МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Костромской государственный университет»

(КГУ)

ФОНД

ОЦЕНОЧНЫХ СРЕДСТВ

ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

СОЦИАЛЬНО-ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Составлены в соответствии с учебным планом КГУ и программой дисциплины для подготовки специалиста среднего специального образования

Специальность: 39.02.01 Социальная работа

Квалификация выпускника: специалист по социальной работе

Кострома

2024 г.

Разработал: Бойцова С.В., к.п.н., доцент

Рецензенты: Заведующий кафедрой Социальной работы к.пед.н., доцент Веричева О.Н.

УТВЕРЖДЕНО:

На заседании кафедры социальной работы
Протокол заседания №7 от 25.03.2024 г.
Заведующий кафедрой социальной работы:

Веричева О.Н., кандидат пед. наук, доцент

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

1.1. Компетенции формируемые в процессе изучения дисциплины

ОК 1 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам

ОК 2 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;

ПК 6. Обеспечивать ведение документации в процессе предоставления социальных услуг лицам пожилого возраста, инвалидам, различным категориям семей и детей (в том числе детям инвалидам), гражданам, находящимся в трудной жизненной ситуации и/или в социально опасном положении.

1.2. Шкала оценивания сформированности компетенций

При оценивании сформированности компетенций по дисциплине Социально-информационная безопасность используется комплексный зачет с оценкой в котором применяется 4-балльная шкала. Шкала соотносится с целями дисциплины и предполагаемыми результатами ее освоения.

Оценка «отлично» ставится, если обучающийся демонстрирует полное соответствие знаний, умений, навыков приведенным в таблицах показателям, оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.

Оценка «хорошо» ставится, если обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

Оценка «удовлетворительно» ставится, если обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям: в ходе контрольных мероприятий обучающийся показывает владение менее 50% приведенных показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Оценка «неудовлетворительно» ставится, если обучающийся демонстрирует полное отсутствие или явную недостаточность (менее 25%) знаний, умений, навыков в соответствие с приведенными показателями.

2. КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (примерный)

2.1 Вопросы по темам/разделам дисциплины (примерные)

Контролируемый раздел дисциплины	Код контролируемой компетенции	Примерный перечень вопросов/заданий	Оценка уровня сформированности
Тема 1 Сущность социально-информацио	ОК 1; ОК 2; ОК 06; ПК 6	1. Дать характеристику теоретических подходов к проблеме социально-	Выполнение представленных заданий /вопросов в рамках шкалы

нной безопасности		информационной безопасности. 2. Составьте тезариус основных понятий курса. 3. Составьте список учебно-методической литературы в рамках дисциплины.	оценивания по формированию компетенции
Тема 2. Государственная политика в области социальной, информационной безопасности	ОК 1; ОК 2; ОК 06; ПК 6	1. Определите основные базовые характеристики современной политики в области информационной и социальной безопасности. 2. Перечислите основные факторы определяющие политику в области информационной безопасности на уровне региона муниципалитета, организации. 3. Роль специалиста социальной сферы в реализации мер социально-информационной безопасности.	Выполнение представленных заданий /вопросов в рамках шкалы оценивания по формированию компетенции
Тема 3. Организационное обеспечение социально-информационной безопасности	ОК 1; ОК 2; ОК 06; ПК 6	1. Выделите особенности управления процессом защиты персональной информации. 2. Составьте схему взаимодействия социального учреждения в рамках межведомственного электронного взаимодействия. 3. Напишите методические рекомендации специалистам по обеспечению информационной безопасности.	Выполнение представленных заданий /вопросов в рамках шкалы оценивания по формированию компетенции
Тема 4. Технологические направления по обеспечению социально-информационной безопасности	ОК 1; ОК 2; ОК 06; ПК 6	1. Перечислите основные причины нарушений информационной безопасности. 2. Рассмотрите роль специалиста при обеспечении целостности информации. 3. напишите вариант административных процедур при работе с личными данными граждан.	Выполнение представленных заданий /вопросов в рамках шкалы оценивания по формированию компетенции

Тема 5 Оценка опыта по обеспечению социально-информационной безопасности	ОК 1; ОК 2; ОК 06; ПК 6	1. Выделите подходы к организации работы при обеспечении информационной безопасности. 2. Рассмотрите деятельность организации с позиции оценки рисков разглашения корпоративной информации 3. Дайте оценку угроз при передаче информации через открытые информационные ресурсы	Выполнение представленных заданий /вопросов в рамках шкалы оценивания по формированию компетенции

2.2. Тематика рефератов

1. Значение информации в современном мире
2. Основы правового обеспечения информационной и социальной безопасности
3. Защита государственной и корпоративной тайны
4. Конфиденциальная информация и ее защита
5. Гащита интеллектуальной собственности
6. Международное сотрудничество в области безопасности
7. Русский язык, культура как объект защиты национальной безопасности
8. Социальная, информационная безопасность молодежи
9. Мошенничество и борьба с ним
10. Условия кодирования персональной информации в профессиональной деятельности специалиста социальной сферы

2.3. Примеры кейсовых заданий

1. Что такое социальная безопасность?
- Охарактеризуйте государство как основной субъект социальной безопасности.
- В чем вы видите особенности построения системы по обеспечению социальной безопасности на современном этапе?
- Назовите основные направления по обеспечению социальной безопасности.
- Раскройте содержание социальной ответственности как важнейшей характеристики обеспечения социальной безопасности.
- Каковы основные задачи социальной безопасности на современном этапе развития российского общества?
- В чем, на ваш взгляд, состоит единство и различие между социальной безопасностью государства и социальной безопасностью человека?

2.4. Примеры тестовых заданий

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности
2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы

- Хищение данных, подкуп системных администраторов, нарушение регламента работы
3) Виды информационной безопасности:
+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная
4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций
5) Основные объекты информационной безопасности:
+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы
6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации
7) К основным принципам обеспечения информационной безопасности относится:
+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы
8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы
9) К основным функциям системы безопасности можно отнести все перечисленное:
+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей
10) Принципом информационной безопасности является принцип недопущения:
+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности
11) Принципом политики информационной безопасности является принцип:
+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

2.5. Тематика учебных проектов

1. Социальная экспертиза и мониторинг реализации мер по обеспечению информационной среды ВУЗа.

2. Социальный проект по реализации мер в рамках информационной безопасности граждан.

3. Социальный проект по реализации мер в рамках социальной безопасности.

4. Критерии обеспечения социальной стабильности молодежи в информационном поле.

2.6. Тематика эссе

1. Возможно ли достичь полной информационной безопасность в нашей стране.
2. Права человека как основа обеспечения информационной и социальной стабильности.
3. Информационные угрозы.
4. Преступность и безопасность общества: мошенничество с использованием персональной информации.
5. Корпоративная безопасность.

6. Государственная тайна.
7. Информационная безопасность: перспективы и возможности.
8. Информационная безопасность и стресс.
9. Роль специалиста в обеспечении информационной и социальной безопасности.

2.7. Тематика деловых, ролевых игр

1. Определение эффективности деятельности государства по направлениям социальной безопасности.
2. Деловая игра «Информационное взаимодействие» (связи, противоречия)

2.8. Описание ситуаций для сюжетно-ролевого взаимодействия

1. Представить социальную структуру общества и определить противоречия, которые там могут быть в информационном поле. Дать анализ данным противоречиям с позиции решения проблемы.
2. Рассмотреть социальные риски и определить меры по их преодолению. Экспертиза может быть в рамках конкретных направлений, может носить комплексный характер.

2.9. Иные формы контрольно-оценочных средств

нет

2. 10. Вопросы и задания к комплексному зачету

1. Понятие информационной безопасности и основные проблемы.
2. Основные задачи в области обеспечения защиты информации органов государственной власти.
2. Законодательство РФ в области защиты информации.
3. Международные нормы по информационной безопасности
4. Информационная безопасность системы.
5. Характеристики информации.
6. Задачи информационной безопасности.
7. Способы обеспечения защиты: законодательные, административные, технические.
8. Политика информационной безопасности.
9. Стандарты в области информационной безопасности
10. Цифровая экономика как условие по улучшению качества жизни населения.
11. Организационное обеспечение социально-информационной безопасности
12. Причины нарушений информационной безопасности.
13. Методы и средства обеспечения информационной безопасности.
14. Программно-технические меры по обеспечению информационной безопасности.
15. Обеспечение информационной безопасности в системе образования, здравоохранения, социальной защите.
16. Общие подходы к организации работы в условиях обеспечения информационной безопасности.
17. Профессиональные стандарты и информационная безопасность.