***Практическая работа №1***

**Направления организационной и управленческой работы**

**в сфере информационной безопасности**

***Цель:*** изучить основные направления организационной и управленческой работы в сфере информационной безопасности.

***Формируемые умения***:

* осуществлять планирование и организацию выполнения мероприятий по защите информации.

**Методические указания**

Отчет к практической работе оформляется в тетради и в электронном документе, который сохраняется на своем носителе или ресурсе, указанном преподавателем.

Каждый из документов содержит название и цель работы, в электронном документе в колонтитуле указывается фамилия, имя студента, номер группы и дата выполнения работы.

Текстовый электронный документ оформляется в соответствии с ГОСТ 2.105-95. Межгосударственный стандарт. Единая система конструкторской документации. Общие требования к текстовым документам (введен Постановлением Госстандарта от 08.08.1995, 426 ред. от 22.06.2006). Основные требования: цвет шрифта – черный, размер – 14 пт, гарнитура – Times New Roman, начертание – обычное (если не указано иное), выравнивание текста – по ширине, межстрочный интервал – полуторный, размеры полей: левое – 3 см, правое – 1,5 см, верхнее и нижнее – 2 см; абзацный отступ – 1,25 см. Допускается использовать компьютерные возможности акцентирования внимания на определенных терминах, утверждениях применяя различные варианты начертания шрифта.

Ответы на задания даются полные, в соответствие с вопросом. При работе с нормативными документами указывается название документа, на который ссылается обучающийся. В качестве источников законодательных актов необходимо использовать справочно-правовые системы КонсультантПлюс, Гарант, официальные сайты организаций и структур.

**Выполнение работы**

*Задание.*Ответьте на предложенные ниже вопросы**,** используя Интернет-ресурс [www.intuit.ru](http://www.intuit.ru). Ответы должны быть полные в соответствии с вопросом.

1. Что понимается под рисками для информационных ресурсов? (Вынести в тетрадь)

2. *В виде схемы* предоставьте классификацию рисков. (Вынести в тетрадь)

3. В качестве методической основы для детализированного анализа рисков в практической работе используют ... заменивший ГОСТ Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения" (Вынести в тетрадь)

3. *В виде схемы* предоставьте виды негативных воздействий на информационные активы... (Вынести в тетрадь)

4. Что является непосредственным источником рисков и негативных воздействий? (Вынести в тетрадь)

5. *В виде схемы* предоставьте классификацию нарушений в зависимости от используемых критериев? (Вынести в тетрадь)

6.Перечислите наиболее распространенные способы нарушения информационной безопасности. (Сохраните в электронном текстовом документе с именем *Управление в сфере информационной безопасности* в папке *МДК.01.01* на своем накопителе).

7. Основными задачами организационно-управленческой деятельности (менеджмента) в сфере информационной безопасности являются... (ответ сохраните в электронный документ, см. задание 6).

8. Какова задача менеджмента в сфере информационной безопасности? (ответ сохраните в электронный документ)

9. Управление человеческими ресурсами в рамках управления информационной безопасностью включает ... (ответ дать в тетради)

10. Безопасная информационная инфраструктура включает в себя... (ответ сохраните в электронный документ).

11. Выделите организационные уровни сферы интересов менеджмента информационной безопасности. (Ответ сохраните в электронный документ).

12. В виде таблицы оформите задачи, роли и методы, используемые на различных уровнях организационной работы в сфере информационной безопасности (ответ сохраните в электронный документ)

**Литература**

1. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
2. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

# ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет-ресурсы**

* [www.consultant.ru](http://www.consultant.ru)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)
* [www.intuit.ru](http://www.intuit.ru).

***Практическая работа № 2***

**Основные направления и структура политики безопасности**

***Цель работы***: систематизация знаний по теме; ознакомление со стандартами Информационной безопасности; классификация разделов политики безопасности предприятия по отдельным направлениям защиты информации.

***Формируемые умения***:

* разрабатывать политику безопасности организации;
* внедрять и сопровождать политику безопасности организации.

**Методические указания**

Отчет к практической работе оформляется в тетради.

Отчет к практической работе содержит название и цель работы.

Ответы на задания даются полные, в соответствие с вопросом. При работе с нормативными документами указывается название документа, на который ссылается обучающийся. В качестве источников законодательных актов необходимо использовать справочно-правовые системы КонсультантПлюс, Гарант, официальные сайты организаций и структур.

**Выполнение работы**

*Задание* 1.Выделите виды внешних и внутренних угроз информационной безопасности на уровне предприятия.

# *Задание* 2. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2012 (название, область применения). Перечислите вопросы обеспечения информационной безопасности организаций и предприятий данного стандарта.

*Задание* 3. Отразите структуру организационной деятельности в сфере информационной безопасности на предприятии.

*Задание* 4.Назовите основные шаги общего жизненный цикл политики информационной безопасности.

*Задание* 5.Отнесите информационные ресурсы предприятия (и соответствующие элементы информационной инфраструктуры) по уровню своей значимости и конфиденциальности.

*Задание* 6.Заполните таблицу «Разделы политики безопасности по отдельным направлениям защиты информации на предприятии.

|  |  |
| --- | --- |
| Раздел политики безопасности | Содержание разделов политики безопасности по  отдельным направлениям защиты информации |
|  |  |
|  |  |

**Литература**

1. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения
2. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
3. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

**Интернет-ресурсы**

* [www.consultant.ru](http://www.consultant.ru)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)
* [www.intuit.ru](http://www.intuit.ru).

***Практическая работа № 3***

**Изучение основных положений закона РФ «О государственной тайне»**

(от 21 июля 1993 г. N 5485-I (с изменениями и дополнениями))

***Цель*:** изучить основные положения закона; составить глоссарий понятий, используемых в настоящем законе; изучить требования по защите информации при работе с секретной информацией.

***Формируемы умения***:

* организовывать работу с персоналом, имеющим доступ к конфиденциальной информации;
* проводить инструктаж персонала по организации работы с конфиденциальной информацией;
* контролировать соблюдение персоналом требований режима защиты информации;

**Методические указания**

Отчет к практической работе оформляется в тетради и в электронном документе, который сохраняется на своем носителе или ресурсе, указанном преподавателем.

Каждый из документов содержит название и цель работы, в электронном документе в колонтитуле указывается фамилия, имя студента, номер группы и дата выполнения работы как показано на рисунке 1.

Выполнил: студент группы \_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

фамилия, имя

Рисунок 1 – Внешний вид колонтитула

Текстовый электронный документ оформляется в соответствии с ГОСТ 2.105-95. Межгосударственный стандарт. Единая система конструкторской документации. Общие требования к текстовым документам (введен Постановлением Госстандарта от 08.08.1995, 426 ред. от 22.06.2006). Основные требования: цвет шрифта – черный, размер – 14 пт, гарнитура – Times New Roman, начертание – обычное (если не указано иное), выравнивание текста – по ширине, межстрочный интервал – полуторный, размеры полей: левое – 3 см, правое – 1,5 см, верхнее и нижнее – 2 см; абзацный отступ – 1,25 см. Допускается использовать компьютерные возможности акцентирования внимания на определенных терминах, утверждениях применяя различные варианты начертания шрифта.

Ответы на задания даются полные, в соответствие с вопросом. При работе с нормативными документами указывается название документа, на который ссылается обучающийся. В качестве источников законодательных актов необходимо использовать справочно-правовые системы КонсультантПлюс, Гарант, официальные сайты организаций и структур.

**Выполнение работы**

*Задание* 1. В тетрадь выпишите понятия, используемые в настоящем Законе: носители сведений, составляющих государственную тайну; допуск к государственной тайне; доступ к сведениям, составляющим государственную тайну; средства защиты информации.

*Задание* 2. В электронном документе к указанным статьям закона разработайте тестовые задания (на знание содержания статьи) с выбором ответа. Каждый вопрос должен содержать четыре варианта ответа. На последнем листе электронного документа укажите правильные ответы к тесту. (Вариант указывает преподаватель).

**Пример оформления**

***Статья 9. Согласие субъекта персональных данных на обработку своих персональных данных***

1. В каких случаях субъект персональных данных обязан предоставить свои персональные данные, даже против своей воли?

* 1. При защите здоровья, нравственности, прав и законных интересов других лиц;
  2. В случаи, если их непредставление нанесет материальный ущерб третьим лицам;
  3. В целях обеспечения обороны страны и безопасности государства;
  4. При защите основ конституционного строя РФ.

***Статья 12. …***

Варианты заданий

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Вариант | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** |
| Статья  закона  (количество вопросов) | **4** (3)  **9** (1)  **12** (1)  **17** (2)  **21** (2)  **28** (1) | **5** (3)  **10** (2)  **13** (1)  **24** (1)  **20** (2)  **27** (1) | **4** (2)  **11** (2)  **14** (1)  **16** (2)  **23** (1)  **30.1**(2) | **5** (3)  **6** (1)  **12** (2)  17 (1)  **22** (2)  **25** (1) | **4** (2)  **7** (3)  **17** (2)  **21** (2)  **24** (1)  **28** (2) | **6** (2)  **8** (1)  **15** (2)  **18** (1)  **20** (2)  **27**(2) | **4** (2)  **5** (2)  **9** (2)  **14** (1)  **21** (2)  **30.1**(1) | **5** (2)  **6** (1)  **12** (2)  **17** (1)  **20** (2)  **28**(2) | **4** (2)  **7** (1)  **13** (2)  **18** (1)  **21** (3)  **25**(1) | **5** (2)  **9** (2)  **14** (2)  **16** (1)  **20** (2)  **24**(1) | **4** (2)  **10** (1)  **15** (2)  **17** (1)  **21** (2)  **23**(2) | **5** (2)  **11** (1)  **16** (2)  **20** (2)  **22** (2)  **27**(1) |

**Интернет-ресурсы**

* [www.consultant.ru](http://www.consultant.ru)
* [www.garant.ru](http://www.garant.ru)

***Практическая работа № 4***

**Изучение основных положений закона РФ «О персональных данных»**

(от 27 июля 2006 г. N 152-ФЗ (с изменениями и дополнениями))

***Цель*:** изучить основные положения закона; составить глоссарий понятий, используемых в настоящем законе; изучить требования по защите информации при работе с персональными данными.

***Формируемы умения***:

* организовывать работу с персоналом, имеющим доступ к конфиденциальной информации;
* проводить инструктаж персонала по организации работы с конфиденциальной информацией;
* контролировать соблюдение персоналом требований режима защиты информации.

**Методические указания**

Отчет к практической работе оформляется в тетради и в электронном документе, который сохраняется на своем носителе или ресурсе, указанном преподавателем.

Каждый из документов содержит название и цель работы, в электронном документе в колонтитуле указывается фамилия, имя студента, номер группы и дата выполнения работы.

Текстовый электронный документ оформляется в соответствии с ГОСТ 2.105-95. Межгосударственный стандарт. Единая система конструкторской документации. Общие требования к текстовым документам (введен Постановлением Госстандарта от 08.08.1995, 426 ред. от 22.06.2006). Основные требования: цвет шрифта – черный, размер – 14 пт, гарнитура – Times New Roman, начертание – обычное (если не указано иное), выравнивание текста – по ширине, межстрочный интервал – полуторный, размеры полей: левое – 3 см, правое – 1,5 см, верхнее и нижнее – 2 см; абзацный отступ – 1,25 см. Допускается использовать компьютерные возможности акцентирования внимания на определенных терминах, утверждениях применяя различные варианты начертания шрифта.

Ответы на задания даются полные, в соответствие с вопросом. При работе с нормативными документами указывается название документа, на который ссылается обучающийся. В качестве источников законодательных актов необходимо использовать справочно-правовые системы КонсультантПлюс, Гарант, официальные сайты организаций и структур.

**Выполнение работы**

*Задание* 1. Выполняется в тетради.

1. Выпишите отношения, на которые не распространяется действие настоящего закона N 152-ФЗ.

2. Какова цель данного закона?

3. Дайте определение понятий, используемых в настоящем Законе: персональные данные (ПДн), оператор, обработка ПДн, автоматизированная обработка ПДн, обезличивание ПДн, информационная система персональных данных (ИСПДн).

*Задание* 2. В электронном документе к указанным статьям закона разработайте тестовые задания (на знание содержания статьи) с выбором ответа. Каждый вопрос должен содержать четыре варианта ответа. На последнем листе электронного документа укажите правильные ответы к тесту. (Вариант указывает преподаватель).

**Пример оформления**

***Статья 9. Согласие субъекта персональных данных на обработку своих персональных данных.***

1. Субъект персональных данных обязан предоставить свои персональные данные, даже против своей воли

1. При защите здоровья, нравственности, прав и законных интересов других лиц.
2. В случаи, если их непредставление нанесет материальный ущерб третьим лицам.
3. В целях обеспечения обороны страны и безопасности государства.
4. При защите основ конституционного строя РФ.

***Статья 12. …***

Варианты заданий

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Вариант** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** |
| **Статья**  **закона**  **(количество вопросов)** | **6** (2)  **7** (1)  **9** (2)  **12** (1)  **17** (1)  **19** (3)  **22** (2) | **5** (2)  **8** (1)  **10** (2)  **13** (1)  **18** (2)  **20** (1)  **23** (3) | **7** (1)  **11** (2)  **15** (1)  **19** (3)  21 (2)  **23** (2)  **24**(1) | **5** (1)  **6** (1)  **9** (2)  **12** (2)  **14** (2)  **18.1**(2)  **21** (2) | **6** (2)  **10** (2)  **13** (1)  **15** (1)  **18** (2)  **20** (1)  **22** (3) | **7** (1)  **9** (2)  **12** (1)  **16** (2)  **19** (2)  **21** (2)  **23**(2) | **5** (1)  **8** (1)  **10** (3)  **13** (1)  **14** (2)  **18.1**(2)  **22.1**(2) | **7** (1)  **11** (1)  **14** (2)  **17** (1)  **19** (2)  **20** (2)  **22**(3) | **5** (2)  **10**(2)  **15** (2)  **18** (2)  **21** (1)  **22.1**(1)  **23**(2) | **6** (2)  **8** (1)  **12** (2)  **18.1**(2)  **19** (1)  **22** (2)  **24**(1) | **4** (2)  **10** (1)  **15** (2)  **17** (1)  **20** (2)  **21** (2)  **23**(2) | **5** (1)  **7** (1)  **9** (2)  **13** (2)  **14** (2)  **19** (2)  **22** (2) |

**Интернет-ресурсы**

* [www.consultant.ru](http://www.consultant.ru)
* [www.garant.ru](http://www.garant.ru)

***Практическая работа №5***

**Изучение инструкции о порядке допуска должностных лиц и граждан**

**Российской Федерации к государственной тайне  
(утв. постановлением Правительства РФ от 6 февраля 2010 г. N 63 с изменениями и дополнениями от 1 ноября 2012 г.)**

***Цель:*** изучить порядок допуска должностных лиц и граждан Российской Федерации к государственной, ознакомится с формами учетной документации.

***Формируемые умения:***

* использовать критерии подбора и расстановки сотрудников подразделений защиты информации;
* организовывать работу с персоналом, имеющим доступ к конфиденциальной информации;
* проводить инструктаж персонала по организации работы с конфиденциальной информацией.

**Методические указания**

Отчет к практической работе оформляется в тетради и в электронном документе, который сохраняется на своем носителе или ресурсе, указанном преподавателем.

Каждый из документов содержит название и цель работы, в электронном документе в колонтитуле указывается фамилия, имя студента, номер группы и дата выполнения работы.

Текстовый электронный документ оформляется в соответствии с ГОСТ 2.105-95. Межгосударственный стандарт. Единая система конструкторской документации. Общие требования к текстовым документам (введен Постановлением Госстандарта от 08.08.1995, 426 ред. от 22.06.2006). Основные требования: цвет шрифта – черный, размер – 14 пт, гарнитура – Times New Roman, начертание – обычное (если не указано иное), выравнивание текста – по ширине, межстрочный интервал – полуторный, размеры полей: левое – 3 см, правое – 1,5 см, верхнее и нижнее – 2 см; абзацный отступ – 1,25 см. Допускается использовать компьютерные возможности акцентирования внимания на определенных терминах, утверждениях применяя различные варианты начертания шрифта.

Ответы на задания даются полные, в соответствие с вопросом. При работе с нормативными документами указывается название документа, на который ссылается обучающийся. В качестве источников законодательных актов необходимо использовать справочно-правовые системы КонсультантПлюс, Гарант, официальные сайты организаций и структур.

**Выполнение работы**

*Задание.*Ответьте на предложенные ниже вопросы**,** используя Интернет-ресурсы. Ответы должны быть полные в соответствии с вопросом.

1. Что определяет инструкции о порядке допуска должностных лиц и граждан РФ к государственной тайне? (Вынести в тетрадь)

2. Дайте определение понятия «доступ к сведениям, составляющим государственную тайну». (Вынести в тетрадь)

3. Какие формы допуска граждан к ГТ устанавливаются в соответствии со степенями секретности сведений, составляющих государственную тайну? (Вынести в тетрадь)

4. Что предусматривает допуск граждан к государственной тайне? (Вынести в тетрадь)

5. Кем принимается  решение о допуске к государственной тайне? (Вынести в тетрадь)

6.Какова форма номенклатуры должностей работников, подлежащих оформлению на допуск к государственной тайне? (Сохраните в электронном текстовом документе с именем *Номенклатура должностей*  в папке *ПМ.01/Гос\_тайна* на своем накопителе).

7. Кем разрабатывается номенклатура должностей? Как часто переутверждается? (Т)

8. Каким образом заполняется анкета гражданами, которым оформляется допуск к государственной тайне? (Т)

9. Какова форма анкеты для допуска к ГТ? (Эл. документ с именем *Анкета к ГТ, см задание 6*).

10. Каково обязательство граждан по соблюдению требований законодательства Российской Федерации о государственной тайне? (Эл. документ с именем *Обязательство\_ГТ, см задание 6*).

11. Где и вместе с чем хранятся карточки учета лиц допущенных к ГТ? (В тетрадь)

12. Какова форма карточки учета лица, допущенного к государственной тайне? (Эл. документ с именем *Карточка учета, см задание 6*).

13. Каковы сроки переоформления допуска к ГТ? (Т)

**Интернет-ресурсы**

* [www.consultant.ru](http://www.consultant.ru)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)
* [www.intuit.ru](http://www.intuit.ru).

***Практическая работа № 6***

**Организация и создание службы безопасности**

**(правовой статус)**

***Цель работы***: систематизация знаний по теме; ознакомление с законом РФ «О частной детективной и охранной деятельности в Российской Федерации»; разработка нормативных документов для создания службы безопасности предприятия.

***Формируемые умения***: организовывать охрану персонала, территорий, зданий, помещений и продукции организаций.

**Методические указания**

Отчет к практической работе оформляется в тетради и в электронном документе, который сохраняется на своем носителе или ресурсе, указанном преподавателем.

Каждый из документов содержит название и цель работы, в электронном документе в колонтитуле указывается фамилия, имя студента, номер группы и дата выполнения работы.

Текстовый электронный документ оформляется в соответствии с ГОСТ 2.105-95. Межгосударственный стандарт. Единая система конструкторской документации. Общие требования к текстовым документам (введен Постановлением Госстандарта от 08.08.1995, 426 ред. от 22.06.2006). Основные требования: цвет шрифта – черный, размер – 14 пт, гарнитура – Times New Roman, начертание – обычное (если не указано иное), выравнивание текста – по ширине, межстрочный интервал – полуторный, размеры полей: левое – 3 см, правое – 1,5 см, верхнее и нижнее – 2 см; абзацный отступ – 1,25 см. Допускается использовать компьютерные возможности акцентирования внимания на определенных терминах, утверждениях применяя различные варианты начертания шрифта.

Ответы на задания даются полные, в соответствие с вопросом. При работе с нормативными документами указывается название документа, на который ссылается обучающийся. В качестве источников законодательных актов необходимо использовать справочно-правовые системы КонсультантПлюс, Гарант, официальные сайты организаций и структур.

**Выполнение работы**

*Задание* 1. Дайте определения понятий в соответствии с законом РФ «О частной детективной и охранной деятельности в Российской Федерации»: объекты охраны; внутриобъектовый режим; пропускной режим (в тетради).

*Задание* 2. Перечислите виды услуг предоставляемых в целях сыска, в соответствии с законом (в тетради).

*Задание* 3. Виды услуг, предоставляемые в целях охраны, перечислите в электронном текстовом документе с именем «Услуги в целях охраны» в папке *Организация и создание службы безопасности* на своем накопителе.

*Задание* 4. В каком случае в сыскной деятельности можно осуществлять устный опрос граждан и должностных лиц? (В ответе в тетради указать на какую статью закона вы ссылаетесь)

*Задание* 5. Перечислите права частных охранников при обеспечении внутриобъектового и пропускного режимов в пределах объекта охраны, а также при транспортировке охраняемых грузов, денежных средств и иного имущества. В электронном документе под именем «Права при пропускном режиме», параметры документа см. задание 3.

*Задание* 6. Каким документом регламентируются действия частных охранников на объектах охраны? (в ответе, указать ссылку на статью, в тетради).

*Задание* 7. Отразите типовые требования к документу задания 6 в электронном виде.

*Задание* 8. Перечислите, в соответствии с законом, кто не может являться учредителями (участниками) частной охранной организации (в тетради).

*Задание* 9. Составьте перечень правил и норм, которыми руководствуются службы безопасности в соответствии с Постановлением Правительства РФ от 14 августа 1992 г. N 587 "Вопросы частной детективной (сыскной) и частной охранной деятельности" (с изменениями и дополнениями).

*Задание* 10. Подготовьте примерное заявление о *согласовании Устава службы безопасности*, предоставляемое предприятием-учредителем в органы внутренних дел (в электронном виде).

**Интернет-ресурсы**

* [www.consultant.ru](http://www.consultant.ru)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)
* [www.intuit.ru](http://www.intuit.ru).

***Практическая работа № 7***

**Разработка пакета документов для обеспечения организационной и**

**правовой защиты информации**

***Цель*:** собрать банк документов в виде примерных инструкций, положений, предложений необходимый для обеспечения полноценной организационной и правовой защиты информации.

***Формируемые умения***: организовывать охрану персонала, территорий, зданий, помещений и продукции организаций.

**Методические указания**

Отчет к практической работе в электронном документе, который сохраняется на своем носителе или ресурсе, указанном преподавателем.

Документ содержит название и цель работы, в электронном документе в колонтитуле указывается фамилия, имя студента, номер группы и дата выполнения работы.

Текстовый электронный документ оформляется в соответствии с ГОСТ 2.105-95. Межгосударственный стандарт. Единая система конструкторской документации. Общие требования к текстовым документам (введен Постановлением Госстандарта от 08.08.1995, 426 ред. от 22.06.2006). Основные требования: цвет шрифта – черный, размер – 14 пт, гарнитура – Times New Roman, начертание – обычное (если не указано иное), выравнивание текста – по ширине, межстрочный интервал – полуторный, размеры полей: левое – 3 см, правое – 1,5 см, верхнее и нижнее – 2 см; абзацный отступ – 1,25 см. Допускается использовать компьютерные возможности акцентирования внимания на определенных терминах, утверждениях применяя различные варианты начертания шрифта.

Ответы на задания даются полные, в соответствие с вопросом. При работе с нормативными документами указывается название документа, на который ссылается обучающийся. В качестве источников законодательных актов необходимо использовать справочно-правовые системы КонсультантПлюс, Гарант, официальные сайты организаций и структур.

**Выполнение работы**

*Задание.* В виде отдельных электронных документов (название должно соответствовать заданию) соберите, используя Интернет-ресурсы поисковых систем, банк примерных инструкций, обязательств, соглашений, перечней и т.д. Сохраните документы *Ваш носитель / МДК.01.02 / Пакет документов*.

1. Положение о КИ предприятия.
2. Перечень документов предприятия, содержащих КИ.
3. Инструкция по защите КИ в информационной системе предприятия.
4. Предложения по внесению изменений в Устав предприятия.
5. Предложения по внесению изменений в трудовой договор, контракт с руководителем и коллективный договор.
6. Соглашение о неразглашении КИ предприятия с сотрудником.
7. Обязательство сотрудника о неразглашении КИ предприятия при увольнении.
8. Предложения о внесении изменений в Правила внутреннего распорядка предприятия (в части регламентации мер физической защиты информации и вопросов режима).
9. Предложения о внесении изменений в должностное (штатное) расписание предприятия (штат СлЗИ).
10. Предложения о внесении дополнений в должностные инструкции всему персоналу.
11. Ведомость ознакомления сотрудников предприятия с Положением о КИ и Инструкцией по защите КИ в ИС предприятия.
12. План проведения занятий с персоналом по сохранению и неразглашению КИ.
13. Предложения о внесении изменений в структуру собеседования при приеме на работу (уточнение обязательств информационно характера с последних мест работы).
14. Предложения о внесении дополнений в стандартные договоры с контрагентами.

**Интернет-ресурсы**

* [www.consultant.ru](http://www.consultant.ru)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)
* [www.intuit.ru](http://www.intuit.ru).

***Практическая работа № 8***

**Организация работы персонала с конфиденциальной информацией**

***Цель*:** изучение требований при организации работы персонала с конфиденциальной информацией, разработка нормативных документов необходимых для организации работы персонала с конфиденциальной информацией.

***Формируемые умения***:

* определять порядок организации и проведения рабочих совещаний;
* организовывать работу с персоналом, имеющим доступ к конфиденциальной информации;
* проводить инструктаж персонала по организации работы с конфиденциальной информацией;
* использовать методы защиты информации в рекламной и выставочной деятельности.

**Методические указания**

Отчет к практической работе в электронном документе, который сохраняется на своем носителе или ресурсе, указанном преподавателем.

Документ содержит название и цель работы, в электронном документе в колонтитуле указывается фамилия, имя студента, номер группы и дата выполнения работы.

Текстовый электронный документ оформляется в соответствии с ГОСТ 2.105-95. Межгосударственный стандарт. Единая система конструкторской документации. Общие требования к текстовым документам (введен Постановлением Госстандарта от 08.08.1995, 426 ред. от 22.06.2006). Основные требования: цвет шрифта – черный, размер – 14 пт, гарнитура – Times New Roman, начертание – обычное (если не указано иное), выравнивание текста – по ширине, межстрочный интервал – полуторный, размеры полей: левое – 3 см, правое – 1,5 см, верхнее и нижнее – 2 см; абзацный отступ – 1,25 см. Допускается использовать компьютерные возможности акцентирования внимания на определенных терминах, утверждениях применяя различные варианты начертания шрифта.

Ответы на задания даются полные, в соответствие с вопросом. При работе с нормативными документами указывается название документа, на который ссылается обучающийся. В качестве источников законодательных актов необходимо использовать справочно-правовые системы КонсультантПлюс, Гарант, официальные сайты организаций и структур.

**Выполнение работы**

*Задание*.В виде отдельных электронных документов (название должно соответствовать заданию) соберите, используя Интернет-ресурсы поисковых систем, банк требований при организации работы персонала с конфиденциальной информацией по различным направлениям:

1. Требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по конфиденциальным вопросам и переговоров.

2. Требования режима защиты информации при приеме в организации посетителей.

3. Организация работы при осуществлении международного сотрудничества.

4. Требования режима защиты информации в процессе рекламной деятельности.

5. Требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати.

**Литература**

1. ГОСТ Р 53114-2008 Обеспечение информационной безопасности в организации. Основные термины и определения.
2. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.
3. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

**Интернет-ресурсы**

* [www.consultant.ru](http://www.consultant.ru)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)
* [www.intuit.ru](http://www.intuit.ru).

***Практическая работа № 9***

**Построение системы защиты контроля управления доступом организации**

***Цель*:** изучение интегрированных систем безопасности (ИСБ); выявление угроз информационной безопасности типового объекта; разработка варианта оснащения подобъектов данного типового объекта оборудованием систем безопасности.

***Формируемые умения***:

* выделять зоны доступа по типу и степени конфиденциальности работ;
* организовывать охрану персонала, территорий, зданий, помещений и продукции организаций;

**Методические указания**

Отчет к практической работе оформляется в тетради.

Документ содержит название и цель работы, в электронном документе в колонтитуле указывается фамилия, имя студента, номер группы и дата выполнения работы.

Ответы на задания даются полные, в соответствие с вопросом. При работе с нормативными документами указывается название документа, на который ссылается обучающийся. В качестве источников законодательных актов необходимо использовать справочно-правовые системы КонсультантПлюс, Гарант, официальные сайты организаций и структур.

*Теоретические сведения*

В настоящее время для противодействия указанным угрозам используются ***автономные системы безопасности***, обеспечивающие выполнение конкретного, строго определенного набора функций, и***частично интегрированные системы безопасности***, обеспечивающие комплексное решение отдельных охранных функций на основе их объединения.

В современных условиях роста преступности в стране, активизации террористической деятельности, увеличения количества техногенных аварий применение **интегрированных систем безопасности (ИСБ)** является наиболее эффективным способом организации инженерно-технической защиты объектов и персонала, поскольку создает необходимые условия для комплексного решения задач по обеспечению сохранности материальных ценностей, сохранности жизни и здоровья людей.

**Современная интегрированная система безопасности включает в свой состав следующие функциональные системы**:

1. **систему охранной сигнализации (СОС),** позволяющую обнаружить факт несанкционированного проникновения нарушителя на охраняемый объект;
2. **систему пожарной сигнализации (СПС),** обеспечивающую оповещение об обнаружении признаков задымления и пожара;
3. **систему тревожной сигнализации (СТрС),** формирующую сигнал тревоги на пульт поста охраны в случае нападения нарушителя;
4. **систему охранного телевидения (СОТ),** осуществляющую круглосуточное видеонаблюдение и видеорегистрацию оперативной обстановки на охраняемом объекте;
5. **систему контроля и управления доступом (СКУД),** решающую задачу обеспечения санкционированного доступа на охраняемый объект;
6. **систему оповещения и управления эвакуацией (СОУЭ),** основной задачей которой является своевременное сообщение людям информации о возникновении чрезвычайной ситуации (пожара, аварии и т.п.) и о путях эвакуации;
7. **систему управления инженерным оборудованием (СУИО),** осуществляющую запуск и остановку различного инженерного оборудования.
8. Для управления вышеперечисленными системами используется **система автоматического управления (САУ),** задачей которой является сбор и обработка информации, а также формирование управляющих воздействий функциональным системам, входящим в состав комплекса.
9. Для облегчения взаимодействия оператора с интегрированной системой безопасности используется **система взаимодействия с оператором (СВО).**

Так жеиспользуют **систему автоматического пожаротушения (АСПТ),** предназначенную для эффективной ликвидации очагов возгорания на объектах с применением современных огнетушащих средств и **систему технологической сигнализации (СТхС),** обеспечивающую сбор информации с датчиков контроля технологических параметров.

**Система охранной сигнализации** *создается с использованием СКШС-04 (сетевой контроллер шлейфов сигнализации), либо с использованием СКШС-02. Тип СКШС выбирается в зависимости от количества охраняемых помещений: к СКШС- 04 можно подключать до 16, а к СКШС-02 — до 8 охранных извещателей, выпускаемых различными производителями.* При этом для обеспечения охраны:

* стен, потолков, полов - рекомендуется применять оптоэлектронные объемные охранные извещатели;
* окон - рекомендуется использовать акустические охранные извещатели обнаружения разрушения стекла;
* дверей - рекомендуется применять магнитоконтактные охранные извещатели, устанавливаемые на двери.

**Система пожарной сигнализации** может быть создана с использованием СКШС-01 (сетевой контроллер шлейфов сигнализации), либо с использованием СКАУ-01 (сетевой контроллер адресных устройств). При необходимости точного определения места возникновения пожара рекомендуется использовать СКАУ-01, который принимает и обрабатывает сигналы от 99 адресно-аналоговых пожарных извещателей, производимых фирмой «Систем Сенсор». При отсутствии необходимости точного определения места возникновения пожара достаточно использовать СКШС-01, который обеспечивает прием сигналов от 4-х шлейфов сигнализации. К каждому шлейфу можно параллельно подсоединять до 20 неадресных пожарных извещателей. *Для типового объекта предлагается вариант исполнения СПС на базе СКШС-01, в котором один шлейф сигнализации прокладывается в каждом помещении и, тем самым, адрес места возникновения пожара определяется с точностью до подобъекта. Данное решение продиктовано экономическим расчётом по обоснованию структуры СПС, так как финансовые затраты на приобретение нескольких СКШС-01 хотя и выше, чем одного СКАУ-01, но затраты на приобретение большого числа неадресных пожарных извещателей будут значительно меньше, чем такого же числа адресных пожарных извещателей.*

В качестве пожарных извещателей рекомендуется применять автоматические дымовые пожарные извещатели, выпускаемые различными производителями и устанавливаемые на каждом подобъекте, в количестве не менее двух на каждое помещение, и ручные пожарные извещатели.

**Система тревожной сигнализации** может строиться с использованием СКШС- 01, СКШС-02, СКШС-04 и тревожных кнопок от различных производителей. Ввиду того, что при использовании СКШС-02, СКШС-04 остается много неиспользуемых контактов ввода, целесообразно применить для данного объекта СКШС-01.

**Система оповещения и управления эвакуацией** может создаваться с использованием СКИУ-02 (сетевой контроллер исполнительных устройств), осуществляющего прием управляющих сигналов и управление исполнительными устройствами - звуковыми оповещателями (сирена), световыми указателями и световыми оповещателями - табло «Выход», выпускаемыми различными производителями. *Все оповещатели рекомендуется установить на подообъектах «Коридор», «Холл» и «Стационар». В соответствии с требованиями НПБ 104-03 данный объект относится ко 2-му типу СОУЭ, если находится в здании с наибольшим числом этажей до 6, и к 3-му типу, если находится в здании с наибольшим числом этажей от 6 до 16. При использовании 3-го типа СОУЭ необходимо дополнить систему оповещения и управления эвакуацией оборудованием речевого оповещения с целью трансляции специальных текстов.*

**Систему контроля и управления доступом** целесообразно создавать с использованием СК-01 (сетевой контроллер устройств считывания кода), который принимает и обрабатывает сигналы от считывателей proximity- карт и управляет электромагнитными замками, турникетами от различных производителей, а также УСК-02Н (устройство считывания кода), которое принимает сигналы от proximity карт и передает их СК-01. Кроме того предлагается использовать УСК-02С (устройство считывания кода сетевое), которое принимает сигналы от proximity карт и управляет электромагнитными замками.

Систему контроля и управления доступом на «КПП для автотранспорта» целесообразно реализовать с использованием СКУСК-01Р (сетевой контроллер радиоканальных устройств считывания кода), который предназначен для работы с радиоканальным оборудованием производства компании Альтоника: приемник RR- 1R, модификация с выходным интерфейсом Wiegand, радиобрелок четырехкнопочный RFS4-R.. СКУСК-01Р управляет приводной автоматикой распашных ворот, выпускаемых различными производителями.

**Система охранного телевидения** может быть создана с использованием видеоплаты ввода и оцифровки телевизионных аналоговых сигналов РМВидео-16- 50, которая обеспечивает возможности подключения 16 источников видеосигнала - видеокамер цветного изображения типа VCC-5775P, VCC-6572P, VCC- 6592P, черно-белого изображения типа VCC-3372P, VCC-3442P, VCC-3512P фирмы "Sanyo" или аналогичных с стандартом видеосигнала "CCIR", "PAL" и уровнем видеосигнала 0,5.. .1 В. Видеоплата устанавливается в PCI-слот персонального компьютера и работает в режиме взаимодействия с ПО «AV-Монитор».

**Система управления инженерным оборудованием** может строиться с использованием СКИУ-02 (сетевой контроллер исполнительных устройств), обеспечивающего управление 4-мя релейными выходами и передачу информации о состоянии релейных выходов в БЦП для включения и выключения светильников охранного освещения, которые обеспечивают освещение периметра охраняемого объекта в темное время суток.

**Систему автоматического управления ИСБ «Рубеж»** рекомендуется выполнить с использованием БЦП (блок центральный процессорный) в исполнении 4, который обеспечивает централизованное управление подключенным оборудованием ИСБ «Р-08». Рекомендация выбора исполнения 4 обусловлена тем, что блок оптимизирован для небольших объектов и имеет встроенный блок бесперебойного питания. БЦП целесообразно разместить на стене в «Помещении поста охраны».

**Систему взаимодействия с оператором** рекомендуется создать на основе автоматизированного рабочего места (АРМ) оператора, включающего аппаратную часть - компьютер, и программную часть - специализированное программное обеспечение «Р-08». АРМ размещается в «Помещении поста охраны».

В помещении «Поста охраны» также рекомендуется установить пульт управления ПУ-02 для обеспечения независимого от АРМ управления охранником поста охраны оборудованием ИСБ «Рубеж» и блок индикации состояний БИС-01, осуществляющий индикацию состояний охраняемых подобъектов.

Для обеспечения бесперебойной подачи питающего напряжения при аварийном отключении от сети переменного предлагается использовать **источник бесперебойного питания** («ИБП-1200»). ИБП обеспечивает:

автоматический переход на резервное питание при отключении сети переменного тока;

* контроль напряжения сети переменного тока;
* контроль состояния аккумуляторной батареи.

Все устройства серии «Рубеж», кроме приёмника RR-1R, предлагается применять в стандартном исполнении IP-20 ввиду их размещения в помещениях с нормальными климатическими условиями. Приёмник RR-1R размещается вне здания на подобъекте «Периметр», поэтому исполнение предпочтительнее выбрать IP-65. Аналогичное требование предъявляется к выбору видеокамер, которые должны быть наружного применения.

**Выполнение работы**

*Задание* 1. Современную интегрированную систему безопасности отразите в таблице:

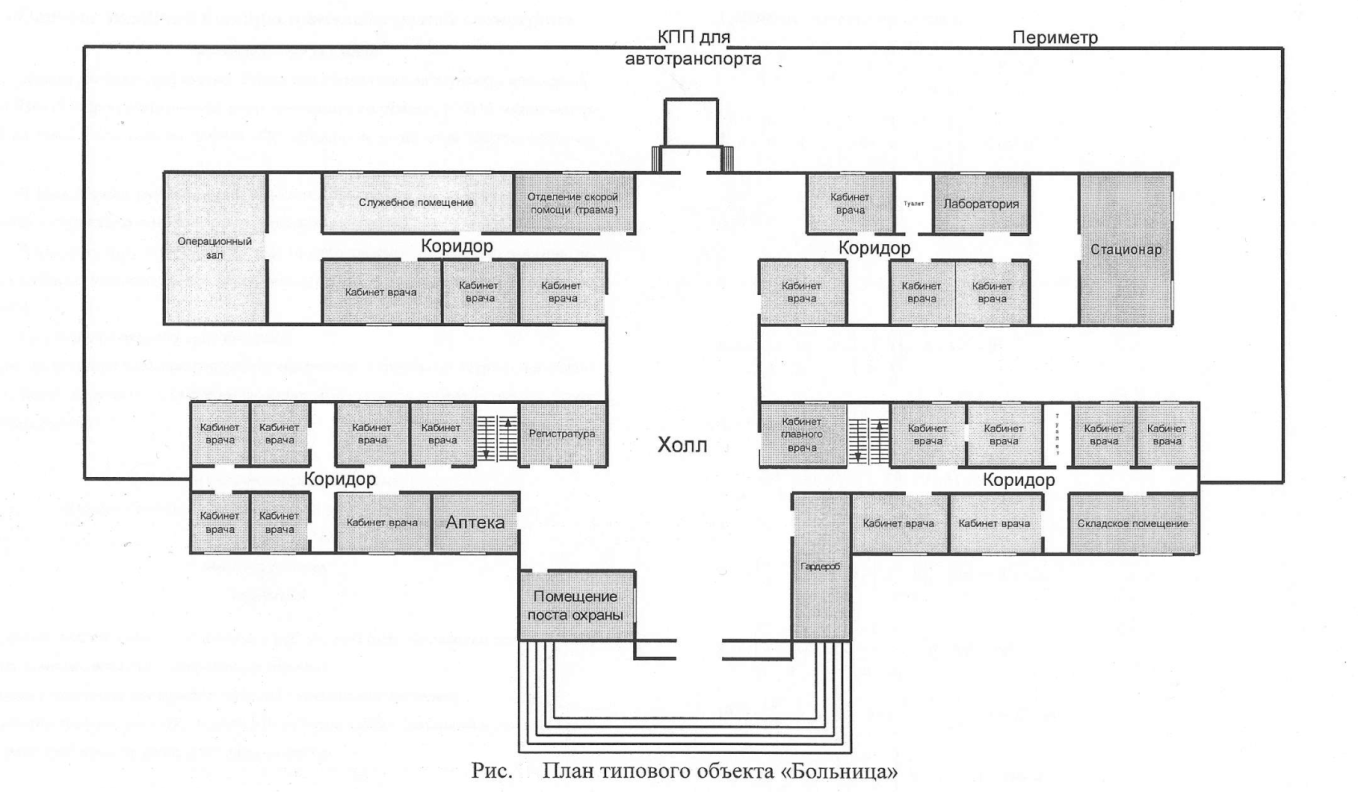
|  |  |  |
| --- | --- | --- |
| **Функциональные системы** | **Назначение** | **Рекомендации**  **в использовании** |
|  |  |  |

*Задание* 2*.*Дайте краткое описание объекта. Опишите угрозы безопасности типового объекта «Больница».

Типовой объект «Больница» представляет собой вид медицинского учреждения, направленного на лечение больных и специализированную углубленную диагностику заболеваний в стационарных условиях. Подобъект «Лаборатория» занимается разработкой и апробацией новых видов лекарств, которые используются для лечения различных видов заболеваний. Защита информации в данной лаборатории особенно важна, так как там находится большая часть образцов, разработанных в институте, в систему которого входит «Больница».

Объект «Больница» включает в свой состав следующие подобъекты:

|  |  |
| --- | --- |
| * «Периметр» * «КПП для автотранспорта» * «Кабинет главного врача» * «Операционный зал» * «Стационар» * «Лаборатория» * «Кабинет врача» * «Помещение поста охраны» * «Регистратура» | * «Отделение скорой помощи» * «Служебное помещение» * «Коридор» * «Холл» * «Аптека» * «Гардероб» * «Складское помещение» * «Туалет» |

****

*Задание* 3*.* С учетом приоритетности противодействия описанным выше угрозам предложите вариант оснащения подобъектов данного типового объекта оборудованием систем безопасности. Размещение систем безопасности отразите в таблице.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Подобъект** | **Системы безопасности** | | | | | | | | |
| **СОС** | **СПС** | **СТрС** | **СОУЭ** | **СКУД** | **СОТ** | **СУИО** | **САУ** | **СВО** |
| Периметр |  |  |  |  |  |  |  |  |  |
| КПП для авто­транспорта |  |  |  |  |  |  |  |  |  |
| Кабинет глав­ного врача |  |  |  |  |  |  |  |  |  |
| И т.д. |  |  |  |  |  |  |  |  |  |

**Интернет-ресурсы**

* [www.consultant.ru](http://www.consultant.ru)
* [www.itsecurity.ru](http://www.itsecurity.ru/)
* [www.oxpaha.ru](http://www.oxpaha.ru/)
* [www.secuteck.ru](http://www.secuteck.ru/)
* [www.intuit.ru](http://www.intuit.ru).