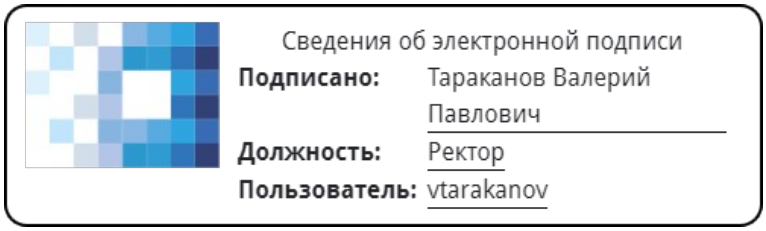
Частное учреждение дополнительного профессионального образования
«Институт цифрового образования»
ЧУ ДПО ИЦО

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

«ПРИМЕНЕНИЕ IT ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

Приложение № 4.2

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

«БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ»

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:

- методы и средства обеспечения информационной безопасности компьютерных сетей;
- варианты построения виртуальных защищенных сетей;
- протоколы формирования защищенных каналов;

уметь:

- использовать в практической деятельности существующие методы и средства контроля и защиты информации в компьютерных сетях;
- применять средства анализа защищенности и обнаружения атак;

владеть:

- техническими и программными средствами обеспечения безопасности компьютерных сетей;
- методами управления средствами сетевой безопасности.

3. Оценочные средства для проведения промежуточной аттестации

Примерные темы эссе:

1. Возможные угрозы безопасности информации в компьютерных сетях и способы их предотвращения.
2. Значение шифрования данных для обеспечения безопасности информации в компьютерных сетях.
3. Влияние социальной инженерии на безопасность информации в компьютерных сетях и меры по ее предотвращению.
4. Роль сетевых межсетевых экранов (firewalls) в обеспечении безопасности информации в компьютерных сетях.
5. Профилактические меры по обеспечению безопасности информации при использовании Wi-Fi сетей.
6. Регулирование и законодательство в области безопасности информации в компьютерных сетях.
7. Управление доступом и аутентификация: эффективные методы обеспечения безопасности информации в компьютерных сетях.
8. Возможности атак на сети Интернет вещей (IoT) и превентивные меры безопасности.
9. Роль предупреждения и мониторинга в обеспечении безопасности информации в компьютерных сетях.
10. Биометрические технологии и их роль в обеспечении безопасности информации в компьютерных сетях.

Пример индивидуального задания для экзамена:

Тема: Значение политик безопасности для обеспечения информационной безопасности в компьютерных сетях.

1. Изучите основные концепции и принципы информационной безопасности в компьютерных сетях.

2. Проанализируйте роль политик безопасности в обеспечении защиты информации в компьютерных сетях. Исследуйте, каким образом политики безопасности определяют цели, политики, процедуры и контрольные механизмы для обеспечения безопасности информации.

3. Рассмотрите различные подходы к разработке и реализации политик безопасности в компьютерных сетях. Проанализируйте основные этапы и средства, используемые для создания и внедрения политик безопасности.

4. Приведите пример политики безопасности, которая может быть применена для обеспечения защиты информации в компьютерной сети организации. Разработайте эту политику, учитывая конкретные требования и риски, связанные с информационной безопасностью данной организации.

5. Обсудите влияние политик безопасности на поведение пользователей компьютерной сети и на культуру безопасности в организации. Рассмотрите различные меры, которые могут быть приняты для повышения осведомленности пользователей и соблюдения политик безопасности.

6. Проанализируйте преимущества и ограничения политик безопасности в обеспечении информационной безопасности в компьютерных сетях. Рассмотрите возможные проблемы при разработке, внедрении и соблюдении политик безопасности.

7. Сделайте выводы о важности политик безопасности и их роли в обеспечении безопасности информации в компьютерных сетях. Предложите рекомендации для усовершенствования процесса разработки и реализации политик безопасности в организациях.

Примерные тестовые задания:

1. Что такое аутентификация в контексте компьютерных сетей?

а) Процесс передачи данных по сети в зашифрованной форме.

б) Процесс проверки подлинности идентификатора пользователя и пароля, прежде чем предоставлять доступ к системе.

в) Процесс обеспечения конфиденциальности передаваемых данных путем шифрования.

г) Процесс предотвращения несанкционированного доступа к сети путем фильтрации трафика.

2. Что делает утилита фаервол в компьютерных сетях?

а) Осуществляет мониторинг активности сети и регистрирует информацию о пакетах данных.

б) Проводит аутентификацию пользователей и предоставляет им доступ к сети на основе учетных данных.

в) Контролирует и фильтрует сетевой трафик на основе заранее заданных правил.

г) Шифрует передаваемую по сети информацию для обеспечения конфиденциальности.

3. Что такое атака переполнения буфера (buffer overflow)?

а) Тип атаки, при котором злоумышленник манипулирует данными в памяти компьютера для переполнения буфера, что может привести к нарушению работы системы.

б) Тип атаки, при котором злоумышленник отправляет огромное количество запросов к серверу в краткое время, что вызывает перегрузку и отказ в обслуживании.

в) Тип атаки, при котором злоумышленник подделывает свой IP-адрес таким образом, чтобы казаться другим участником сети.

г) Тип атаки, при котором злоумышленник перехватывает исходящий сетевой трафик и замещает его собственными данными.

4. Какой протокол обеспечивает безопасность передаваемой по сети информации путем шифрования?

а) TCP (Transmission Control Protocol)

б) IP (Internet Protocol)

в) HTTPS (Hypertext Transfer Protocol Secure)

г) DNS (Domain Name System)

5. Что такое многофакторная аутентификация?

а) Процесс проверки подлинности идентификатора пользователя и пароля на основе нескольких предоставленных им данных.

б) Процесс шифрования передаваемых по сети данных с помощью нескольких различных алгоритмов.

в) Процесс проверки безопасности сети с помощью нескольких различных утилит.

г) Процесс контроля доступа к сети на основе физического ключа и пароля.

4. Литература

1. **Аверченков, В.И.** Организационная защита информации [Электронный ресурс]: учебное пособие/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: БГТУ, 2018.— 184 с.— http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks».
2. **Белянина, Н.В.**, Корнеева, Е.В. Технологии обнаружения вторжений. Управление сетевой безопасностью. [Электронный ресурс]: рабочий учебник/ Белянина, Н.В., Корнеева, Е.В. - 2018. - http://lib.muh.ru.
3. **Борисова И.В.** Цифровые методы обработки информации [Электронный ресурс]: учебное пособие/ Борисова И.В.— Электрон. текстовые данные.— Новосибирск: Новосибирский государственный технический университет, 2018.— 139 с.— http://www.iprbookshop.ru/45061.— ЭБС «IPRbooks»
4. **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»
5. **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»