Государственное бюджетное профессиональное образовательное учреждение
«Южно-Уральский государственный колледж»

МЕТОДИЧЕСКАЯ РАЗРАБОТКА
Лекция

Составляющие информационной безопасности

Специальность: 09.02.07 Информационные системы и программирование

ОП.13 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Разработал преподаватель

Чераева О.А.

РАССМОТРЕНО:

На заседании ПЦК

«Информационных технологий»

от 25.09.23 протокол № 2

Председатель
ПЦК _____/Н.А.Назарова/

Челябинск, 2023

Методическая разработка учебного занятия

Учебная дисциплина: ОП.13 Информационная безопасность

Специальность: 09.02.07 Информационные системы ипрограммирование

Курс: 2

Тема занятия: составляющие информационной безопасности

Вид занятия: лекция

Мотивация темы: необходимость знания составляющих информационной безопасности позволяют определить дальнейшие способы защиты информации, и устранение последствий нарушений.

Продолжительность занятия: 90 минут

Место проведения занятия: лекционная аудитория

Формирование профессиональной компетенции (ПК 7.5): проводить аудит систем безопасности баз данных и серверов с использованием регламентов по защите информации.

Цели занятия:

Обучающая*:*

- сформировать целостное представление о составляющих информационной безопасности
- изучить различные модели составляющих информационной безопасности.

Развивающая:

- развивать память и логическое мышление;
- развивать речевую активность путем обогащения и усложнения словарного запаса;
- развивать коммуникативные навыки и навыки самоконтроля.

Воспитательная:

- вызвать интерес к изучению информационных технологий;
- возбудить готовность решать задачи самостоятельно.

По итогам обучения обучающийся должен:

Знать:

– аспекты информационной безопасности;

– модели информационной безопасности.

Уметь: приводить примеры аспектов информационной безопасности.

Методы обучения, методические приемы: словесный; наглядный; практический.

Внутридисциплинарные связи: аспекты информационной безопасности.

Междисциплинарные связи: ОП. 11 Компьютерные сети, ОП. 08 Основы проектирования баз данных, МДК.09.0 Обеспечение безопасности веб-приложений

Учебное оборудование (оснащение) занятия: ПК; мультимедийный проектор.

Методическое обеспечение занятия: опорный конспект, презентация.

Критерии и методы диагностики эффективности занятия: рефлексия.

ХОД УРОКА

1. Вступительная часть занятия. Здравствуйте, ребята! Садитесь. Староста, сообщите, пожалуйста, кто отсутствует на занятии.

Сегодня мы с вами познакомимся с аспектами информационной безопасности (Презентация - Приложение 1).

Цель занятия: ознакомиться с аспектами информационной безопасности, основными моделями угроз информационной безопасности.

2. Актуализация опорных знаний.

На предыдущем занятии мы познакомились с основными понятиями информационной безопасности теперь мы переходим к следующей теме «Аспекты информационной безопасности»

3. Изложение нового материала.

Одной из первых и наиболее популярных по сей день моделей безопасности является модель, предложенная Джерри Зальцером и Майклом Шрёдером. Авторы постулировали, что все возможные нарушения информационной безопасности всегда могут быть отнесены по меньшей мере к одной из трех групп: нарушения конфиденциальности, нарушения целостности, нарушения доступности. *(Слайд 4)*

Информационная система находится в состоянии безопасности, если она защищена от нарушений конфиденциальности, целостности и доступности, где:

1. конфиденциальность (confidentiality) — это состояние ИС, при котором информационные ресурсы доступны только тем пользователям, которым этот доступ разрешен;

2. целостность (integrity) — это состояние системы, при котором информация, хранящаяся и обрабатываемая этой И С, а также процедуры обработки информации не могут быть изменены, удалены или дополнены неавторизованным образом;

3. доступность (availability) — это состояние системы, при котором услуги, оказываемые системой, могут гарантированно и с приемлемой задержкой быть предоставлены пользователям, имеющим на это право

Некоторые виды нарушений безопасности могут быть приведены к модели КЦД только путем расширительного толкования основополагающих понятий конфиденциальности, доступности и целостности.

С момента публикации статьи Зальцера и Шредера, информационные системы и среда, в которой они функционируют, претерпели значительные изменения. Появились новые типы нарушений, которые намного труднее трактовать в терминах КЦД. Одной из наиболее популярных альтернатив триаде КЦД является так называемая гексада Паркера. (слайд 9). Российский государственный стандарт ГОСТ 13335-1:2006 дает определение информационной безопасности на основе гексады Паркера (слайд 11).

Модель STRIDE — это модель угроз, разработанная в Microsoft для выявления компьютерная безопасность угрозы. Она предоставляет мнемонику для угроз безопасности в шести категориях. (слайд 12). К угрозам относятся:

S пуфинг

T усиление

R раскрытие информации

I раскрытие информации (нарушение конфиденциальности или утечка данных)

D запрос на обслуживание

E повышение привилегий

STRIDE изначально был создан как часть процесса моделирования угроз . STRIDE — это модель угроз, используется для обоснования и поиска угроз для системы. Он используется вместе с моделью целевой системы, которая может быть построена параллельно. Это включает полную разбивку процессов, хранилищ данных, потоков данных и границ доверия.

Сегодня он часто используется экспертами по безопасности, чтобы помочь ответить на вопрос «что может пойти не так в этой системе, над которой мы работаем?»

Каждая угроза — это нарушение желаемого свойства системы:

Угроза Желаемое свойство

Подделка Аутентичность

Подделка Целостность

Отказ Отсутствие отказа от авторства

Раскрытие информации Конфиденциальность

Отказ о f Сервис Доступность

Повышение привилегий Авторизация

4. Закрепление изученного материала

(Слайд 14)

Приведите примеры доступности информации.

Приведите примеры целостности информации.

Приведите примеры конфиденциальности информации.

Каким образом взаимосвязаны между собой составляющие «информационной безопасности»? Приведите собственные примеры.

5. Проверка усвоения нового материала

А теперь вспомним, что нового мы узнали сегодня:

- Какие основные аспекты информационной безопасности мы изучили? *(целостность, конфиденциальность, доступность)?*
- Какие модели информационной безопасности вы знаете? *(Модель CIA, Гексада Паркера, Модель STRIDE)*

6. Выдача домашнего задания. Повторить лекцию и подготовиться к опросу.

7. Рефлексия

Преподаватель вместе со студентами подводят итоги урока, формируют рефлексивные навыки с помощью опорного алгоритмасамоанализа:

- на уроке я узнал...
- на уроке я понял...
- на уроке я научился...
- лучше всего на занятии у меня получалось...
- основные трудности были... Спасибо за урок. До свидания!

Методическое обеспечение занятия:

1. Нестеров, С. А. Основы информационной безопасности: учебник для СПО / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022. — 324 с.

2. Партыка, Т. Л. Информационная безопасность: учеб. пособие / Т.Л.

Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва: ФОРУМ: ИНФРА-М, 2021. — 432 с

3. Прохорова, О. В. Информационная безопасность и защита информации / О. В. Прохорова. — 4-е изд., стер. — Санкт-Петербург: Лань, 2023. — 124 с

4. Чераева О.А., Подин М.С. Информационная безопасность: электронное учебное пособие / О.А., Чераева, М.С. Подин. — Текст: электронный // Система электронного обучения ЮУГК. — URL: https://els.ecol.edu.ru/course/view.php?id=93 (дата обращения 30.09.2023). — Режим доступа: для авториз. Пользователей

5. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. — Москва: ФОРУМ: ИНФРА-М, 2021. — 416 с

Технологическая карта урока

ФИО педагогического работника: Чераева Ольга Александровна

Тип занятия: изучения и первичного закрепления новых знаний и способов деятельности

Дисциплина: ОП.13 Информационная безопасность

Тема: Составляющие информационной безопасности

Нормативные документы:

1) ФГОС СПО по специальности 09.02.07 Информационные системы и программирование

2) Учебная программа ОП.13 Информационная безопасность

С целью овладения профессиональными компетенциями обучающихся в ходе освоения дисциплины должен:

Уметь: приводить примеры аспектов информационной безопасности.

Знать:

— аспекты информационной безопасности;

— модели информационной безопасности.

Цель:

Обучающая: сформировать целостное представление о составляющих информационной безопасности; изучить различные модели составляющих информационной безопасности.

Развивающая: развивать память и логическое мышление; развивать речевую активность путем обогащения и усложнения словарного запаса; развивать коммуникативные навыки и навыки самоконтроля.

Воспитательная: вызвать интерес к изучению информационных технологий; возбудить готовность решать задачи самостоятельно.

Форма занятия: комбинированный урок

Межпредметные связи: ОП. 11 Компьютерные сети, ОП. 08 Основы проектирования баз данных, МДК.09.0 Обеспечение безопасности веб-приложений

Структура занятия:

1. Сообщение темы и цели урока - 2 мин
2. Актуализация опорных знаний – 10 мин

3. Изложение нового материала - 45 мин
4. Закрепление изученного материала – 10 мин
5. Проверка усвоения нового материала - 5 мин
6. Подведение итогов занятия – 5 мин
7. Выдача домашнего задания - 2 мин
8. Рефлексия – 5 мин

Используемая литература:

1. Нестеров, С. А. Основы информационной безопасности: учебник для СПО / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022. — 324 с.

2. Партыка, Т. Л. Информационная безопасность: учеб. пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва: ФОРУМ: ИНФРА-М, 2021. — 432 с

3. Прохорова, О. В. Информационная безопасность и защита информации / О. В. Прохорова. — 4-е изд., стер. — Санкт-Петербург: Лань, 2023. — 124 с

4. Чераева О.А., Подин М.С. Информационная безопасность: электронное учебное пособие / О.А., Чераева, М.С. Подин. — Текст: электронный // Система электронного обучения ЮУГК. — URL: https://els.ecol.edu.ru/course/view.php?id=93 (дата обращения 30.09.2023). — Режим доступа: для авториз. Пользователей

5. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. — Москва: ФОРУМ: ИНФРА-М, 2021. — 416 с

Ход урока

Этапы	Цель	Деятельность преподавателя	Деятельность студента	Результат
1. Сообщение темы и цели урока	Организация группы на урок Мотивация учебной деятельности	Приветствие обучающихся, проверка присутствующих	Приветствие преподавателя, подготовка к уроку	Готовность группы к уроку
Метод - словесный Методический приём-информационно-сообщающий Форма обучения - групповая Средства обучения - ПК, проектор				
2. Актуализация опорных знаний	Проверка знаний и умений обучающихся, актуализация знаний	Задает вопросы по предыдущей теме	Отвечают на вопросы преподавателя	Готовность группы к восприятию новых знаний
Метод – словесный Методический приём - информационно-сообщающий Форма обучения – групповая Средства обучения - ПК, проектор				
3. Изложение нового материала	Обеспечение восприятия, первичного запоминания знаний и способов деятельности	Предъявление информации.	Восприятие и осознание знаний, их запоминание	Запись и первичное осмысление новых знаний.
Метод - Объяснительно-иллюстративный Методический приём- информационно-сообщающий Форма обучения - групповая Средства обучения – ПК, проектор				

4. Закрепление изученного материала	Обеспечение осмысления способов деятельности.	Организация действий учащихся.	Приводят примеры нарушения аспектов информационной безопасности	Активные действия учащихся по пройденному материалу
Метод – репродуктивный Методический приём - выполнение задания с опорой на материал презентации Форма обучения - индивидуальная Средства обучения – ПК, проектор				
5. Проверка усвоения нового материала	Проверка усвоения новых знаний	Задает вопросы по изученной теме: Какие основные аспекты информационной безопасности мы изучили? Какие модели информационной безопасности вы знаете?	Отвечают на вопросы преподавателя	Адекватность самооценки обучающихся оценке преподавателя
Метод - словесный Методический прием – опрос по изученным функциям Форма контроля – фронтальная Средства обучения – ПК, проектор				
6. Подведение итогов занятия	Уточнение и разъяснение сложных моментов в новых знаниях	Поясняет особо трудные моменты лекции, выставление оценок	Задают вопросы преподавателю	Осмысление новых знаний
Метод - словесный Методический приём – информационно-сообщающий Форма обучения- фронтальная Средства обучения – ПК, проектор				

7. Выдача домашнего задания	Установление уровня осознанности выполнения домашнего задания	Озвучение требований к изучению пройденного материала	Осознание выполнения домашнего задания	Правильность выполнения домашнего задания
Метод - словесный Методический приём - запись на экране ПК Форма обучения - фронтальная Средства обучения - ПК, проектор				
8. Рефлексия	Мобилизация обучающихся на рефлексию своей деятельности	Выявляет сложности в освоении изученного материала.	Задают вопросы и отвечают на вопросы преподавателя	Открытость обучающихся в осмыслении своих действий и в их самооценке
Метод- словесный Методический приём - обобщение и выводы Форма обучения- фронтальная Средства обучения – ПК				