деятельности обучающегося является самостоятельная работа, которая включает в себя изучение лекционного материала, учебников и учебных пособий, первоисточников, подготовку сообщений, выступления на групповых занятиях, выполнение заданий преподавателя.

Методические рекомендации обучающимся по изучению рекомендованной литературы

Самостоятельная работа обучающихся включает в себя выполнение различного рода заданий, которые ориентированы на более глубокое усвоение материала изучаемого учебного предмета. По каждой теме учебного предмета обучающимся предлагается перечень заданий для самостоятельной работы.

К выполнению заданий для самостоятельной работы предъявляются следующие требования: задания должны исполняться самостоятельно и представляться в установленный срок, а также соответствовать установленным требованиям по оформлению.

Обучающимся следует:

- выполнять все плановые задания, выдаваемые преподавателем для самостоятельного выполнения, и разбирать на консультациях неясные вопросы;

- при подготовке к экзамену параллельно прорабатывать соответствующие теоретические и практические разделы учебного предмета, фиксируя неясные моменты для их обсуждения на плановой консультации.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации обучающиеся могут воспользоваться электронной библиотекой ВУЗа, расположенной по электронному адресу https://e.muiv.ru/local/library/index.php, где они имеют возможность получить доступ к учебно-методическим материалам как библиотеки ВУЗа, так и иных электронных библиотечных систем. В свою очередь, обучающиеся могут взять на дом необходимую литературу на абонементе в библиотеке, а также воспользоваться читальным залом.

Методические рекомендации по балльно-рейтинговой системе учета и оценки достижений обучающихся

Общие положения

- Балльно-рейтинговая система учета и оценки достижений, обучающихся (далее – БРС) в Частном образовательном учреждении высшего образования «Московский университет имени А. С. Грибоедова» (далее - Университет) предназначена для решения следующих задач:

- стимулирования обучающихся к регулярной учебной и внеучебной деятельности;

- организации непрерывного контроля освоения обучающимися элементов основных профессиональных образовательных программ среднего профессионального образования;

- комплексной оценки результативности учебной и внеучебной деятельности обучающихся в течение семестра;

- создания для преподавателей, руководства факультетов и кафедр надежного инструментария для осуществления систематического и регулярного контроля за учебной и внеучебной деятельностью обучающихся.

БРС является обязательной для всех участников образовательного процесса и реализуется в электронной информационно-образовательной среде «Электронный университет» (далее – ЭИОС) для всех форм и технологий обучения.

БРС обеспечивает рейтинговый учет и оценку достижений обучающегося за семестр и включает в себя учебный (далее – Rуд) и внеучебный (далее – Rвр) рейтинги.

Учебный рейтинг обучающихся

Перечень дисциплин к изучению в семестре Вы можете увидеть в Личном кабинете в ЭИОС «Электронный Университет» (далее Личный кабинет). Чтобы попасть в Личный кабинет, Вам нужно перейти по ссылке https://impe.lms.mirapolis.ru/mira/ и ввести свой логин и пароль, выданный при поступлении в Университет.

Ваш учебный рейтинг по дисциплине будет формироваться на основе результатов выполнения следующих мероприятий:

- прохождение рубежного контроля (тестирования) по результатам изучения каждого модуля (раздела) дисциплины;

- выполнение рейтинговой работы (домашней творческой работы, расчетноаналитического задания, реферата, контрольной работы, группового проекта) при ее наличии.

Доступ к тестовым заданиям по всем модулям изучаемых дисциплин (рубежному контролю) обеспечивается с начала семестра, однако проходить тестирование необходимо только по окончании изучения каждого модуля (раздела) дисциплины.

Рейтинговая работа должна быть выполнена и передана на проверку преподавателю не позднее, чем за 2 недели до начала экзаменационной сессии через Личный кабинет. Выполнение обучающимся рейтинговой работы допускается не более одного раза в течение установленного календарным учебным графиком периода. Представленная на проверку работа исправлению не подлежит.

При возникновении вопросов по процедуре тестирования, некорректного отображения контента, иных вопросов, связанных с технической поддержкой системы тестирования, обращайтесь в Центр поддержки.

Для прохождения тестирования Вам предоставляются две попытки с ограничением по времени (45 минут). Выполнение тестирования допускается не более 2-ух раз в течение установленного календарным учебным графиком периода. Как итоговый учитывается Ваш лучший результат из двух попыток.

Допуск обучающегося к промежуточной аттестации осуществляется с любым количеством баллов, набранных в ходе выполнения Рейтинговых мероприятий по учебной дисциплине, в том числе с количеством баллов – 0.

Если по результатам выполнения всех рейтинговых мероприятий (тестирования по всем модулям дисциплины и выполнения рейтинговой работы) Вы набрали средний балл - 75 баллов и более, Вы можете претендовать на оценку «хорошо», «отлично» или «зачтено» по итогам работы в семестре без прохождения промежуточной аттестации (т.е. «автоматом»).

Средний балл рассчитывается как сумма баллов за все элементы рейтингового контроля (тестирование по каждому модулю, выполнение рейтинговой работы) разделенная на количество элементов контроля. При этом оценка определяется в соответствии со шкалой:

75-84 балла – хорошо, 85-100 баллов – отлично, 75-100 – зачтено.

Если средний балл менее 75, или Вы претендуете на более высокую оценку, то Вы сдаете зачет/экзамен по дисциплине на общих основаниях.

Промежуточная аттестация **для обучающихся по очной, очно-заочной и заочной формам обучения с применением дистанционных образовательных технологий** осуществляется в форме проведения и/или устных зачетов и выполнения итогового тестирования по дисциплине.

Промежуточная аттестация **для обучающихся с применением дистанционных образовательных технологий** осуществляется в форме письменных экзаменов.

Если студент, обучающийся с применением ЭИОС, претендует на более высокую оценку, чем «автомат», то для открытия итогового тестирования необходимо обратиться в сервис «Центр поддержки».

Для выполнения итогового тестирования предоставляются также две попытки.

Обращаем Ваше внимание на то, что если в течение семестра Вы оформляли отсрочку оплаты обучения, то за две недели до начала зачетно-экзаменационной сессии финансовая задолженность должна быть погашена. В противном случае у Вас не будет возможности получить оценки по дисциплинам «автоматом» или пройти промежуточную аттестацию.

Внеучебный рейтинг обучающихся

Внеучебный рейтинг применяется для активизации обучающихся к участию в творческой, спортивной, общественной и научно-исследовательской деятельности Университета и является составной частью портфолио обучающегося, складывается из баллов, полученных обучающимися за участие в различных внеучебных мероприятиях. Подтверждение суммы баллов за внеучебный рейтинг осуществляется деканами на основе анализа представленных Вами документов (сертификатов, грамот, свидетельств, благодарностей и иных материалов) и заполненного Вами в Личном кабинете портфолио.

Ликвидация академической задолженности

Если в ходе промежуточной аттестации по учебной дисциплине Вы получили неудовлетворительную оценку или не явились на зачет/экзамен (не прошли итоговое тестирование), то у Вас образуется академическая задолженность.

Все набранные ранее в течение семестра по результатам выполнения рейтинговых мероприятий баллы обнуляются.

Ликвидировать академическую задолженность Вы должны в течение года, следующего за семестром образования академической задолженности (но не более двух раз).

Ликвидация академической задолженности проходит в форме выполнения итогового теста. Шкала оценивания при ликвидации академической задолженности:

при форме контроля по дисциплине – **экзамен/ зачет с оценкой: зачет:**

- «неудовлетворительно» – 49 баллов и менее;
- «удовлетворительно» – от 50 до 65
- «хорошо» – от 66 до 84 баллов;

при форме контроля по дисциплине – «не зачтено» – 49 баллов и менее; «зачтено» – от 50 до 100 баллов баллов; «отлично» – от 85 до 100 баллов

Пройти итоговое тестирование Вы можете не более двух раз в течение установленного календарным графиком периода. Учитывается лучший результат, полученный Вами в ходе выполнения итогового тестирования. Для выполнения одного сеанса тестирования устанавливается время – один академический час (45 минут).