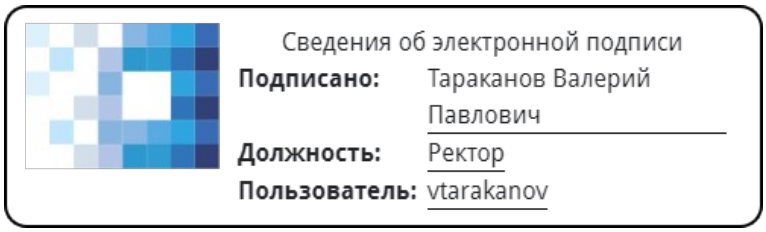
Частное учреждение дополнительного профессионального образования
«Институт цифрового образования»
ЧУ ДПО ИЦО

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 № 3.2

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Москва, 2023 год

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

1. Цели и задачи дисциплины

Цель дисциплины – ознакомить слушателей с наиболее важными сервисами и механизмами защиты информации, с проблемами информационной безопасности в компьютерных сетях.

Задачи дисциплины:

- анализ угроз сетевой безопасности и обеспечение информационной безопасности сетей;
- технологии защиты межсетевого обмена и обнаружения вторжений;
- управление сетевой безопасностью.

2. Планируемые результаты обучения по дисциплине:

В результате изучения дисциплины обучающийся должен

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. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Проблемы информационной безопасности сетей	**Анализ угроз сетевой безопасности.** Введение в сетевой информационный обмен. Проблемы безопасности сетей. Причины уязвимости компьютерных сетей. Показатели и методы оценки уязвимости информации в компьютерных сетях. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей. **Обеспечение информационной безопасности сетей.** Способы обеспечения информационной безопасности. Защита информации при межсетевом взаимодействии. Криптографические протоколы, используемые для защиты технологии клиент-сервер. Защита информации в Web-технологиях. Основные схемы сетевой защиты на базе межсетевых экранов. Защита электронной почты. **Обеспечение Интернет-безопасности с помощью стандартных средств операционных систем.** Угрозы безопасности ОС. Понятие защищенности ОС. Основные функции подсистемы защиты ОС. Защита от Web-угроз. Защита от атак из Интернета. Настройка системы защиты ОС.

2	Технологии защиты межсетевого обмена	**Построение защищенных виртуальных сетей VPN.** Основные понятия и функции сетей VPN. Варианты построения виртуальных защищенных сетей. Средства обеспечения безопасности сетей VPN. Классификация сетей VPN. Основные варианты архитектуры сетей VPN. Достоинства применения технологий VPN. **Защита на канальном, сеансовом, сетевом уровнях.** Протоколы формирования защищенных каналов на канальном уровне: протокол PPTP, протокол L2TP. Протоколы формирования защищенных каналов на сеансовом уровне: протоколы SSL/TSL, протокол SOCKS. Защита беспроводных сетей. Защита на сетевом уровне – протокол IPSec. Архитектура средств безопасности IPSec. Особенности реализации средств IPSec. **Инфраструктура защиты на прикладном уровне.** Управление идентификацией и доступом. Организация защищенного удаленного доступа. Протоколы аутентификации удаленных пользователей. Централизованный контроль удаленного доступа. Протокол Kerberos. Инфраструктура управления открытыми ключами PKI.
3	Технологии обнаружения вторжений. Управление сетевой безопасностью	**Анализ защищенности и обнаружение атак.** Технологии анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности ОС. Технологии обнаружения атак. Методы анализа сетевой безопасности. Системы обнаружения атак. Методы реагирования на угрозу безопасности информации. Стандарты, используемые при проведении аудита. Анализ рисков и управление рисками. Программные средства, используемые для анализа и управления рисками. **Методы управления средствами сетевой безопасности.** Задачи управления системой сетевой безопасности. Архитектура управления средствами сетевой безопас-ности. Функционирование системы управления средствами безопасности. Аудит и мониторинг безопасности.

4. Примерный перечень контрольных вопросов для самостоятельной работы.

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

1. Основные классы угроз информационной безопасности при подключении к Интернет.
2. Проблемы безопасности сетей.
3. Компьютерные преступления в кредитно-финансовой и экономической сферах, совершаемые через Интернет.
4. Причины уязвимости Интернет.
5. Понятие интрасети и задачи ее защиты.
6. Удаленные атаки на интрасети.

7. Классические методы взлома интрасетей.
8. Сетевые вирусы в интрасетях.
9. Отечественные и зарубежные средства предотвращения, выявления и ликвидации последствий вирусных атак.
10. Назначение и функции подсистемы управления доступом интрасети.
11. Защита архитектуры клиент – сервер.
12. Защита на уровне приложений для архитектуры клиент – сервер.
13. Защита хостов в интрасети.
14. Средства анализа защищенности операционных систем.
15. Защита каналов связи.
16. Программные и аппаратные межсетевые экраны.
17. Основные компоненты межсетевых экранов.
18. Протоколы Интернета со встроенными возможностями шифрования.
19. Серверы аутентификации в Интернете.
20. Основные понятия и функции сетей VPN.
21. Достоинства применения технологий VPN.
22. Протоколы формирования защищенных каналов на сеансовом уровне.
23. Стандарты, используемые при проведении аудита.
24. Задачи управления системой сетевой безопасности.
25. Защита беспроводных сетей.

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

а) 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. **Метелица Н.Т.** Вычислительные сети и защита информации [Электронный ресурс]: учебное пособие/ Метелица Н.Т.— Электрон. текстовые данные.— Краснодар: Южный институт менеджмента, 2017.— 48 с.— http://www.iprbookshop.ru/25962.— 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. **Борисова И.В.** Цифровые методы обработки информации [Электронный ресурс]: учебное пособие/ Борисова И.В.— Электрон. текстовые данные.— Новосибирск: Новосибирский государственный технический университет, 2018.— 139 c.— http://www.iprbookshop.ru/45061.— 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.