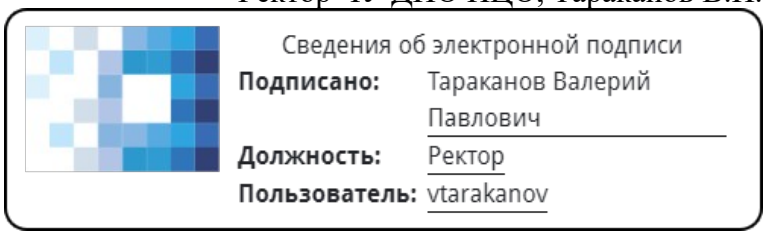
Частное учреждение дополнительного профессионального образования
«Институт цифрового образования»
ЧУ ДПО ИЦО

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 ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«ЦИФРОВАЯ БЕЗОПАСНОСТЬ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ»

Приложение № 3.4

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЦИФРОВАЯ БЕЗОПАСНОСТЬ

Москва, 2023 год

Содержание:

ЦИФРОВАЯ БЕЗОПАСНОСТЬ

1. Цели и задачи дисциплины

Цель дисциплины – ознакомить обучающихся с наиболее важными сервисами и механизмами защиты информации, с проблемами цифровой безопасности компьютеров и компьютерных сетей.

Задачи дисциплины:

- познакомить обучающихся с основами цифровой безопасности, видами угроз информационной безопасности, их классификаций, правовыми основами информационной безопасности, механизмами защиты информации;
- получить представление о способах предотвращения удаленных атак на информационные системы, программно-аппаратных средствах обеспечения безопасности информационных сетей;
- привить умения и навыки безопасной работы в сети Интернет.

2. Планируемые результаты обучения по дисциплине:

В результате изучения дисциплины обучающийся должен

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. Содержание дисциплины

№	Наименование модуля	Содержание модуля
1	Цифровая безопасность	**Основы цифровой безопасности**. Основные понятия и определения. Классификация угроз информационной безопасности. Вредоносные программы. Анализ угроз информационной безопасности. Нормативно-правовая база в области цифровой безопасности. Механизмы защиты информации. Инженерно-технические средства защиты

№	Наименование модуля	Содержание модуля
		информации. Безопасная работа в информационной системе. Антивирусные средства защиты информации. Криптографические методы защиты информации. Способы предотвращения удаленных атак на информационные системы. Программно-аппаратные средства обеспечения безопасности информационных сетей. Безопасная работа в сети Интернет. Сбор данных о пользователе. Безопасная работа с веб-браузером. Безопасность при работе с электронной почтой и с системами обмена сообщениями. Безопасная работа с банковскими картами и платежными системами. Безопасность в социальных сетях.

4. Примерный перечень контрольных вопросов для самостоятельной работы.

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

1. Что такое цифровая безопасность, каковы ее основные аспекты?
2. Приведите определение понятий «конфиденциальность информации», «целостность информации», «доступность информации».
3. Выделите основные классы угроз информационной безопасности при подключении к Интернету.
4. В чем различие идентификации и аутентификации пользователей?
5. Назовите основные способы аутентификации. Какой из этих способов является, по вашему мнению, наиболее эффективным?
6. Были ли в Вашей практике случаи попыток несанкционированного получения информации? Охарактеризуйте проявившийся в каждом конкретном случае канал несанкционированного доступа и оцените возможную уязвимость информации.
7. Каковы основные признаки заражения компьютера?
8. Какая программа является вредоносной?
9. Чем отличается симметричная криптографическая система от асимметричной?
10. Какие классы антивирусных программ вам известны?
11. Почему, по вашему мнению, действительно эффективная защита информации может быть обеспечена только при комплексном системном подходе к решению этой проблемы? В чем заключается комплексность?
12. С чем, по Вашему мнению, связана необходимость организационно-правового обеспечения защиты информации?
13. Приведите примеры инженерно-технических средств защиты информации.
14. Опишите правила безопасной работы в информационной системе.
15. Опишите известные Вам методы обнаружения вирусов.
16. Каково назначение стеганографических систем?
17. Приведите примеры удаленных атак.
18. Перечислите известные Вам способы предотвращения удаленных атак.
19. Каковы функции межсетевого экрана?
20. Опишите правила безопасной работы в сети Интернет.
21. По каким признакам можно распознать мошеннический сайт?
22. Каким образом настраиваются параметры конфиденциальности в Вашем браузере?
23. Как можно обеспечить безопасность при работе с электронной почтой?
24. Как можно обеспечить безопасность при работе в социальных сетях?

25. Опишите правила безопасной работы с банковскими картами и платежными системами.

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

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.

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».

Материально-техническое обеспечение

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

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.