Частное учреждение дополнительного профессионального образования
«Институт цифрового образования»
ЧУ ДПО ИЦО

УТВЕРЖДАЮ:
Ректор ЧУ ДПО ИЦО, Тараканов В.П.
.

Сведения об электронной подписи
Подписано: Тараканов Валерий Павлович
Должность: Ректор
Пользователь: vtarakanov

1 сентября 2023 г.

Решение Педагогического совета ЧУ ДПО ИЦО,
Протокол б/н от 01.09.2023 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«ЦИФРОВАЯ БЕЗОПАСНОСТЬ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ»

Приложение № 4.3

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Москва, 2023 год

1.Общие положения

Контроль и оценка результатов освоения учебной дисциплины осуществляется в процессе изучения занятий с помощью тестирования, написания эссе по темам, практических занятий слушателей, а также выполнения обучающимися индивидуальных заданий. Оценка качества освоения учебной программы включает текущий контроль успеваемости, промежуточную аттестацию по итогам освоения дисциплины.

2. Планируемые результаты обучения по дисциплине:

знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;

уметь:

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации;

владеть:

применения основных правил и документов систем сертификации Российской Федерации.

3. Оценочные средства для проведения промежуточной аттестации

Примерные темы эссе:

1. Развитие информационных технологий и роль информационной безопасности в современном мире.
2. Основные принципы и принципы информационной безопасности.
3. Типы угроз и атак на информационные системы и данные.
4. Роль человеческого фактора в информационной безопасности и методы обучения сотрудников.
5. Защита информационных систем от внешних угроз и атак.
6. Методы шифрования и протоколы безопасной передачи данных.
7. Защита от внутренних угроз и угроз со стороны сотрудников организации.
8. Разработка и применение политики информационной безопасности.
9. Защита от социальной инженерии и мошенничества.
10. Новые тенденции и вызовы в области информационной безопасности, такие как интернет вещей (IoT), облачные сервисы и искусственный интеллект (AI)

Пример индивидуального задания:

Тема: Анализ и оценка уязвимостей информационной системы.

1. Изучите основные концепции и принципы информационной безопасности, а также методы и инструменты анализа уязвимостей информационных систем.

2. Выберите информационную систему, которую вы будете анализировать, и определите ее функциональность, архитектуру, используемые технологии и предназначение.

3. Проведите исследование угроз, связанных с выбранной информационной системой, и определите потенциальные уязвимости.

4. Выполните анализ уязвимостей с использованием специализированных инструментов, таких как сканеры уязвимостей, проникновение в систему (pentesting), анализ кода и т. д.

5. Оцените риск, связанный с каждой уязвимостью, и определите потенциальные последствия для организации или пользователя информационной системы.

6. Разработайте план мероприятий по устранению уязвимостей и повышению безопасности информационной системы.

7. Реализуйте предлагаемые меры и протестируйте их эффективность, проведите повторный анализ уязвимостей для оценки уровня безопасности системы.

8. Составьте отчет о проведенном анализе уязвимостей и предложенных мерах по обеспечению безопасности информационной системы. В отчете укажите список обнаруженных уязвимостей, рекомендации по их устранению, оценку риска и последствий, а также результаты тестирования устранения уязвимостей.

9. Сформулируйте выводы о результатах анализа уязвимостей информационной системы и предложите рекомендации для улучшения ее безопасности. Обсудите меры, которые можно принять для предотвращения будущих уязвимостей и обеспечения надежной защиты информации.

10. Проведите анализ сетевой безопасности информационной системы и предложите меры по защите от сетевых атак, включая методы сетевого анализа и мониторинга, настройку брэндмауэров, обнаружение вторжений и использование шифрования данных.

Примерные тестовые задания:

1. Что такое информационная безопасность?
   а) Защита информации от несанкционированного доступа, использования или разглашения.
   б) Процесс обеспечения конфиденциальности, целостности и доступности информационных ресурсов.
   в) Управление рисками, связанными с использованием информационных технологий.
   г) Все вышеперечисленное.

2. Какие основные угрозы информационной безопасности существуют?
   а) Вирусы и вредоносное программное обеспечение.
   б) Социальная инженерия и фишинг.
   в) Несанкционированный доступ и утечка данных.
   г) Все вышеперечисленное.

3. Что означает аутентификация в контексте информационной безопасности?
   а) Проверка подлинности пользователя или устройства перед предоставлением доступа к системе.
   б) Метод шифрования данных для защиты их от несанкционированного доступа.
   в) Процесс резервного копирования и восстановления данных.
   г) Все вышеперечисленное.

4. Какие основные меры защиты можно применить для обеспечения информационной безопасности?
   а) Использование сложных паролей и регулярное их изменение.
   б) Регулярное обновление программного обеспечения и установка антивирусных программ.

в) Ограничение прав доступа пользователей и мониторинг сетевой активности.
г) Все вышеперечисленное.

5. Что такое политика информационной безопасности и какая роль ей отводится в организации?
а) Совокупность правил, процедур и руководящих принципов, которые регулируют безопасное использование информации.
б) Разработка и внедрение мер безопасности для защиты информационных систем.
в) Мониторинг соответствия действующих нормативных требований, связанных с безопасностью информации.
г) Все вышеперечисленное.

4. Литература

1. **Липаев В.В.** Надежность и функциональная безопасность комплексов программ реального времени [Электронный ресурс]/ Липаев В.В.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2017.— 207 c. http://www.iprbookshop.ru/27295.— ЭБС «IPRbooks»
2. **Борисова И.В.** Цифровые методы обработки информации [Электронный ресурс]: учебное пособие/ Борисова И.В.— Электрон. текстовые данные.— Новосибирск: Новосибирский государственный технический университет, 2017.— 139 c.— http://www.iprbookshop.ru/45061.— ЭБС «IPRbooks»
3. **Метелица Н.Т.** Вычислительные сети и защита информации [Электронный ресурс]: учебное пособие/ Метелица Н.Т.— Электрон. текстовые данные.— Краснодар: Южный институт менеджмента, 2017.— 48 c.— http://www.iprbookshop.ru/25962.— ЭБС «IPRbooks»
4. **Аверченков, В.И.** Организационная защита информации [Электронный ресурс]: учебное пособие/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: БГТУ, 2017.— 184 c.— http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks».