



МЧС РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Уральский институт Государственной противопожарной службы
Министерства Российской Федерации по делам гражданской обороны,
чрезвычайным ситуациям и ликвидации последствий стихийных бедствий»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

**Методические рекомендации для
самостоятельного изучения дисциплины**

Направление подготовки 38.03.04
Государственное и муниципальное управление
(уровень бакалавриата)

Профиль-управление в кризисных ситуациях

Екатеринбург
2020

Информационная безопасность [Текст]: методические рекомендации для самостоятельного изучения дисциплины. Направление подготовки 38.03.04 Государственное и муниципальное управление/ сост. Н.П. Мураев. Екатеринбург: ФГБОУ ВО Уральский институт ГПС МЧС России, 2020. - 7 с.

Автор - составитель: Мураев Н.П., доцент кафедры безопасности в ЧС Уральского института ГПС МЧС России, кандидат педагогических наук.

Методические рекомендации для самостоятельного изучения дисциплины «Информационная безопасность» предназначены для использования в образовательном процессе по направлению подготовки 38.03.04 Государственное и муниципальное управление (профиль - управление в кризисных ситуациях) для обучающихся, пропустивших учебные занятия. Методические рекомендации позволят самостоятельно освоить учебный материал по темам изучаемой дисциплины.

СОДЕРЖАНИЕ

1. Введение	4
2. Тематический план изучения дисциплины	4
ТЕМА 1 Основы государственной политики в области информационной безопасности	5
ТЕМА 2 Основные угрозы информационной безопасности компьютерных систем.....	6
ТЕМА 3 Стратегии, способы и средства защиты информации	6

1. Введение

Целями освоения дисциплины «Информационная безопасность» является:

- приобретение обучающимися необходимых знаний, умений и навыков обеспечения информационной безопасности в системах и процессах государственного и муниципального управления;
- формирование общекультурных навыков работы с информацией, необходимых в профессиональной деятельности государственного и муниципального служащего.

Для достижения указанных целей предусматривается решение следующих основных задач:

- формирование системных знаний об институтах, принципах, нормах, действие которых призвано обеспечить информационную безопасность в государственном и муниципальном управлении;
- ознакомление с основными тенденциями развития государственного и муниципального управления в области информационной безопасности;
- изучение функций и задач современного государственного и муниципального служащего в области информационной безопасности;
- изучение и овладение навыками применения современных методов, моделей и технологий обеспечения информационной безопасности в профессиональной деятельности;
- овладение навыками целостного анализа информационной безопасности в системах и процессах управления.

В соответствии с рабочим учебным планом на изучение дисциплины отводится 72 часа.

В соответствии с рабочим учебным планом на изучение дисциплины отводится 72 часа.

2. Тематический план изучения дисциплины

№ п/п	Наименование тем
1	Основы государственной политики в области информационной безопасности
2	Основные угрозы информационной безопасности компьютерных систем
3	Стратегии, способы и средства защиты информации
Итоговый контроль - зачет	

Тема 1. Основы государственной политики в области информационной безопасности

Изучаемые вопросы:

1. Основные понятия, термины и определения. Классификация объектов и субъектов информации.
2. Основные понятия, термины и определения. Доступ к информации. Разграничение доступа к информации.
3. Основные понятия, термины и определения. Потребительские качества информации.
4. Область применения, основные понятия и подходы Стратегии национальной безопасности Российской Федерации в области информационной безопасности.
5. Область применения, основные понятия и подходы Доктрины информационной безопасности Российской Федерации.
6. Область применения, основные понятия и требования закона «О государственной тайне» в области информационной безопасности.
7. Область применения, основные понятия и требования закона «О коммерческой тайне» в области информационной безопасности.
8. Область применения, основные понятия и требования закона «О персональных данных» в области информационной безопасности.
9. Область применения, основные понятия и требования закона «Об информации, информационных технологиях и о защите информации».
10. Служебная и профессиональная тайна.

При освоении темы №1 обучающийся должен изучить следующие нормативно-правовые акты и рекомендуемую литературу:

1. Указ Президента Российской Федерации от 12 мая 2009 года № 537 «О стратегии национальной безопасности Российской Федерации до 2020 года».
2. Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении Перечня сведений конфиденциального характера».
3. Доктрина информационной безопасности Российской Федерации (утв. Президентом Российской Федерации 9 сентября 2000 г.).
4. Закон Российской Федерации от 21.07.1993 г. № 5485-1 «О государственной тайне».
5. Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне».
6. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

ТЕМА 2. Основные угрозы информационной безопасности компьютерных систем

Изучаемые вопросы:

1. Классификация угроз информационной безопасности компьютерных систем.
2. Непреднамеренные искусственные угрозы.
3. Преднамеренные искусственные угрозы.
4. Уязвимости компьютерных систем обработки информации.
5. Источники угроз по отношению к компьютерным системам.
6. Несанкционированное чтение, изменение, уничтожение информации.
7. Активное и пассивное воздействие на компьютерные системы обработки информации.
8. Угрозы, связанные с использованием легальных каналов получения информации, скрытых каналов получения информации и с созданием новых каналов получения информации.
9. Угрозы, классифицируемые по типу используемой слабости защиты.
10. Описание модели гипотетического нарушителя.

При освоении темы №2 обучающийся должен изучить следующие нормативно-правовые акты и рекомендуемую литературу:

1. 2. Прохорова О.В. Информационная безопасность и защита информации: учебник / Прохорова О.В.— С.: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. 113с. — Режим доступа: <http://www.iprbookshop.ru/43183.html>.— ЭБС «IPRbooks»
2. Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с.— Режим доступа: <http://www.iprbookshop.ru/33857.html>.— ЭБС «IPRbooks».

ТЕМА 3. Стратегии, способы и средства защиты информации

Изучаемые вопросы:

1. Нормативно-правовые и морально-этические меры защиты информации.
2. Административные и физические меры защиты информации.

3. Программно-аппаратные меры защиты информации.
4. Произвольное управление доступом.
5. Принудительное управление доступом. Метки безопасности
6. Безопасность повторного использования объектов
7. Шифрование (криптозащита).
8. Электронная подпись.
9. Механизмы контроля целостности данных.
10. Механизмы аутентификации.

При освоении темы №3 обучающийся должен изучить следующие нормативно-правовые акты и рекомендуемую литературу:

1. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».

2. Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с.— Режим доступа: <http://www.iprbookshop.ru/33857.html>.— ЭБС «IPRbooks».

3. Нестеров, С.А. Основы информационной безопасности. [Электронный ресурс] — Электрон. дан. — СПб. : Лань, 2017. — 324 с. — Режим доступа: <http://e.lanbook.com/book/90153>.