Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»

УТВЕРЖДАЮ
Заместитель директора
по учебно-производственной работе
_____ О.В. Фомичева
«__» _____ 2023 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по выполнению внеаудиторной самостоятельной работы обучающихся
по МДК.03.05 Основы криптографической защиты данных
ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

для специальности

09.02.06 Сетевое и системное администрирование

Санкт-Петербург
2023 г.

Методические рекомендации рассмотрены на заседании методического совета СПб ГБПОУ «АУГСГиП»
Протокол № 2 от «29» 11 202 3 г.

Методические рекомендации одобрены на заседании цикловой комиссии информационных технологий
Протокол № 4 от «24» 11 202 3 г.

Председатель цикловой комиссии: Караченцева М.С. _____

Разработчики: преподаватели СПб ГБПОУ «АУГСГиП»

С О Д Е Р Ж А Н И Е

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая тетрадь по организации внеаудиторной самостоятельной работы разработана с целью оказания помощи обучающимся при МДК.03.05 Основы криптографической защиты данных.

Целью Рабочей тетради по самостоятельной работе является повышение эффективности учебного процесса, в том числе благодаря самостоятельной работе, в которой обучающийся становится активным субъектом обучения, что означает:

- способность занимать в обучении активную позицию;
- готовность мобилизовать интеллектуальные и волевые усилия для достижения учебных целей;
- умение проектировать, планировать и прогнозировать учебную деятельность;
- привычку инициировать свою познавательную деятельность на основе внутренней положительной мотивации;
- осознание своих потенциальных учебных возможностей и психологическую готовность составить программу действий по саморазвитию.

Рабочая тетрадь предназначена для самостоятельной работы над закреплением полученных знаний и умений во внеаудиторное время.

В Рабочей тетради приведен алгоритм выполнения различных видов самостоятельной работы, предусмотренной рабочей программой МДК.03.05 Основы криптографической защиты данных.

Внеаудиторная самостоятельная работа по МДК.03.05 Основы криптографической защиты данных выполняется обучающимся по заданию преподавателя, но без его непосредственного участия.

Проверка выполнения заданий в Рабочей тетради осуществляются преподавателем по мере изучения тем. Результаты выполнения обучающимися самостоятельной работы оцениваются преподавателем и регистрируются в специальном журнале.

1. **ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ И НОРМЫ ВРЕМЕНИ ДЛЯ РЕАЛИЗАЦИИ ФОРМ САМОСТОЯТЕЛЬНОЙ РАБОТЫ**

Таблица 1

№ п/п	**Вид (форма выполнения) самостоятельной работы**	**Количество часов**
1.	Самостоятельная работа №1	4
2.	Самостоятельная работа №2	4
3.	Самостоятельная работа №3	4
4.	Самостоятельная работа №4	4
5.	Самостоятельная работа №5	4

2. МЕТОДИКА ВЫПОЛНЕНИЯ ОТДЕЛЬНЫХ ВИДОВ РАБОТ

Самостоятельная работа № 1

ЗАДАНИЕ:

Создайте презентацию по теме. При выполнении презентации необходимо учитывать требования к оформлению учебных презентаций.
Презентация должна содержать:

- титульный слайд с названием учебной дисциплины и темы презентации и фамилии студента;
- 8-10 слайдов, раскрывающих сущность темы: учебный материал на слайдах должен быть представлен схематично с использованием функции SmartArt;
- на слайдах необходимо представить информацию: понятие спроса и предложения, факторы, влияющие на спрос и предложение, графики спроса и предложения. Привести условие какой- либо задачи по теме и ее решение на следующем слайде;
- слайды не должны быть выполнены с использованием анимации.

Тему презентации выберите из следующего списка:

1. Тайнопись в античном мире: шифры «Сциталь», Цезаря, Полибия и др.
2. Криптография в странах средневекового арабского Востока.
3. Криптография в средневековой Западной Европе: шифры Тритемия, Кардано, Порты и др.
4. Защита документов, тайнопись и тайные коммуникации в Византии и странах Восточной Европе (IV—XV вв.).
5. Опишите формы византийской тайнописи.
6. Тайнопись в Древней и Средневековой Руси (XIII—XVII вв.): «Пермская азбука», «Простая и мудрая литорея», «Фиоть и Хвиоть», «Уголки», «Тарабарщина» и др.
7. Европейская криптография в Новое время: шифр Виженера, «латинские квадраты», большой и малый шифры Наполеона и др.
8. Становление математических основ криптографии (XVIII—XIX вв.).
9. Криптография в России (XVIII—XIX вв.).
10. Начало формирования научных приемов защиты информации во второй половине XIX — начале XX в.
11. Создание совершенно стойкого шифра. «Одноразовый шифроблокнот» и его применения.
12. История создания и применения роторных шифровальных машин.
13. Разработка теоретико-информационного подхода к обеспечению стойкости криптосистем Клодом Шенноном и его научной школой.
14. Этапы развития криптографии во второй половине XX в. в их связи с историей информационных технологий.
15. Практически стойкие шифры (1960—1970-е гг.).
16. Развитие математических основ «компьютерной» криптографии во второй половине XX в.
17. Зарождение асимметричной криптографии в 70—80-е гг. XX в.
18. Разработка тсорстико-сложностного подхода к обеспечению стойкости криптосистем в 80—90-е гг. XX в.
19. Пути развития современной криптологии (конец XX — начало XXI в.).'
20. История стеганографии.
21. История защиты от фальсификации денежных знаков, ценных бумаг и документов.

Самостоятельная работа № 2

ЗАДАНИЕ:

1. Прочитайте конспект по данной теме в рабочей тетради.
2. Зашифровать шифром Цезаря предложения (ключ 3)
   - *Байты сохраняются в виде файлов*
   - *ФИО*

Самостоятельная работа № 3

ЗАДАНИЕ:

Выполняется совместно двумя студентами. Произвести расчет ключа.

1. Прочитайте конспект по данной теме в рабочей тетради.
2. Совместно с удалённой стороной устанавливать открытые параметры p и g (обычно значения p и g генерируются на одной стороне и передаются другой), где p является случайным простым числом (p-1)/2 также должно быть случайным простым числом (для повышения безопасности) g является первообразным корнем по модулю p.
3. Вычислить открытый ключ A, используя преобразование над закрытым ключом

A = ga mod p для каждого студента.

4. Обменяться открытыми ключами с удалённой стороной.
5. Вычислить общий секретный ключ K, используя открытый ключ удаленной стороны B и свой закрытый ключ a

K = Ba mod p

K получается равным с обеих сторон, потому что:

Ba mod p = (gb mod p)a mod p = gab mod p = (ga mod p)b mod p = Ab mod p

6. Сравнить общие ключи.

Самостоятельная работа № 4

ЗАДАНИЕ:

Создайте презентацию по теме. При выполнении презентации необходимо учитывать требования к оформлению учебных презентаций.

Презентация должна содержать:

- титульный слайд с названием учебной дисциплины и темы презентации и фамилии студента;
- 8-10 слайдов, раскрывающих сущность темы: учебный материал на слайдах должен быть представлен схематично с использованием функции SmartArt;
- на слайдах необходимо представить информацию: понятие спроса и предложения, факторы, влияющие на спрос и предложение, графики спроса и предложения. Привести условие какой- либо задачи по теме и ее решение на следующем слайде;
- слайды не должны быть выполнены с использованием анимации.

Тему презентации выберите из следующего списка:

1. Пластиковые карты.
2. Суррогатные платежные средства в Internet.
3. Расчеты пластиковыми карточками в Internet.
4. Электронные кошелки в Internet.

5. Цифровые деньги.
6. Биткойн.

Самостоятельная работа № 5

ЗАДАНИЕ:

1. Прочитайте материал по данной теме в учебном пособии.
2. Дополните конспект темы в рабочей тетради, ответами на следующие вопросы:
   - Назовите основные отличия кодовых систем от криптографических.
   - Дайте характеристику общедоступным кодовым системам.
   - Перечислите основные способы обеспечения конфиденциальности информации в секретных кодовых системах.