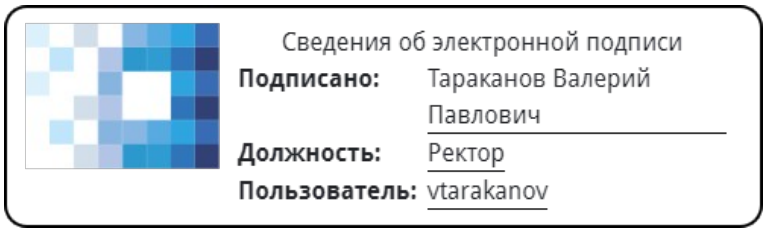
Частное учреждение дополнительного профессионального образования
«Институт цифрового образования»
ЧУ ДПО ИЦО

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



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 № 4.4

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

«ЦИФРОВАЯ БЕЗОПАСНОСТЬ»

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:

- принципы конфиденциальности, целостности и доступности информации; направления государственной политики в области информационной безопасности;
- способы защиты конфиденциальности; методы и способы сокрытия данных;
- способы обеспечения целостности данных с помощью технологий, продуктов и процедур; цифровые подписи; сертификацию целостности;
- законодательные акты в области кибербезопасности; доктрину по информационной безопасности;

уметь:

- определять соотношение принципов конфиденциальности, целостности и доступности с состояниями данных;
- определять необходимость применения методов сохранения конфиденциальности; регулировать и соблюдать процедуры по обеспечению конфиденциальности;
- применять на практике способы обеспечения целостности данных; использовать цифровую подпись;
- определять состав мероприятий по обеспечению высокой доступности; проводить процедуры по аварийному восстановлению;
- объяснять принципы использования технологий, процессов и процедур для защиты всех компонентов сетевой инфраструктуры;
- объяснять основные цели и положения нормативно-законодательных актов в сфере кибербезопасности;

владеть:

- методами и средствами обеспечения цифровой безопасности.

3. Оценочные средства для проведения промежуточной аттестации

Примерные темы эссе:

1. Развитие цифровой безопасности и ее роль в современном информационном обществе.
2. Основные проблемы и угрозы, связанные с цифровой безопасностью, такие как киберпреступления, атаки на данные и системы, социальная инженерия.
3. Технические аспекты цифровой безопасности, включая защиту сетей и систем, шифрование и криптографию, механизмы аутентификации и управление доступом.
4. Роль человеческого фактора в цифровой безопасности, включая обучение пользователей, осведомленность о безопасности, социальную инженерию и меры предотвращения.
5. Защита данных и конфиденциальности, включая методы шифрования, инкрементное резервное копирование, управление цифровыми сертификатами и политики обработки данных.
6. Защита от кибератак и вирусов, включая использование антивирусных программ, брандмауэров, мониторинга сетевой активности и выполнение регулярных обновлений.

7. Защита веб-приложений и серверов, включая предотвращение взлома, SQL-инъекции, кросс-сайтовых сценариев и других уязвимостей.

8. Применение этических и легальных аспектов в цифровой безопасности, включая этический взлом, договоренности о неразглашении, законы о защите данных и законодательство о кибербезопасности.

9. Аудит и контроль безопасности, включая методы и инструменты для сканирования и анализа уязвимостей, системы обнаружения вторжений и системы логирования.

10. Новые тенденции и вызовы в области цифровой безопасности, такие как облачные сервисы, интернет вещей (IoT), искусственный интеллект (AI) и блокчейн-технологии.

Пример индивидуального задания:

Тема: Анализ уязвимостей веб-приложений и разработка мер безопасности

1. Изучите основные уязвимости веб-приложений, такие как SQL-инъекции, кросс-сайтовые сценарии (XSS), небезопасный ввод данных и другие.

2. Выберите веб-приложение для анализа уязвимостей и определите его функциональность, архитектуру и используемые технологии.

3. Проведите анализ уязвимостей веб-приложения с использованием специализированных инструментов, таких как сканеры уязвимостей, обнаружение уязвимостей в коде и анализ сетевой активности.

4. Определите уязвимости веб-приложения и оцените их уровень критичности и потенциальные последствия для приложения и пользователя.

5. Разработайте меры безопасности для устранения уязвимостей и повышения безопасности веб-приложения.

6. Реализуйте предложенные меры безопасности веб-приложения и протестируйте их эффективность.

7. Разработайте план защиты веб-приложения от атак и угроз. Укажите меры, которые необходимо принять для защиты от известных и потенциальных угроз.

8. Составьте отчет о проведенном анализе уязвимостей и предложенных мерах безопасности для веб-приложения. Укажите список обнаруженных уязвимостей, рекомендации по их устранению, оценку риска и последствий, а также результаты тестирования мер безопасности.

9. Сформулируйте выводы о результатах анализа уязвимостей веб-приложения и предложите рекомендации для улучшения его безопасности. Обсудите меры, которые можно принять для предотвращения будущих уязвимостей и обеспечения надежной защиты данных.

10. Исследуйте новые методы и подходы к защите веб-приложений от современных угроз, таких как атаки на сеансы, криптографические уязвимости и злоумышленная маскировка. Обсудите, какие дополнительные меры безопасности могут быть применены для защиты веб-приложения.

Примерные тестовые задания:

1. Что такое хакер?

а) Компьютерный эксперт, способный взламывать системы и получать несанкционированный доступ к информации.

б) Синоним компьютерного преступника.

в) Общее название для всех специалистов по информационной безопасности.

г) Все вышеперечисленное.

2. Что такое вирус в компьютерной безопасности?
а) Вредоносная программа, которая может копировать и распространяться самостоятельно, заражая другие файлы или системы.
б) Компьютерная программа, которая улучшает безопасность системы.
в) Шпионское программное обеспечение, собирающее персональные данные пользователя.
г) Все вышеперечисленное.

3. Какой метод аутентификации основан на использовании биометрических данных?
а) Пароль.
б) PIN-код.
в) Отпечаток пальца.
г) Все вышеперечисленное.

4. Что такое фишинг?
а) Тип атаки, при которой злоумышленники подделывают легитимные веб-сайты или отправляют электронные письма, чтобы получить конфиденциальные данные от пользователей.
б) Тестирование безопасности компьютерной системы на наличие уязвимостей.
в) Защитное программное обеспечение, блокирующее доступ злоумышленников к системе.
г) Все вышеперечисленное.

5. Что такое шифрование данных и зачем оно используется?
а) Процесс преобразования данных в непонятный для человека вид для защиты от несанкционированного доступа.
б) Способность программного обеспечения обнаруживать и блокировать вредоносные программы.
в) Технология, позволяющая восстановить утраченные данные.
г) Все вышеперечисленное.

4. Литература

1. **Шаньгин В. Ф.** Информационная безопасность и защита информации [Электронный ресурс] / В. Ф. Шаньгин. — Электрон. текстовые данные. — Саратов : Профобразование, 2017. — 702 c. — 978-5-4488-0070-2. — http://www.iprbookshop.ru/63594.html.
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. — 2227-8397. — http://www.iprbookshop.ru/52160.html.
3. Программно-аппаратные средства защиты информационных систем [Электронный ресурс] : учебное пособие / Ю. Ю. Громов, Иванова О. Г., К. В. Стародубов, А. А. Кадыков. — Электрон. текстовые данные. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2017. — 193 c. — 978-5-8265-1737-6. — http://www.iprbookshop.ru/85968.html.
4. Технологии защиты информации в компьютерных сетях [Электронный ресурс] / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 2-е изд. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 368 c. — 2227-8397. — http://www.iprbookshop.ru/73732.html.