



**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 по подготовке к зачету**

**Направление подготовки 38.03.04  
Государственное и муниципальное управление  
(уровень – бакалавриата)**

**Профиль-управление в кризисных ситуациях**

**Екатеринбург  
2020**

Информационная безопасность [Текст]: методические рекомендации по подготовке к зачету. Направление подготовки 38.03.04 Государственное и муниципальное управление/ сост. Н.П. Мураев. Екатеринбург: ФГБОУ ВО Уральский институт ГПС МЧС России, 2020. - 8 с.

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

Методические рекомендации рассмотрены и одобрены на заседании кафедры безопасности в ЧС «31» августа 2020 г., протокол № 1.

Методические рекомендации по подготовке к зачету «Информационная безопасность» предназначены для использования в образовательном процессе по направлению подготовки 38.03.04 Государственное и муниципальное управление (профиль - управление в кризисных ситуациях).

## СОДЕРЖАНИЕ

1. Введение .....	4
2. Тематический план изучения дисциплины .....	4
3. Перечень вопросов для подготовки к зачету .....	5
4. Перечень литературы, необходимой для подготовки к зачету .....	6
5. Критерии оценки ответов обучающихся.....	8

## 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.

## 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
<b>Итоговый контроль - зачет</b>	

### **3. Перечень вопросов для подготовки к зачету**

#### **Тема 1. Основы государственной политики в области информационной безопасности**

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.

#### **Тема 2. Основные угрозы информационной безопасности компьютерных систем**

11. Классификация угроз информационной безопасности компьютерных систем.
12. Непреднамеренные искусственные угрозы.
13. Преднамеренные искусственные угрозы.
14. Уязвимости компьютерных систем обработки информации.
15. Источники угроз по отношению к компьютерным системам.
16. Несанкционированное чтение, изменение, уничтожение информации.
17. Активное и пассивное воздействие на компьютерные системы обработки информации.
18. Угрозы, связанные с использованием легальных каналов получения информации, скрытых каналов получения информации и с созданием новых каналов получения информации.
19. Угрозы, классифицируемые по типу используемой слабости защиты.
20. Описание модели гипотетического нарушителя.

### **Тема 3. Стратегии, способы и средства защиты информации**

21. Нормативно-правовые и морально-этические меры защиты информации.
22. Административные и физические меры защиты информации.
23. Программно-аппаратные меры защиты информации.
24. Произвольное управление доступом.
25. Принудительное управление доступом. Метки безопасности
26. Безопасность повторного использования объектов
27. Шифрование (криптозащита).
28. Электронная подпись.
29. Механизмы контроля целостности данных.
30. Механизмы аутентификации.

## **4. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ**

### **Основная литература**

1. Артемов А.В. Информационная безопасность: учебное пособие / Артемов А.В.— О.: Межрегиональная Академия безопасности и выживания (МАБИБ), 2014. 256— с. — Режим доступа: <http://www.iprbookshop.ru/33430> — ЭБС «IPRbooks»
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»
3. 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».

### **Дополнительная литература**

1. Жигулин, Г.П. Организационное и правовое обеспечение информационной безопасности. [Электронный ресурс] — Электрон. дан. — СПб.: НИУ ИТМО, 2014. — 173 с. — Режим доступа: [Шр://e.lanbook.com/book/70952](http://e.lanbook.com/book/70952).
2. Нестеров, С.А. Основы информационной безопасности. [Электронный ресурс] — Электрон. дан. — СПб. : Лань, 2017. — 324 с. — Режим доступа: [Шр://e.lanbook.com/book/90153](http://e.lanbook.com/book/90153).
3. Указ Президента Российской Федерации от 12 мая 2009 года № 537 «О стратегии национальной безопасности Российской Федерации

до 2020 года».

4. Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении Перечня сведений конфиденциального характера».

5. Доктрина информационной безопасности Российской Федерации (утв. Президентом Российской Федерации 9 сентября 2000 г.).

6. Закон Российской Федерации от 21.07.1993 г. № 5485-1 «О государственной тайне».

7. Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне».

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

9. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

10. Постановление Правительства РФ от 03.11.1994 № 1233 (ред. от 20.07.2012) «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии».

11. Постановление Правительства РФ от 26.06.1995 № 608 (ред. от 21.04.2010) «О сертификации средств защиты информации».

12. Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности потехническойзащите конфиденциальной информации».

13. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

14. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

15. ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

16. ГОСТ Р 51624-00. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования.

17. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

18. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

19. ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

20. ГОСТ Р ИСО/МЭК 15408-3-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.

### **Перечень ресурсов информационно -телекоммуникационной сети «Интернет»**

1. <http://www.mchs.gov.ru> – официальный сайт МЧС России.

## **5. КРИТЕРИИ ОТВЕТОВ ОЦЕНКИ ОБУЧАЮЩИХСЯ**

Зачет проводится по завершению изучения дисциплины и имеет целью определить уровень знаний и усвоения материала обучающимися по дисциплине.

Знания обучающихся определяются оценками **«зачтено»**, **«не зачтено»**. Оценка объявляется студенту по окончании им ответа на зачете.

Время проведения зачета - 4 часа.

Зачет проводится по билетной системе, письменно в аудитории.

В каждом билете 2 вопроса.

В ходе ответа оценка выставляется обучающемуся за ответы по каждому вопросу билета, оценка за ответы на дополнительные вопросы и общая оценка за теоретическую часть экзамена. При этом учитывается не только степень усвоения теории того или иного вопроса, но и структура, содержание, логическая последовательность и стиль изложения, умение обосновывать излагаемые положения, а также увязать теорию с практикой.

Частная оценка за ответ на каждый вопрос экзаменационного билета выставляется:

**«ОТЛИЧНО»**, если обучающийся показал глубокие знания программного материала, грамотно и логично его излагает, быстро и уверенно отвечает на дополнительные вопросы.

**«ХОРОШО»**, если обучающийся твердо знает программный материал, грамотно его излагает, не допускает существенных неточностей в ответе, уверенно отвечает на дополнительные вопросы.

**«УДОВЛЕТВОРИТЕЛЬНО»**, если обучающийся показал знания только основного материала, но не усвоил его деталей, не допускает грубых ошибок в ответе, требует в отдельных случаях наводящих вопросов, допускает неточности при ответе на дополнительные вопросы.

**«НЕУДОВЛЕТВОРИТЕЛЬНО»**, если обучающийся допускает грубые ошибки в ответе, не реагирует на наводящие вопросы и не отвечает на дополнительные вопросы.

Общая оценка складывается из оценок за каждый вопрос, при этом:

**«Зачет»** - если по двум ответам на вопросы слушатель оценен не ниже «Удовлетворительно».

**«Незачет»** - если не выполнены условия на «зачет».

Результат сдачи зачета объявляется студенту преподавателем после ответа на все вопросы. «Зачтено» заносится преподавателем в зачетную книжку, ведомость и журнал. «Не зачтено» заносится только в ведомость.