

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



**УТВЕРЖДАЮ**  
Заместитель директора  
по учебно-производственной работе  
О.В. Фомичева  
декабря 2023 г.

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ  
по выполнению внеаудиторной самостоятельной работы обучающихся  
по учебной дисциплине  
ОП.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

для специальности  
**10.02.05 Обеспечение информационной безопасности автоматизированных систем**

Санкт-Петербург  
2023 г.

Методические рекомендации рассмотрены на заседании методического совета  
СПб ГБПОУ «АУГСГиП»

Протокол № 2 от «29» ноября 2023 г.

Методические рекомендации одобрены на заседании цикловой комиссии общетехнических  
дисциплин и компьютерных технологий

Протокол № 4 от «21» ноября 2023 г.

Председатель цикловой комиссии: Караченцева М.С. \_\_\_\_\_



Разработчики: преподаватели СПб ГБПОУ «АУГСГиП»

## СОДЕРЖАНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА .....	4
1. ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ И НОРМЫ ВРЕМЕНИ ДЛЯ РЕАЛИЗАЦИИ ФОРМ САМОСТОЯТЕЛЬНОЙ РАБОТЫ .....	5
2. МЕТОДИКА ВЫПОЛНЕНИЯ ОТДЕЛЬНЫХ ВИДОВ РАБОТ .....	6
Самостоятельная работа № 1 .....	6
Самостоятельная работа № 3 .....	7
Самостоятельная работа № 4 .....	9
Самостоятельная работа № 5 .....	12

## ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая тетрадь по организации внеаудиторной самостоятельной работы разработана с целью оказания помощи обучающимся при освоении дисциплины «Основы информационной безопасности», предусмотренной Федеральным государственным образовательным стандартом по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

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 дисциплины «Основы информационной безопасности».

Внеаудиторная самостоятельная работа по дисциплине «Основы информационной безопасности» 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

№ п/п	Название раздела или темы	Тема	Количество часов
1.	Тема 1. Критическая информационная инфраструктура (КИИ) РФ	Самостоятельная работа № 1	2
2.	Тема 2. Сущность и понятие информационной безопасности (ИБ), характеристика составляющих ИБ	Самостоятельная работа № 2	2
3.	Тема 3. Информация как объект защиты	Самостоятельная работа № 3	2
4.	Тема 4. Меры по предотвращению угроз. Современные средства и способы обеспечения информационной безопасности	Самостоятельная работа № 4	2
5.	Тема 5. Сертификация и лицензирование	Самостоятельная работа №5	2

## 2. МЕТОДИКА ВЫПОЛНЕНИЯ ОТДЕЛЬНЫХ ВИДОВ РАБОТ

### Самостоятельная работа № 1

Используя справочно-правовую систему, найдите Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и ответьте на вопросы:

1. Кратко сформулируйте обязанности субъекта КИИ:

---

---

---

---

---

---

---

---

---

---

2. В каких случаях производится плановая проверка обеспечения безопасности значимых объектов КИИ?

---

---

---

---

---

---

---

---

---

---

3. В каких случаях может быть проведена внеплановая проверка обеспечения безопасности значимых объектов КИИ?

---

---

---

---

---

---

---

---

---

4. Сформулируйте связь между объектами и субъектами КИИ:

---

---

---

5. Чем компьютерная атака отличается от компьютерного инцидента?

---

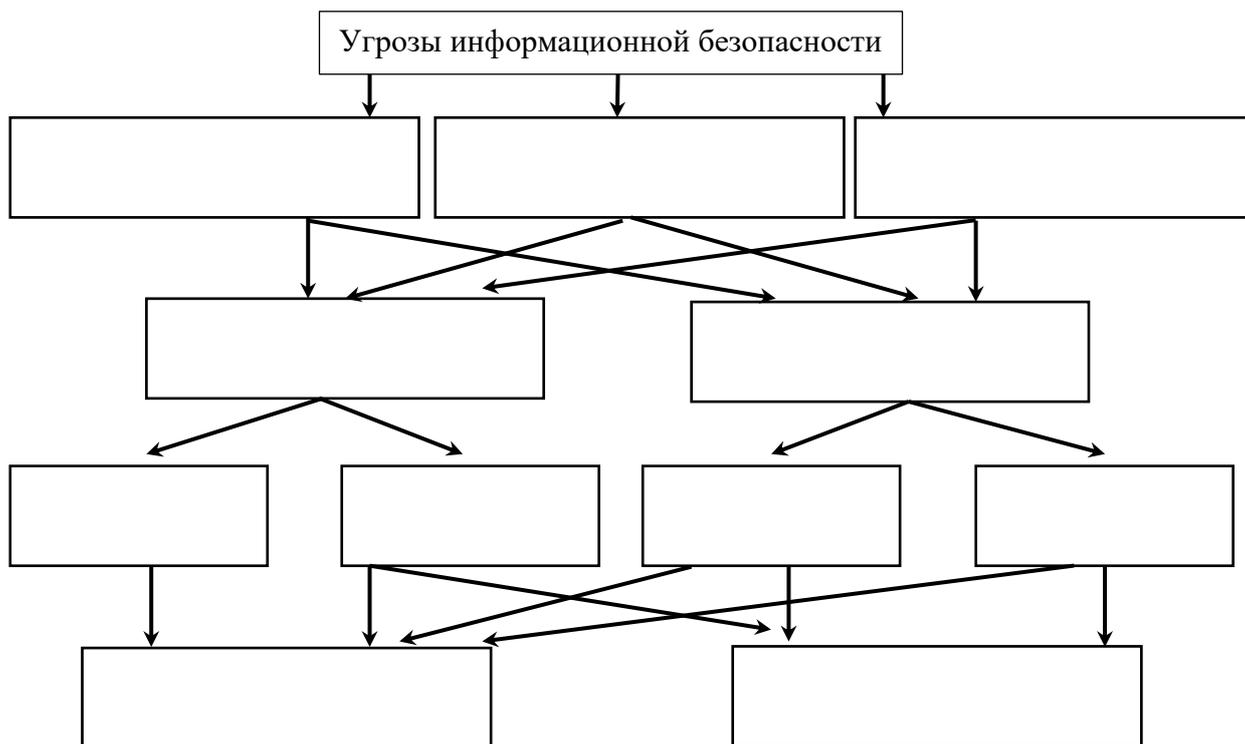
---

---

### **Самостоятельная работа № 3**

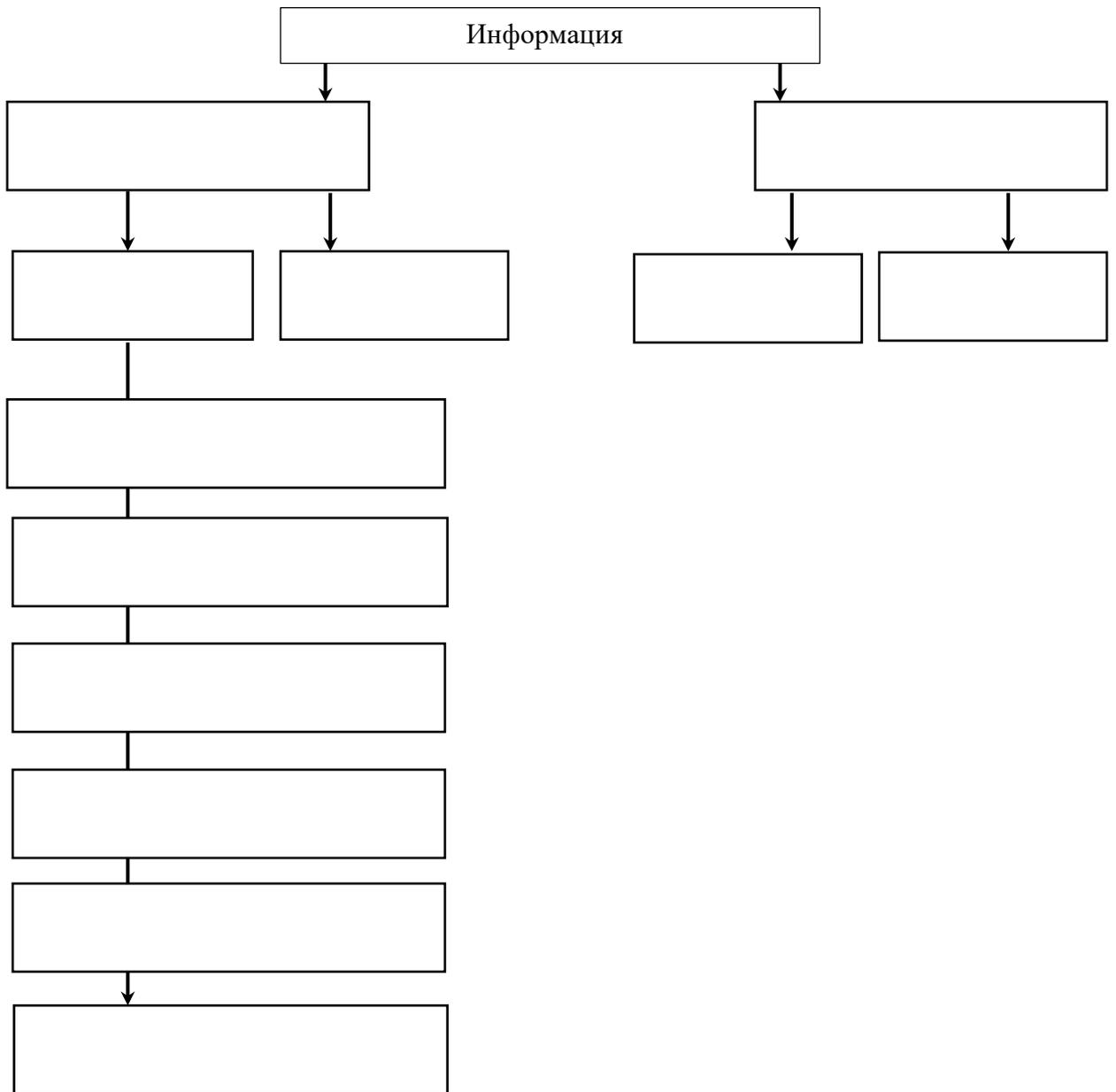
1. Составьте кроссворд, используя 20 основных понятий ИБ.

2. Заполните схему, отражающую виды угроз безопасности информации.



### Самостоятельная работа № 4

1. Заполните схему, отражающую виды информации в зависимости от категории доступа.



2. Используя текст Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации», другие федеральные законы и конспект, заполните таблицу.

Вопрос	Ответ
Какие нормативно-правовые документы могут ограничивать доступ к информации?	
Какая информация предоставляется бесплатно?	
Доступ к какой информации не может быть ограничен?	
Что относится к общедоступной информации?	
Какой ФЗ устанавливает порядок доступа к персональным данным граждан?	
Отнесение сведений к государственной тайне и их засекречивание – это	
Рассекречивание сведений и их носителей – это	

3. Приведите не менее трех примеров информации различных категорий доступа.

Общедоступная информация	
Государственная тайна	
Банковская тайна	
Адвокатская тайна	
Врачебная тайна	
Персональные данные	
Коммерческая тайна	
Тайна следствия	
Тайна изобретения	
Тайна страхования	
Тайна судопроизводства	
Информация, доступ к которой не может быть ограничен	

## Самостоятельная работа № 5

### 1. Ответьте на вопросы:

Назовите подходы к обеспечению ИБ.

Чем различаются фрагментарный и комплексный подход.

Назовите недостатки фрагментарного подхода

Назовите недостатки комплексного подхода

Перечислите направления защиты информации в организации.

Напишите определение правовой защиты

Напишите определение организационной защиты

Что входит в понятие технического направления защиты информации

**2. Заполните таблицу:**

Вид правового документа	Номер правового документа	Название правового документа
Указ Президента РФ	683	
Указ Президента РФ	646	
Федеральный закон	149-ФЗ	
Федеральный закон	187--ФЗ	
Закон РФ	5485	
Федеральный закон	152-ФЗ	
Федеральный закон	63-ФЗ	
Федеральный закон	99-ФЗ	
Приказ ФСТЭК	17	
Приказ ФСТЭК	21	
Приказ Федеральной службы безопасности	378	

### 3. Используя ресурсы сети Интернет, ответьте на вопросы о вредоносном ПО

1. Определите свой вариант с учетом рекомендаций преподавателя.

Вариант 1	Червь Морриса
Вариант 2	ILOVEYOU
Вариант 3	Nimda
Вариант 4	WannaCry

Вариант №

Год создания

Создатель

История появления

Объект заражения

Механизм действия

Размер нанесенного ущерба

### 4. Ответьте на вопросы

Дайте определение НСД

Приведите 3-4 примера реализации несанкционированного доступа:

Перечислите виды защиты от НСД

Какому требованию должен обязательно удовлетворять идентификатор объекта/субъекта?

Перечислите группы методов аутентификации

Для чего нужна многофакторная аутентификация?

Для чего используются модели доступа?

Перечислите виды моделей доступа

На основе каких локальных документов организации строится ролевая модель управления доступом?

Дайте определение вредоносного программного обеспечения

Перечислите виды вредоносного ПО

Дайте определение антивирусного ПО

Перечислите функции антивирусного ПО

Что означает понятие «сигнатура компьютерного вируса»?

Какие требования предъявляются к антивирусному ПО?

Что означает организационный метод защиты от вирусного ПО?

Дайте определение СОВ

Что такое датчик СОВ?

Что такое анализатор?

Перечислите подсистемы СОВ.

В чем отличие СОВ уровня сети и СОВ уровня узла?

Для каких организаций и структур разработаны требования к СОВ?

Сколько существует классов защиты применительно к СОВ?

Сколько профилей защиты разработано для СОВ?