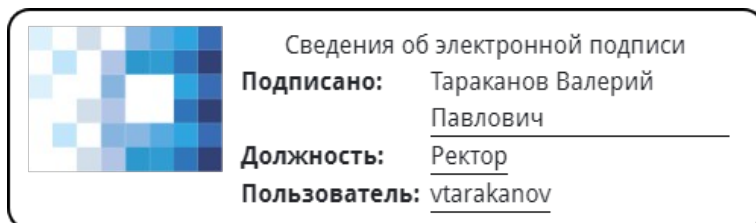


**Частное учреждение дополнительного профессионального образования
«Институт цифрового образования»
ЧУ ДПО ИЦО**

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 ИТ ТЕХНОЛОГИЙ В ЮРИСПРУДЕНЦИИ»

Приложение № 4.4

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И
ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ**

**«ЗАЩИТА ИНФОРМАЦИИ
В РАСПРЕДЕЛЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ (РАС)»**

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:

- основные технологии обеспечения безопасности РАС и соответствующие методы и средства;
- научные основы обеспечения безопасности РАС;
- сущность и содержание типовых задач в области разработки и применения защищенных РАС;
- основные направления и перспективы развития технологий защиты информации в РАС;

уметь:

- ставить и решать типовые задачи в области разработки и применения защищенных РАС;
- подбирать и использовать адекватные формы, методы и средства разработки и практического применения защищенных РАС;
- оценивать эффективность применения РАС;

владеть:

- техническими и программными средствами обеспечения безопасности РАС.

3. Оценочные средства для проведения промежуточной аттестации

Примерные темы эссе:

1. Возможные уязвимости и атаки на распределенные автоматизированные системы и методы их защиты.
2. Роль аутентификации и авторизации в обеспечении безопасности информации в распределенных автоматизированных системах.
3. Значение криптографии для обеспечения конфиденциальности и целостности данных в распределенных автоматизированных системах.
4. Проблемы безопасности при использовании облачных вычислений и меры по их решению.
5. Использование многоуровневых сетевых защитных механизмов для обеспечения безопасности в распределенных автоматизированных системах.
6. Роль мониторинга и регистрации событий в предотвращении и выявлении инцидентов безопасности в распределенных автоматизированных системах.
7. Возможности и пределы технологий обнаружения и предотвращения вторжений в распределенных автоматизированных системах.
8. Значение управления уязвимостями и патч-менеджмента в обеспечении безопасности информации в распределенных автоматизированных системах.
9. Социальные аспекты безопасности информации в распределенных автоматизированных системах: социальная инженерия и обучение пользователей.
10. Роль правовых и нормативных аспектов в обеспечении безопасности информации в распределенных автоматизированных системах.

Пример индивидуального задания:

Тема: Роль многофакторной аутентификации в обеспечении безопасности информации в распределенных автоматизированных системах.

1. Изучите основные принципы и концепции многофакторной аутентификации и ее значение в обеспечении безопасности информации в распределенных автоматизированных системах.

2. Рассмотрите различные факторы аутентификации, которые могут использоваться для обеспечения безопасности информации в распределенных автоматизированных системах, включая что-то, что пользователь знает (например, пароль), что-то, что пользователь имеет (например, токен) и что-то, что пользователь является (например, биометрические данные).

3. Проанализируйте преимущества и ограничения каждого типа факторов аутентификации в контексте распределенных автоматизированных систем. Рассмотрите их эффективность, безопасность, удобство использования и возможные уязвимости.

4. Исследуйте методы и технологии, которые могут быть использованы для реализации многофакторной аутентификации в распределенных автоматизированных системах. Рассмотрите примеры реализации и их применение для защиты информации.

5. Проанализируйте роль облачных решений в поддержке многофакторной аутентификации. Рассмотрите преимущества и ограничения использования облачных сервисов для обеспечения безопасности информации в распределенных автоматизированных системах.

6. Рассмотрите социальные и организационные аспекты внедрения многофакторной аутентификации в организации. Проанализируйте возможные проблемы и вызовы при внедрении и использовании многофакторной аутентификации для обеспечения безопасности информации.

7. Сделайте выводы о роли многофакторной аутентификации в обеспечении безопасности информации в распределенных автоматизированных системах. Предложите рекомендации для реализации многофакторной аутентификации и улучшения уровня безопасности информации в данной системе.

Примерные тестовые задания:

1. Что такое распределенная автоматизированная система (РАС)?

а) Сеть компьютеров, в которой каждый компьютер выполняет свою отдельную задачу без взаимодействия с другими компьютерами.

б) Устройство, позволяющее управлять системой автоматизации с заданными параметрами из центрального пункта.

в) Система, в которой несколько компьютеров и устройств обмениваются данными и работают совместно для выполнения задач.

г) Система, в которой данные хранятся на удаленных серверах, а пользователи получают к ним доступ через интернет.

2. Какие основные проблемы безопасности могут возникнуть в распределенных автоматизированных системах?

а) Доступ к защищенной информации, передаваемой через открытые сети.

б) Сохранение целостности данных, передаваемых между различными устройствами.

в) Управление доступом пользователей к различным ресурсам и функциям системы.

г) Все вышеперечисленное.

3. Что такое архитектура клиент-сервер в распределенных автоматизированных системах?
- а) Модель, в которой все компьютеры в сети работают независимо друг от друга и выполняют свои отдельные задачи.
 - б) Полностью централизованная модель, в которой все ресурсы и функции находятся на одном компьютере.
 - в) Модель, в которой один компьютер (сервер) предоставляет ресурсы и функции другим компьютерам (клиентам) в сети.
 - г) Модель, в которой все компьютеры в сети равноправны и взаимодействуют друг с другом для выполнения задач.
4. Какая из следующих мер защиты является методом аутентификации в РАС?
- а) Шифрование данных перед их передачей по сети.
 - б) Использование сетевых межсетевых экранов для фильтрации трафика.
 - в) Использование паролей, пин-кодов или биометрических данных для подтверждения легитимности пользователя.
 - г) Установка антивирусной программы для обнаружения и удаления вредоносных программ.
5. Что такое защита целостности данных в РАС?
- а) Методы и механизмы предотвращения несанкционированного доступа к данным.
 - б) Методы и механизмы обнаружения и предотвращения вредоносных программ.
 - в) Методы и механизмы обеспечения точности, непрерывности и неповрежденности данных в РАС.
 - г) Методы и механизмы шифрования данных для обеспечения конфиденциальности.

4. Литература

1. **Симонян А.Г.** Методы и средства технической защиты информации в РАС [Электронный ресурс]: рабочий учебник/Симонян А.Г. - 2018. - <http://lib.muh.ru>
2. **Симонян А.Г.** Технологии защиты данных в РАС [Электронный ресурс]: рабочий учебник/Симонян А.Г. - 2017. - <http://lib.muh.ru>
3. **Симонян А.Г.** Технологии защиты меж сетевого обмена данными в РАС [Электронный ресурс]: рабочий учебник/Симонян А.Г. - 2017. - <http://lib.muh.ru>
4. **Симонян А.Г.** Технологии обнаружения вторжений в РАС. Управление сетевой безопасностью [Электронный ресурс]: рабочий учебник/Симонян А.Г. - 2018. - <http://lib.muh.ru>
5. **Симонян А.Г.** Построение и организация функционирования комплексных систем защиты информации в РАС [Электронный ресурс]: рабочий учебник/Симонян А.Г. - 2016. - <http://lib.muh.ru>
6. **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»
7. **Симонян А.Г.** Организационно-правовое обеспечение информационной безопасности РАС [Электронный ресурс]: рабочий учебник/Симонян А.Г. - 2017. - <http://lib.muh.ru>
8. **Титов, А.А.** Инженерно-техническая защита информации [Электронный ресурс]: учебное пособие/ Титов А.А.— Электрон. текстовые данные. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2016. — 197 с.— <http://www.iprbookshop.ru/13931>. — ЭБС «IPRbooks»