

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Борисова Виктория Валерьевна
Должность: Ректор
Дата подписания: 19.06.2026 16:17:07
Уникальный программный ключ:
8d665791f4048370b679b22cf26583a2f341522e

**Негосударственное образовательное частное учреждение высшего
образования «МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ
ПСИХОЛОГО-ПЕДАГОГИЧЕСКИХ ИННОВАЦИЙ»**

УТВЕРЖДАЮ:

**Ректор
Ю.Н. В.С. «МУППИ»**

В.В. Борисова
подпись
«08» февраля 2024 г.

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕРКИ
СФОРМИРОВАННОСТИ КОМПЕТЕНЦИИ
ОПК-9. Способен понимать принципы работы современных
информационных технологий и использовать их для решения задач
профессиональной деятельности**

**направление подготовки
40.03.01 Юриспруденция**

**Профиль подготовки:
«Гражданско-правовой»**

Квалификация (степень) выпускника – бакалавр

**Форма обучения
Очно-заочная, Заочная**

Москва 2024 г.

ОПК-9. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

ИОПК 9.1. Знает основы информационных технологий

ИОПК 9.2. Умеет выполнять практические работы по настройке компьютерной техники

ИОПК 9.3. Владеет навыками работы с прикладным программным обеспечением

Компетенция формируется дисциплинами:

Очно-заочная форма обучения

Цифровая грамотность	1 семестр
Правоприменительная практика	6 семестр

Заочная форма обучения

Цифровая грамотность	1 семестр
Правоприменительная практика	6 семестр

Вопросы и задания для проверки сформированности компетенции

Дисциплина «Цифровая грамотность»

Задания в открытой форме:

1. Способность безопасно и эффективно использовать цифровые технологии в повседневной и профессиональной деятельности. Необходима для работы, обучения, коммуникации, получения услуг. О чем речь?

2. Включает умение работать с информацией, использовать программы и сервисы, общаться в сети, обеспечивать цифровую безопасность, критически оценивать контент. Что описано?

3. Информационная, компьютерная, коммуникационная, медиа-грамотность, цифровая безопасность, отношение к технологическим инновациям. Что перечислено?

4. Интегральный показатель уровня владения цифровыми навыками в обществе. Рассчитывается на основе данных опросов и оценивает уровень владения цифровыми компетенциями. Что описано?

5. Формирование национальных стратегий, программ обучения, инфраструктуры доступа, повышения квалификации кадров, поддержки уязвимых групп населения. Что описано?

6. Цифровые технологии и цифровые услуги.

7. Использование электронных сервисов: госуслуги, онлайн-банкинг, телемедицина, электронная торговля, образовательные платформы, развлекательные сервисы. Что описано?

8. Модель предоставления вычислительных ресурсов и хранения данных через интернет. Виды: IaaS, PaaS, SaaS. Преимущества: масштабируемость, доступность, экономичность. О чем речь?

9. Платформы для создания, обмена и обсуждения контента пользователями: социальные сети, блоги, мессенджеры, форумы. Влияют на коммуникацию, маркетинг, общественное мнение. О чем речь?

10. Системы дистанционного обучения (LMS): Moodle, GetCourse, корпоративные платформы. Используются для повышения квалификации, адаптации сотрудников, проведения тренингов. О чем речь?

11. Использование систем электронного документооборота, CRM, ERP, HRM, BI-систем для управления процессами, документами, персоналом, аналитикой. Что описано?
12. Сбор и анализ данных с использованием цифровых инструментов: бизнес-аналитика, веб-аналитика, big data. Помогает принимать обоснованные решения, прогнозировать развитие. Что это?
13. Совокупность мер защиты информации, устройств, сервисов и пользователей от киберугроз. Включает технические, организационные, правовые и образовательные меры. О чем речь?
14. Антивирусная защита, межсетевые экраны, разграничение прав доступа, резервное копирование, политика паролей, обучение персонала, регламенты реагирования на инциденты. О чем речь?
15. Обеспечение конфиденциальности, целостности и доступности информации. Достигается техническими, программными и организационными средствами защиты. Что описано?
16. Принятие политики ИБ, назначение ответственных, регламентация доступа, обучение сотрудников, контроль соблюдения требований, аудит, реагирование на инциденты. Что описано?
17. Тренинги по распознаванию фишинга, правилам создания паролей, обращению с подозрительными ссылками, использованию двухфакторной аутентификации, защите личных данных. Что перечислено?
18. Использование антивирусов, обновление ПО, фильтрация контента, ограничение доступа к опасным ресурсам, информирование о видах мошенничества, родительский контроль. Что перечислено?

Ответы на задания в открытой форме:

Вопрос (наименование вопроса)	Ответ (краткий ответ)
Способность безопасно и эффективно использовать цифровые технологии в повседневной и профессиональной деятельности. Необходима для работы, обучения, коммуникации, получения услуг. О чем речь?	Цифровая грамотность как важный жизненный навык.
Включает умение работать с информацией, использовать программы и сервисы, общаться в сети, обеспечивать цифровую безопасность, критически оценивать контент. Что описано?	Цифровая грамотность и базовые компетенции личности.
Информационная, компьютерная, коммуникационная, медиа-грамотность, цифровая безопасность, отношение к технологическим инновациям. Что перечислено?	Компоненты цифровой грамотности.
Интегральный показатель уровня владения цифровыми навыками в обществе. Рассчитывается на основе данных опросов и оценивает уровень владения цифровыми компетенциями. Что описано?	Индекс цифровой грамотности.
Формирование национальных стратегий, программ обучения, инфраструктуры доступа, повышения квалификации кадров, поддержки уязвимых групп	Стратегические подходы к цифровой грамотности.

населения. Что описано?	
Цифровые технологии и цифровые услуги.	Цифровые технологии — средства обработки информации. Услуги — электронные сервисы.
Использование электронных сервисов: госуслуги, онлайн-банкинг, телемедицина, электронная торговля, образовательные платформы, развлекательные сервисы. Что описано?	Потребление цифровых услуг.
Модель предоставления вычислительных ресурсов и хранения данных через интернет. Виды: IaaS, PaaS, SaaS. Преимущества: масштабируемость, доступность, экономичность. О чем речь?	Облачные технологии.
Платформы для создания, обмена и обсуждения контента пользователями: социальные сети, блоги, мессенджеры, форумы. Влияют на коммуникацию, маркетинг, общественное мнение. О чем речь?	Социальные медиа.
Системы дистанционного обучения (LMS): Moodle, GetCourse, корпоративные платформы. Используются для повышения квалификации, адаптации сотрудников, проведения тренингов. О чем речь?	Учебные платформы и их использование в организации.
Использование систем электронного документооборота, CRM, ERP, HRM, BI-систем для управления процессами, документами, персоналом, аналитикой. Что описано?	Администрирование организации с помощью цифровых технологий.
Сбор и анализ данных с использованием цифровых инструментов: бизнес-аналитика, веб-аналитика, big data. Помогает принимать обоснованные решения, прогнозировать развитие. Что это?	Цифровая аналитика.
Совокупность мер защиты информации, устройств, сервисов и пользователей от киберугроз. Включает технические, организационные, правовые и образовательные меры. О чем речь?	Понятие цифровой безопасности.
Антивирусная защита, межсетевые экраны, разграничение прав доступа, резервное копирование, политика паролей, обучение персонала, регламенты реагирования на инциденты. О чем речь?	Цифровая безопасность в организации.
Обеспечение конфиденциальности, целостности и доступности информации. Достигается техническими, программными и организационными средствами защиты.	Информационная безопасность компьютеров и информационных систем.

Что описано?	
Принятие политики ИБ, назначение ответственных, регламентация доступа, обучение сотрудников, контроль соблюдения требований, аудит, реагирование на инциденты. Что описано?	Организационные меры по защите информации в организации.
Тренинги по распознаванию фишинга, правилам создания паролей, обращению с подозрительными ссылками, использованию двухфакторной аутентификации, защите личных данных. Что перечислено?	Обучение пользователей правилам безопасной работы в сети.
Использование антивирусов, обновление ПО, фильтрация контента, ограничение доступа к опасным ресурсам, информирование о видах мошенничества, родительский контроль. Что перечислено?	Защита пользователей от Интернет-угроз.

Дисциплина «Правоприменительная практика»

Задания в открытой форме:

1. Каким образом в организации функционирует система информационной/цифровой безопасности?
2. Каким образом в организации функционирует защита от Интернет-угроз.

Ответы на задания в открытой форме:

Вопрос (наименование вопроса)	Ответ (краткий ответ)
Каким образом в организации функционирует система информационной/цифровой безопасности?	Применяются антивирусы, межсетевые экраны, разграничение прав доступа, резервное копирование, политика паролей, регламент реагирования на инциденты, обучение сотрудников.
Каким образом в организации функционирует защита от Интернет-угроз.	Используются средства фильтрации трафика, антифишинговые системы, ограничение доступа к опасным ресурсам, обновление ПО, обучение пользователей, мониторинг событий безопасности.

Методика оценки сформированности компетенции

Оценка сформированности компетенции проводится по 100 – бальной системе.

Код и наименование индикатора достижения компетенции	Критерии оценивания сформированности компетенции (части компетенции)
ИОПК 9.1. Знает основы информационных технологий ИОПК 9.2. Умеет выполнять практические работы по настройке компьютерной техники ИОПК 9.3. Владеет навыками работы с прикладным программным обеспечением	выполнение 70% и более оценочных средств по определению уровня достижения результатов обучения по дисциплине

--	--