Образовательное частное учреждение высшего образования

«МОСКОВСКИЙ УНИВЕРСИТЕТ ИМЕНИ А.С. ГРИБОЕДОВА»

(ИМПЭ им. А.С. Грибоедова)

ФАКУЛЬТЕТ ЛИНГВИСТИКИ

УТВЕРЖДАЮ
Декан факультета лингвистики
_____ /Н. А. Никитская/
«06» июня 2024 г

Рабочая программа дисциплины

Основы информационной безопасности в профессиональной деятельности

Укрупненная группа специальностей 45.00.00

Специальность 45.05.01 Перевод и переводоведение
(уровень специалитета)

Специализация:
«Лингвистическое обеспечение межгосударственных отношений»

Форма обучения: очная

Москва

Рабочая программа дисциплины составлена на основании федерального государственного образовательного стандарта высшего образования – Направление подготовки 45.05.01 Перевод и переводоведение (уровень специалитета) Специализация: «Лингвистическое обеспечение межгосударственных отношений», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 18 марта 2021 г. № 134н (зарегистрирован Министерством юстиции Российской Федерации 21 апреля 2021 г. регистрационный № 63195), профессиональным стандартом «Педагог дополнительного образования детей и взрослых», от 22 сентября 2021 г. № 652н (зарегистрирован Министерством юстиции Российской Федерации 17 декабря 2021 г. регистрационный № 66403), профессиональным стандарт «Специалист в области перевода», от 18 марта 2021 г. № 134н (зарегистрирован Министерством юстиции Российской Федерации 21 апреля 2021 г. регистрационный № 63195).

Разработчики:	к.ф.н., доцент М.Э. Данилова
Ответственный рецензент:	Доктор филологических наук, профессор кафедры английского языка и переводоведения факультета иностранных языков института русской и романо-германской филологии ФГБОУ ВО «Брянский государственный университет им. акад. И.Г. Петровского», Василенко А.П.
	(Ф.И.О., уч. степень, уч. звание, должность)

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры перевода, переводоведения и межкультурных коммуникаций 06.06.2024 г. протокол №10

Заведующий кафедрой _____/ к.ф.н., доцент М.Э. Данилова/

Согласовано от Библиотеки _____/О.Е. Стёпкина/

Раздел 1. Цели и задачи освоения дисциплины

Целью освоения учебной дисциплины является формирование у обучаемых знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

Задачи дисциплины конкретизируют сформулированную общую цель и способствуют ее реализации:

- *приобретение информационной культуры;*
- *владение методами и средствами получения, хранения, обработки информации, навыками использования компьютерной техники, программно-информационных систем, компьютерных сетей;*
- *способность понимать сущность и значение информации в развитии современного информационного общества, соблюдать основные требования информационной безопасности;*
- *способность распознавания опасности и угроз, возникающих в процессе использования информации и применения основных способов защиты от внешних и внутренних угроз.*

Раздел 2. Планирование результатов обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	**ИУК-1.1. Знает** основные способы анализа и обобщения информации, системного подхода **ИУК-1.2. Умеет** использовать приемы анализа информации, подходить к решению поставленных задач с учетом системного подхода **ИУК-1.3. Владеет** навыками осуществления поиска, критического анализа и синтеза информации для решения поставленных задач
ОПК-2	Способен применять систему знаний о видах, приемах, стратегиях, технологиях и закономерностях перевода, а также требованиях, предъявляемых к переводу	**ИОПК-2.1.** Знает систему знаний о видах, приемах, стратегиях, технологиях и закономерностях перевода, а также требованиях, предъявляемых к переводу; **ИОПК-2.2**. Умеет переводить с учетом системы знаний о видах, приемах, стратегиях, технологиях и закономерностях перевода, а также требованиях, предъявляемых к перевод

Код компетенции	Формулировка компетенции	Индикаторы достижения компетенции
		ИОПК-2.3. Владеет навыками перевода с учетом системы лингвистических и нелингвистических знаний

РАЗДЕЛ 3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Основы информационной безопасности в профессиональной деятельности» изучается в 7 семестре, относится к Блоку Б1.О.07 «Дисциплины (модули)», «Часть, формируемая участниками образовательных отношений».

Общая трудоемкость дисциплины составляет 3 з.е.

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

Трудоемкость дисциплины и виды учебной нагрузки

Семестр 7										
з.е.	Итого	Лекции	Лабораторные занятия	Практические занятия	Семинары	Курсовое проектирование	Самостоятельная работа под руководством преподавателя	Самостоятельная работа	Текущий контроль	Контроль, промежуточная аттестация
3	108	34		34				38		2 зачет

Тематический план дисциплины

Очная форма обучения

Разделы / Темы	Лекции	Лабораторные занятия	Практические занятия	Семинары	Самостоятельная работа	Текущий контроль	Контроль, промежуточная аттестация	Всего часов
7 семестр								
Тема 1. Введение в информационную безопасность	6		6		8			20
Тема 2. Защита от компьютерных вирусов.	6		6		8			20

Тема 3. Криптографическое закрытие информации	6		6		8			20
Тема 4. Защита от потери информации из-за отказов программно-аппаратных средств	6		6		8			20
Тема 5. Защита информационно-программного обеспечения на уровне операционных систем и систем управления базами данных	6		4		10			20
Тема 6. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях	4		6		10			20
Текущий контроль								
Зачет							2	2
Всего часов	**34**		**34**		**52**		**2**	**108**

Наименование раздела дисциплины	**Содержание раздела дисциплины**
Тема 1. Введение в информационную безопасность	Роль и место системы обеспечения информационной безопасности (ИБ) в системе национальной безопасности РФ; доктрина ИБ, история проблемы ИБ, угрозы ИБ; методы и средства обеспечения

	ИБ; методологические и технологические основы комплексного обеспечения ИБ; модели, стратегии и системы обеспечения ИБ; методы управления, организации и обеспечения работ по обеспечению ИБ; проблемы информационной войны; правовые и нормативные акты в области ИБ. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Основные этапы допуска к ресурсам вычислительной системы. Использование простого пароля. Использование динамически изменяющегося пароля. Взаимная проверка подлинности и другие случаи опознания. Способы разграничения доступа к компьютерным ресурсам. Разграничение доступа по спискам. Использование матрицы установления полномочий. Произвольное и принудительное управление доступом. Разграничение доступа по уровням секретности и категориям. Понятие меток безопасности. Управление метками безопасности. Парольное разграничение доступа и комбинированные методы. Особенности программной реализации контроля установленных полномочий. Защита программных средств от несанкционированного копирования, исследования и модификации. Привязка программ к среде функционирования. Защита программ от несанкционированного запуска.
Тема 2. Защита от компьютерных вирусов.	История появления компьютерных вирусов и факторы, влияющие на их распространение. Понятие компьютерного вируса. Основные этапы жизненного цикла вирусов. Объекты внедрения, режимы функционирования и специальные функции вирусов. Схемы заражения файлов. Схемы заражения загрузчиков. Способы маскировки, используемые вирусами. Классификация компьютерных вирусов. Общая организация защиты от компьютерных вирусов. Транзитный и динамический режимы антивирусной защиты. Поиск вирусов по сигнатурам и обезвреживание обнаруженных вирусов. Углубленный анализ на наличие вирусов путем контроля эталонного состояния компьютерной системы. Защита от деструктивных действий и размножения вирусов. Использование средств аппаратного и программного контроля. Стратегия заблаговременной подготовки к эффективной ликвидации последствий вирусной эпидемии. Технология гарантированного восстановление вычислительной системы после заражения компьютерными вирусами.
Тема 3. Криптографическое закрытие информации	Введение в криптографию. Представление защищаемой информации; угрозы безопасности информации; ценность информации; основные термины и понятия криптографии; открытые сообщения и их характеристики; модели открытых сообщений; исторический очерк развития криптографии; Типы криптографических систем. Простые методы шифрования: шифры подстановки и перестановки. Подстановки с переменным коэффициентом сдвига. Многослойные шифры. Использование псевдослучайных чисел для генерации ключей. Выбор порождающего числа и максимизация длины последовательности чисел ключа. Режимы шифрования. Особенности шифрования данных в режиме реального времени.

	Шифрование ключа при необходимости его хранения с зашифрованными данными. Скоростные и недетерминированные программные шифры. Основы скоростного шифрования. Внесение неопределенностей в процесс криптографических преобразований. Стандарты шифрования. Протоколы распределения ключей; протоколы установления подлинности; электронная цифровая подпись; Общая организация криптографической защиты информации. Использование общесистемных и специализированных программных средств для шифрования файлов и работы с секретными внешними носителями информации.
Тема 4. Защита от потери информации из-за отказов программно-аппаратных средств	Уничтожение остаточных данных. Виды остаточных данных. Способы защиты от несанкционированного использования остаточной информации. Использование специализированных программ по уничтожению остаточных данных. Специальные режимы и особенности шифрования данных в режиме реального времени с возможность мгновенного уничтожения данных. Использование общесистемных и специализированных программных средств для мгновенного уничтожения данных. Основные способы защиты от потери информации и нарушений работоспособности вычислительных средств. Внесение функциональной и информационной избыточности. Способы резервировании информации. Правила обновления резервных данных. Методы сжатия информации. Архивация файловых данных. Особенности архивации на магнитные диски и магнитную ленту. Резервирование системных данных. Подготовка программных средств восстановления. Безопасная инсталляция программных средств. Общие сведения о нарушении доступа к дисковой и оперативной памяти. Технология восстановления дисковой и оперативной памяти. Диагностирование и устранение логических и физических дефектов магнитных дисков. Отмена результатов форматирования и восстановление поврежденных файлов данных. Защита файлов от удаления и восстановление удаленных файлов. Безопасное кэширование и дефрагментация дисковой памяти. Восстановление и оптимизация оперативной памяти компьютера. Ручное восстановление данных. Безопасное окончание работы на компьютере.
Тема 5. Защита информационно-программного обеспечения на уровне операционных систем и систем управления базами данных	Общие сведения о реализации защиты информационно-программного обеспечения в операционных системах. Классификация функций защиты по уровням безопасности, поддерживаемых операционной системой (ОС). Ядро безопасности ОС. Аппаратная основа реализации защиты на уровне ОС. Стандарты по оценке уровня безопасности ОС. Внесение функциональной и информационной избыточности ресурсов на уровне ОС. Основы надежного администрирования ОС. Используемые способы разграничения доступа к компьютерным ресурсам, а также службы регистрации и сигнализации. Средства ОС по диагностированию и локализации несанкционированного доступа к ресурсам ВС. Безопасные файловые системы современных ОС (HPFS, NTFS). Подсистемы безопасности современных ОС (Windows 95, Windows NT, UNIX), их недостатки и основные направления совершенствования. Концептуальные вопросы построения уровней

	защиты систем управления базами данных (СУБД). Основные требования к подсистеме безопасности СУБД. Общие сведения о разграничении доступа к базам данных. Обязанности администратора по защите баз данных от несанкционированного доступа. Определение полномочий пользователей по доступу к базе данных. Использование матрицы полномочий для разграничения доступа к элементам баз данных. Мандатная система разграничения доступа. Защита данных при статистической обработке. Общее понятие о целостности базы данных. Типы ошибок, ведущих к нарушению целостности. Задание ограничений целостности. Транзакция и ее свойства. Восстановление базы данных. Особенности восстановления распределенной базы данных. Проблема непротиворечивости при параллельной обработке данных. Использование блокирования для управления параллельной обработкой. Метод независимого выполнения транзакций. Управление параллельными транзакциями на основе временных и версионных отметок. Метод обнаружения противоречивых записей журнала регистрации. Метод использования теста правильности. Разрешение тупиковых ситуаций. Инструментальные средства СУБД по обеспечению целостности баз данных.
Тема 6. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях	Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности. Угрозы информационно-программному обеспечению, характерные только для распределенной вычислительной среды. Использование криптографических систем для защиты данных, циркулирующих в вычислительной сети. Особенности применения симметрических и асимметрических систем шифрования. Распределение ключей между узлами вычислительной сети. Выработка секретных ключей по Диффи-Хеллману. Распределение ключей с помощью асимметрических систем шифрования. Взаимное подтверждение подлинности при обмене сообщениями в сети. Поддержание целостности циркулирующих в сети сообщений. Формирование и проверка цифровой подписи. Защита от отрицания фактов отправки и приема сообщений. Защита от наблюдения за потоком сообщений (трафиком) в сети. Защита в Internet и Intranet. Использование межсетевых экранов (брандмауэров) для защиты информации в локальных вычислительных сетях. Типы межсетевых экранов, их достоинства и недостатки. Ограничение доступа из локальной сети в Internet с помощью proxy-серверов. Безопасность JAVA-приложений.

Занятия семинарского типа (Семинарские занятия)

Общие рекомендации по подготовке к семинарским занятиям. При подготовке к работе во время проведения занятий семинарского 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 семинарского 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 семинарского 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. Введение в информационную безопасность.

Задание №1 Управление шаблонами безопасности в Windows

Задание 2 Назначение прав пользователей при произвольном управлении доступом в Windows 2000 (XP)

Тема № 2. Правовое обеспечение информационной безопасности.

Содержание практического занятия (темы\задания\кейсы\иное)

Задание № 1 С использованием поисково-справочной системы КонсультантПлюс найти и рассмотреть основные положения нормативных и законодательных актов.

Тема № 3. Компьютерные вирусы и борьба с ними.

Задание № 1 Профилактика проникновения «троянских программ»

Задание № 2 Настройка, изучение режимов работы и сравнение различных антивирусных пакетов. Антивирусное программное обеспечение

Задание № 3 Настройка, изучение режимов работы и сравнение различных антивирусных пакетов. Антивирусное программное обеспечение

Тема № 4. Восстановление электронной информации.

Содержание практического занятия (темы\задания\кейсы\иное)

Задание № 1 Восстановление зараженных файлов

Задание № 2 Защита программ и файлов от несанкционированного доступа

Тема № 5. Электронный документооборот. Электронная цифровая подпись.

Содержание практического занятия (темы\задания\кейсы\иное)

Задание № 1 Установите сертификат удостоверяющего центра и личный служебный сертификат с ключевого носителя.

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

Наряду с чтением лекций и проведением семинарских 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 бакалавра. 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.

Самостоятельная работа

Наименование разделов/тем	Виды занятий для самостоятельной работы
Тема 1. Введение в информационную безопасность	- *усвоение изучаемого материала по рекомендуемой учебной, учебно- методической и научной литературе и/или по конспекту лекции;* - *выполнение устных упражнений;* - *выполнение письменных упражнений и практических работ;* - *выполнение творческих работ;* - *подготовка рефератов (докладов), эссе, статей, тематических сообщений и выступлений*
Тема 2. Защита от компьютерных вирусов.	- *усвоение изучаемого материала по рекомендуемой учебной, учебно- методической и научной литературе и/или по конспекту лекции;* - *выполнение устных упражнений;* - *выполнение письменных упражнений и практических работ;* - *выполнение творческих работ;* - *подготовка рефератов (докладов), эссе, статей, тематических сообщений и выступлений*
Тема 3. Криптографическое закрытие информации	- *усвоение изучаемого материала по рекомендуемой учебной, учебно- методической и научной литературе и/или по конспекту лекции;* - *выполнение устных упражнений;* - *выполнение письменных упражнений и практических работ;* - *выполнение творческих работ;* - *подготовка рефератов (докладов), эссе, статей, тематических сообщений и выступлений*
Тема 4. Защита от потери информации из-за отказов программно-аппаратных средств	- *усвоение изучаемого материала по рекомендуемой учебной, учебно- методической и научной литературе и/или по конспекту лекции;* - *выполнение устных упражнений;* - *выполнение письменных упражнений и практических работ;* - *выполнение творческих работ;* - *подготовка рефератов (докладов), эссе, статей, тематических сообщений и выступлений*
Тема 5. Защита информационно-программного обеспечения на уровне операционных систем и систем управления базами данных	- *усвоение изучаемого материала по рекомендуемой учебной, учебно- методической и научной литературе и/или по конспекту лекции;* - *выполнение устных упражнений;* - *выполнение письменных упражнений и практических работ;* - *выполнение творческих работ;*

Наименование разделов/тем	Виды занятий для самостоятельной работы
	- *подготовка рефератов (докладов), эссе, статей, тематических сообщений и выступлений*
Тема 6. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях	- *усвоение изучаемого материала по рекомендуемой учебной, учебно- методической и научной литературе и/или по конспекту лекции;* - *выполнение устных упражнений;* - *выполнение письменных упражнений и практических работ;* - *выполнение творческих работ;* - *подготовка рефератов (докладов), эссе, статей, тематических сообщений и выступлений*

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

6.1. Форма промежуточной аттестации обучающегося по учебной дисциплине

В процессе освоения учебной дисциплины для оценивания сформированности требуемых компетенций используются оценочные материалы (фонды оценочных средств), представленные в таблице

Индикаторы компетенций в соответствии с основной образовательной программой	Типовые вопросы и задания	Примеры тестовых заданий
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий		
ИУК-1.1.	П. 6.2 настоящей рабочей программы дисциплины	П. 6.3 настоящей рабочей программы дисциплины
ИУК-1.2.	П. 6.2 настоящей рабочей программы дисциплины	П. 6.3 настоящей рабочей программы дисциплины
ИУК-1.3.	П. 6.2 настоящей рабочей программы дисциплины	П. 6.3 настоящей рабочей программы дисциплины
ОПК-2 Способен применять систему знаний о видах, приемах, стратегиях, технологиях и закономерностях перевода, а также требованиях, предъявляемых к переводу		
ИОПК-2.1.	П. 6.2 настоящей рабочей программы дисциплины	П. 6.3 настоящей рабочей программы дисциплины
ИОПК-2.2.	П. 6.2 настоящей рабочей программы дисциплины	П. 6.3 настоящей рабочей программы дисциплины

ИОПК-2.3.	П. 6.2 настоящей рабочей программы дисциплины	П. 6.3 настоящей рабочей программы дисциплины

6.3. Примерные тестовые задания

Полный банк тестовых заданий для проведения компьютерного тестирование находятся в электронной информационной образовательной среде и включает более 60 заданий из которых в случайном порядке формируется тест, состоящий из 20 заданий.

<table>
<tr><th>Компетенции</th><th>Типовые вопросы и задания</th></tr>
<tr><td>УК-1</td><td>
1. В каком правовом документе дается определение термина «информационная безопасность»?
а) Федеральныйзакон«Обезопасности».
б) СтратегиянациональнойбезопасностиРоссийскойФедерациидо2020 года.
в) ДоктринаинформационнойбезопасностиРоссийскойФедерации.
г) Конституция.
д) Федеральныйзакон «Обинформации, информационныхтехнологияхиозащитеинформации».
2. Основнымиаспектамидеятельности (задачами) информационнойбезопасностивыступают –
а) Конфиденциальность.
б) Доступность.
в) Системность.
г) Целостность.
д) Защитаинформации.
3. Постройтесоответствиемеждуметодамизащитыинформации(леваяколонка) ииххарактеристиками(праваяколонка):
<table>
<tr><td>1.Правовые методы</td><td>A. Подбор сотрудников компании, а также обеспечение того, чтобы непроверенные лица не допускались к охраняемой информации</td></tr>
<tr><td>2. Программный метод</td><td>B. Разработканормативныхактов, подразумевающихадминистративнуюиуголовнуюответственностьзахищениеинформации, нарушениеавторскихправпрограммистовикиберпреступления</td></tr>
<tr><td>3. Программно-аппаратный метод</td><td>C. Использованиеантивирусныхпрограммипассивнойзащиты (брандмауэр, файрволит.п.)</td></tr>
<tr><td>4. Физические методы</td><td>D. Изготовлениеаппаратныхсредствзащитыинформации, например, сетевыхадаптероввпамятикотороговстроенаантивирусная программа</td></tr>
<tr><td>5. Организационные методы</td><td>E. Включаетвсебязащитукабельныхсистем, использованиевсевозможныхисточниковбесперебойного питания, защитупомещенийотпостороннегодоступа, резервноекопированиеинформации</td></tr>
<tr><td>6. Административные методы</td><td>F. Формирование политики информационной безопасности компании</td></tr>
</table>
</td></tr>
</table>

ОПК-2	***1.*** **Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов:** a) *Информация* *b) Информационные технологии* *c) Информационная система* *d) Информационно-телекоммуникационная сеть* *e) Обладатель информации* ***2.*** **Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации:** a) *Источник информации* *b) Потребитель информации* *c) Уничтожитель информации* *d) Носитель информации* *e) Обладатель информации* ***3.*** **Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники это:** a) *База данных* *b) Информационная технология* *c) Информационная система* *d) Информационно-телекоммуникационная сеть* *e) Медицинская информационная система*

6.4.*Оценочные шкалы*

6.4.1. Оценивание текущего контроля

Целью проведения текущего контроля является достижение уровня результатов обучения в соответствии с индикаторами компетенций.

Текущий контроль может представлять собой письменные индивидуальные задания состоящие из 5/3 вопросов или в форме тестовых заданий по изученным темам до проведения промежуточной аттестации. Рекомендованный планируемый период проведения текущего контроля за 6/3 недели до промежуточной аттестации.

Шкала оценивания при тестировании

Оценка	***Критерии выставления оценки***
Зачтено	*Количество верных ответов в интервале: 71-100%*
Не зачтено	*Количество верных ответов в интервале: 0-70%*

Шкала оценивания при письменной работе

Оценка	***Критерии выставления оценки***
Зачтено	*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.
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*

6.4.2. Оценивание самостоятельной письменной работы (контрольной работы, эссе)

При оценке учитывается:

1. Правильность оформления
2. Уровень сформированности компетенций.
3. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
4. Уровень знания фактического материала в объеме программы.
5. Логика, структура и грамотность изложения письменной работы.
6. Полнота изложения материала (раскрытие всех вопросов)
7. Использование необходимых источников.
8. Умение связать теорию с практикой.
9. *Умение делать обобщения, выводы.*

Шкала оценивания контрольной работы и эссе

Оценка	***Критерии выставления оценки***
Зачтено	*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.*
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*

6.4.3. 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.

6.4.4. Тестирование

Шкала оценивания

Оценка	***Критерии выставления оценки***
Отлично	*Количество верных ответов в интервале: 71-100%*
Хорошо	*Количество верных ответов в интервале: 56-70%*
Удовлетворительно	*Количество верных ответов в интервале: 41-55%*
Неудовлетворительно	*Количество верных ответов в интервале: 0-40%*
Зачтено	*Количество верных ответов в интервале: 41-100%*
Не зачтено	*Количество верных ответов в интервале: 0-40%*

6.5.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 практикоориентированных 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.

Коллоквиум может служить формой не только проверки, но и повышения производительности труда студентов. На коллоквиумах обсуждаются отдельные части, разделы, темы, вопросы изучаемого курса, обычно не включаемые в тематику семинарских и других практических учебных занятий, а также рефераты, проекты и иные работы обучающихся.

Доклад, сообщение – продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы.

Контрольная работа – средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.

Профессионально-ориентированное эссе – это средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной проблемы, самостоятельно проводить анализ этой проблемы с использованием аналитического инструментария соответствующей дисциплины, делать выводы, обобщающие авторскую позицию по поставленной профессионально-ориентированной проблеме.

Реферат – продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.

Ситуационный анализ (кейс) – это комплексный анализ ситуации, имевший место в реальной практике профессиональной деятельности специалистов. Комплексный анализ включает в себя следующие составляющие: причинно-следственный анализ (установление причин, которые привели к возникновению данной ситуации, и следствий ее развертывания), системный анализ (определение сущностных предметно-содержательных характеристик, структуры ситуации, ее функций и др.), ценностно-мотивационный анализ (построение системы оценок ситуации, ее составляющих, выявление мотивов, установок, позиций действующих лиц); прогностический анализ (разработка перспектив развития событий по позитивному и негативному сценарию), рекомендательный анализ (выработка рекомендаций относительно поведения действующих лиц ситуации), программно-целевой анализ (разработка программ деятельности для разрешения данной ситуации).

Творческое задание – это частично регламентированное задание, имеющее нестандартное решение и позволяющее диагностировать умения интегрировать знания различных научных областей, аргументировать собственную точку зрения, доказывать правильность своей позиции. Может выполняться в индивидуальном порядке или группой обучающихся.

Деловая и/или ролевая игра – совместная деятельность группы обучающихся и преподавателя под управлением преподавателя с целью решения учебных и

профессионально-ориентированных задач путем игрового моделирования реальной проблемной ситуации. Позволяет оценивать умение анализировать и решать типичные профессиональные задачи.

«Круглый стол», дискуссия – интерактивные оценочные средства, позволяющие включить обучающихся в процесс обсуждения спорного вопроса, проблемы и оценить их умение аргументировать собственную точку зрения. Занятие может проводить по традиционной (контактной) технологии, либо с использованием телекоммуникационных технологий.

Проект – конечный профессионально-ориентированный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся.

РАЗДЕЛ 7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

7.1. Методические рекомендации по написанию эссе

Эссе(от французского essai – опыт, набросок) – жанр научно-публицистической литературы, сочетающей подчеркнуто-индивидуальную позицию автора по конкретной проблеме.

Главными особенностями, которые характеризуют эссе, являются следующие положения:

- собственная позиция обязательно должна быть аргументирована и подкреплена ссылками на источники, авторитетные точки зрениями и базироваться на фундаментальной науке. Небольшой объем (4–6 страниц), с оформленным списком литературы и сносками на ее использование;
- стиль изложения – научно-исследовательский, требующий четкой, последовательной и логичной системы доказательств; может отличаться образностью, оригинальностью, афористичностью, свободным лексическим составом языка;
- исследование ограничивается четкой, лаконичной проблемой с выявлением противоречий и разрешением этих противоречий в данной работе.

7.2. Методические рекомендации по использованию кейсов

Кейс-метод (Casestudy) – метод анализа реальной ситуации, описание которой одновременно отражает не только какую-либо практическую проблему, но и актуализирует определенный комплекс знаний, который необходимо усвоить при разрешении данной проблемы. При этом сама проблема не имеет однозначных решений.

Кейс как метод оценки компетенций должен удовлетворять следующим требованиям:

- соответствовать четко поставленной цели создания;
- иметь междисциплинарный характер;
- иметь достаточный объем первичных и статистических данных;
- иметь соответствующий уровень сложности, иллюстрировать типичные ситуации, иметь актуальную проблему, позволяющую применить разнообразные методы анализа при поиске решения, иметь несколько решений.

Кейс-метод оказывает содействие развитию умения решать проблемы с учетом конкретных условий и при наличии фактической информации. Он развивает такие квалификационные характеристики, как способность к проведению анализа и диагностики проблем, умение четко формулировать и высказывать свою позицию, умение общаться, дискутировать, воспринимать и оценивать информацию, которая поступает в вербальной и невербальной форме.

7.3. Требования к компетентностно-ориентированным заданиям для демонстрации выполнения профессиональных задач

Компетентностно-ориентированное задание – это всегда практическое задание, выполнение которого нацелено на демонстрирование доказательств наличия у обучающихся компетенций, знаний, умений, необходимых для будущей профессиональной деятельности.

Компетентностно-ориентированные задания бывают разных видов:

- направленные на подготовку конкретного практико-ориентированного продукта (анализ документов, текстов, критика, разработка схем и др.);
- аналитического и диагностического характера, направленные на анализ различных аспектов и проблем;
- связанные с выполнением основных профессиональных функций (выполнение конкретных действий в рамках вида профессиональной деятельности, например формулирование целей миссии, и т. п.).

8.Учебно-методическое и информационное обеспечение дисциплины

Основная литература[1]

Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 c. -ЭБС «IPRsmarts». — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

Дополнительная литература[2]

Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс] / А.Е. Фаронов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 154 c. -ЭБС «IPRsmarts». — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/52160.html

Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 c. -ЭБС «IPRsmarts». — 978-5-94774-821-5. — Режим доступа: http://www.iprbookshop.ru/52209.html

Крылов Г.О. Понятийный аппарат информационной безопасности [Электронный ресурс] : словарь / Г.О. Крылов, С.Л. Ларионова, В.Л. Никитина. — Электрон. текстовые данные. — Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016. -ЭБС «IPRsmarts». — 978-5-00094-308-3. — Режим доступа: http://www.iprbookshop.ru/64306.html

Нормативные источники

[1]Из ЭБС

[2] Из ЭБС

1. *Конституция РФ.*
2. *Федеральный конституционный закон от 28.04.1995 № 1-ФКЗ «Об арбитражных судах в Российской Федерации».*
3. *Закон РФ от 05.03.1992 № 2446-1 «О безопасности».*
4. *Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности».*
5. *Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».*
6. *Закон от 27.12.1991 № 2124-1 «О средствах массовой информации».*
7. *Федеральный закон от 13.01.1995 № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации».*
8. *Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».*
9. *Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».*
10. *Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».*
11. *Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».*
12. *Федеральный закон от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».*
13. *Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».*
14. *Федеральный закон от 10.01.2003 № 20-ФЗ «О Государственной автоматизированной системе Российской Федерации «Выборы».*
15. *Федеральный закон от 25.07.1998 № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации».*
16. *Доктрина информационной безопасности Российской Федерации.*
17. *Указ Президента РФ от 12.05.2009 № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года».*
18. *Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».*
19. *Указ Президента РФ от 01.09.2004 № 1135 «Об утверждении Положения об Управлении информационного и документационного обеспечения Президента Российской Федерации».*
20. *Указ Президента РФ от 27.07.1992 № 802 «О научном и информационном обеспечении проблем инвалидности и инвалидов».*
21. *Указ Президента РФ от 28.06.1993 № 966 «О Концепции правовой информатизации России».*
22. *Указ Президента РФ от 20.01.1994 № 170 «Об основах государственной политики в сфере информатизации».*
23. *Указ Президента РФ от 19.10.2005 № 1222 «Об основных документах, удостоверяющих личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащих электронные носители информации».*
24. *Постановление Правительства РФ от 22.10.2007 № 689 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».*
25. *Постановление Правительства РФ от 24.11.2009 № 953 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и*

федеральных органов исполнительной власти» (вместе с «Требованиями к технологическим, программным и лингвистическим средствам обеспечения пользования официальным сайтом Правительства Российской Федерации в сети Интернет»).

26. *Постановление Правительства РФ от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».*
27. *Постановление Правительства РФ от 28.01.2002 № 65 «О федеральной целевой программе «Электронная Россия (2002 - 2010 годы)».*
28. *Приказ ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».*
29. *Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».*

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Интернет-ресурсы, современные профессиональные базы данных, информационно-справочные и поисковые системы

ЭБС «IPRsmarts» http://www.iprbookshop.ru

1. security lab | http://www.securitylab.ru/

Проект компании positivetechnologies. помимо новостей, экспертных статей, софта, форума, на сайте есть раздел, где оперативно публикуется информация об уязвимостях, а также даются конкретные рекомендации по их устранению.

2. Threatpost https://threatpos

Новостной сайт об информационной безопасности от KasperskyLab. Авторитетный источник, на который ссылаются ведущие новостные агентства, такие как TheNewYorkTimes и TheWallStreetJournal.

3. Anti-Malware | https://www.anti-malware.ru/

Информационно-аналитический центр, посвященный информационной безопасности. Anti-Malware проводит сравнительные тесты антивирусов, публикует аналитические статьи, эксперты принимают участие в дискуссиях на форуме.

4. Geektimes | https://geektimes.ru/hub/infosecurity/

Популярный хаб сайта geektimes.ru про информационную безопасность. Десятки тысяч просмотров статей, публикации о новинках индустрии и активное обсуждение в комментариях.

5. CNEWS http://safe.cnews.ru/

Раздел новостного издания о высоких технологиях CNEWS, посвященный информационной безопасности. Публикуются новости и экспертные статьи.

6. Блог Алексея Лукацкого http://lukatsky.blogspot.it/

Алексей Лукацкий – признанный эксперт в области информационной безопасности, обладатель множества наград, автор статей, книг, курсов, участвует в экспертизе нормативно-правовых актов в сфере ИБ и защиты персональных данных.

7. Блог Евгения Царева https://www.tsarev.biz/

Блог участника судебных процессов в качестве эксперта по вопросам кибербезопасности и защиты информации. Публикуются еженедельные обзоры всего самого интересного в мире кибербезопасности, новости об изменениях в нормативно-правовых актах.

8. Персональный сайт Алексея Комарова | https://zlonov.ru/
Сайт эксперта в области информационной безопасности, информационных технологий, информационной безопасности автоматизированных промышленных систем управления технологическим процессом.

9. Научный журнал «Вопросы кибербезопасности» http://cyberrus.com/
Печатаются статьи российских и иностранных ученых по кибербезопасности, безопасности приложений, технической защите информации, аудиту безопасности систем и программного кода, тестированию, анализу защищенности и оценке соответствия ПО требованиям безопасности информации.

10. Журнал “Information Security” http://www.itsec.ru/articles2/allpubliks
В журнале публикуются технические обозрения, тесты новых продуктов, а также описания комплексных интегрированных решений, внедренных на российских предприятиях и в государственных органах.

11. Клуб информационной безопасности http://wiki.informationsecurity.club/doku.php/main
Клуб информационной безопасности — некоммерческая организация, развивающая ИБ и решающая задачи в этой сфере. На сайте есть «База знаний», где можно найти нормативные документы, программное обеспечение, книги, ссылки на интересные ресурсы.

12. ISO27000.RU http://www.iso27000.ru/
Интернет-портал ISO27000.RU – это площадка для общения специалистов по ИБ. Есть тематический каталог ссылок на ресурсы по информационной безопасности и защите информации.

13. Ассоциация по вопросам защиты информации BISA http://bis-expert.ru/
Сообщество, созданное под эгидой Ассоциации BusinessInformationSecurity (BISA), выпускает свой журнал, проводит вебинары, а также является организатором мероприятий.

14. Видеоканал компании CISCO
https://www.youtube.com/playlist?list=PLEnXkMoWGlq2ZroboDpbUjwrqB3wIcMYC
Публикуются как видео для обычных пользователей, так и видео для профессионалов с разбором конкретных кейсов.

15. Канал интернет-телекомпании BIS TV
|https://www.youtube.com/channel/UCinmAF3guG-A5u81cWiVrRg
Канал интернет-телекомпании BIS TV специализируется на информационной безопасности банков, кредитных организаций и платёжных систем.

16. Dark Reading http://www.darkreading.com/
Сообщество профессионалов, где обсуждаются кибер-угрозы, уязвимости и методы защиты от атак, а также ключевые технологии и методы, которые могут помочь защитить данные в будущем.

17. Security Weekly https://securityweekly.com/
Самое актуальное в формате подкастов, видео, live-трансляций. Еженедельные шоу от Securityweekly – это интервью с профессионалами, обсуждение последних событий в области информационной безопасности.

18. Naked Security https://nakedsecurity.sophos.com/

Авторитетный новостной сайт компании Sophos, цитируемый крупными изданиями. Освещается широкий круг вопросов: последние события в мире информационной безопасности, новые угрозы, обзор самых важных новостей недели.

19. (IN) SECURE Magazine https://www.helpnetsecurity.com/insecuremag/
(IN) SECURE Magazine выпускается с 2005 года и публикуется ежеквартально. Фокусируются на новых тенденциях, инсайтах, исследованиях и мнениях. В специальных ежегодных выпусках журнала освещаются такие крупные события RSA Conference и InfosecurityEurope.

20. Security Bloggers Network | http://securitybloggersnetwork.com/
Около 300 блогов и подкастов об информационной безопасности. Отличительная черта – более технический, практический подход к освещению актуальных вопросов ИБ и кибербезопасности.

Интернет-ресурсы

ЭБС «IPRsmarts» http://www.iprbookshop.ru

УМО по классическому университетскому образованию России http://www.umo.msu.ru

Министерство образования и науки Российской Федерации http://mon.gov.ru

Современные профессиональные базы данных

Правотека.ру. – Б.г. – Доступ к данным: открытый. – Режим доступа : http://www.pravoteka.ru/

Российская национальная библиотека. – Б.г. – Доступ к данным: Открытый. – Режим доступа : http://www.nlr.ru/

Информационно-справочные системы

http://www.consultant.ru/

http://www.kremlin.ru/

https://digital.gov.ru/ru/documents/

Поисковые системы

http://www.sciencedirect.com

https://elibrary.ru/

КОМПЛЕКТ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Microsoft Open Value Subscription для решений Education Solutions № Tr000544893 от 21.10.2020 г. MDE Windows, Microsoft Office и Office Web Apps. (срок действия до 01.11.2023 г.)

Антивирусное программное обеспечение ESET NOD32 Antivirus Business Edition договор № ИС00-006348 от 14.10.2022 г. (срок действия до 13.10.2025 г.)

Программное обеспечение «Мираполис» система вебинаров - Лицензионный договор 244/09/16-к от 15.09.2016 (Спецификация к Лицензионному договору 244/09/16-к от 15.09.2016, от 11.05.2022 г.) (срок действия до 10.07.2023 г.)

Электронная информационно-образовательная среда «1С: Университет» договор от 10.09.2018 г. №ПРКТ-18281 (бессрочно)

Информационная система «ПервыйБит» сублицензионный договор от 06.11.2015 г. №009/061115/003 (бессрочно)

Система тестирования Indigo лицензионное соглашение (Договор) от 08.11.2018 г. №Д-54792 (бессрочно)

Информационно-поисковая система «Консультант Плюс» - договор об информационно поддержке от 26.12.2014, (бессрочно)

Электронно-библиотечная система IPRsmart лицензионный договор от 01.09.2022 г. №9489/22С (срок действия до 31.08.2024 г.)

Научная электронная библиотека eLIBRARY лицензионный договор SCIENC INDEX № SIO -3079/2022 от 12.01.2022 г. (срок действия до 27.01.2024 г.)

СВОБОДНО РАСПРОСТРАНЯЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Комплект онлайн сервисов GNU ImageManipulationProgram, свободно распространяемое программное обеспечение

Программное обеспечение отечественного производства:

Программное обеспечение «Мираполис» система вебинаров - Лицензионный договор 244/09/16-к от 15.09.2016 (Спецификация к Лицензионному договору 244/09/16-к от 15.09.2016, от 11.05.2022 г.) (срок действия до 10.07.2023 г.)

Электронная информационно-образовательная среда «1С: Университет» договор от 10.09.2018 г. №ПРКТ-18281 (бессрочно)

Информационная система «ПервыйБит» сублицензионный договор от 06.11.2015 г. №009/061115/003 (бессрочно)

Система тестирования Indigo лицензионное соглашение (Договор) от 08.11.2018 г. №Д-54792 (бессрочно)

Информационно-поисковая система «Консультант Плюс» - договор об информационно поддержке от 26.12.2014, (бессрочно)

Электронно-библиотечная система IPRsmart лицензионный договор от 01.09.2022 г. №9489/22С (срок действия до 31.08.2024 г.)

Научная электронная библиотека eLIBRARY лицензионный договор SCIENC INDEX № SIO -3079/2022 от 12.01.2022 г. (срок действия до 27.01.2024 г.)

РАЗДЕЛ 9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Специализированная учебная мебель: комплект специальной учебной мебели. Технические средства обучения, служащие для предоставления учебной информации большой аудитории: доска аудиторная, компьютер, проектор, экран
Помещение для самостоятельной работы	Комплект специальной учебной мебели. Мультимедийное оборудование: видеопроектор, экран, компьютер с возможностью подключения к сети "Интернет" и ЭИОС