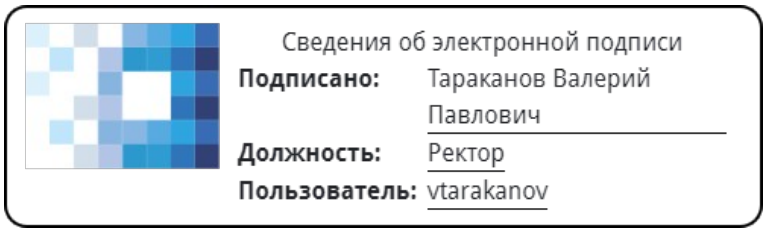
Частное учреждение дополнительного профессионального образования
«Институт цифрового образования»
ЧУ ДПО ИЦО

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 № 3.4

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ (РАС)

Москва, 2023 год

ЗАЩИТА ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ (РАС)

1. Цели и задачи дисциплины

Цель дисциплины – усвоение общей методологии, современных проблем и широкого круга специальных вопросов информационной безопасности распределенных автоматизированных систем (РАС).

Задачи дисциплины:

- раскрыть структуру и содержание круга современных проблем информационной безопасности РАС;
- охарактеризовать основные направления, средства и методы решения проблем обеспечения безопасности РАС;
- сформировать представления о научных основах решения проблем безопасности РАС;
- обеспечить формирование профессиональных навыков в области решения проблем безопасности РАС;
- выработка научного подхода к практике применения теоретических знаний в области защиты информации;
- повышение мотивации к процессу изучения научной дисциплины и научной деятельности.

2. Планируемые результаты обучения по дисциплине:

В результате изучения дисциплины обучающийся должен

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. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Введение в информационную безопасность РАС	**Информация как объект защиты.** Свойства, виды и формы представления информации. Информация и информационные ресурсы. Информация как объект права собственности. Информация как коммерческая тайна. Информация как рыночный продукт. Автоматизированные системы (АС) как объекты защиты информации.

		РАС как объекты обработки и защиты информации. Классическая архитектура «клиент-сервер». Архитектура «клиент-сервер», основанная на Web-технологии. Технологии распределенной обработки информации. Доступ к базам данных. Управление информацией о ресурсах и пользователях РАС. Условия и режимы эксплуатации РАС. **Основные понятия и анализ угроз информационной безопасности.** Основные понятия защиты информации и информационной безопасности (ИБ). Обзор и классификация угроз информации, обрабатываемой в РАС. Обзор способов реализации угроз безопасности информации. Несанкционированный доступ (НСД) к информации в РАС.
2	Обеспечение безопасности информации в РАС	**Анализ существующих подходов к обеспечению безопасности информации.** Законодательный, административный и процедурный уровни информационной безопасности. Основные понятия политики безопасности. Структура политики безопасности организации. Программно-технический уровень информационной безопасности. Сервисы безопасности. **Особенности защиты информации в РАС.** Обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных РАС. Защита информации на уровне подсистемы управления РАС. Защита информации в каналах связи. Подтверждение подлинности информации, получаемой по коммуникационной подсети. Особенности защиты информации в базах данных. **Общие теоретические подходы к защите информации.** Математические модели управления доступом к информации. Политика безопасности и модели доступа. Способы анализа моделей доступа. Модели нарушителей ИБ. Основы построения защиты информации. Модель элементарной защиты. Модель многозвенной защиты. Многоуровневая защита.
3	Организационно-правовое обеспечение информационной безопасности РАС	**Международные и отечественные стандарты в сфере защиты информации.** Роль стандартов ИБ. Международные стандарты ИБ. Стандарты для беспроводных сетей. Стандарты ИБ в Интернет. Отечественные стандарты в сфере защиты информации. Руководящие документы: «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации», «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации».

		Сертификация и аттестация в области защиты информации. Назначение и общая характеристика. Проведение сертификационных испытаний. Аттестация объектов информатизации. Сертификация на региональном и международном уровнях. **Основы правового обеспечения защиты информации.** Международный опыт правового обеспечения ИБ. Государственная система правового обеспечения ИБ. Содержание основных законов РФ в области ИБ. Понятие и виды юридической ответственности за нарушение правовых норм по защите информации.
4	Методы и средства технической защиты информации в РАС	**Виды и методы технической защиты информации.** Пассивные и активные методы защиты информации. Средства технической защиты информации. Защита помещений. Системы охранной сигнализации на территории и в помещениях. Системы видеонаблюдения. Системы контроля доступа. Системы контроля вскрытия аппаратуры. **Технические каналы утечки информации.** Общая характеристика технических каналов утечки информации и их классификация. Каналы утечки речевой информации. Технические средства и методы получения информации по этим каналам. Утечка информации по проводным коммуникациям и за счет побочных электромагнитных излучений и наводок. Технические средства и методы получения информации с использованием этих каналов. **Методы и средства защиты информации от утечки по техническим каналам.** Основные методы, используемые при создании систем защиты информации. Заземление технических средств передачи информации. Использование сетевых фильтров. Экранирование помещений. Методы защиты от утечек по акустическим каналам. Защита средств связи и телекоммуникаций.
5	Технологии защиты данных в РАС	**Современные методы защиты информации в РАС.** Ограничение и разграничение доступа. Контроль доступа к аппаратуре. Разграничение и контроль доступа к информации. Идентификация и установление подлинности объекта (субъекта). Криптографическое преобразование информации. Методы защиты информации от компьютерных вирусов. **Криптографические средства защиты информации.** Основные принципы и классификация методов криптографического преобразования информации. Обзор методов шифрования. Выбор метода преобразования информации. Симметричные алгоритмы шифрования. Асимметричные алгоритмы

		шифрования. Электронная цифровая подпись (ЭЦП) и функции хэширования. Процедуры выработки ЭЦП. Защита электронного документооборота с использованием ЭЦП. **Технологии аутентификации.** Аутентификация, авторизация и администрирование действий пользователей. Методы аутентификации, использующие одноразовые и многоразовые пароли и PIN-коды. Аутентификация, основанная на симметричных и асимметричных алгоритмах. Биометрическая аутентификация пользователей.
6	Технологии защиты межсетевого обмена данными в РАС	**Технологии межсетевых экранов.** Противодействие несанкционированному межсетевому доступу. Функции межсетевого экранирования. Особенности межсетевого экранирования на различных уровнях модели OSI. Установка и конфигурирование межсетевых экранов. Критерии оценки межсетевых экранов. Обзор современных межсетевых экранов. **Технологии защищенных виртуальных сетей.** Способы создания защищенных виртуальных каналов. Туннелирование на канальном уровне. Защита виртуальных каналов на сетевом уровне. Построение защищенных виртуальных сетей на сеансовом уровне. Организация безопасного удаленного доступа. Обзор средств построения защищенных виртуальных сетей. Построение защищенных виртуальных сетей на базе маршрутизаторов, межсетевых экранов, специализированного программного обеспечения, специализированных аппаратных средств.
7	Технологии обнаружения вторжений в РАС. Управление сетевой безопасностью	**Анализ защищенности и обнаружения атак.** Концепции адаптивного управления безопасностью. Технологии анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности операционных систем (ОС). Технологии обнаружения атак. Методы анализа сетевой информации. Классификация систем обнаружения атак. Методы реагирования. **Защита от вирусов в РАС.** Компьютерные вирусы и проблемы антивирусной защиты. Основные каналы распространения вирусов и других вредоносных программ. Антивирусные программы и комплексы. Построение системы антивирусной защиты РАС. **Методы управления средствами сетевой безопасности РАС.** Задачи управления системой сетевой безопасности. Архитектура управления средствами сетевой безопасности. Функционирование системы управления средствами безопасности. Аудит и мониторинг безопасности. Стандарты, используемые при проведении аудита. Анализ рисков и управление

		рисками. Программные средства, используемые для анализа и управления рисками.
8	Построение и организация функционирования комплексных систем защиты информации в РАС	**Построение комплексных систем защиты информации.** Концепция создания защищенных РАС. Этапы создания комплексной системы защиты информации (КСЗИ). Моделирование КСЗИ. Выбор показателей эффективности и критериев оптимальности КСЗИ. Математическая постановка задачи разработки КСЗИ. Подходы к оценке эффективности КСЗИ. Создание организационной структуры КСЗИ. **Организация функционирования комплексных систем защиты информации.** Пути и проблемы практической реализации концепции комплексной защиты информации. Применение КСЗИ. Техническая эксплуатация КСЗИ.

4. Примерный перечень контрольных вопросов для самостоятельной работы.

В рамках освоения программы повышения квалификации обучающегося выполняет самостоятельную работу по подготовке к аттестации.

1. Основные составляющие информационной безопасности.
2. РАС как объекты обработки и защиты информации.
3. Основные понятия защиты информации и информационной безопасности.
4. Технологии распределенной обработки информации.
5. Задачи, решаемые на законодательном, процедурном и административном уровнях информационной безопасности.
6. Особенности защиты информации в РАС.
7. Подтверждение подлинности информации, получаемой по коммуникационной подсети.
8. Модели защиты информации в РАС.
9. Роль стандартов информационной безопасности.
10. Организационное обеспечение информационной безопасности.
11. Сертификация и аттестация в области защиты информации.
12. Содержание основных законов РФ в области информационной безопасности.
13. Каналы утечки речевой информации.
14. Механические системы защиты в задачах информационной безопасности РАС.
15. Системы оповещения. Системы опознавания.
16. Защита средств связи и телекоммуникаций.
17. Методы криптографического преобразования данных.
18. Разграничение и контроль доступа к информации.
19. Симметричные и асимметричные алгоритмы шифрования.
20. Защита электронного документооборота с использованием электронной цифровой подписи.
21. Функции межсетевых экранов.
22. Персональные и распределенные межсетевые экраны.
23. Основные понятия и функции виртуальных защищенных сетей.
24. Достоинства технологий виртуальных защищенных сетей.
25. Основные каналы распространения вирусов и других вредоносных программ.
26. Антивирусные программы и комплексы.
27. Анализ защищенности и обнаружения атак.

28. Методы управления средствами сетевой безопасности РАС.
29. Программные средства, используемые для анализа и управления рисками.
30. Выбор показателей эффективности и критериев оптимальности комплексной системы защиты информации.

5. Учебно-методическое, информационное и материально-техническое обеспечение

а) 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 межсетевого 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»

б) Информационное обеспечение

Ресурсы информационно-телекоммуникационной сети Интернет:

- http://www.anti-malware.ru/
- http://download.live.com/familysafety
- ligainternet.ru
- http://www.citforum.ru/security/

Программное обеспечение, являющееся частью электронной информационно-образовательной среды и базирующееся на телекоммуникационных технологиях:

- компьютерные обучающие программы.
- тренинговые и тестирующие программы.
- интеллектуальные роботизированные системы оценки качества выполненных работ.

- Роботизированные системы для доступа к компьютерным обучающим, тренинговым и тестирующим программам:

- ИС «Комбат»;
- ИС «ЛиК»;
- ИР «КОП»;
- ИИС «Каскад».

в) Материально-техническое обеспечение

- сервера на базе MS SQL Server, файловый сервер с электронным образовательным ресурсом, базами данных;
- компьютеры с выходом в сеть Internet;
- сайт «Личная студия» с возможностью работы с электронным образовательным ресурсом;
- электронные библиотечные ресурсы.

Учебный кабинет этаж № 1, помещение №103:

- Письменный стол преподавателя – 1 шт.
- Стул преподавателя – 1 шт.
- Стул-парта – 4 шт.
- Стулья – 4 шт.
- Стенка-стеллаж – 1 шт.
- Шкаф – 1 шт.
- Вешалка – 1 шт.
- Информационная система «Исток» - для слабослышащих
- Клавиатура Брайля – 1 шт.
- Ноутбук с функцией цифрового диктофона – 1 шт.
- Копировальный аппарат – 1 шт.
- Стационарный компьютер – 4 шт.

Учебный кабинет этаж № 3, помещение № 315:

- Письменный стол преподавателя - 1 шт.
- Стул преподавателя - 1 шт.
- Стулья - 6 шт.
- Шкаф - 1 шт.
- Доска ученическая - 1 шт.
- Стол-парта - 6 шт.
- Стенка стеллаж - 1 шт
- Вешалка -1 шт.

6. Методические рекомендации по организации изучения дисциплины

Освоение дополнительной профессиональной программы - программы повышения квалификации проводится с применением электронного обучения и дистанционных образовательных технологий. Для планомерного изучения дисциплин обучающиеся знакомятся с учебным планом программы. Имеют календарный учебный график изучения дисциплин. Имеют примерные вопросы для самостоятельной работы, промежуточной аттестации, пример творческих заданий, список литературы.