

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по выполнению практических занятий
по дисциплине «Защита объектов критической информационной инфраструктуры»
для студентов направления подготовки
10.03.01 «Информационная безопасность»
Направленность (профиль)
«Организация и технологии защиты информации (по отрасли или в сфере
профессиональной деятельности)»

СОДЕРЖАНИЕ

Тема 1. Практическое занятие №1. Основные понятия и определения изучаемой дисциплины. Правовые основы обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Тема 2. Практическое занятие №2. Организационно-правовые основы аттестации значимых объектов КИИ, лицензирования деятельности в области защиты информации. Система сертификации средств защиты информации.

Тема 3. Практическое занятие №3. Угрозы безопасности информации, обрабатываемой на объектах КИИ.

Тема 4. Практическое занятие №4. Источники угроз безопасности информации. Уязвимости объектов КИИ, классификация уязвимостей.

Тема 5. Практическое занятие №5. Способы реализации угроз безопасности информации и их последствия. Банк данных угроз безопасности информации. Структура модели угроз безопасности информации значимого объекта КИИ

Тема 6. Практическое занятие №6. Категорирование объектов КИИ. Реестр значимых объектов КИИ. Перечень показателей критериев значимости объектов КИИ Российской Федерации и их значения. Требования по обеспечению безопасности значимых объектов КИИ.

Тема 7. Практическое занятие №7. Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ. Требования к классам защиты средств защиты информации и средствам вычислительной техники для различных категорий значимости объектов КИИ.

Тема 8. Практическое занятие №8. Система безопасности значимого объекта КИИ. Стадии (этапы) работ по созданию систем безопасности значимого объекта КИИ.

Тема 9. Практическое занятие №9. Контроль за обеспечением безопасности значимого объекта КИИ.комплекса СПРУТ-МИНИ-А.

ВВЕДЕНИЕ

1. Цель и задачи освоения дисциплины

Целью изучения дисциплины «Защита объектов критической информационной инфраструктуры» является освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе организации и проведения аудита информационной безопасности, а также приобретение набора общекультурных и общепрофессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

Задачами дисциплины являются:

- теоретическая и практическая подготовка бакалавров к настройке параметров безопасности различных типов операционных систем;
- объяснение принципов построения подсистем защиты в ОС различной архитектуры, средств и методов несанкционированного доступа к ресурсам ОС;
- привитие студентам системного подхода к проблеме защиты информации в ОС; механизмов защиты информации и возможностей по их преодолению.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-3 Способен обеспечивать защиту информации в автоматизированных системах в процессе их эксплуатации	ИД-3 Способен проводить аудит защищённости информации в автоматизированных системах	Управляет защитой информации на объектах информационной безопасности в полном объеме
ПК-6 Способен проводить контроль защищённости информации	ИД-2 Способен проводить контроль защищённости информации от несанкционированного доступа	Проводит оценку защищенности информации от несанкционированного доступа и специальных воздействий Оформляет отчетные материалы по результатам контроля защищенности информации от несанкционированного доступа и специальных воздействий (протокол контроля защищенности информации от

		несанкционированного доступа и специальных воздействий)
--	--	---

Тема 1.

Практическое занятие №1

Цель занятия:

1. Закрепление теоретических знаний по вопросам государственного лицензирования деятельности в области защиты информации.
2. Получение практических навыков по порядку проведения лицензирования в области защиты информации.

Формируемые компетенции: ПК-3, ПК-6

Время – 4 ч.

1. Подготовка к занятию

1. Ознакомиться с заданием на практическую работу.
2. Ознакомиться с программой практической работы.

2. Распределение времени занятия:

Всего: 180 мин.

Вступительная часть 2 мин.

Проверка готовности студентов к занятию 5 мин.

3. Программа практической работы

Вступительная часть 10 мин.

Основная часть

1. Организационная структура системы государственного лицензирования в области защиты информации 50 мин.
2. Общий порядок проведения лицензирования в области защиты информации 30 мин.
3. Контроль за деятельностью лицензиатов 30 мин.
4. Особенности лицензирования деятельности по технической защите конфиденциальной информации 50 мин.
3. Заключительная часть 10 мин.

4. Методические указания студентам по подготовке и проведению практического занятия

При изучении учебного вопроса «Организационная структура системы государственного лицензирования в области защиты информации» необходимо использовать источник [1] статьи 2-6, 8,9.

При изучении учебного вопроса «Общий порядок проведения лицензирования в области защиты информации» необходимо использовать источник [1] статьи 12-14.

При изучении учебного вопроса «Контроль за деятельностью лицензиатов» необходимо использовать источник [1] статьи 19-21.

При изучении учебного вопроса «Особенности лицензирования деятельности по технической защите конфиденциальной информации» необходимо использовать источник [4] в полном объеме.

Для дополнения изученного материала в части, касающейся темы занятия, студенты используют источники [2-3].

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию. Затем студенты последовательно усваивают учебные вопросы, касающиеся организационной структуры системы государственного лицензирования в области защиты информации, порядка лицензирования и контроля лицензиатов, изучения видов деятельности предприятий в области защиты информации, подлежащих лицензированию, лично отрабатывают контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя. По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

5. Контрольные вопросы

1. Сформулируйте основные понятия, принятые в сфере государственного лицензирования в области защиты информации.
2. Организационная структура системы государственного лицензирования в области защиты информации.
3. Функции государственных органов по лицензированию в области защиты информации.
4. Функции лицензионных центров по лицензированию в области защиты информации.
5. Права и обязанности лицензиатов.
6. Порядок проведения лицензирования и контроля за деятельностью лицензиатов.
7. Назовите случаи приостановления или прекращения действия лицензии.
8. В каких случаях предприятию отказывают в выдаче лицензии?
9. Какие документы предоставляются для получения лицензии?
10. Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?
11. Какие лицензионные требования предъявляются к соискателю лицензии на осуществление лицензируемого вида деятельности по технической защите информации (юридическое лицо)?
12. Какие лицензионные требования предъявляются к соискателю лицензии на осуществление лицензируемого вида деятельности по технической защите информации (физическое лицо)?
13. Какие документы направляет или представляет в лицензирующий орган соискатель для получения лицензии по технической защите информации?

Литература

1. Федеральный закон «О лицензировании отдельных видов деятельности» от 4 мая 2011 года N 99-ФЗ.

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года N 149-ФЗ.

3. Федеральный закон «О техническом регулировании» от 27 декабря 2002 года N 184-ФЗ.

Постановление Правительства РФ от 03.02.2012 N 79 «Положение о лицензировании деятельности по технической защите конфиденциальной информации».

Тема 2.

Практическое занятие №2

Цель занятия:

1. Закрепление теоретических знаний по вопросам аттестации объектов информатизации по требованиям безопасности информации.
2. Получение практических навыков по аттестации объектов информатизации по требованиям безопасности информации.
3. Совершенствование навыков анализа процессов на объектах информатизации и формулировки выводов.

Формируемые компетенции: ПК-3, ПК-6

Время – 4 ч.

1. Подготовка к занятию

1. Ознакомиться с заданием на практическую работу.
2. Ознакомиться с программой практической работы.

2. Распределение времени занятия:

Всего: 180 мин

3. Программа практической работы

Вступительная часть 10 мин.

Основная часть

1. Система объектов информатизации по требованиям безопасности информации. Функции ФСТЭК и органов по аттестации в области аттестации объектов информатизации по требованиям безопасности информации - 40 мин.
2. Исследование этапа подачи заявки на проведение аттестации объекта информатизации на соответствие требованиям безопасности информации - 120 мин.
5. Заключительная часть 10 мин.

4. Методические рекомендации по выполнению практической работы

4.1 Система объектов информатизации по требованиям безопасности информации. Функции ФСТЭК и органов по аттестации в области аттестации объектов информатизации по требованиям безопасности информации

Под объектами информатизации, аттестуемыми по требованиям безопасности информации, понимают автоматизированные системы различного уровня и назначения, системы связи, отображения и размножения, предназначенные для обработки и передачи информации, подлежащей защите, вместе с помещениями, в которых они установлены, а также помещения, предназначенные для ведения конфиденциальных переговоров (рис. 1). То есть

к объектам информатизации относятся объекты ТСПИ (технических систем передачи информации).

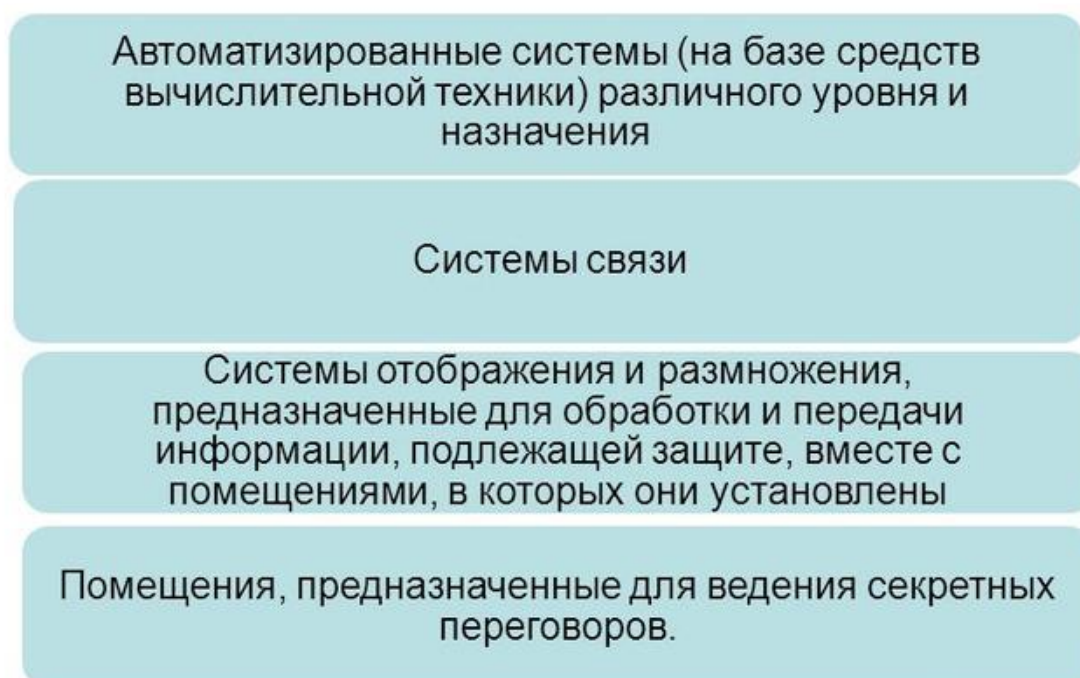


Рисунок 1 – Объекты информатизации, аттестуемые по требованиям безопасности информации

На рис. 2 представлены примеры выделенных помещений (ВП) и автоматизированных систем (АС) и указаны мероприятия, проводимые в них при аттестации.

Различают следующие объекты информатизации по виду обрабатываемой информации:

- 1) объекты информатизации, предназначенные для обработки информации, **содержащей сведения, составляющие государственную тайну;**
- 2) объекты информатизации, предназначенные для обработки **информации конфиденциального характера.**

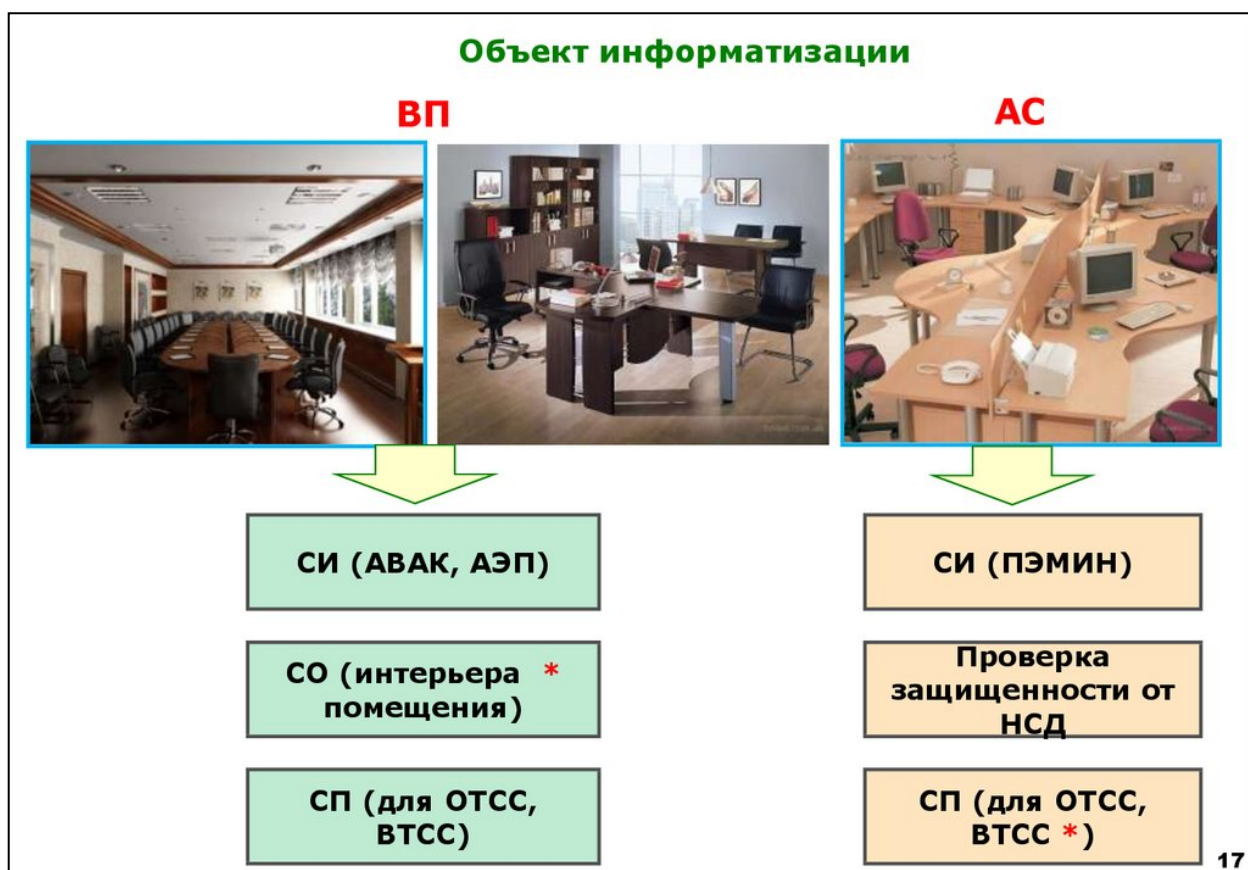


Рисунок 2 - Примеры выделенных помещений и автоматизированных систем и мероприятия при их аттестации

Процедура аттестации для объектов информатизации первого и второго вида отличается друг от друга в части различия органа по аттестации, который может участвовать в этом процессе, что иллюстрируется на рис. 3.

Под **аттестацией объектов информатизации** понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа — «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов иных нормативно — технических документов по безопасности информации, утвержденных федеральным органом по сертификации и аттестации в пределах его компетенции.

Организационную структуру системы аттестации объектов информатизации образуют (рис. 4):

- 1) федеральный орган по сертификации средств и аттестации объектов информатизации по требованиям безопасности информации;
- 2) органы по аттестации объектов информатизации по требованиям безопасности информации;
- 3) испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации;
- 4) заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации).



Рисунок 3 – Взаимосвязь между видами объектов информатизации и органом (организацией), имеющей право на проведение их аттестации

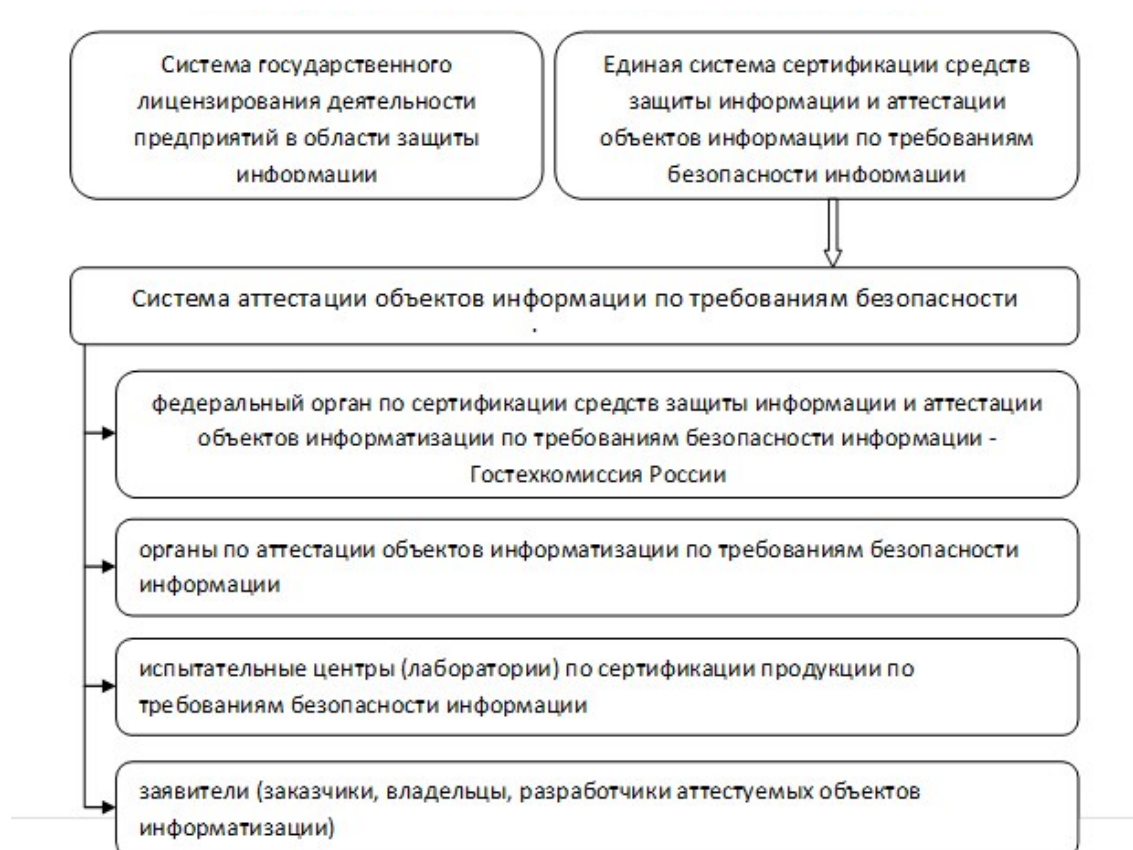


Рисунок 4 - Организационная структура системы аттестации объектов информатизации

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

1) обеспечения безопасности информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере; противодействия иностранным техническим разведкам на территории Российской Федерации;

2) обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;

3) защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

4) осуществления экспортного контроля.

Наличие на объекте информатизации действующего аттестата соответствия дает право обработки информации с уровнем секретности (конфиденциальности) и на период времени, установленном в нем (рис. 5).

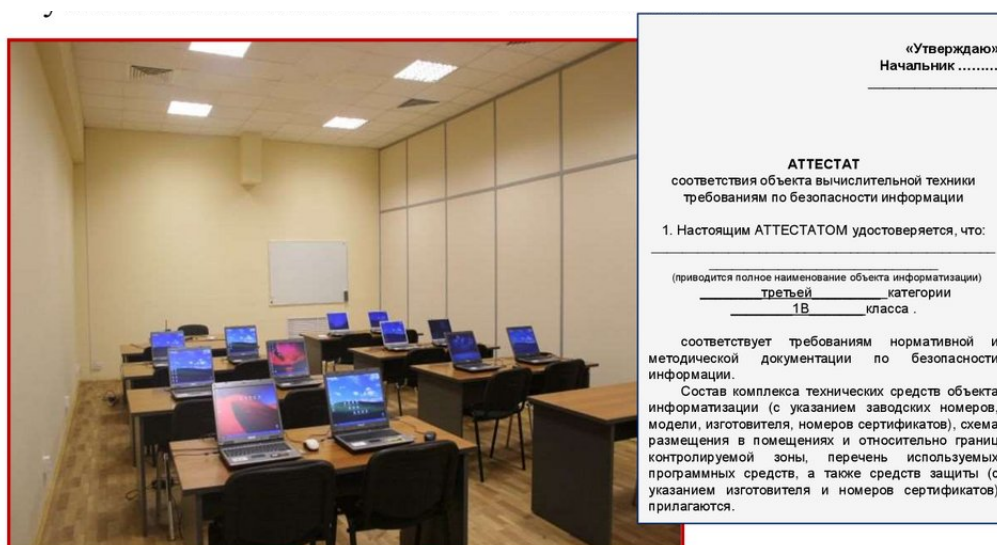


Рисунок 5 – Иллюстрация объекта информатизации и действующего аттестата соответствия

Органы по аттестации это организации, которые непосредственно осуществляют аттестацию объекта информатизации, которые в обязательном порядке аккредитуются ФСТЭК России и получают от нее лицензию на право проведения аттестации объектов информатизации. Правила аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации". Актуальный перечень органов по аттестации представлен на сайте ФСТЭК (рис. 6).

Испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации по заказам заявителей проводят испытания несертифицированной продукции, используемой на объекте информатики, подлежащем обязательной аттестации, в соответствии с «Положением о сертификации средств защиты информации по требованиям безопасности информации».

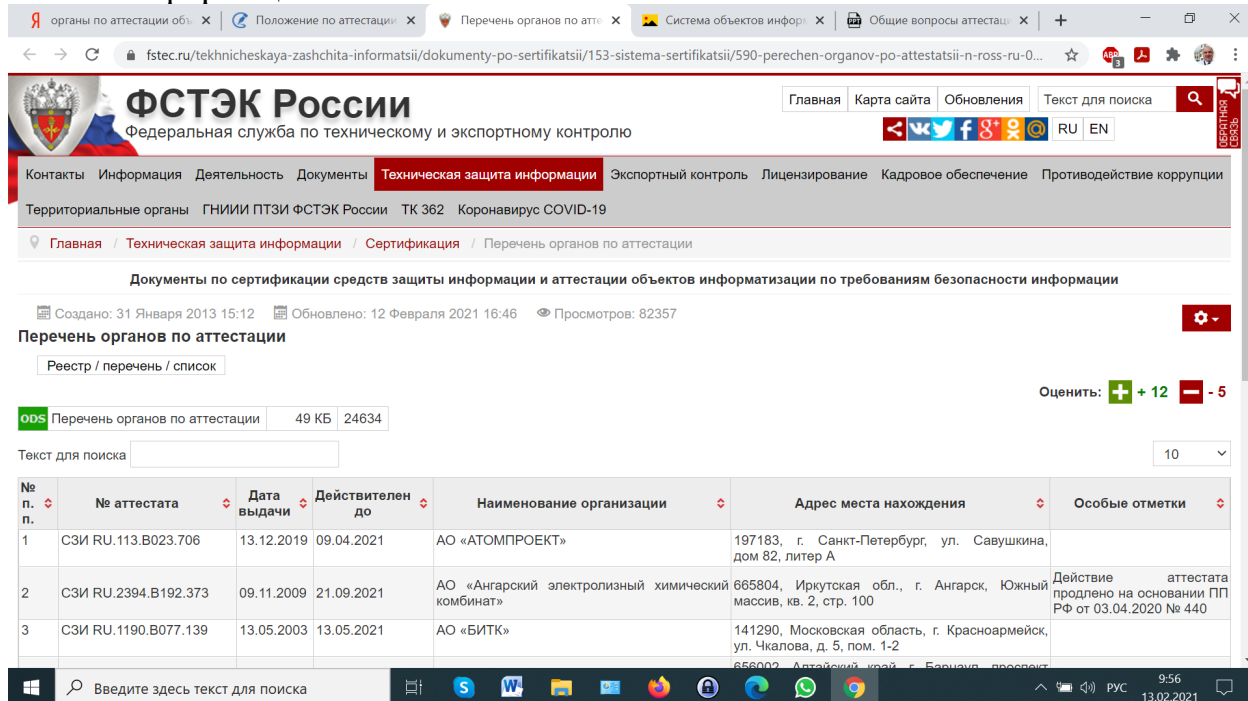


Рисунок 6 – Иллюстрация фрагмента сайта ФСТЭК с перечнем органов по аттестации

Заявители – это организации или физические лица, являющиеся заказчиками, владельцами, разработчиками аттестуемых объектов информатизации.

Расходы по проведению всех работ и услуг по обязательной и добровольной аттестации объектов информатизации оплачивают заявители.

Оплата работ по обязательной аттестации производится в соответствии с договором по утвержденным расценкам в порядке, установленном федеральным органом по сертификации и аттестации в пределах его компетенции, по согласованию с Министерством финансов Российской Федерации, а при их отсутствии – по договорной цене.

Расходы по проведению всех видов работ и услуг по аттестации объектов информатизации оплачивают заявители за счет средств, выделенных на разработку (доработку) и введение в действие защищаемого объекта информатизации.

4.2 Исследование этапа подачи заявки на проведение аттестации объекта информатизации на соответствие требованиям безопасности информации

Аттестация объектов информатизации осуществляется федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями, которым на праве собственности или ином законном основании принадлежат объекты информатизации, а также лицами, заключившими контракт на создание объектов информатизации, или лицами, осуществляющими эксплуатацию объектов информатизации (далее - владельцы объектов информатизации).

Порядок аттестации применяется также для аттестации следующих объектов информатизации, для которых их владельцами установлено требование по проведению оценки соответствия систем защиты информации этих объектов требованиям по защите информации в форме аттестации [1]:

1) значимых объектов критической информационной инфраструктуры Российской Федерации;

2) информационных систем персональных данных (за исключением государственных, муниципальных информационных систем персональных данных);

3) автоматизированных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

Для проведения аттестационных испытаний владелец объекта информатизации привлекает организацию, имеющую лицензию на осуществление деятельности по технической защите конфиденциальной информации (с правом проведения работ и оказания услуг по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации), выданную ФСТЭК России – орган по аттестации.

При изучении данного учебного вопроса необходимо использовать источник [1] п. 11.

Для проведения работ по аттестации владелец объекта информатизации представляет в орган по аттестации следующие документы или их копии:

а) технический паспорт на объект информатизации по форме согласно приложениям №1, 2 к порядку, представленному в [1];

б) акт классификации информационной (автоматизированной) системы по форме согласно приложению №3 к порядку, представленному в [1], акт категорирования значимого объекта критической информационной инфраструктуры Российской Федерации (далее - акт категорирования значимого объекта);

в) модель угроз безопасности информации (в случае ее разработки в соответствии с требованиями по защите информации);

г) техническое задание на создание (развитие, модернизацию) объекта информатизации и (или) частное техническое задание на создание (развитие,

модернизацию) системы защиты информации объекта информатизации (для объекта информатизации, входящего в состав объекта капитального строительства, задание на проектирование (реконструкцию) объекта капитального строительства) (в случае их разработки в ходе создания объекта информатизации);

д) проектную документацию на систему защиты информации объекта информатизации (в случае ее разработки в ходе создания объекта информатизации);

е) эксплуатационную документацию на систему защиты информации объекта информатизации и применяемые средства защиты информации;

ж) организационно-распорядительные документы по защите информации владельца объекта информатизации, регламентирующие защиту информации в ходе эксплуатации объекта информатизации, в том числе план мероприятий по защите информации на объекте информатизации, документы по порядку оценки угроз безопасности информации, управлению (администрированию) системой защиты информации, управлению конфигурацией объекта информатизации, реагированию на инциденты безопасности, информированию и обучению персонала, контролю за обеспечением уровня защищенности информации (далее - документы по защите информации владельца объекта информатизации);

з) документы, содержащие результаты анализа уязвимостей объекта информатизации и приемочных испытаний системы защиты информации объекта информатизации (в случае проведения анализа и испытаний в ходе создания объекта информатизации).

По решению владельца объекта информатизации указанные в настоящем пункте документы (их копии) представляются в орган по аттестации в виде электронных документов.

Рассмотрим начальный этап проведения работ по аттестации объекта информатизации «Подача и рассмотрение заявки на аттестацию».

Заявитель для получения «Аттестата соответствия» заблаговременно направляет в орган по аттестации заявку на проведение аттестации с исходными данными по аттестуемому объекту информатизации по следующей форме.

Приложение 1

Кому: _____
(наименование органа по аттестации
и его адрес)

ЗАЯВКА
на проведение аттестации объекта информатизации

1. (наименование заявителя) просит провести аттестацию (наименование объекта информатизации) на соответствие требованиям по безопасности информации: _____

2. Необходимые исходные данные по аттестуемому объекту информатизации прилагаются.

3. Заявитель готов предоставить необходимые документы и условия для проведения аттестации.

4. Заявитель согласен на договорной основе оплатить расходы по всем видам работ и услуг по аттестации указанного в данной заявке объекта информатизации.

5. Дополнительные условия или сведения для договора:

5.1. Предварительное ознакомление с аттестуемым объектом предлагаю провести в период _____

5.2. Аттестационные испытания объекта информатики предлагаю провести в период _____

5.3. Испытания несертифицированных средств и систем информатизации (наименование средств и систем) предусмотрено провести в испытательных центрах (лабораториях) (наименование испытательных центров) в период _____ (или предлагается провести непосредственно на аттестуемом объекте в период _____).

Другие условия (предложения).

печать

Руководитель (органа заявителя)

(подпись, дата) (Фамилия, И.О.)

Рисунок 6 – Форма заявки на проведение аттестации

К заявке прилагаются исходные данные по аттестуемому объекту информатизации в соответствии с п. 11 порядка, представленного в [1].

На основе анализа документов, предусмотренных пунктом 11 настоящего Порядка, и предварительного ознакомления с объектом информатизации в условиях его эксплуатации орган по аттестации разрабатывает программу и методики аттестационных испытаний.

Срок проведения работ по аттестации объекта информатизации устанавливается владельцем объекта информатизации по согласованию с органом по аттестации, но не может превышать четырех месяцев.

Практическое исследовательское задание №1

Вы являетесь заявителем аттестуемого объекта (организация: ФГАОУ ВО «Северо-Кавказский федеральный университет», номер аудитории выбирается в соответствии с вариантом).

Вам необходимо получить аттестат соответствия объекта информатизации. Опишите Ваши действия для получения данного аттестата на этапе подачи заявки на проведение аттестации указанного помещения в орган по

аттестации (указаны на сайте ФСТЭК). Исходные данные возьмите из таблицы 1.

Практическое исследовательское задание №2

Вы являетесь органом по аттестации объекта информатизации. Опишите Ваши действия по аттестации объекта информатизации, оговоренного в практическом исследовательском задании №1. Выберите схему аттестации с учетом характера и уровня секретности обрабатываемой информации. Обоснуйте свое решение.

Таблица 1 – Исходные данные и варианты заданий

вариант	№9. Корпус №	Характер и уровень секретности	Наименование органа по аттестации
1	аудитории, назначение учебная	НТИ*, общедоступная	ФГБОУ ВО «АГТУ».
2	310, конф. делопроизводство	Эконом. , обработка коммерческой тайны	ФГАОУ ВО «Самарский национальный исследовательский университет имени академика С.П.Королева».
3	312, учебная	Производственная, обработка ПДн	ФГАОУ ВО «НИУ «МИЭТ».
4	314, АП ГИС	Производственная, обработка ПДн	ФГАНУ «Спецвузавтоматика». НИИ
5	513, делопроизводство ГТ	Производственная, обработка ГТ***	ФАУ «ГНИИИ ПТЗИ ФСТЭК России».
6	514, открытое делопроизводство	Производственная, открытый документооборот	Управление МВД России по Астраханской области.
7	516, служебное делопроизводство	Производственная, служебная тайна	УФК по Волгоградской области.

8	310, учебная	Производственная, обработка ПДн	УМВД России по г. Севастополю.
9	311, делопроизводство ГТ	Производственная, обработка ГТ***	Симферопольский НТЦ ФГУП «НПП «Гамма».
10	312, учебная	НТИ*, общедоступная	Представительство АО «СофтЛайн Трейд» в г. Воронеж.
11	314, учебная	Производственная, обработка ПДн	Ростовский НТЦ ФГУП «НПП «Гамма».
12	513, конф. делопроизводство	Эконом., обработка коммерческой тайны	С-КАВ ж.д. ОАО «РЖД».
13	514, АП ГИС	Производственная, обработка ПДн	ОТС-филиал РТУ РЭБОТИ (г. Ростов-на-Дону).
14	516, открытое делопроизводство	Производственная, открытый документооборот	ООО АКБ «Барьер».
15	310, служебное делопроизводство	Производственная, служебная тайна	ООО «РАЦ».
16	311, АП ГИС	Производственная, обработка ПДн	ООО «РЦИБ».
17	312, конф. делопроизводство	Эконом., обработка коммерческой тайны	ООО «МТУ «Телеком-С».
18	314, делопроизводство ГТ	Производственная, обработка ГТ***	ООО «Информационные системы и аутсорсинг».

19	513, учебная	Производственная, обработка ПДн	ООО «Каскад».	
20	514, открытое делопроизводство	Производственная, открытый документооборот	ГУ МВД России по Ставропольскому краю.	
21	516, учебная	Производственная, обработка ПДн	ООО «Идентификация».	
22	310, служебное делопроизводство	Производственная, служебная тайна	ООО «Геро».	
23	311, АП ГИС	Производственная, обработка ПДн	ООО «АТЭК-С».	
24	312, конф. делопроизводство	Эконом., обработка коммерческой тайны	МВД по Республике Дагестан.	
25	314, делопроизводство ГТ	Производственная, обработка ГТ***	МВД по Республике Калмыкия.	
26	513, учебная	Производственная, обработка ПДн	МВД по Республике Северная Осетия-Алания.	
27	514, открытое делопроизводство	Производственная, открытый документооборот	МВД по Республике Крым.	
28	516, учебная	Производственная, обработка ПДн	ЗАО «Контур-Сервис ТВ».	

29	310, учебная	НТИ*, общедоступна я	ООО «Евромост-Защита».
30	311, конф. делопроизво дство	Эконом. , обработка коммерческой тайны	АО «НПО «Инфобезопасность».

Примечания:

*НТИ – научно-техническая информация;

**АП ГИС – абонентский пункт государственной информационной системы;

*** ГТ – государственная тайна.

5. Контрольные вопросы

1. Объекты информатизации, аттестуемые по требованиям безопасности информации, и их характеристика.
2. Основные виды объектов информатизации по виду обрабатываемой информации.
3. Определение выделенных помещений и мероприятия при их аттестации.
4. Определение автоматизированных систем и мероприятия при их аттестации.
5. Организационная структура системы аттестации объектов информатизации.
6. Назначение Федеральной службы по техническому и экспортному контролю (ФСТЭК России).
7. Основные функции органов по аттестации при аттестации объектов информатизации.
8. Основные функции испытательных центров (лабораторий) по сертификации продукции по требованиям безопасности информации.
9. Основные функции заявителей при аттестации объектов информатизации.
10. Порядок проведения аттестации объектов информатизации на соответствие требованиям безопасности информации.
11. Характеристика этапа «Подача и рассмотрение заявки на аттестацию».
12. Приведите перечень исходных данных, прилагаемых к заявке по аттестуемому объекту информатизации.

Литература

1. ПРИКАЗ Федеральной службы по техническому и экспортному контролю от 29 апреля 2021 года №77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

Тема 3.

Практическое занятие №3

Цель занятия:

1. Закрепление теоретических знаний по вопросам аттестации объектов информатизации по требованиям безопасности информации.
2. Получение практических навыков по аттестации объектов информатизации по требованиям безопасности информации.
3. Совершенствование навыков анализа процессов на объектах информатизации и формулировки выводов.

Формируемые компетенции: ПК-3, ПК-6

Время – 4 ч.

1. Подготовка к занятию

1. Ознакомиться с заданием на практическую работу.
2. Ознакомиться с программой практической работы.

2. Распределение времени занятия:

Всего: 180 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

3. Программа практической работы

Вступительная часть 10 мин.

Основная часть

1. Изучение порядка предварительного ознакомления с аттестуемым объектом – 20 мин.
2. Исследование процесса предварительного ознакомления с аттестуемым объектом - 120 мин.
5. Заключительная часть 10 мин.

4. Методические рекомендации по выполнению практической работы

4.1 Изучение порядка предварительного ознакомления с аттестуемым объектом

Для проведения аттестационных испытаний владелец объекта информатизации привлекает организацию, имеющую лицензию на осуществление деятельности по технической защите конфиденциальной информации (с правом проведения работ и оказания услуг по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации), выданную ФСТЭК России в соответствии с Положением о лицензировании деятельности по технической защите конфиденциальной информации,

утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79.

Для проведения аттестационных испытаний органом по аттестации из числа своих работников назначается аттестационная комиссия в составе руководителя комиссии и не менее двух экспертов, обладающих знаниями и навыками в области технической защиты конфиденциальной информации и аттестации объектов информатизации (далее – эксперты органа по аттестации).

При назначении экспертов органа по аттестации должна быть обеспечена их независимость от владельца объекта информатизации с целью исключения возможности влияния владельца аттестуемого объекта информатизации на результаты аттестационных испытаний, проведенных экспертами органа по аттестации.

Назначение экспертов органов по аттестации из числа работников, участвующих в разработке и (или) внедрении системы защиты информации объекта информатизации, не допускается.

Эксперты органа по аттестации проводят анализ документов, представляемых владельцем объекта информатизации в соответствии с пунктом 11 Приказа ФСТЭК РФ №77 от 29.04.2021г., и аттестационные испытания объекта информатизации в соответствии с требованиями по технической защите информации, который изложен в следующем виде.

Пункт 11 Приказа ФСТЭК РФ №77 от 29.04.2021г.

Для проведения работ по аттестации владелец объекта информатизации представляет в орган по аттестации следующие документы или их копии:

а) технический паспорт на объект информатизации по форме согласно приложениям № 1, 2 к настоящему Порядку;

б) акт классификации информационной (автоматизированной) системы по форме согласно приложению № 3 к настоящему Порядку, акт категорирования значимого объекта критической информационной инфраструктуры Российской Федерации (далее – акт категорирования значимого объекта);

в) модель угроз безопасности информации (в случае ее разработки в соответствии с требованиями по защите информации);

г) техническое задание на создание (развитие, модернизацию) объекта информатизации и (или) частное техническое задание на создание (развитие, модернизацию) системы защиты информации объекта информатизации (для объекта информатизации, входящего в состав объекта капитального строительства, задание на проектирование (реконструкцию) объекта капитального строительства) (в случае их разработки в ходе создания объекта информатизации);

д) проектную документацию на систему защиты информации объекта информатизации (в случае ее разработки в ходе создания объекта информатизации);

е) эксплуатационную документацию на систему защиты информации объекта информатизации и применяемые средства защиты информации;

ж) организационно-распорядительные документы по защите информации владельца объекта информатизации, регламентирующие защиту информации в ходе эксплуатации объекта информатизации, в том числе план мероприятий по защите информации на объекте информатизации, документы по порядку оценки угроз безопасности информации, управлению (администрированию) системой защиты информации, управлению конфигурацией объекта информатизации, реагированию на инциденты безопасности, информированию и обучению персонала, контролю за обеспечением уровня защищенности информации(далее – документы по защите информации владельца объекта информатизации);

з) документы, содержащие результаты анализа уязвимостей объекта информатизации и приемочных испытаний системы защиты информации объекта информатизации (в случае проведения анализа и испытаний в ходе создания объекта информатизации).

По решению владельца объекта информатизации указанные в настоящем пункте документы (их копии) представляются в орган по аттестации в виде электронных документов.

Выводы экспертов органа по аттестации по результатам проведенных аттестационных испытаний не должны противоречить требованиям по технической защите информации.

Срок проведения работ по аттестации объекта информатизации устанавливается владельцем объекта информатизации по согласованию с органом по аттестации, но не может превышать четырех месяцев.

Информация об объекте информатизации, полученная органом по аттестации в ходе аттестации объекта информатизации, подлежит защите в соответствии с частью 4 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

На основе анализа документов, предусмотренных пунктом 11 источника [1], и предварительного ознакомления с объектом информатизации в условиях его эксплуатации орган по аттестации разрабатывает программу и методики аттестационных испытаний.

При изучении первого учебного вопроса необходимо использовать источник [1] п.п. 5-12 с. 6-8.

При недостаточности исходных данных по аттестуемому объекту информатизации в схему аттестации включаются работы по предварительному ознакомлению с аттестуемым объектом, проводимые до этапа аттестационных испытаний.

При использовании на аттестуемом объекте информатизации несертифицированных средств и систем защиты информации в схему аттестации могут быть включены работы по их испытаниям в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям

безопасности информации или непосредственно на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств.

Испытания отдельных несертифицированных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации проводятся до аттестационных испытаний объектов информатизации. В этом случае заявителем к началу аттестационных испытаний должны быть представлены заключения органов по сертификации средств защиты информации по требованиям безопасности информации и сертификаты.

4.2 Исследование процесса предварительного ознакомления с аттестуемым объектом

Практическое исследовательское задание №1

В соответствии с исходными данными, представленными в приложении А (таблица А1), провести предварительное ознакомление с аттестуемым объектом. В процессе предварительного ознакомления изучить особенности помещения объекта информатизации, особенности прокладки электропроводки, электрических кабелей системы охранно-пожарной сигнализации, местоположение основных и вспомогательных технических средств, а также линий телекоммуникаций, подключенных к ним. Также на данном этапе необходимо уточнить границы контролируемой зоны.

Результаты ознакомления представить в виде план-схемы изучаемого помещения, изображенной с помощью графического редактора Microsoft Visio.

Для примера на рисунке 1 показан вариант план-схемы изучаемого помещения. На рисунке красным цветом показаны линии охранно-пожарной сигнализации, синим цветом показаны линии электропитания 220 В светильников и розеток.

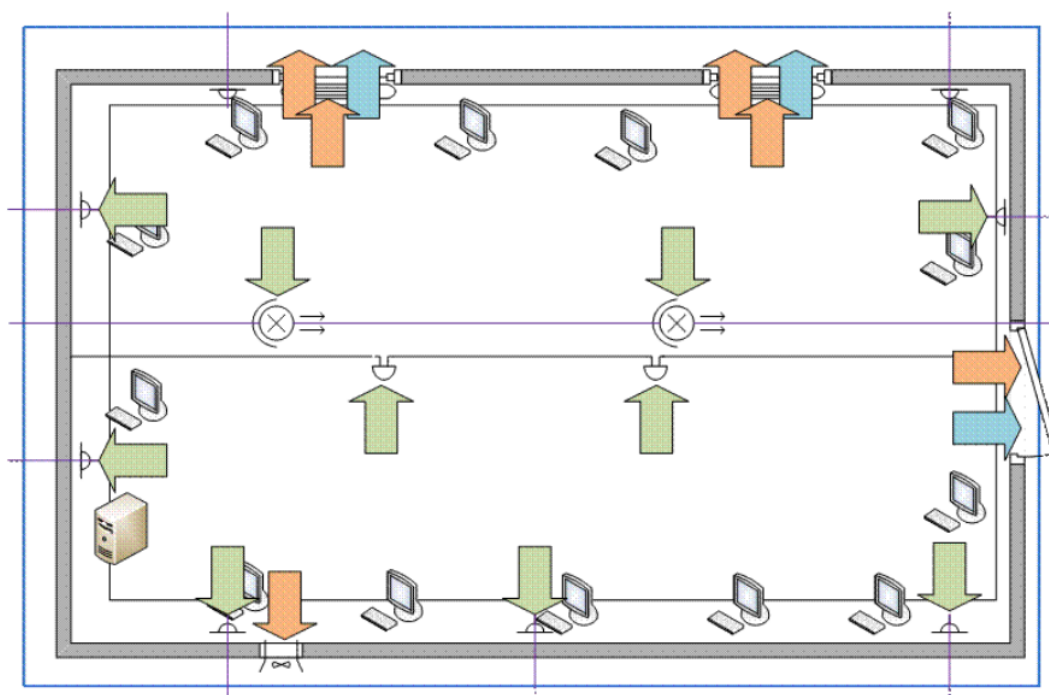


Рисунок 2 - Схема индикаторов технических каналов утечки информации (ТКУИ) изучаемого помещения

Далее для рассматриваемого помещения необходимо разработать план-схему возможных способов съема информации в изучаемом помещении. Вариант план-схемы возможных способов съема информации в изучаемом помещении представлен на рис. 3.

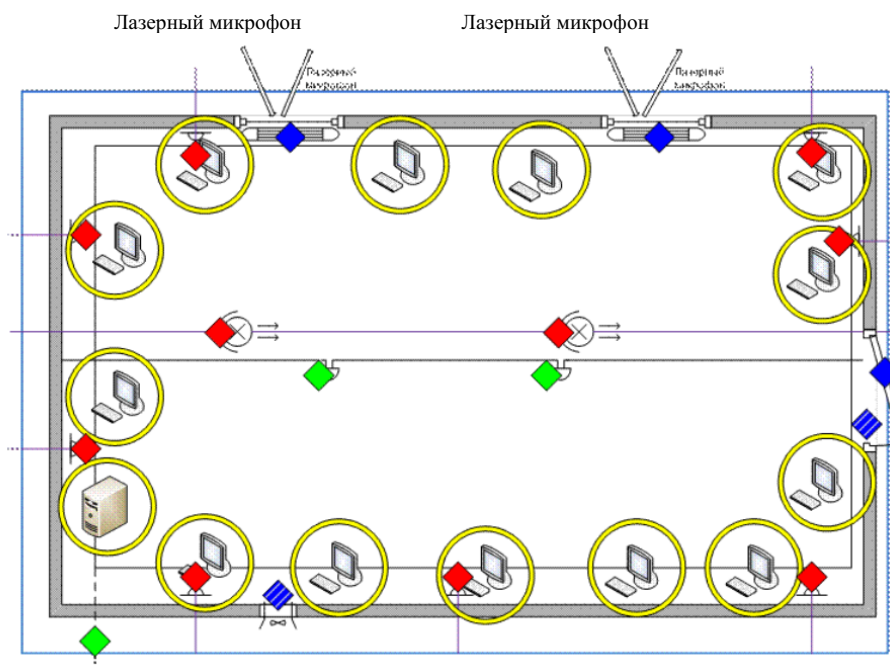


Рисунок 3 - Вариант схемы возможных способов съема информации в изучаемом помещении

На рис. 3 используются следующие обозначения.

 - съем информации по электрическому каналу сети электропитания 220 В (фильтрация полезного сигнала);

 - съем информации за счет побочных электромагнитных излучений и наводок (с помощью средств выделения полезного сигнала из ПЭМИН);

 - съем информации по акустическому каналу утечки информации (направленные микрофоны, лазерные микрофоны и др.);

 - съем информации по электрическому каналу утечки информации (радиозакладки, электромагнитные преобразователи и др.);

 - съем информации по виброакустическому каналу утечки информации (стетоскоп, виброакустический преобразователь и др.).

С учетом составленных схем и размещаемого в изучаемом помещении оборудования, ОТСС и ВТСС составить исходные данные по аттестуемому объекту информатизации по следующим разделам:

1. Полное и точное название объекта информатизации, его назначение.
2. Характер обрабатываемой конфиденциальной информации. Наличие информации с уровнем секретности (для государственной тайны).
3. Организационную структуру объекта информатизации.
4. Перечень оборудования, установленного на рассматриваемом объекте информатизации. Например

Таблица 1 - Перечень оборудования, установленного на рассматриваемом объекте информатизации

№ п/п	Наимено вание оборудования	Мо дель	Заводс кой номер	Изготов итель
1	2	3	4	5
		ОТСС		
1	ПЭВМ 1	DE LL A8	400126 73412	DELL
2				
....				
N	ПЭВМ N	DE LL A8	400126 73412	DELL
		ВТСС		
N	Извещат	Op	329000	Орион
+1	ели ОПС	ион Ф-1	004	
N	Пульт	Op	389770	Орион
+2	управления	ион ПУ	004	
				
				

5. Особенности и схему расположения объекта информатизации с указанием границы контролируемой зоны (рис. 1).

6. Структуру используемого программного обеспечения. Например:

Таблица 2 - Структура используемого программного обеспечения на рассматриваемом объекте информатизации

Наименование	Характеристика
Windows 8	Операционная система ПЭВМ
Windows 10	Универсальная операционная система ПЭВМ
Maple	Мощная математическая программа. Позволяет рассчитывать сложные математические модели и строить сложнейшие графики
MathCAD	Один из лучших математических пакетов. Поддерживает различные математические операции
MatLAB	Программа, выполняющая множество задач для поддержки научных и инженерных работ, начиная со сбора и анализа данных до разработки приложений. Среда программы объединяет математические вычисления, визуализацию и мощный технический язык
AutoCAD	Система автоматизированного проектирования, предоставляющая совершенные средства двумерного проектирования и оформления чертежей, а также удобные средства трехмерного моделирования
3ds MAX	Программа 3D моделирования, анимации и рендеринга
GraphiSoft ArchiCAD	Специализированное средство для строительного проектирования, изначально разработанное для решения архитектурных задач
Revit Architecture	Программа 3D моделирования архитектурных и инженерных решений здания
Complete Home Designer	Программа, предоставляющая все необходимые инструменты для создания полноценного проекта здания, его модернизации и реконструкции
Microsoft Office Word	Текстовый редактор (процессор)
Microsoft Office Excel	Приложение для работы с электронными таблицами
Microsoft Office Access	Приложение для управления реляционными базами данных
Microsoft Office PowerPoint	Приложение для подготовки презентаций. Позволяет создавать материалы профессионального

Наименование	Характеристика
	качества, которые могут применяться для личных целей или размещаться в Интернете
Microsoft Office Publisher	Приложение для подготовки публикаций. Существенно упрощает создание, оформление и публикацию маркетинговых и информационных материалов профессионального качества
Microsoft Visio	Программное средство для построения схем и диаграмм различного типа, а также для наглядного представления бизнес-процессов

7. Режим обработки конфиденциальной информации: однопользовательский, многопользовательский.

8. Описание системы защиты информации, используемой на объекте информатизации. Например, в соответствии с рис. 1-3: система защиты информации организована на основе системы ОПС с пультом управления на вход в помещение.

9. Технические и программные средства в защищённом исполнении, средства защиты и контроля на аттестуемом объекте информатизации. Например, отсутствуют (или перечислить имеющиеся).

10. Наличие на аттестуемом объекте информатизации службы безопасности информации, службы администратора (автоматизированной системы, сети, базы данных).

Например, администратор – сотрудник кафедры ОТЗИ. Служба безопасности отсутствует.

11. Наличие и основные характеристики физической защиты объекта информатизации.

Например, отсутствие посторонних лиц в аудитории обеспечивается сотрудниками службы комплексной безопасности на КПП учебного корпуса №Х, за счет механического замка и системы ОПС.

12. Руководство по защите информации на объекте информатизации. Например, отсутствует.

13. Схема индикаторов технических каналов утечки информации (ТКУИ) изучаемого помещения (рис. 2).

14. Схема возможных способов съема информации в изучаемом помещении.

15. Перечень и характеристика возможных ТКУИ. Например:

Электромагнитные каналы утечки информации,
обрабатываемой средствами вычислительной техники:

- побочные электромагнитные излучения, возникающие вследствие протекания информативных сигналов по элементам ТСОИ;
- модуляция информативным сигналом побочных электромагнитных излучений высокочастотных генераторов ТСОИ (на частотах работы высокочастотных генераторов);
- модуляция информативным сигналом паразитного электромагнитного излучения ТСОИ (например, возникающего вследствие самовозбуждения усилителей низкой частоты).

Побочные электромагнитные излучения и наводки возникают при следующих режимах обработки информации средствами вычислительной техники:

- вывод информации на экран монитора;
- ввод данных с клавиатуры;
- запись информации на накопители;
- чтение информации с накопителей;
- передача данных в каналы связи;
- вывод данных на периферийные печатные устройства - принтеры, плоттеры; запись данных от сканера на магнитный носитель и т.д.

и др.

Акустический канал утечки информации:

- перехват акустического сигнала микрофонами, объединенными с устройствами записи (диктофонами);
- перехват акустического сигнала направленными микрофонами через открытые окна помещения, направленными во двор университета;
- перехват акустического сигнала микрофонами, объединенными с устройствами передачи акустического сигнала по радиоканалу (радиозакладками);
- перехват акустического сигнала микрофонами, объединенными с устройствами передачи акустического сигнала по электрическим цепям (проводная закладка);
- перехват акустического сигнала микрофонами, объединенными с устройствами передачи акустического сигнала по оптическому каналу в ИК-диапазоне (ИК-закладками);
- перехват акустического сигнала микрофонами, объединенными с устройствами передачи акустического сигнала по телефонной линии.

И др.

Приложение А

Таблица А1 – Исходные данные и варианты заданий

варианта	Корпус №9. № аудитории, назначение	Характер и уровень секретности	Наименование органа по аттестации
31	310, учебная	НТИ*, общедоступная	ФГБОУ ВО «АГТУ».
32	311, конф. делопроизводство	Эконом., обработка коммерческой тайны	ФГАОУ ВО «Самарский национальный исследовательский университет имени академика С.П. Королева».
33	312, учебная	Производственная, обработка ПДн	ФГАОУ ВО «НИУ «МИЭТ».
34	314, АП ГИС	Производственная, АП ГИС**	ФГАНУ НИИ «Спецвузавтоматика».
35	513, делопроизводство ГТ	Производственная, обработка ГТ***	ФАУ «ГНИИИ ПТЗИ ФСТЭК России».
36	514, открытое делопроизводство	Производственная, открытый документооборот	Управление МВД России по Астраханской области.
37	516, служебное делопроизводство	Производственная, служебная тайна	УФК по Волгоградской области.
38	310, учебная	Производственная, обработка ПДн	УМВД России по г. Севастополю.
39	311, делопроизводство ГТ	Производственная, обработка ГТ***	Симферопольский НТЦ ФГУП «НПП «Гамма».

40	312, учебная	НТИ*, общедоступна я	Представительство «СофтЛайн Трейд» в г. Воронеж. АО
41	314, учебная	Произво дственная, обработка ПДн	Ростовский НТЦ ФГУП «НПП «Гамма».
42	513, конф. делопроизво дство	Эконом. , обрабока коммерческой тайны	С-КАВ ж.д. ОАО «РЖД».
43	514, АП ГИС	Произво дственная, АП ГИС**	ОТС-филиал РТУ РЭБОТИ (г. Ростов-на-Дону).
44	516, открытое делопроизво дство	Произво дственная, открытый документообо рот	ООО АКБ «Барьер».
45	310, служебное делопроизво дство	Произво дственная, служебная тайна	ООО «РАЦ».
46	311, АП ГИС	Произво дственная, АП ГИС**	ООО «РЦИБ».
47	312, конф. делопроизво дство	Эконом. , обрабока коммерческой тайны	ООО «МТУ «Телеком-С».
48	314, делопроизво дство ГТ	Произво дственная, обработка ГТ***	ООО «Информационные системы и аутсорсинг».
49	513, учебная	Произво дственная, обработка ПДн	ООО «Каскад».
50	514, открытое делопроизво дство	Произво дственная, открытый документообо рот	ГУ МВД России по Ставропольскому краю.

51	516, учебная	Производственная, обработка ПДн	ООО «Идентификация».
52	310, служебное делопроизводство	Производственная, служебная тайна	ООО «Геро».
53	311, АП ГИС	Производственная, АП ГИС**	ООО «АТЭК-С».
54	312, конф. делопроизводство	Эконом., обработка коммерческой тайны	МВД по Республике Дагестан.
55	314, делопроизводство ГТ	Производственная, обработка ГТ***	МВД по Республике Калмыкия.
56	513, учебная	Производственная, обработка ПДн	МВД по Республике Северная Осетия-Алания.
57	514, открытое делопроизводство	Производственная, открытый документооборот	МВД по Республике Крым.
58	516, учебная	Производственная, обработка ПДн	ЗАО «Контур-Сервис ТВ».
59	310, учебная	НТИ*, общедоступная	ООО «Евромост-Защита».
60	311, конф. делопроизводство	Эконом., обработка коммерческой тайны	АО «НПО «Инфобезопасность».

Примечания:

*НТИ – научно-техническая информация;

**АП ГИС – абонентский пункт государственной информационной системы;

*** ГТ – государственная тайна.

5. Контрольные вопросы

1. В каком случае и каким образом проводятся работы по предварительному ознакомлению с аттестуемым объектом?
2. Поясните, что и каким образом указывается на план-схеме изучаемого помещения?
3. Поясните, что и каким образом указывается схеме индикаторов технических каналов утечки информации (ТКУИ) изучаемого помещения?
4. Поясните, что и каким образом указывается схеме возможных способов съема информации в изучаемом помещении?
5. Поясните состав перечня оборудования, установленного на рассматриваемом объекте информатизации.
6. Поясните структуру используемого программного обеспечения на рассматриваемом объекте информатизации.
7. Поясните что входит в перечень и характеристику возможных ТКУИ?

Литература

2. Приказ ФСТЭК РФ от 29 апреля 2021 г. N 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

Тема 4.

Практическое занятие № 4

Цель занятия:

1. Закрепление теоретических знаний по вопросам аттестации объектов информатизации по требованиям безопасности информации.
2. Получение практических навыков по классификации автоматизированных систем при аттестации объектов информатизации по требованиям безопасности информации.
3. Совершенствование навыков анализа процессов при аттестации объектов информатизации по требованиям безопасности информации и формулировки выводов.

Формируемые компетенции: ПК-3, ПК-6

Время – 4 ч.

1. Подготовка к занятию

1. Ознакомиться с заданием на практическую работу.
2. Ознакомиться с программой практической работы.

2. Распределение времени занятия:

Всего: 180 мин

Вступительная часть 2 мин

Проверка готовности студентов к занятию 5 мин

3. Программа практической работы

Вступительная часть 10 мин.

Основная часть

1. Изучение порядка классификации автоматизированных систем при аттестации объектов информатизации по требованиям безопасности информации – 50 мин.
2. Разработка акта классификации автоматизированных систем - 110 мин.
5. Заключительная часть 10 мин.

4. Изучение порядка классификации автоматизированных систем при аттестации объектов информатизации по требованиям безопасности информации

4.1 Классификация защищённости автоматизированных систем

Классификация объекта информатизации осуществляется на основании руководящего документа «Автоматизированные системы. Защита от

несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.).

Классификация распространяется на все действующие и проектируемые АС учреждений, организаций и предприятий, обрабатывающие конфиденциальную информацию.

Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации.

Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала.

Основными этапами классификации АС являются:

- разработка и анализ исходных данных;
- выявление основных признаков АС, необходимых для классификации;
- сравнение выявленных признаков АС с классифицируемыми;
- присвоение АС соответствующего класса защиты информации от НСД.

Необходимыми исходными данными для проведения классификации конкретной АС являются:

- перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;
- перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;
- матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;
- режим обработки данных в АС.

Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации.

К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- режим обработки данных в АС - коллективный (многопользовательский) или индивидуальный (однопользовательский).

Устанавливается **девять классов защищенности** АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС (рис. 1).



Рисунок 1 - Иерархия классов защищенности АС

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или)

хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

4.2 Определение класса защищенности государственной информационной системы

Определение класса защищенности государственной информационной системы осуществляется в соответствии с приказом ФСТЭК РФ от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Класс защищенности информационной системы (**первый класс (К1), второй класс (К2), третий класс (К3)**) определяется в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый).

Уровень значимости информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации.

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)],

где степень возможного ущерба определяется обладателем информации (заказчиком) и (или) оператором самостоятельно экспертным или иными методами и может быть:

1) высокой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции;

2) средней, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций;

3) низкой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

Информация имеет высокий уровень значимости (УЗ 1), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба.

Информация имеет средний уровень значимости (УЗ 2), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба.

Информация имеет низкий уровень значимости (УЗ 3), если для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

При обработке в информационной системе двух и более видов информации (служебная тайна, налоговая тайна и иные установленные законодательством Российской Федерации виды информации ограниченного доступа) уровень значимости информации (УЗ) определяются отдельно для каждого вида информации. Итоговый уровень значимости информации, обрабатываемой в информационной системе, устанавливается по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности, доступности информации каждого вида информации.

Класс защищенности государственной информационной системы определяется в соответствии с таблицей 1.

Таблица 1 - Классы защищенности государственных информационных систем

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	K1	K1	K1
УЗ 2	K1	K2	K2
УЗ 3	K2	K3	K3

4.3 Определение уровня защищённости информационных систем персональных данных

При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

Определение требуемого уровня защищенности персональных данных при их обработке в информационных системах персональных данных осуществляется в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных» (утв. постановлением Правительства РФ от 1 ноября 2012 г. №1119).

Определяющие признаки при определении уровня защищенности персональных данных (рис. 2):

- категория обрабатываемых персональных данных:
 - 1) ИСПДн-С – специальные.
 - 2) ИСПДн-Б – биометрические.
 - 3) ИСПДн-О – общедоступные.
 - 4) ИСПДн-И иные.
- категория субъектов персональных данных (сотрудники оператора, не являющиеся сотрудниками оператора)
 - актуальные угрозы (АУ) безопасности персональных данных (угрозы 1-го, 2-го, 3-го типа)
 - количество субъектов персональных данных (менее 10 000, более 10 000)

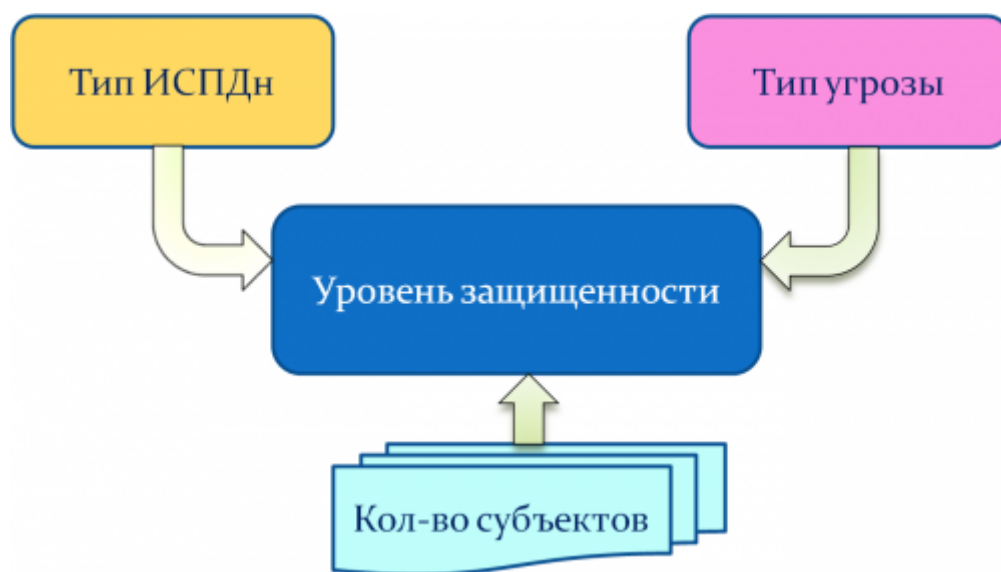


Рисунок 2 - Определяющие признаки при определении уровня защищенности персональных данных

Уровень защищенности персональных данных определяется в соответствии с таблицей 2.

Таблица 2 - Уровни защищенности персональных данных

Категория ПДн + количество	АУ 1 типа	АУ 2 типа	АУ 3 типа
----------------------------	--------------	--------------	--------------

ИСПДн-С более чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора	1	1	2
ИСПДн-С сотрудников оператора или специальные категории персональных данных менее чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора	1	2	3
ИСПДн-Б	1	2	3
ИСПДн-И более чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора	1	2	3
ИСПДн-И данных сотрудников оператора или иные категории ПДн менее чем 100000 субъектов ПДн, не являющихся сотрудниками оператора	1	3	4
ИСПДн-О более чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора	2	2	4
ИСПДн-О сотрудников оператора или общедоступные ПДн менее чем 100 000 субъектов ПДн, не являющихся сотрудниками оператора	2	3	4

4.4 Определение класса защищённости автоматизированных систем управления производственными и технологическими процессами

Определение класса защищенности государственной информационной системы управления производственными и технологическими процессами (АСУ ТП) осуществляется в соответствии с приказом ФСТЭК РФ от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Класс защищенности автоматизированной системы управления (первый класс (К1), второй класс (К2), третий класс (К3)) определяется в зависимости от уровня значимости (критичности) обрабатываемой в ней информации (УЗ).

Уровень значимости (критичности) информации (УЗ) определяется степенью возможного ущерба от нарушения ее целостности (неправомерные уничтожение или модифицирование), доступности (неправомерное блокирование) или конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), в результате которого возможно нарушение штатного режима функционирования автоматизированной системы

управления или незаконное вмешательство в процессы функционирования автоматизированной системы управления.

УЗ = [(целостность, степень ущерба) (доступность, степень ущерба) (конфиденциальность, степень ущерба)],

где степень возможного ущерба определяется заказчиком или оператором экспертным или иным методом и может быть:

1) высокой, если в результате нарушения одного из свойств безопасности информации (целостности, доступности, конфиденциальности), повлекшего нарушение штатного режима функционирования автоматизированной системы управления, возможно возникновение чрезвычайной ситуации федерального или межрегионального характера* или иные существенные негативные последствия в социальной, политической, экономической, военной или иных областях деятельности;

2) средней, если в результате нарушения одного из свойств безопасности информации (целостности, доступности, конфиденциальности), повлекшего нарушение штатного режима функционирования автоматизированной системы управления, возможно возникновение чрезвычайной ситуации регионального или межмуниципального характера* или иные умеренные негативные последствия в социальной, политической, экономической, военной или иных областях деятельности;

3) низкой, если в результате нарушения одного из свойств безопасности информации (целостности, доступности, конфиденциальности), повлекшего нарушение штатного режима функционирования автоматизированной системы управления, возможно возникновение чрезвычайной ситуации муниципального (локального) характера или возможны иные незначительные негативные последствия в социальной, политической, экономической, военной или иных областях деятельности.

В случае, если для информации, обрабатываемой в автоматизированной системе управления, не требуется обеспечение одного из свойств безопасности информации (в частности конфиденциальности) уровень значимости (критичности) определяются для двух других свойств безопасности информации (целостности, доступности). В этом случае:

УЗ = [(целостность, степень ущерба) (доступность, степень ущерба) (конфиденциальность, не применяется)].

Информация, обрабатываемая в автоматизированной системе управления, имеет **высокий уровень значимости (критичности) (УЗ 1)**, если хотя бы для одного из свойств безопасности информации (целостности, доступности, конфиденциальности) определена высокая степень ущерба.

Информация, обрабатываемая в автоматизированной системе управления, имеет **средний уровень значимости (критичности) (УЗ 2)**, если хотя бы для одного из свойств безопасности информации (целостности, доступности, конфиденциальности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба.

Информация, обрабатываемая в автоматизированной системе управления, имеет **низкий уровень значимости (критичности) (УЗ 3)**, если для всех свойств безопасности информации (целостности, доступности, конфиденциальности) определены низкие степени ущерба.

При обработке в автоматизированной системе управления двух и более видов информации (измерительная информация, информация о состоянии процесса) уровень значимости (критичности) информации (УЗ) определяется отдельно для каждого вида информации. Итоговый уровень значимости (критичности) устанавливается по наивысшим значениям степени возможного ущерба, определенным для целостности, доступности, конфиденциальности каждого вида информации.

Класс защищенности автоматизированной системы управления определяется в соответствии с таблицей 3.

Таблица 3 - Классы защищенности автоматизированных систем управления

Уровень значимости (критичности) информации	Класс защищенности автоматизированной системы управления
УЗ 1	К1
УЗ 2	К2
УЗ 3	К3

4.5 Изучение порядка классификации автоматизированных систем при аттестации объектов информатизации по требованиям безопасности информации

Для проведения классификации автоматизированной системы (информационной системы, государственной информационной системы, информационной системы персональных данных, государственной информационной системы управления производственными и технологическими процессами) **заявитель издает приказ** (исходя из типа классифицируемой системы) следующего содержания:

1 Для проведения процедуры классификации автоматизированной системы (информационной системы, информационной системы персональных данных) наименование автоматизированной системы, расположенной в помещении (помещениях) №___ наименование организации-заявителя на соответствие требованиям по безопасности информации приказываю назначить комиссию в составе_____. Комиссии в срок до _____ провести классификацию автоматизированной системы (информационной системы, информационной системы персональных данных) в соответствии с перечень нормативно-методических документов, на соответствие которым производится классификация.

2 По результатам проведения классификации подготовить и предоставить для утверждения «Акт классификации автоматизированной системы (информационной системы, информационной системы персональных данных)».

3 Контроль исполнения приказа возложить на заместителя руководителя организации, ответственного за защиту информации в организации.

Акт классификации автоматизированной системы содержит данные:

1 состав комиссии, проводившей процедуру классификации, со ссылкой на приказ о назначении комиссии;

2 наименование автоматизированной системы, место расположения, состав автоматизированной системы;

3 указание документов, в соответствии с которыми осуществлялась классификация, а также основных параметров системы, повлиявших на присвоение того или иного класса;

4 режим работы системы и количество пользователей;

5 решение о присвоении автоматизированной системе того или иного класса защищенности.

Форма акта классификации приведена в «Специальных требованиях и рекомендациях по технической защите конфиденциальной информации», утвержденных приказом Гостехкомиссии России от 30 августа 2002г. № 282

Акты классификации для иных видов систем оформляется аналогично. Акт классификации подписывается всеми членами комиссии, назначенной приказом.

5. Разработка акта классификации автоматизированных систем

Практическое исследовательское задание №1

В соответствии с исходными данными, представленными в таблице 4, определить исходные данные для издания приказа для проведения классификации автоматизированной системы на аттестуемом объекте и разработки акта классификации автоматизированной системы.

В соответствии с установленными исходными данными разработать проект приказа для проведения классификации автоматизированной системы на аттестуемом объекте (пример представлен в приложении А).

В соответствии с установленными исходными данными разработать проект акт классификации автоматизированной системы на аттестуемом объекте (пример представлен в приложении Б).

Таблица 4 – Исходные данные и варианты заданий

вариант	Корпус №9. № аудитории, назначение	Характер и уровень секретности	Режим обработки данных в АС
61	310, учебная	НТИ*, общедоступная	многопользовательский
62	311, конф. делопроизводство	Эконом., обработка коммерческой тайны	многопользовательский
63	312, учебная	Производственная, обработка ПДн	многопользовательский
64	314, АП ГИС	Производственная, АП ГИС**	многопользовательский
65	513, делопроизводство ГТ	Производственная, обработка ГТ***	однопользовательский
66	514, открытое делопроизводство	Производственная, открытый документооборот	многопользовательский
67	516, служебное делопроизводство	Производственная, служебная тайна	однопользовательский
68	310, учебная	Производственная, обработка ПДн	многопользовательский
69	311, делопроизводство ГТ	Производственная, обработка ГТ***	однопользовательский
70	312, учебная	НТИ*, общедоступная	многопользовательский
71	314, учебная	Производственная, обработка ПДн	многопользовательский
72	513, конф. делопроизводство	Эконом., обработка коммерческой тайны	однопользовательский
73	514, АП ГИС	Производственная, АП ГИС**	многопользовательский

вариант	Корпус №9. № аудитории, назначение	Характер и уровень секретности	Режим обработки данных в АС
74	516, открытое делопроизводство	Производственная, открытый документооборот	многопользовательский
75	310, служебное делопроизводство	Производственная, служебная тайна	многопользовательский
76	311, АП ГИС	Производственная, АП ГИС**	многопользовательский
77	312, конф. делопроизводство	Эконом., обработка коммерческой тайны	многопользовательский
78	314, делопроизводство ГТ	Производственная, обработка ГТ***	однопользовательский
79	513, учебная	Производственная, обработка ПДн	многопользовательский
80	514, открытое делопроизводство	Производственная, открытый документооборот	многопользовательский
81	516, учебная	Производственная, обработка ПДн	многопользовательский
82	310, служебное делопроизводство	Производственная, служебная тайна	многопользовательский
83	311, АП ГИС	Производственная, АП ГИС**	многопользовательский
84	312, конф. делопроизводство	Эконом., обработка коммерческой тайны	многопользовательский

варианта	Корпус №9. № аудитории, назначение	Характер и уровень секретности	Режим обработки данных в АС
85	314, делопроизводство ГТ	Производственная, обработка ГТ***	однопользовательский
86	513, учебная	Производственная, обработка ПДн	многопользовательский
87	514, открытое делопроизводство	Производственная, открытый документооборот	многопользовательский
88	516, учебная	Производственная, обработка ПДн	многопользовательский
89	310, учебная	НТИ*, общедоступная	многопользовательский
90	311, конф. делопроизводство	Эконом., обработка коммерческой тайны	многопользовательский

Примечания:

*НТИ – научно-техническая информация;

**АП ГИС – абонентский пункт государственной информационной системы;

*** ГТ – государственная тайна.

6. Контрольные вопросы

1. Основные этапы классификации АС и необходимые исходные данные.
2. Классы защищенности АС от НСД к информации и порядок их определения.
3. Классы защищенности государственных информационных систем и порядок их определения.
4. Уровни защищенности информационных систем персональных данных и порядок их определения.
5. Классы защищенности автоматизированных систем управления производственными и технологическими процессами и порядок их определения.
6. Назначение, порядок оформления и основное содержание приказа на проведение процедуры классификации автоматизированной системы.

7. Назначение, порядок оформления и основное содержание акта классификации автоматизированной системы.

Литература

3. Приказ ФСТЭК РФ от 29 апреля 2021 г. N 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

4. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.).

5. Приказ ФСТЭК РФ от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

6. Требования к защите персональных данных при их обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 1 ноября 2012 г. №1119).

7. Приказ ФСТЭК РФ от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Тема 5.

Практическое занятие №5

Цель занятия:

1. Закрепление теоретических знаний по вопросам аттестации объектов информатизации по требованиям безопасности информации.
2. Получение практических навыков по разработке программы и методик аттестационных испытаний при аттестации объекта информатизации по требованиям безопасности информации.
3. Совершенствование навыков анализа процессов при аттестации объектов информатизации по требованиям безопасности информации и формулировки выводов.

Формируемые компетенции: ПК-3, ПК-6

Время – 4 ч.

1. Подготовка к занятию

1. Ознакомиться с заданием на практическую работу.
2. Ознакомиться с программой практической работы.

2. Распределение времени занятия:

Всего: 180 мин

Вступительная часть 5 мин

Проверка готовности студентов к занятию 15 мин

Основная часть 150 мин

Заключительная часть 10 мин

3. Программа практической работы

Основная часть

1. Изучение порядка разработки программы и методик аттестационных испытаний при аттестации объекта информатизации по требованиям безопасности информации – 50 мин.
2. Разработка программы и методик аттестационных испытаний объекта информатизации - 100 мин.

4. Содержание занятия

Учебный вопрос 1. Изучение порядка разработки программы и методик аттестационных испытаний при аттестации объекта информатизации по требованиям безопасности информации

По результатам рассмотрения заявки и анализа исходных данных, а также предварительного ознакомления с аттестуемым объектом органом по аттестации разрабатываются программа аттестационных испытаний, предусматривающая перечень работ и их продолжительность, методики испытаний (или используются типовые методики), определяются количественный и профессиональный состав аттестационной комиссии, назначаемой органом по аттестации объектов информатизации, необходимость использования контрольной аппаратуры и тестовых средств на аттестуемом объекте информатизации или привлечения испытательных центров (лабораторий) по сертификации средств защиты информации по требованиям безопасности информации.

В соответствии с п. 13 источника [1] программа и методики аттестационных испытаний объекта информатизации состоят из следующих разделов:

- а) общие положения;
- б) программа аттестационных испытаний объекта информатизации;
- в) методики аттестационных испытаний объекта информатизации.

Раздел, касающийся общих положений, должен включать следующие сведения:

- а) наименование и краткое описание архитектуры объекта информатизации, класс защищенности информационной (автоматизированной) системы, категорию значимого объекта;
- б) фамилии, имена, отчества (при наличии), должности экспертов органа по аттестации, назначенных для проведения аттестации объекта информатизации;
- в) наименование и реквизиты документов ФСТЭК России, устанавливающих требования по защите информации, на соответствие которым проводится аттестация объекта информатизации;
- г) угрозы безопасности информации, актуальные для объекта информатизации, или сведения о модели угроз безопасности информации в случае ее разработки в соответствии с требованиями по защите информации.

Раздел, касающийся программы аттестационных испытаний объекта информатизации, должен включать перечень работ по аттестации объекта информатизации, в том числе работы по обследованию объекта информатизации в условиях его эксплуатации, проведению аттестационных испытаний в соответствии с разрабатываемыми методиками испытаний, оформлению результатов аттестационных испытаний, а также общий срок проведения аттестации объекта информатизации и сроки выполнения каждой работы по аттестации объекта информатизации, фамилию и инициалы эксперта органа по аттестации, ответственного за проведение каждой работы.

Раздел, касающийся методик аттестационных испытаний объекта информатизации, должен включать для каждого аттестационного испытания порядок, условия, исходные данные и методы испытаний, применяемые при проведении испытаний средства контроля эффективности защиты информации

от несанкционированного доступа, а также контрольно-измерительное и испытательное оборудование.

Программа и методики аттестационных испытаний объекта информатизации согласовываются органом по аттестации с владельцем объекта информатизации и утверждаются руководителем органа по аттестации до начала аттестационных испытаний.

В ходе аттестационных испытаний объекта информатизации орган по аттестации может вносить изменения в программу и методики аттестационных испытаний объекта информатизации по согласованию с владельцем объекта информатизации.

Программа и методики аттестационных испытаний объекта информатизации согласовываются органом по аттестации с владельцем объекта информатизации и утверждаются руководителем органа по аттестации до начала аттестационных испытаний.

В ходе аттестационных испытаний объекта информатизации орган по аттестации может вносить изменения в программу и методики аттестационных испытаний объекта информатизации по согласованию с владельцем объекта информатизации.

Измерения и оценка защищенности осуществляются с помощью инструментальных средств контроля эффективности защиты информации в соответствии с действующими нормативными и методическими документами по защите информации от ее утечки по техническим каналам. Перечень используемых инструментальных средств контроля защищенности информации от НСД приводится в виде таблицы (пример представлен в виде таблицы 1).

Таблица 1

Используемые средства	Сведения о сертификате, знаке соответствия
Программа фиксации и контроля исходного программного комплекса ФИКС 2.0.2 (Копия № 5266)	сертификат ФСТЭК № 1548, ЗС А275380
Средство контроля защищенности АС от НСД «Ревизор 2 ХР» (Копия № 2955)	сертификат ФСТЭК № 990, ЗС А275696
Программа контроля полномочий доступа к информационным ресурсам «Ревизор 1 ХР» (Копия № 2933)	сертификат ФСТЭК № 989, ЗС А276974
Программа поиска и гарантированного уничтожения информации на дисках “Terrier 3.0” (Копия №3022)	сертификат ФСТЭК № 1193, ЗС А274966
Сетевой сканер безопасности «Ревизор сети 3.0» (Копия №2022)	сертификат ФСТЭК № 3413, ЗС А260822

Проверка и испытания комплекса функций защиты информации от НСД проводятся для программно-технической среды ОИ в целом в соответствии с действующими документами по защите информации от НСД.

Проверка соответствия ОИ требованиям безопасности информации проводится на основании анализа общих результатов испытаний и выявленных в процессе испытаний недостатков и нарушений.

В случае выявления по результатам испытаний несоответствия ОИ установленным требованиям по защите информации комиссия может рассмотреть возможность оперативного устранения выявленных недостатков и нарушений. При этом могут рекомендоваться следующие меры:

- Доработка организационно-распорядительной документации;
- Исключение отдельных технических средств из состава ОИ;
- Применение дополнительных организационных и технических мер защиты;
- Применение дополнительных сертифицированных средств защиты информации.

В разделе II. Программа аттестационных испытаний ОИ на соответствие требованиям безопасности информации

Аттестационные испытания ОИ проводятся в соответствии с программой, включающей следующий перечень работ и порядок их проведения.

1. Проверка структуры, состава и условий эксплуатации ОИ, включающая:

- анализ полноты исходных данных и проверку их соответствия реальным условиям размещения, монтажа и эксплуатации ОИ;

- исследование технологического процесса обработки, хранения, и передачи информации;
- анализ информационных потоков;
- определение состава использованных для обработки, хранения и передачи технических средств.

2. Проверка состояния организации работ и выполнения требований по защите информации, включающая:

- оценку правильности классификации ОИ;
- оценку полноты разработки организационно-распорядительной, проектной и эксплуатационной документации;
- оценку уровня подготовки специалистов, обеспечивающих защиту информации в ОИ, и проверку наличия распределения ответственности пользователей ОИ за выполнение требований безопасности информации.

3. Проверка ОИ на соответствие требованиям безопасности информации, включающая:

- Проверку наличия необходимых документов и соответствия их содержания установленным требованиям, наличия сертификатов соответствия требованиям безопасности информации и (или) предписаний на эксплуатацию, проверка их выполнения;

- Проверку уровня подготовки специалистов, обеспечивающих защиту информации на ОИ, и распределения ответственности должностных лиц, эксплуатирующих данные объекты, за выполнение требований безопасности информации;

- Проверку выполнения требований безопасности информации к помещению, в котором проводится обработка информации.

4. Проведение испытаний ОИ на соответствие требованиям по защите информации от НСД.

5. Подготовка отчетной документации и оценка результатов испытаний аттестуемого ОИ производится в следующем порядке:

6. Результаты проведения испытаний ОИ на соответствие требованиям по защите информации отражаются в протоколе контроля защищенности информации или оценки эффективности принятых мер по защите информации от утечки за счет ПЭМИН и в протоколе проверки выполнения требований по защите информации от НСД;

7. Материалы аттестационных испытаний оформляются протоколами испытаний, содержащими: - наименование аттестуемого объекта; - цель испытаний; - перечень использованных нормативных документов и методик испытаний; - перечень средств измерений и средств контроля защиты информации от НСД; - описание проверок; - результаты испытаний;

8. На основании данных документов составляется заключение по результатам аттестационных испытаний, включающее: - оценку соответствия ОИ требованиям безопасности информации; - перечень выявленных недостатков и нарушений; - вывод о возможности (невозможности) выдачи «Аттестата соответствия».

9. Продолжительность работ по пунктам «Программы аттестационных испытаний» (для аттестации одного автоматизированного рабочего места) составляет: от 2-х - до 3-х дней.

10. Контроль соответствия системы защиты информации аттестованного ОИ требованиям безопасности информации в процессе эксплуатации производится в виде ежегодного объектового контроля.

11. Контроль организуется ответственным по защите информации организации - владельца ОИ и осуществляется организацией, имеющей лицензию уполномоченного федерального органа исполнительной власти (в части осуществления мероприятий по контролю защищенности информации).

12. К проведению контроля привлекаются сотрудники, ответственные за эксплуатацию аттестованного ОИ и, при необходимости, сотрудники режимно-секретного подразделения (подразделения, отвечающего за обеспечение безопасности информации ограниченного доступа) организации.

13. В ходе проведения контроля осуществляются следующие мероприятия:
- на основе анализа материалов аттестационных испытаний проверяется неизменность условий эксплуатации ОИ и правильность ведения документации на ОИ;

- проверяется выполнение требований по защите информации от НСД.

14. По результатам контроля непосредственно на проверяемом ОИ представителями организации, проводящей работы по контролю, и представителями собственника ОИ (оператора информационной системы) составляется в двух экземплярах двусторонний акт о проведенных при контроле

работах и выявленных нарушениях, влияющих на безопасность информации (или их отсутствии).

15. Материалы контроля аттестованного ОИ оформляются организацией, проводящей работы по контролю, в виде заключения по результатам контроля защищенности информации и выдаются владельцу проверяемого ОИ (оператору информационной системы). К заключению по результатам контроля защищенности информации с учетом выполненных проверок прилагают:

- протокол контроля системы защиты информации от несанкционированного доступа (в части проверки соответствия контрольных сумм и действительности сертификата, неизменности установленного программного обеспечения и актуальности антивирусных баз данных);

- протокол контроля защищенности информации от утечки за счет ПЭМИН (при отсутствии в ОИ СЗИ от утечки за счет ПЭМИН проверяется неизменность условий эксплуатации).

В разделе III. Методики аттестационных испытаний ОИ на соответствие требованиям безопасности информации указывается следующее:

Настоящие методики предназначены для проведения аттестационных испытаний ОИ на соответствие требованиям безопасности информации.

1. Аттестационные испытания проводятся в указанном ниже порядке и включают:

- анализ полноты исходных данных, проверку их соответствия реальным условиям размещения, монтажа и эксплуатации ОИ, исследование технологического процесса обработки, хранения и передачи информации, анализ информационных потоков, определение состава использованных для обработки, хранения и передачи информации технических средств;

- проверку состояния организации работ и выполнения требований по защите информации, оценку правильности категорирования и классификации ОИ, оценку полноты разработки организационно-распорядительной и эксплуатационной документации, оценку уровня подготовки специалистов, обеспечивающих защиту информации в ОИ и распределения ответственности пользователей ОИ выполнение требований безопасности информации;

- проверку ОИ на соответствие требованиям по защите информации от утечки за счет побочных электромагнитных излучений от технических средств и наводок информативных сигналов на цепи электропитания и заземления технических средств;

- проверку выполнения требований по защите ОИ от утечки информации за счет возможно внедренных электронных закладочных устройств в технические средства иностранного производства;

- проверку ОИ на соответствие требованиям по защите информации от НСД;

- проверку ОИ на соответствие требованиям по защите информации от специальных программных воздействий на нее и ее носители;

- подготовку отчетной документации.

1.1 Для **анализа полноты исходных данных**, проверка их соответствия реальным условиям размещения, монтажа и эксплуатации автоматизированной системы, исследование технологического процесса обработки, хранения и передачи информации, анализ информационных потоков, определения состава использованных для обработки, хранения и передачи информации основных технических средств и систем.

Аттестационной комиссии должны быть представлены:

- перечень защищаемых информационных ресурсов с документальным подтверждением уровня конфиденциальности каждого ресурса;
- акт классификации ОИ по требованиям защиты информации от НСД (в соответствии с нормативными правовыми актами и методическими документами уполномоченного федерального органа исполнительной власти и национальными стандартами);
- оформленный технический паспорт на ОИ;
- сертификаты соответствия требованиям безопасности информации на программные и технические средства защиты;
- состав технических и программных средств, входящих в ОИ;
- план размещения ОТСС и ВТСС в помещении объекта информатизации;
- план КЗ;
- схемы прокладки линий данных ОТСС (ВОСП) и проводных линий ВТСС;
- схемы и характеристики систем электропитания и заземления ОТСС и ВТСС;
- состав и схемы размещения средств защиты информации;
- организационно-распорядительная документация разрешительной системы доступа пользователей ОИ к защищаемым информационным ресурсам ОИ;
- описание технологического процесса обработки информации в ОИ;
- перечень программного обеспечения, установленного в ОИ;
- инструкции администратору защиты информации и пользователям ОИ;
- инструкции по эксплуатации средств защиты информации;
- данные о наличии нормативной и методической документации по защите информации и контролю эффективности защиты;
- данные по уровню подготовки специалистов, обеспечивающих защиту информации.

Приведенный перечень исходных данных и документации при необходимости может уточняться по результатам анализа и проверки в зависимости от особенностей ОИ по согласованию с аттестационной комиссией.

При исследовании технологического процесса автоматизированной обработки и хранения информации проверяют:

- объект доступа - средства обработки и передачи информации, носители информации на магнитной и бумажной основе, накопители и все виды памяти ЭВМ, которые могут содержать информацию, отдельные документы и их

архивы, используемые в технологическом процессе обработки информации, файлы, записи и другие информационные ресурсы, доступ к которым необходимо регламентировать;

- субъект доступа - пользователи ОИ, а также программные средства, посредством которых осуществляется доступ к объектам доступа.

Используя разрешительную систему доступа пользователей ОИ к защищаемым информационным ресурсам и данные по технологии обработки и передачи защищаемой информации, анализируют обобщенную технологическую схему ОИ с существующими и возможными информационными потоками, возможностями доступа к обрабатываемой и передаваемой информации.

Проверяют соответствие описания технологического процесса обработки, хранения и передачи защищаемой информации реальному технологическому процессу обработки.

Проверяют паспортные (исходные) данные ОИ, комплектность и характеристик средств защиты и устанавливают угрозы безопасности информации в ОИ, уязвимые критические места ОИ, снижающие уровень ее защиты.

Проверяют наличие оформленных разрешений на допуск пользователей ОИ к информации, соответствие им грифов секретности (уровня конфиденциальности) на носителях информации, соответствие инструкций пользователей и администратора защиты информации ОИ установленным требованиям.

По результатам исследований уточняют схему технологического процесса в отношении отдельных средств обработки информации и передачи информации и каждого пользователя ОИ.

1.2. Проверка состояния организации работ и выполнения требований безопасности информации.

Проверка соответствия содержания предоставленных документов установленным требованиям.

Проверяют соответствие предоставленных документов требованиям нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти, а также стандартов и иных документов органов государственного управления в пределах компетенции.

Проверяют соответствие приведенных в предоставленных документах сведений о составе ОИ (типы, заводские номера, места размещения и т.д.) ее реальному составу.

Проверка считается успешной, если предоставленные документы полностью соответствуют требуемому составу, не содержат противоречивых сведений и оформлены в соответствии с установленными требованиями.

Проверка соответствия состава и структуры программно-технических средств ОИ представленной документации.

С представленной документацией сверяют и структуру программнотехнических средств ОИ, включенных в реальный технологический процесс обработки информации.

С использование стандартных средств операционной системы или других программ фиксируют перечень технических и программных средств и сверяют с приведенным в техническом паспорте, документах разрешительной системы доступа и описании технологического процесса обработки защищаемой информации.

Проверка считается успешной, если состав, номенклатура, структура программно-технических средств ОИ и их размещение полностью соответствуют представленной документации на ОИ.

Проверка правильности категорирования ОТСС (для предназначенной для обработки секретной информации).

Проверку проводят на основании исходных данных о максимальной степени секретности обрабатываемой информации, которые должны быть подтверждены документально в перечне защищаемых информационных ресурсов ОИ.

По результатам проверки определяют допустимые категории технических средств.

Эти категории сравнивают с категориями, указанными в актах категорирования соответствующих технических средств.

Проверка правильности классификации ОИ.

Определяют максимальную степень конфиденциальности обрабатываемой в ОИ информации, анализируют уровни полномочий по доступу к конфиденциальной информации различных пользователей ОИ, режимы обработки данных в ОИ и устанавливают класс ОИ в соответствии с нормативными правовыми актами и методическими документами уполномоченного федерального органа исполнительной власти и национальными стандартами.

Проверка считается успешной, если класс аттестуемой ОИ соответствует представленному на аттестационные испытания акту классификации автоматизированной системы.

Проверка уровня подготовки специалистов и распределения ответственности пользователей ОИ.

Проверку проводят на основе следующих показателей: - оценка знания инструкций по безопасности информации пользователями ОИ;

- наличие системы распределения ответственности пользователей ОИ за выполнение требований безопасности информации.

На основании опроса пользователей ОИ проверяют знание ими руководящих документов и инструкций.

Проводят выборочную проверку персонала из каждой категории организационно-штатной структуры ОИ на предмет владения технологиями безопасной обработки информации и знания соответствующих инструкций.

Проверяют организацию обучения и повышения квалификации пользователей ОИ.

Проверка считается успешной, если уровень подготовки пользователей ОИ обеспечивает выполнение требований безопасности информации.

Экспертиза протоколов специальных исследований и предписаний на эксплуатацию технических средств и систем.

Проверяют соответствие содержания и оформления протоколов специальных исследований и предписаний на эксплуатацию технических средств и систем установленным требованиям.

Проверка считается успешной при выполнении всех установленных требований.

Проверка выполнения требований к помещениям, в которых производится обработка информации.

Внешним осмотром проверяют соответствие помещения ОИ установленным к нему требованиям.

Проверяют выполнение установленных требований действующей инструкции по обеспечению режима конфиденциальности.

Проверяют выполнение установленных требований по условиям размещения ОТСС внутри помещения. Размещение ОТСС должно исключать возможность несанкционированного просмотра информации с экранов мониторов, с распечаток принтеров и с других устройств ввода-вывода информации лицами, не имеющими права доступа к обрабатываемой информации.

Проверка считается успешной при выполнении всех установленных требований.

По результатам проверок аттестационная комиссия делает выводы о соответствии (или несоответствии) предъявленных документов и исходных данных установленным требованиям.

1.3. Испытания ОИ на соответствие требованиям по защите информации от несанкционированного доступа.

Испытания проводятся на соответствие требованиям руководящих документов. По результатам испытаний аттестационная комиссия делает выводы о выполнении требований по защите информации от НСД.

Проверка наличия сертификатов на средства защиты информации, выполнения правил их эксплуатации.

Проверяют соответствие представленных сертификатов установленным в ОИ средствам защиты информации от НСД. Основным инструментальным средством аттестационных испытаний на данном этапе является программа фиксации и контроля исходного состояния. Программа используется в режиме фиксации исходного состояния файлов программного комплекса. При этом рассчитывают контрольные суммы для указанных в формуляре (паспорте) программных модулей СЗИ от НСД. Расчет производят по алгоритму формирования имитовставки в соответствии с ГОСТ 15 28147 или по контрольным суммам другого аттестованного алгоритма. Полученные значения

контрольного суммирования сравнивают со значениями, указанными в формуляре (паспорте) средства защиты информации.

Проверка считается успешной:

- если действующие сертификаты соответствуют требованиям безопасности информации на все используемые в ОИ средства защиты информации от НСД;
- если используемое СЗИ от НСД соответствует классу ОИ и используемой технологии обработки информации;
- если результаты контрольного суммирования программных модулей СЗИ от НСД полностью соответствуют значениям, указанным в формуляре (паспорте) данного средства защиты.

1.4. Проверка соответствия описания технологического процесса обработки и хранения защищаемой информации реальному процессу

Заявитель представляет аттестационной комиссии описание технологического процесса обработки информации в аттестуемой ОИ, которое включает:

- перечень объектов и субъектов доступа;
- перечень штатных средств доступа к информации в ОИ;
- перечень средств защиты информации;
- описание реализованных правил разграничения доступа;
- описание информационных потоков в ОИ.

В качестве объектов доступа могут быть приняты:

- система в целом;
- терминалы, ЭВМ, узлы сети ЭВМ, каналы связи, внешние устройства ЭВМ;
- программы;
- тома, каталоги, файлы, записи, поля записей.

Носители информации должны иметь метку конфиденциальности и находиться на учете.

В качестве субъектов доступа могут рассматриваться лица и процессы (программы пользователей), имеющие возможность доступа к штатными средствами ОИ. Субъекты доступа должны иметь официальное разрешение на доступ к информации определенной уровня конфиденциальности.

Примечание: под штатными средствами ОИ понимаются общесистемные и прикладные системы, средства и программы, предоставляющие субъектам документированные возможности доступа к объектам доступа.

Аттестационная комиссия проверяет:

- соответствие технологического процесса обработки и хранения защищаемой информации требованиям безопасности информации
- соответствие описания технологического процесса обработки и хранения защищаемой информации реальному процессу.

1.5. Испытания подсистемы управления доступом.

Для проведения испытаний требуются следующие средства:

- загрузочный компакт-диск (CD);

- программа фиксации и контроля исходного состояния;
- средство контроля защищенности ОИ от НСД (наименование средства).

Проверка подсистемы идентификации и аутентификации субъектов доступа.

Проверка наличия и работоспособности подсистемы идентификации.

Проверяют правильность идентификации субъектов доступа путем обращения субъектов доступа ОИ к объектам доступа при помощи штатных средств.

При обращении должна проводиться проверка принадлежности предъявленного субъектом идентификатора множеству всех зарегистрированных в ОИ идентификаторов. Если субъект доступа предъявляет идентификатор, не известный подсистеме идентификации, то средства управления должны прекращать процесс предоставления доступа.

Проверка наличия и надежности подсистемы аутентификации.

Проверяют правильность аутентификации субъекта доступа. Если субъект доступа предъявляет пароль, не соответствующий идентификатору субъекта, то средства управления должны прекращать процесс предоставления доступа.

Проверяют возможность компрометации пароля методом его подбора. Для ОИ, где подсистема аутентификации предусматривает средства, обеспечивающие блокировку подбора пароля. Проверку осуществляют следующим образом. Выполняют неоднократные попытки ввода неверного пароля. При превышении предельного числа попыток ввода информации идентификации/аутентификации, установленного политикой безопасности, подсистема управления доступом должна полностью блокировать ввод информации идентификации/аутентификации субъекта доступа. Правом снятия блокировки должен обладать исключительно администратор (служба) защиты информации в ОИ.

Проверка отсутствия условий компрометации подсистемы идентификации и аутентификации.

Проверяют условия хранения, выдачи, использования устройств и информации об идентификации и аутентификации. Организационные и технические мероприятия ОИ должны надежно препятствовать несанкционированному получению или хищению устройств и информации об идентификации и аутентификации.

Проверяют возможность несанкционированного изменения информации об идентификации и аутентификации. Доступ субъектов ОИ к файлам, содержащим информацию об идентификации и аутентификации, должен быть полностью закрыт для прикладных программ. На СВТ, входящих в состав ОИ, должны отсутствовать прикладные программные средства прямого доступа к устройствам и оперативной памяти, средства разработки и отладки программ.

Проверка средств загрузки операционной системы ОИ в обход подсистемы идентификации и аутентификации.

Для проведения испытаний необходимы загрузочная дискета или загрузочный CD.

Осуществляют попытки загрузки операционной системы с загрузочной дискеты или загрузочного CD. Настройка СЗИ от НСД ОИ должна обеспечивать блокировку загрузки операционной системы с устройств, не предусмотренных технологией инициализации ОИ.

Проверка времени действия пароля.

На ЭВМ производят перевод системного времени вперед, при этом не превышая установленного политикой безопасности времени действия пароля. Затем осуществляют попытку входа пользователя в систему. Подсистема

идентификации и аутентификации должна разрешить вход пользователя в систему, но соответствующим сообщением предупредить его о необходимости замены пароля.

На ЭВМ производят перевод системного времени вперед на интервал, больший установленного политикой безопасности времени действия пароля. Затем осуществляют попытку входа пользователя в систему. Подсистема идентификации и аутентификации должна блокировать вход пользователя в систему.

После проведения испытаний на ЭВМ устанавливают текущее время.

Проверка длины пароля.

Подсистема контроля доступа должна предусматривать средства, обеспечивающие установку минимальной длины пароля. Проверку осуществляют попыткой смены длины пароля субъектом доступа. Проверка считается успешной, если подсистема контроля доступа отказала субъекту в замене пароля.

Право установки минимальной размерности пароля должно предоставляться администратору АС.

Проверка подсистемы идентификации объектов доступа.

Проверка идентификации аппаратурных объектов доступа.

Идентификация внешних устройств ЭВМ должна осуществляться по одному из ниже перечисленных типов идентификаторов:

- по логическим адресам (номерам);
- по логическим именам;
- по логическим именам и (или) адресам;
- по физическим адресам (номерам);
- по уникальным встроенным устройствам.

Основными средствами проверки являются средства контроля защищенности ОИ от НСД. С их помощью производится сканирование периферийных устройств ЭВМ (принтеров, НЖМД, приводов CD-ROM), доступных для пользователя. Перед началом сканирования в настройках этих средств контроля необходимо задать поиск неизвестных устройств.

Проверка считается успешной, если во время работы со средствами контроля защищенности ОИ от НСД не выявлены неизвестные (неидентифицированные) объекты доступа.

Проверка идентификации информационных объектов доступа.

Проверяют механизм подсистемы контроля доступа, обеспечивающий проверку идентификации программ, томов, каталогов, файлов, записей, полей записей по именам.

Основными средствами проверки являются средства контроля защищенности ОИ от НСД.

С помощью средств контроля защищенности ОИ от НСД проводится сканирование ресурсов файловой системы ОИ (логических дисков, каталогов, файлов), доступных для пользователя. Перед началом сканирования в настройках комплекса необходимо задать поиск неизвестных устройств.

Проверка считается успешной, если в выходном отчете комплексов средств контроля не будут указаны неизвестные (неидентифицированные) объекты доступа.

Проверка подсистемы управления потоками информации.

Основными средствами аттестационных испытаний на данном этапе являются средства контроля защищенности ОИ от НСД средства операционной системы.

Для проведения проверки подсистемы управления потоками информации необходимо проанализировать матрицу доступа. При этом классификационные категории должны быть объединены в иерархические группы, по которым строятся комбинации иерархических и неиерархических категорий — классификационные уровни. Каждому классификационному уровню должна соответствовать уникальная классификационная метка.

Классификационные метки, как основа мандатного принципа доступа, должны присваиваться каждому объекту и отражать место данного объекта в соответствующей иерархии.

Разработка модели подсистемы разграничения доступа с помощью средства контроля защищенности ОИ от НСД должна осуществляться в полном соответствии с политикой безопасности и матрицей доступа, учитывающей мандатные правила разграничения доступа, принятые в аттестуемой АС.

Проверка считается успешной, если в ОИ осуществляется управление потоками информации с помощью меток, соответствующих уровню конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на них информации.

Проверяется настройка СЗИ от НСД в части назначения объектам меток, соответствующих уровням конфиденциальности ресурсов. С использованием штатных средств операционной системы осуществляются попытки переноса информации на носитель с уровнем конфиденциальности.

Проверка считается успешной, если СЗИ от НСД запретила операцию копирования.

1.6. Испытания подсистемы регистрации и учета.

Для проведения испытаний необходимы:

- программа фиксации и контроля исходного состояния;
- программа поиска информации на дисках.

Регистрация и учет событий должны проводиться на всех этапах технологического процесса хранения и обработки защищаемой информации.

Испытания включают:

- проверку регистрации начала и окончания работ;
- проверку регистрации выдачи документов на «твердую» копию;
- проверку регистрации использования программных средств;
- проверку регистрации доступа программных средств к защищаемым файлам;
- проверку регистрации доступа программных средств к дополнительным защищаемым объектам доступа;
- проверку автоматического учета создания новых объектов доступа;
- проверку учета защищаемых носителей информации;
- проверку очистки освобождаемых областей памяти.

Проверка регистрации начала и окончания работ.

Проверка осуществляется штатными средствами ОИ.

Проводится загрузка операционной системы и запуск программных комплексов ОИ, предусмотренных технологией инициализации ОИ.

Осуществляются попытки входа в систему по неверному идентификатору доступа, по верному идентификатору доступа и неверному паролю, по идентификатору и паролю легитимного субъекта доступа.

Производится программный останов ОИ.

Производится загрузка операционной системы, запуск программных комплексов ОИ, предусмотренных технологией инициализации ОИ, вход в систему с правами администратора защиты и исследование журнала регистрации доступа.

Проверка считается успешной, если организационными и техническими мероприятиями, проводимыми в соответствии с политикой безопасности АС, обеспечивается ведение журнала регистрации доступа (аппаратного журнала), в котором фиксируется регистрация входа (выхода) субъектов доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. При этом регистрационные записи для каждого события должны содержать:

- дату и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная несанкционированная;
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа.

Проверка регистрации выдачи документов на «твердую» копию.

В соответствии с принятой в ОИ технологией проводится выдача произвольного документа на «твердую» копию.

В соответствии с принятой в ОИ технологией проводится выдача документа иного уровня конфиденциальности на «твердую» копию. Во время операции вывода документа на «твердую» копию проводится принудительное

отключение электропитания устройства вывода и выполняются действия, предусмотренные документацией ОИ для внештатных ситуаций.

Проверка считается успешной, если организационными и техническими мероприятиями, проводимыми в соответствии с политикой безопасности ОИ, обеспечивается регистрация выдачи документов на «твердую» копию. При этом регистрационные записи для каждого события должны содержать:

- дату и время выдачи документа (обращения к подсистеме вывода документа);
- спецификацию устройства выдачи (логическое имя внешнего устройства);
- краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
- идентификатор субъекта доступа, запросившего документ;

Выдача документов сопровождается автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами ОИ с указанием на последнем листе документа общего количества листов (страниц).

Проверка регистрации использования программных средств

В соответствии с принятой в ОИ технологией производится запуск программ обработки информации и объектами обработки выбираются файлы, входящие в перечень защищаемых ресурсов.

Запуск программ производится как в штатном режиме, предусматривающем безаварийную (штатную) обработку информации и завершение работы, так и во внештатном. В последнем случае моделируется ситуация несанкционированного использования программы. При этом используют следующие приемы:

- задают неверные параметры обработки;
- задают в качестве объекта обработки несуществующий файл;
- делают попытки запустить программы, доступ к которым закрыт подсистемой разграничения доступа.

Проверка считается успешной, если организационными и техническими мероприятиями, проводимыми в соответствии с политикой безопасности ОИ, была обеспечена регистрация запуска и завершения использованных на данном этапе испытаний программ и процессов (заданий, задач).

При этом регистрационные записи для каждого события должны содержать:

- дату и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс);
- результат запуска (успешный, неуспешный — несанкционированный).

Проверка регистрации доступа программных средств к защищаемым файлам

В соответствии с принятой в ОИ технологией производится запуск программ обработки информации и объектами обработки выбираются файлы, входящие в перечень защищаемых ресурсов.

Запуск программ производится как в штатном режиме, предусматривающем безаварийную (штатную) обработку информации и завершение работы, так и во внештатном. В последнем случае моделируется ситуация несанкционированного доступа к объектам защиты штатными программными средствами. При этом используют следующие приемы:

- задают неверные параметры обработки;
- задают в качестве объекта обработки несуществующий файл;
- задают в качестве объекта обработки файл, доступ к которому закрыт подсистемой разграничения доступа.

Проверка считается успешной, если организационными и техническими мероприятиями, проводимыми в соответствии с политикой безопасности АС, была обеспечена регистрация попыток доступа использованных на данном этапе испытаний программных средств (программ, процессов, задач, заданий) к защищаемым файлам. При этом регистрационные записи для каждого события должны содержать:

- дату и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;
- спецификацию защищаемого файла.

Проверка регистрации доступа программных средств к дополнительным защищаемым объектам доступа

Составляется список объектов испытаний. В список включаются объекты доступа, входящие в перечень защищаемых ресурсов, по одному (как минимум) для каждого из следующих типов:

- внешние устройства ЭВМ;
- программы;
- тома, каталоги, файлы;
- записи, поля записей.

В соответствии с принятой в ОИ технологией производится запуск программ, алгоритм работы которых предусматривает обращение к объектам, входящим в список объектов испытания.

Запуск программ производится как в штатном режиме, так и во внештатном. В последнем случае моделируется ситуация несанкционированного доступа к объектам защиты. При этом используют следующие приемы:

- задают неверные параметры запуска (обращения к устройствам);
- задают неверные логические имена (номера);
- осуществляют обращение к объекту, доступ к которому закрыт подсистемой разграничения доступа.

Проверка считается успешной, если средствами ЗИ обеспечивается регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к заданным на данном этапе испытаний дополнительным

защищаемым объектам доступа. При этом регистрационные записи для каждого события должны содержать:

- дату и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;
- спецификацию защищаемого объекта [логическое имя (номер)].

Проверка автоматического учета создания новых объектов доступа

Субъект доступа, имеющий полномочия администратора защиты, создает новые объекты доступа, предусмотренные политикой безопасности ОИ. В качестве новых объектов доступа рассматриваются файлы защищаемой информации.

С помощью штатных средств подсистемы разграничения доступа осуществляется контроль маркирования вновь созданных объектов доступа и проверка соответствия маркировки степени секретности (уровню конфиденциальности). При создании субъектом нового объекта доступа подсистема регистрации и учета должна установить для данного объекта метку доступа (маркер), соответствующую минимальному уровню доступа субъекта по записи.

Проверка считается успешной:

- если подсистема регистрации и учета ОИ произвела автоматический учет создаваемых на данном этапе испытаний объектов доступа с помощью их дополнительной маркировки, используемой в подсистеме управления доступом;
- если маркировка отражает степень секретности (уровень конфиденциальности) объекта доступа.

Проверка учета защищаемых носителей информации

Проверяется выполнение организационных и технических мероприятий по учету защищаемых носителей информации.

Проверка считается успешной, если организационно-технические мероприятия, проводимые в соответствии с политикой безопасности АС, обеспечивают:

- учет всех защищаемых носителей информации с помощью их маркировки и занесения учетных данных в журнал (учетную карточку);
- учет защищаемых носителей в журнале (картотеке) регистрации их выдачи приема;
- дополнительный (дублирующий) учет защищаемых носителей информации с регистрацией их выдачи приема.

Проверка очистки освобождаемых областей памяти

Исследуются сертификаты (при необходимости — эксплуатационная документация) СЗИ на предмет подтверждения соответствия используемых методов очистки (обнуления, обезличивания) освобождаемых (перераспределяемых) областей оперативной памяти и внешних носителей требованиям нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти, а также требованиям документов по стандартизации в области защиты информации.

Проверка считается успешной, если сертификаты и эксплуатационная документация СЗИ подтверждают возможность выполнения очистки (обнуления, обезличивания) освобождаемых (перераспределяемых) областей оперативной памяти и внешних носителей двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

Проверка очистки внешней памяти при ее освобождении (перераспределении)

Основным средством проверки очистки внешней памяти при проведения аттестационных испытаний ОИ является программа, которая 26

используется для контроля очистки памяти при ее освобождении на внешних носителях информации посредством поиска задаваемых экспертом сигнатур. Объектами исследований являются накопители на гибких и жестких магнитных дисках. Поиск задают или по всему физическому диску, или в пределах логического диска. Область применения охватывает операционные среды MS Windows.

Проверка считается успешной:

- если контекст контрольной информации не был обнаружен на внешнем носителе;
- если сектора, которые ранее содержали контекст контрольной информации,
- заполнены маскирующей информацией.

1.7. Испытание подсистемы обеспечения целостности

Проверка организационно-штатных мероприятий по защите информации

Исследуется организационно-штатная структура и нормативная документация ОИ на предмет организации службы защиты информации ОИ.

Методом выборочного опроса проверяют знание должностными лицами службы защиты информации их функциональных обязанностей и оценивают уровень их профессиональной подготовки.

Проверка считается успешной:

- если организационно-штатная структура ОИ предусматривает наличие службы (администратора) защиты информации;
- если уровень профессиональной подготовки должностных лиц службы защиты информации обеспечивает выполнение требований безопасности информации в ОИ;
- если деятельность службы защиты информации регламентирована организационно-распорядительными документами ОИ.

Проверка средств контроля целостности программных компонентов СЗИ НСД

Перед проведением проверки штатными средствами ОИ осуществляется резервное копирование программных компонентов СЗИ от НСД.

Производится моделирование несанкционированных действий по нарушению целостности программных компонентов СЗИ от НСД. Производится

удаление либо переименование определенных программных модулей СЗИ от НСД.

Производится перезагрузка системы. По завершении инициализации СЗИ от НСД анализируется реакция средств подсистемы обеспечения целостности.

Проверка считается успешной, если СЗИ от НСД зафиксировали изменения в составе программных компонентов.

Проверка тестирования функций СЗИ от НСД

Исследуется организационно-распорядительная документация на ОИ, определяющая порядок проведения тестирования всех функций СЗИ от НСД, используемых в ОИ.

Проверяется наличие средств тестирования функций СЗИ от НСД, в частности настройка и использование средств диагностики СЗИ от НСД.

Проверяется периодичность проведения тестирования всех функций СЗИ от НСД. Проверка осуществляется методом экспертизы эксплуатационной документации и журналов регистрации событий СЗИ от НСД.

Проверка считается успешной, если средства тестирования всех функций СЗИ от НСД и периодичность проверок соответствуют требованиям нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти, а также требованиям документов по стандартизации в области защиты информации

Проверка средств восстановления СЗИ от НСД

Исследуется организационно-распорядительная документация ОИ, определяющая порядок проведения резервного копирования СЗИ от НСД, используемого в ОИ.

Проверяется периодичность обновления и контроля работоспособности копий. Проверка осуществляется методом экспертизы эксплуатационной документации и журналов регистрации событий СЗИ от НСД.

Проверка считается успешной, если в ОИ осуществляется ведение двух копий программных СЗИ от НСД, а также производится периодическое обновление и контроль работоспособности копий.

Проверка обеспечения целостности (неизменности) программной среды

Исследуется технология внесения новых программных средств в операционную среду ОИ. Технология должна содержать:

- процедуры экспертной оценки и верификации новых программных средств на предмет выявления потенциально опасных для СЗИ программных функций;
- критерии санкционирования ввода программ в операционную среду;
- критерии допуска определенных категорий пользователей к этим программам;
- порядок проведения антивирусного контроля программных комплектов ОИ.

Проверяется наличие и работоспособности средств и мер предотвращения несанкционированного ввода программ в операционную среду, средств антивирусного контроля.

Проверяется наличие установленных антивирусных средств на СВТ ОИ, а также их работоспособность, наличие механизма обновления и актуальность антивирусных баз, параметры их функционирования, наличие доверенного канала получения обновлений антивирусных баз.

Проводится экспертиза программного обеспечения ОИ на отсутствие:

- средств модификации объектного кода программ;
- средств разработки и отладки программ;
- программ, использование которых не требует трансляции с языков высокого уровня.

Проверка считается успешной, если принятые в ОИ меры обеспечения целостности (неизменности) программной среды соответствуют требованиям нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти, а также требованиям документов по стандартизации в области защиты информации.

Учебный вопрос 2. Разработка программы и методик аттестационных испытаний объекта информатизации

В соответствии с исходными данными, представленными в таблице 1, а также в соответствии с результатами, полученными в ходе рассмотрения предыдущих лабораторных работ, разработать программу и методику аттестационных испытаний аттестуемого объекта.

Программы и методики аттестационных испытаний аттестуемого объекта должны содержать следующие разделы:

- а) общие положения;
- б) программа аттестационных испытаний объекта информатизации;
- в) методики аттестационных испытаний объекта информатизации.

Содержание каждого раздела должно быть составлено с учетом заданных исходных данных и рекомендаций, рассмотренных выше.

Представить разработанный документ «Программы и методики аттестационных испытаний аттестуемого объекта» на проверку преподавателю.

Таблица 1 – Исходные данные и варианты заданий

вариант	Корпус №9. № аудитории, назначение	Характер и уровень секретности	Наименование органа по аттестации
---------	--	--------------------------------	-----------------------------------

91	310, учебная	НТИ*, общедоступна я	ФГБОУ ВО «АГТУ».
92	311, конф. делопроизво дство	Эконом. , обработка коммерческой тайны	ФГАОУ ВО «Самарский национальный исследовательский университет имени академика С.П.Королева».
93	312, учебная	Произво дственная, обработка ПДн	ФГАОУ ВО «НИУ «МИЭТ».
94	314, АП ГИС	Произво дственная, АП ГИС**	ФГАНУ НИИ «Спецвузавтоматика».
95	513, делопроизво дство ГТ	Произво дственная, обработка ГТ***	ФАУ «ГНИИИ ПТЗИ ФСТЭК России».
96	514, открытое делопроизво дство	Произво дственная, открытый документообо рот	Управление МВД России по Астраханской области.
97	516, служебное делопроизво дство	Произво дственная, служебная тайна	УФК по Волгоградской области.
98	310, учебная	Произво дственная, обработка ПДн	УМВД России по г. Севастополю.
99	311, делопроизво дство ГТ	Произво дственная, обработка ГТ***	Симферопольский НТЦ ФГУП «НПП «Гамма».
100	312, учебная	НТИ*, общедоступна я	Представительство АО «СофтЛайн Трейд» в г. Воронеж.
101	314, учебная	Произво дственная, обработка ПДн	Ростовский НТЦ ФГУП «НПП «Гамма».
102	513, конф.	Эконом. , обработка	С-КАВ ж.д. ОАО «РЖД».

	делопроизводство	коммерческой тайны	
103	514, АП ГИС	Производственная, АП ГИС**	ОТС-филиал РТУ РЭБОТИ (г. Ростов-на-Дону).
104	516, открытое делопроизводство	Производственная, открытый документооборот	ООО АКБ «Барьер».
105	310, служебное делопроизводство	Производственная, служебная тайна	ООО «РАЦ».
106	311, АП ГИС	Производственная, АП ГИС**	ООО «РЦИБ».
107	312, конф. делопроизводство	Эконом., обработка коммерческой тайны	ООО «МТУ «Телеком-С».
108	314, делопроизводство ГТ	Производственная, обработка ГТ***	ООО «Информационные системы и аутсорсинг».
109	513, учебная	Производственная, обработка ПДн	ООО «Каскад».
110	514, открытое делопроизводство	Производственная, открытый документооборот	ГУ МВД России по Ставропольскому краю.
111	516, учебная	Производственная, обработка ПДн	ООО «Идентификация».
112	310, служебное делопроизводство	Производственная, служебная тайна	ООО «Геро».

113	311, АП ГИС	Производственная, АП ГИС**	ООО «АТЭК-С».
114	312, конф. делопроизводство	Эконом., обработка коммерческой тайны	МВД по Республике Дагестан.
115	314, делопроизводство ГТ	Производственная, обработка ГТ***	МВД по Республике Калмыкия.
116	513, учебная	Производственная, обработка ПДн	МВД по Республике Северная Осетия-Алания.
117	514, открытое делопроизводство	Производственная, открытый документооборот	МВД по Республике Крым.
118	516, учебная	Производственная, обработка ПДн	ЗАО «Контур-Сервис ТВ».
119	310, учебная	НТИ*, общедоступная	ООО «Евромост-Защита».
120	311, конф. делопроизводство	Эконом., обработка коммерческой тайны	АО «НПО «Инфобезопасность».

Примечания:

*НТИ – научно-техническая информация;

**АП ГИС – абонентский пункт государственной информационной системы;

*** ГТ – государственная тайна.

5. Контрольные вопросы

1. Укажите структурные элементы «Программы аттестационных испытаний».
2. Укажите структурные элементы «Методик аттестационных испытаний».
3. Опишите основное содержание раздела «Общие положения».
4. Опишите основное содержание раздела «Программа аттестационных испытаний ОИ на соответствие требованиям безопасности информации»

5. Опишите основное содержание раздела «Методики аттестационных испытаний ОИ на соответствие требованиям безопасности информации».

6. Дайте характеристику методам проверок, предусматриваемых в «Программ и методик аттестационных испытаний».

7. Дайте характеристику методам экспертиз, предусматриваемых в «Программ и методик аттестационных испытаний».

Литература

8. Приказ ФСТЭК РФ от 29 апреля 2021 г. N 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

9. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.).

10. Приказ ФСТЭК РФ от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

11. Требования к защите персональных данных при их обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 1 ноября 2012 г. №1119).

12. Приказ ФСТЭК РФ от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Тема 6.

Практическое занятие №6

Цель занятия:

1. Закрепление теоретических знаний по вопросам аттестационных испытаний технических средств обработки информации объекта информатизации.
2. Получение практических навыков по разработке протокола аттестационных испытаний, разрабатываемого при аттестации объекта информатизации по требованиям безопасности информации.
3. Совершенствование навыков анализа процессов при аттестации объектов информатизации по требованиям безопасности информации и формулировки выводов.

Формируемые компетенции: ПК-3, ПК-6

Время – 4 ч.

1. Подготовка к занятию

1. Ознакомиться с заданием на практическую работу.
2. Ознакомиться с программой практической работы.

2. Распределение времени занятия:

Всего: 180 мин

Вступительная часть 5 мин

Проверка готовности студентов к занятию 15 мин

Основная часть 150 мин

Заключительная часть 10 мин

3. Программа практической работы

Основная часть

1. Изучение порядка аттестационных испытаний технических средств обработки информации объекта информатизации – 50 мин.
2. Разработка протокола аттестационных испытаний объекта информатизации - 100 мин.

4. Содержание занятия

Учебный вопрос 1. Изучение порядка аттестационных испытаний технических средств обработки информации объекта информатизации

Аттестационные испытания предусматривают комплексную проверку защищаемого объекта в реальных условиях эксплуатации в целях оценки

соответствия использованного комплекса мер и средств защиты требуемому уровню безопасности информации и проводятся в следующем порядке [1, 2]:

- анализ и оценка исходных данных и документации по защите информации на объекте информатизации, оценка правильности категорирования выделенных помещений и объектов информатизации;
- оценка уровня подготовки кадров и распределения ответственности за выполнение требований по защите информации;
- специальное обследование объекта информатизации;
- проведение испытаний отдельных средств и систем защиты информации в испытательных центрах по сертификации продукции по требованиям безопасности информации (при необходимости);
- специальные проверки технических средств на наличие возможно внедренных специальных электронных устройств перехвата информации;
- специальные проверки помещений на наличие возможно внедренных специальных электронных устройств перехвата информации;
- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте с помощью специальной контрольно-измерительной аппаратуры;
- анализ результатов специального обследования и аттестационных испытаний, разработка рекомендаций по совершенствованию принятых мер по защите информации от утечки по техническим каналам, закрытию выявленных каналов утечки информации;
- подготовка отчетной документации - протоколов испытаний и заключения по результатам аттестационных испытаний с выводами комиссии о соответствии (или несоответствии) объекта информатизации установленным требованиям, которая представляется в орган по аттестации для принятия решения о выдаче «Аттестата соответствия».

Для проведения испытаний заявитель представляет органу по аттестации следующие исходные данные и документацию:

- приемо-сдаточную документацию на объект информатизации;
- акты категорирования выделенных помещений и объектов информатизации;
- инструкции по эксплуатации средств защиты информации;
- технический паспорт на аттестуемый объект;
- документы на эксплуатацию (сертификаты соответствия требованиям безопасности информации) ТСОИ;
- сертификаты соответствия требованиям безопасности информации на ВТСС;
- сертификаты соответствия требованиям безопасности информации на технические средства защиты информации;
- акты на проведенные скрытые работы;
- протоколы измерения звукоизоляции выделенных помещений и эффективности экранирования сооружений и кабин (если они проводились);

- протоколы измерения величины сопротивления заземления;
- протоколы измерения реального затухания информационных сигналов до мест возможного размещения средств разведки;
- данные по уровню подготовки кадров, обеспечивающих защиту информации;
- данные о техническом обеспечении средствами контроля эффективности защиты информации и их метрологической поверке;
- нормативную и методическую документацию по защите информации и контролю эффективности защиты.

Приведенный общий объем исходных данных и документации может уточняться заявителем в зависимости от особенностей аттестуемого объекта информатизации по согласованию с аттестационной комиссией.

- пояснительную записку, содержащую информационную характеристику и организационную структуру объекта защиты, сведения об организационных и технических мероприятиях по защите информации от утечки по техническим каналам;
- перечень объектов информатизации, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
- перечень выделенных помещений, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
- перечень устанавливаемых ТСОИ с указанием наличия сертификата (предписания на эксплуатацию) и мест их установки;
- перечень устанавливаемых ВТСС с указанием наличия сертификата и мест их установки;
- перечень устанавливаемых технических средств защиты информации с указанием наличия сертификата и мест их установки;
- схему (в масштабе) с указанием плана здания, в котором расположены защищаемые объекты, границы контролируемой зоны, трансформаторной подстанции, заземляющего устройства, трасс прокладки инженерных коммуникаций, линий электропитания, связи, пожарной и охранной сигнализации, мест установки разделительных устройств и т.п.;
- технологические поэтажные планы здания с указанием мест расположения объектов информатизации и выделенных помещений и характеристиками их стен, перекрытий, материалов отделки, типов дверей и окон;
- планы объектов информатизации с указанием мест установки ТСОИ, ВТСС и прокладки их соединительных линий, а также трасс прокладки инженерных коммуникаций и посторонних проводников;
- план-схему инженерных коммуникаций всего здания, включая систему вентиляции;
- план-схему системы заземления объекта с указанием места расположения заземлителя;

- план-схему системы электропитания здания с указанием места расположения разделительного трансформатора (подстанции), всех щитов и разводных коробок;
- план-схему прокладки телефонных линий связи с указанием мест расположения распределительных коробок и установки телефонных аппаратов;
- план-схему систем охранной и пожарной сигнализации с указанием мест установки и типов датчиков, а также распределительных коробок;
- схемы систем активной защиты (если они предусмотрены).

Проводится анализ разработанной документации по защите информации с точки зрения полноты и достаточности представленных документов и соответствия их требованиям организационно-распорядительной и нормативно-методической документации.

Проверяется состояние организации работ и выполнения организационно-технических требований по защите информации, оценка правильности категорирования выделенных помещений и объектов информатизации и выбора средств и систем защиты информации.

Проводится оценка уровня подготовки кадров и распределения ответственности за выполнение требований по защите информации.

При проведении специального обследования аттестуемого объекта [1, 2]:

- определяется состав технических средств, используемых для обработки, передачи и хранения защищаемой информации;
- изучается технологический процесс обработки, передачи и хранения защищаемой информации, анализ информационных потоков;
- проверяется соответствие реального состава ТСОИ, ВТСС и средств защиты указанному в техническом паспорте на аттестуемый объект, сертификатах соответствия (предписаниях на эксплуатацию) и представленных исходных данных;
- проверяется соответствие представленных заявителем исходных данных реальным условиям размещения, монтажа ТСОИ, ВТСС и средств защиты;
- проверяется состояние и сохранность печатей на технических средствах, выявляются ТСОИ, ВТСС и средства защиты информации, подвергшиеся несанкционированному вскрытию;
- изучаются условия расположения аттестуемого объекта и определяется граница контролируемой зоны;
- устанавливаются места расположения трансформаторной подстанции, электрощитовой, распределительных щитов. Измеряется длина линий электропитания от защищаемых объектов до возможных мест подключения средств перехвата информации (распределительных щитов, помещений и т.п.), находящихся за пределами контролируемой зоны;
- определяются помещения, смежные с защищаемыми и находящиеся за пределами контролируемой зоны;

- определяются соединительные линии вспомогательных технических средств и систем (линии телефонной связи, оповещения, систем охранной и пожарной сигнализации, часофикации и т.п.), выходящие за пределы контролируемой зоны, места расположения их распределительных коробок. Измеряется длина линий от защищаемых объектов до мест возможного подключения средств перехвата информации за пределами контролируемой зоны;

- определяются инженерные коммуникации и посторонние проводники, выходящие за пределы контролируемой зоны, измеряется их длина от защищаемых объектов до мест возможного подключения средств перехвата информации;

- устанавливается местоположение заземлителя, к которому подключен контур заземления защищаемого объекта.

Все выявленные нарушения и недостатки, отступления от проектных решений включаются в заключение по результатам аттестационных испытаний.

При проведении испытаний отдельных несертифицированных средств и систем защиты информации в испытательных центрах по сертификации эти испытания проводятся до аттестационных испытаний объектов информатизации. В этом случае заявителем к началу аттестационных испытаний должны быть представлены заключения и сертификаты органов по сертификации средств защиты информации по требованиям безопасности информации [2].

Наиболее часто в испытательных центрах проводятся сертификационные испытания помехоподавляющих фильтров, систем активной защиты (генераторов шума) и средств защиты ВТСС.

Измерение и оценка уровней защищенности проводятся в соответствии с действующими нормативными и методическими документами по защите информации от ее утечки по техническим каналам с использованием проверенной контрольно-измерительной аппаратуры.

При аттестации объектов информатизации для каждого ТСОИ:

- измеряются напряженности электромагнитного поля по магнитной H_i (в диапазоне частот 9 кГц – 30 МГц) и электрической E_i (в диапазоне частот 9 кГц – 1800 МГц) составляющим, создаваемые информативным сигналом ТСОИ;

- измеряются уровни информативных сигналов ТСОИ в диапазоне частот 9 кГц - 300 МГц в соединительных линиях вспомогательных технических средств и систем, инженерных коммуникациях, посторонних проводниках, имеющих выход за границу контролируемой зоны;

- определяются коэффициенты удельного затухания информативного сигнала в линиях электропитания, в соединительных линиях вспомогательных технических средств и систем, инженерных коммуникациях, посторонних проводниках, имеющих выход за границу контролируемой зоны, и рассчитывается затухание в них информационного сигнала;

- рассчитывается величина максимально возможной зоны разведки (перехвата) побочных электромагнитных излучений ТСОИ (зоны R_2 , представленной на рис. 1);

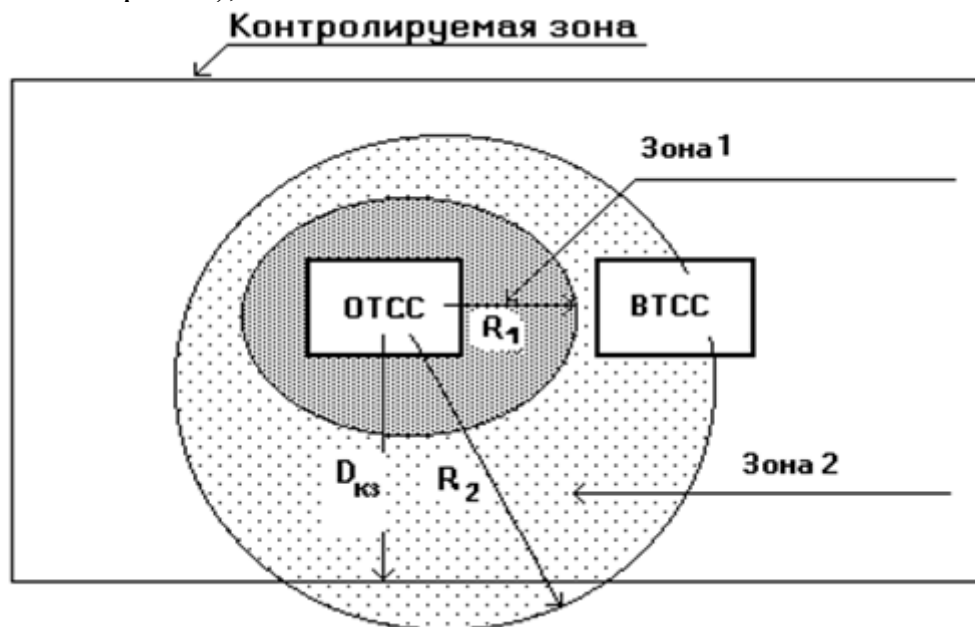


Рисунок 1 – Схема обозначений при определении контролируемой зоны

- рассчитываются предельные расстояния от ТСОИ до вспомогательных технических средств и систем и их кабельных коммуникаций, посторонних проводников и инженерных коммуникаций, имеющих выход за границу контролируемой зоны (зоны $r1, r1'$, представленные на рис. 1);
- измеряется сопротивление заземления каждого ТСОИ;
- измеряется минимальное расстояние от каждого ТСОИ до границы контролируемой зоны.

При использовании на объекте информатизации систем активной защиты (САЗ) дополнительно проводятся:

- измерения напряженности электромагнитного поля по магнитной H_i (в диапазоне частот 9 кГц – 30 МГц) и электрической E_i (в диапазоне частот 9 кГц – 1800 МГц) составляющим, создаваемой помеховыми сигналами САЗ;
- измерения уровней помеховых сигналов в диапазоне частот 9 кГц - 300 МГц, создаваемых САЗ в соединительных линиях вспомогательных технических средств и систем, инженерных коммуникациях, посторонних проводниках, имеющих выход за границу контролируемой зоны.

Специальные проверки на наличие возможно внедренных специальных электронных устройств перехвата информации проводятся по решению руководителя предприятия (учреждения, фирмы). Проверке подлежат:

- выделенные помещения, предназначенные для проведения закрытых мероприятий;
- технические средства, предназначенные для обработки информации ограниченного доступа;

- вспомогательные технические средства, устанавливаемые в выделенных помещениях и на объектах информатизации.

По результатам специальной проверки технических средств по выявлению специальных электронных устройств перехвата информации составляется акт, на основании которого потребителю выдается заключение.

По результатам специальной проверки выделенного помещения оформляется акт с указанием итогов проверки и рекомендаций по защите помещения, который утверждается начальником, организующим проведение специальных проверок. Акт исполняется в двух экземплярах, один из которых отправляется в адрес владельца проверяемого помещения, другой остается в организации, проводившей специальную проверку.

По результатам аттестации оформляются протоколы испытаний и заключение с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатизации в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации.

Заключение аттестационной проверки объекта информатизации должно включать:

- состав аттестационной комиссии (группы);
- дату проведения аттестации;
- перечень руководящих документов, в соответствии с которыми проводилась аттестация;
- перечень документов по защите информации на объекте информатизации, представленных аттестационной комиссией;
- характеристику объекта информатизации (наименование объекта, назначение, местоположение, условия размещения и т.д.);
- перечень технических средств обработки информации ограниченного доступа (ТСОИ), установленных на объекте информатизации, с указанием их места установки и категорий;
- перечень вспомогательных технических средств и систем (ВТСС), установленных на объекте информатизации, с указанием их места установки;
- перечень технических средств защиты информации, установленных на объекте информатизации, с указанием их места установки;
- характеристику организационных мероприятий по защите информации. Вывод о выполнении (невыполнении) организационных мероприятий по защите информации при ее обработке;
- виды работ, проводимых в ходе аттестации;
- перечень использованной в ходе инструментальной проверки (аттестационных испытаний) аппаратуры (перечисляется вся используемая аппаратура контроля по оцениваемым каналам и ее заводские номера);
- результаты анализа документации по защите информации на объекте информатизации. Вывод о соответствии (несоответствии) разработанной

документации по защите информации требованиям нормативно-методических документов ФСТЭК РФ;

- оценку правильности категорирования объектов информатизации;
- оценку уровня подготовки кадров и распределения ответственности за выполнение требований по защите информации;
- результаты специального обследования объекта информатизации;
- условия расположения объекта информатизации относительно границы контролируемой зоны, минимальное расстояние до границы контролируемой зоны;
- вывод о соответствии (несоответствии) реального состава ТСОИ, ВТСС и средств защиты информации указанному в техническом паспорте на аттестуемый объект, сертификатах соответствия (предписаниях на эксплуатацию) и представленных исходных данных;
- вывод о состоянии и сохранности печатей и пломб на ТСОИ (в случае выявления перечисляются технические средства, подвергавшиеся несанкционированному вскрытию);
- вывод о соответствии (несоответствии) мест установки ТСОИ, ВТСС и средств защиты информации и прокладки их соединительных линий техническому паспорту на объект информатизации;
- вывод о соответствии (несоответствии) реального разноса ТСОИ и их соединительных линий относительно ВТСС и посторонних проводников требованиям нормативно-методических документов ФСТЭК РФ и сертификатов соответствия (предписаний на эксплуатацию);
- характеристику системы электропитания объекта информатизации и технических средств защиты информации от утечки по цепям электропитания (указываются номера и места расположения трансформаторной подстанции, электрощитовой, распределительных щитов, от которых осуществляется питание ТСОИ. Описывается схема электропитания объекта с указанием типов и марки используемых кабелей электропитания. Перечисляются технические средства защиты цепей электропитания с указанием их мест установки. При наличии сертификатов соответствия на средства защиты цепей электропитания указывается срок их действия. Указывается длина линий электропитания от защищаемых ТСОИ до возможных мест подключения к ним средств перехвата информации (распределительных щитов, помещений и т.п.), находящихся за пределами контролируемой зоны. Вывод о соответствии (или несоответствии) системы электропитания объекта информатизации требованиям нормативно-методических документов ФСТЭК РФ и сертификатов соответствия (предписаний на эксплуатацию) ТСОИ;
- характеристику системы заземления объекта информатизации и технических средств защиты информации от утечки по цепям заземления в случае их использования. Описывается схема заземления ТСОИ. Указывается тип и местоположение заземляющего устройства, расстояние от него до границы контролируемой зоны. Указываются типы заземляющих проводников и способы их подключения к ТСОИ и т.п. Приводятся даты и результаты измерений

сопротивления заземления ТСОИ. Вывод о соответствии (несоответствии) системы заземления объекта информатизации требованиям нормативно-методических документов ФСТЭК РФ и сертификатов соответствия (предписаний на эксплуатацию) ТСОИ;

- характеристику вспомогательных технических средств и систем, соединительные линии которых выходят за пределы контролируемой зоны (наименование, тип, назначение и т.п.). Указывается длина соединительных линий от ВТСС до возможных мест подключения к ним средств перехвата информации, находящихся за пределами контролируемой зоны. Перечисляются технические средства защиты ВТСС с указанием их мест установки. При наличии сертификатов соответствия на средства защиты ВТСС, указывается срок их действия;

- перечень посторонних проводников и инженерных коммуникаций, выходящих за пределы контролируемой зоны. Указывается их длина от защищаемых объектов до мест возможного подключения средств перехвата информации, расположенных за пределами контролируемой зоны. Указывается наличие (отсутствие) диэлектрических вставок в инженерных коммуникациях. При использовании систем линейного зашумления указывается их тип и место установки, а при наличии сертификатов соответствия - срок их действия;

- результаты проведения испытаний ТСОИ на побочные электромагнитные излучения;

- величину максимально возможной зоны разведки (перехвата) побочных электромагнитных излучений ТСОИ (зона $R2$);

- предельные расстояния от ТСОИ и их соединительных линий до вспомогательных технических средств и систем, установленных на объекте информатизации и имеющих соединительные линии, выходящие за пределы контролируемой зоны (зоны $r1$);

- предельные расстояния от ТСОИ и их соединительных линий до линий ВТСС, посторонних проводников и инженерных коммуникаций, выходящих за границу контролируемой зоны (зоны $r1$);

- вывод о соответствии (несоответствии) эффективности защиты ТСОИ от утечки информации за счет побочных электромагнитных излучений требованиям нормативно-методических документов ФСТЭК РФ;

- результаты проведения испытаний системы активной защиты (САЗ) объекта информатизации (при ее использовании):

- величину максимально возможной зоны разведки (перехвата) побочных электромагнитных излучений ТСОИ (зона $R2$), при использовании САЗ;

- предельные расстояния от ТСОИ и их соединительных линий до вспомогательных технических средств и систем, установленных на объекте информатизации и имеющих соединительные линии, выходящие за пределы контролируемой зоны (зоны $r1$), при использовании САЗ;

- предельные расстояния от ТСОИ и их соединительных линий до линий ВТСС, посторонних проводников и инженерных коммуникаций, выходящих за границу контролируемой зоны (зоны $r1$), при использовании САЗ;
- вывод о соответствии (несоответствии) эффективности защиты ТСОИ от утечки информации за счет побочных электромагнитных излучений требованиям нормативно-методических документов ФСТЭК РФ;
- результаты проведения испытаний помехоподавляющих фильтров, используемых для защиты цепей электропитания ТСОИ (испытания проводятся, если срок действия сертификата соответствия на них на момент аттестации истек). Вывод о соответствии (несоответствии) фильтров требованиям нормативно-методических документов ФСТЭК РФ;
- результаты проведения испытаний средств защиты ВТСС (испытания проводятся, если срок действия сертификата соответствия на них на момент аттестации истек). Вывод о соответствии (несоответствии) средств защиты требованиям нормативно-методических документов ФСТЭК РФ;
- недостатки, выявленные в ходе аттестации;
- общий вывод о соответствии (несоответствии) эффективности защиты объекта информатизации требованиям нормативно-методических документов ФСТЭК РФ, о возможности (невозможности) выдачи «Аттестата соответствия» и допуске ТСОИ к обработке информации соответствующего уровня конфиденциальности (секретности).

Протокол аттестационных испытаний должен включать:

- вид испытаний;
- объект испытаний;
- дату и время проведения испытаний;
- место проведения испытаний;
- перечень использованной в ходе испытаний аппаратуры (наименование, тип, заводской номер, номер свидетельства о поверке и срок его действия);
- перечень нормативно-методических документов, в соответствии с которыми проводились испытания;
- методику проведения испытания (краткое описание);
- результаты измерений;
- результаты расчетов;
- выводы по результатам испытаний.

Протоколы испытаний подписываются экспертами – членами аттестационной комиссии, проводившими испытания, с указанием должности, фамилии и инициалов.

Заключение и протоколы испытаний подлежат утверждению органом по аттестации.

Учебный вопрос 2. Разработка протокола аттестационных испытаний объекта информатизации

В соответствии с исходными данными и результатами, полученными в предыдущих лабораторных работах разработать протокол аттестационных испытаний объекта информатизации.

Порядок и пример оформления протокола аттестационных испытаний объекта информатизации приведен в файле «Протокол испытаний».

Представить разработанный вариант протокола аттестационных испытаний рассматриваемого объекта информатизации преподавателю для проверки.

5. Контрольные вопросы

1. Опишите состав аттестационных испытаний объекта информатизации.
2. Укажите структурные элементы «Протокола аттестационных испытаний».
3. Опишите порядок проведения специального обследования ОИ на соответствие требованиям безопасности информации».
4. порядок проведения специальной проверки ОИ на соответствие требованиям безопасности информации».
5. Дайте характеристику составу заключения аттестационной проверки ОИ.

Литература

1. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. – М.: Горячая линия – Телеком, 2005, с. 416.
2. Приказ ФСТЭК РФ от 29 апреля 2021 г. N 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».
3. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.).
4. Приказ ФСТЭК РФ от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
5. Требования к защите персональных данных при их обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 1 ноября 2012 г. №1119).
6. Приказ ФСТЭК РФ от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Тема 7.

Практическое занятие №7

Цель занятия:

1. Закрепление теоретических знаний по вопросам аттестационных испытаний выделенных помещений объекта информатизации.
2. Получение практических навыков по разработке аттестата соответствия, разрабатываемого при аттестации выделенного помещения объекта информатизации по требованиям безопасности информации.
3. Совершенствование навыков анализа процессов при аттестации объектов информатизации по требованиям безопасности информации и формулировки выводов.

Формируемые компетенции: ПК-3, ПК-6

Время – 4 ч.

1. Подготовка к занятию

1. Ознакомиться с заданием на практическую работу.
2. Ознакомиться с программой практической работы.

2. Распределение времени занятия:

Всего: 180 мин

Вступительная часть 5 мин

Проверка готовности студентов к занятию 15 мин

Основная часть 150 мин

Заключительная часть 10 мин

3. Программа практической работы

Основная часть

1. Изучение порядка аттестационных испытаний выделенных помещений объекта информатизации – 50 мин.
2. Разработка аттестата соответствия выделенного помещения объекта информатизации - 100 мин.

4. Содержание занятия

Учебный вопрос 1. Изучение порядка аттестационных испытаний выделенных помещений объекта информатизации

Аттестационные испытания предусматривают комплексную проверку защищаемого объекта в реальных условиях эксплуатации в целях оценки соответствия использованного комплекса мер и средств защиты требуемому уровню безопасности информации и проводятся в следующем порядке [1, 2]:

- анализ и оценка исходных данных и документации по защите информации на объекте информатизации, оценка правильности категорирования выделенных помещений и объектов информатизации;
- оценка уровня подготовки кадров и распределения ответственности за выполнение требований по защите информации;
- специальное обследование объекта информатизации;
- проведение испытаний отдельных средств и систем защиты информации в испытательных центрах по сертификации продукции по требованиям безопасности информации (при необходимости);
- специальные проверки технических средств на наличие возможно внедренных специальных электронных устройств перехвата информации;
- специальные проверки помещений на наличие возможно внедренных специальных электронных устройств перехвата информации;
- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте с помощью специальной контрольно-измерительной аппаратуры;
- анализ результатов специального обследования и аттестационных испытаний, разработка рекомендаций по совершенствованию принятых мер по защите информации от утечки по техническим каналам, закрытию выявленных каналов утечки информации;
- подготовка отчетной документации - протоколов испытаний и заключения по результатам аттестационных испытаний с выводами комиссии о соответствии (или несоответствии) объекта информатизации установленным требованиям, которая представляется в орган по аттестации для принятия решения о выдаче «Аттестата соответствия».

Для проведения испытаний заявитель представляет органу по аттестации следующие исходные данные и документацию:

- приемо-сдаточную документацию на объект информатизации;
- акты категорирования выделенных помещений и объектов информатизации;
- инструкции по эксплуатации средств защиты информации;
- технический паспорт на аттестуемый объект;
- документы на эксплуатацию (сертификаты соответствия требованиям безопасности информации) ТСОИ;
- сертификаты соответствия требованиям безопасности информации на ВТСС;
- сертификаты соответствия требованиям безопасности информации на технические средства защиты информации;
- акты на проведенные скрытые работы;

- протоколы измерения звукоизоляции выделенных помещений и эффективности экранирования сооружений и кабин (если они проводились);
- протоколы измерения величины сопротивления заземления;
- протоколы измерения реального затухания информационных сигналов до мест возможного размещения средств разведки;
- данные по уровню подготовки кадров, обеспечивающих защиту информации;
- данные о техническом обеспечении средствами контроля эффективности защиты информации и их метрологической поверке;
- нормативную и методическую документацию по защите информации и контролю эффективности защиты.

Приведенный общий объем исходных данных и документации может уточняться заявителем в зависимости от особенностей аттестуемого объекта информатизации по согласованию с аттестационной комиссией.

- пояснительную записку, содержащую информационную характеристику и организационную структуру объекта защиты, сведения об организационных и технических мероприятиях по защите информации от утечки по техническим каналам;
- перечень объектов информатизации, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
- перечень выделенных помещений, подлежащих защите, с указанием мест их расположения и установленной категории защиты;
- перечень устанавливаемых ТСОИ с указанием наличия сертификата (предписания на эксплуатацию) и мест их установки;
- перечень устанавливаемых ВТСС с указанием наличия сертификата и мест их установки;
- перечень устанавливаемых технических средств защиты информации с указанием наличия сертификата и мест их установки;
- схему (в масштабе) с указанием плана здания, в котором расположены защищаемые объекты, границы контролируемой зоны, трансформаторной подстанции, заземляющего устройства, трасс прокладки инженерных коммуникаций, линий электропитания, связи, пожарной и охранной сигнализации, мест установки разделительных устройств и т.п.;
- технологические поэтажные планы здания с указанием мест расположения объектов информатизации и выделенных помещений и характеристиками их стен, перекрытий, материалов отделки, типов дверей и окон;
- планы объектов информатизации с указанием мест установки ТСОИ, ВТСС и прокладки их соединительных линий, а также трасс прокладки инженерных коммуникаций и посторонних проводников;
- план-схему инженерных коммуникаций всего здания, включая систему вентиляции;

- план-схему системы заземления объекта с указанием места расположения заземлителя;
- план-схему системы электропитания здания с указанием места расположения разделительного трансформатора (подстанции), всех щитов и разводных коробок;
- план-схему прокладки телефонных линий связи с указанием мест расположения распределительных коробок и установки телефонных аппаратов;
- план-схему систем охранной и пожарной сигнализации с указанием мест установки и типов датчиков, а также распределительных коробок;
- схемы систем активной защиты (если они предусмотрены).

Проводится анализ разработанной документации по защите информации с точки зрения полноты и достаточности представленных документов и соответствия их требованиям организационно-распорядительной и нормативно-методической документации.

Проверяется состояние организации работ и выполнения организационно-технических требований по защите информации, оценка правильности категорирования выделенных помещений и объектов информатизации и выбора средств и систем защиты информации.

Проводится оценка уровня подготовки кадров и распределения ответственности за выполнение требований по защите информации.

При проведении специального обследования аттестуемого объекта [1, 2]:

- определяется состав технических средств, используемых для обработки, передачи и хранения защищаемой информации;
- изучается технологический процесс обработки, передачи и хранения защищаемой информации, анализ информационных потоков;
- проверяется соответствие реального состава ТСОИ, ВТСС и средств защиты указанному в техническом паспорте на аттестуемый объект, сертификатах соответствия (предписаниях на эксплуатацию) и представленных исходных данных;
- проверяется соответствие представленных заявителем исходных данных реальным условиям размещения, монтажа ТСОИ, ВТСС и средств защиты;
- проверяется состояние и сохранность печатей на технических средствах, выявляются ТСОИ, ВТСС и средства защиты информации, подвергшиеся несанкционированному вскрытию;
- изучаются условия расположения аттестуемого объекта и определяется граница контролируемой зоны;
- устанавливаются места расположения трансформаторной подстанции, электрощитовой, распределительных щитов. Измеряется длина линий электропитания от защищаемых объектов до возможных мест подключения средств перехвата информации (распределительных щитов, помещений и т.п.), находящихся за пределами контролируемой зоны;

- определяются помещения, смежные с защищаемыми и находящиеся за пределами контролируемой зоны;

- определяются соединительные линии вспомогательных технических средств и систем (линии телефонной связи, оповещения, систем охранной и пожарной сигнализации, часофикации и т.п.), выходящие за пределы контролируемой зоны, места расположения их распределительных коробок. Измеряется длина линий от защищаемых объектов до мест возможного подключения средств перехвата информации за пределами контролируемой зоны;

- определяются инженерные коммуникации и посторонние проводники, выходящие за пределы контролируемой зоны, измеряется их длина от защищаемых объектов до мест возможного подключения средств перехвата информации;

- устанавливается местоположение заземлителя, к которому подключен контур заземления защищаемого объекта.

Все выявленные нарушения и недостатки, отступления от проектных решений включаются в заключение по результатам аттестационных испытаний.

При проведении испытаний отдельных несертифицированных средств и систем защиты информации в испытательных центрах по сертификации эти испытания проводятся до аттестационных испытаний объектов информатизации. В этом случае заявителем к началу аттестационных испытаний должны быть представлены заключения и сертификаты органов по сертификации средств защиты информации по требованиям безопасности информации [2].

Наиболее часто в испытательных центрах проводятся сертификационные испытания помехоподавляющих фильтров, систем активной защиты (генераторов шума) и средств защиты ВТСС.

Измерение и оценка уровней защищенности проводятся в соответствии с действующими нормативными и методическими документами по защите информации от ее утечки по техническим каналам с использованием проверенной контрольно-измерительной аппаратуры.

При аттестации выделенного помещения:

- измеряются уровни акустического сигнала и шумов в октавных полосах частот со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц в местах возможной установки микрофонных датчиков средств речевой разведки;

- измеряются уровни вибрационного сигнала и шумов в октавных полосах частот со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц в местах возможной установки датчиков контактного типа средств речевой разведки;

- определяются коэффициенты звукоизоляции ограждающих конструкций (окон, дверей, стен, пола, потолка) выделенного помещения в октавных полосах частот со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц;

- определяются коэффициенты виброизоляции ограждающих конструкций выделенного помещения, а также различных элементов инженерно-технических систем, включая их коммуникации, в октавных полосах частот со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц;

- при использовании в выделенном помещении систем виброакустической маскировки дополнительно проводятся измерения уровней акустический и вибрационных шумов в октавных полосах частот со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц в местах возможной установки датчиков средств акустической разведки;

- измеряются уровни информационных сигналов на выходе ВТСС, возникающих вследствие акустоэлектрического преобразования акустических сигналов элементами ВТСС, в октавных полосах частот со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц;

- измеряются уровни шумов на выходе в октавных полосах частот со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц;

- рассчитывается словесная разборчивость речи W для каждого типа аппаратуры речевой разведки.

Специальные проверки на наличие возможно внедренных специальных электронных устройств перехвата информации проводятся по решению руководителя предприятия (учреждения, фирмы). Проверке подлежат:

- выделенные помещения, предназначенные для проведения закрытых мероприятий;

- технические средства, предназначенные для обработки информации ограниченного доступа;

- вспомогательные технические средства, устанавливаемые в выделенных помещениях и на объектах информатизации.

По результатам специальной проверки технических средств по выявлению специальных электронных устройств перехвата информации составляется акт, на основании которого потребителю выдается заключение.

По результатам специальной проверки выделенного помещения оформляется акт с указанием итогов проверки и рекомендаций по защите помещения, который утверждается начальником, организующим проведение специальных проверок. Акт исполняется в двух экземплярах, один из которых отправляется в адрес владельца проверяемого помещения, другой остается в организации, проводившей специальную проверку.

По результатам аттестации оформляются протоколы испытаний и заключение с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатизации в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации.

Заключение аттестационной проверки выделенного помещения должно включать:

- состав аттестационной комиссии (группы);

- дату проведения аттестации;
- перечень руководящих документов, в соответствии с которыми проводилась аттестация;
- перечень документов по защите информации в выделенном помещении, представленных аттестационной комиссии;
- характеристику выделенного помещения (назначение, местоположение, условия размещения и т.д.);
- перечень вспомогательных технических средств и систем (ВТСС), установленных на объекте информатизации;
- перечень технических средств защиты информации, установленных в выделенном помещении;
- характеристику организационных мероприятий по защите информации;
- виды работ, проводимых в ходе аттестации;
- перечень использованной в ходе инструментальной проверки (аттестационных испытаний) аппаратуры (перечисляется вся используемая аппаратура контроля по оцениваемым каналам и ее заводские номера);
- результаты анализа документации по защите информации в выделенном помещении. Вывод о соответствии (несоответствии) разработанной документации по защите информации требованиям нормативно-методических документов ФСТЭК РФ;
- оценку правильности категорирования выделенного помещения;
- оценку уровня подготовки кадров и распределения ответственности за выполнение требований по защите информации;
- результаты специального обследования выделенного помещения;
- условия расположения выделенного помещения относительно границы контролируемой зоны, характеристику смежных с ним помещений, минимальное расстояние до границы контролируемой зоны;
- характеристику вспомогательных технических средств и систем, соединительные линии которых выходят за пределы контролируемой зоны (наименование, тип, назначение и т.п.). Указывается длина соединительных линий от ВТСС до возможных мест подключения к ним средств перехвата информации, находящихся за пределами контролируемой зоны. Перечисляются технические средства защиты ВТСС с указанием их мест установки. При наличии сертификатов соответствия на средства защиты ВТСС указывается срок их действия. Вывод о соответствии (несоответствии) реального состава ВТСС, средств их защиты указанному в техническом паспорте на выделенное помещение и представленных исходных данных. Вывод о состоянии и сохранности печатей и пломб на ВТСС (в случае выявления перечисляются технические средства, подвергавшиеся несанкционированному вскрытию);
- характеристику системы электропитания выделенного помещения (описывается схема электропитания выделенного помещения, указываются номера и места расположения трансформаторной подстанции, электрощитовой,

распределительных щитов, от которых осуществляется розеточной и осветительной сетей электропитания выделенного помещения и их расположение относительно границы контролируемой зоны);

- перечень инженерных коммуникаций, выходящих за пределы контролируемой зоны. Указывается их длина от выделенного помещения до мест возможного подключения средств перехвата информации, расположенных за пределами контролируемой зоны. Указывается наличие (отсутствие) специальных вставок в инженерных коммуникациях;

- результаты акустовибрационных измерений:

- коэффициенты звукоизоляции ограждающих конструкций (окон, дверей, стен, пола, потолка) выделенного помещения в октавных полосах частот и словесная разборчивость речи W в местах возможного подключения средств перехвата информации с датчиками микрофонного типа;

- коэффициенты виброизоляции ограждающих конструкций выделенного помещения, а также различных элементов инженерно-технических систем, включая их коммуникации, в октавных полосах частот и словесная разборчивость речи W в местах возможного подключения средств перехвата информации с датчиками контактного типа;

- вывод о соответствии (несоответствии) эффективности защиты выделенного помещения от утечки информации по прямым акустическим, акустовибрационным и акустооптическим каналам требованиям нормативно-методических документов ФСТЭК РФ;

- результаты проведения испытаний системы виброакустической маскировки (СВАМ) выделенного помещения (при ее использовании):

- словесная разборчивость речи W в местах возможного подключения средств перехвата информации с датчиками микрофонного типа;

- словесная разборчивость речи W в местах возможного подключения средств перехвата информации с датчиками контактного типа;

- вывод о соответствии (несоответствии) эффективности защиты выделенного помещения от утечки информации по прямым акустическим, акустовибрационным и акустооптическим каналам при использовании СВАМ требованиям нормативно-методических документов ФСТЭК РФ;

- измеряются уровни информационных сигналов на выходе ВТСС, возникающих вследствие акустоэлектрического преобразования акустических сигналов элементами ВТСС, в октавных полосах частот со среднегеометрическими частотами 250, 500, 1000, 2000, 4000 Гц;

- результаты акустоэлектрических измерений:

- словесная разборчивость речи W в соединительных линиях ВТСС, имеющих в своем составе элементы, обладающие микрофонным эффектом;

- проведения испытаний средств защиты ВТСС;

- вывод о соответствии (несоответствии) эффективности защиты ВТСС от утечки информации по акустоэлектрическим каналам требованиям нормативно-методических документов ФСТЭК РФ;

- недостатки, выявленные в ходе аттестации;
- общий вывод о соответствии (несоответствии) эффективности защиты выделенного помещения требованиям нормативно-методических документов ФСТЭК РФ, о возможности (невозможности) выдачи «Аттестата соответствия» и разрешения ведения переговоров соответствующего уровня конфиденциальности (секретности).

В случае если эффективность защиты объекта информатизации или выделенного помещения не соответствует требованиям нормативно-методических документов ФСТЭК РФ, то формулируются предложения по устранению выявленных в ходе аттестации нарушений, сроки и условия представления для повторной аттестации объекта информатизации или выделенного помещения.

Заключение по результатам аттестации подписывается членами аттестационной комиссии, утверждается руководителем органа аттестации и представляется заявителю [2].

К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод.

Протокол аттестационных испытаний должен включать:

- вид испытаний;
- объект испытаний;
- дату и время проведения испытаний;
- место проведения испытаний;
- перечень использованной в ходе испытаний аппаратуры (наименование, тип, заводской номер, номер свидетельства о поверке и срок его действия);
- перечень нормативно-методических документов, в соответствии с которыми проводились испытания;
- методику проведения испытания (краткое описание);
- результаты измерений;
- результаты расчетов;
- выводы по результатам испытаний.

Протоколы испытаний подписываются экспертами – членами аттестационной комиссии, проводившими испытания, с указанием должности, фамилии и инициалов.

Заключение и протоколы испытаний подлежат утверждению органом по аттестации.

Учебный вопрос 2. Оформление аттестата соответствия выделенного помещения объекта информатизации

В соответствии с исходными данными и результатами, полученными в предыдущих лабораторных работах оформить технический паспорт и аттестат соответствия выделенного помещения объекта информатизации, с учетом

предположения, что в результате проверок выделенного помещения замечаний не выявлено.

Порядок и пример оформления технического паспорта и аттестата соответствия выделенного помещения объекта информатизации приведен соответственно в приложениях 2 и 4 к «Порядку организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации, не составляющей государственную тайну» (приказ ФСТЭК России от 29 апреля 2021 г. № 77) в файле Приказ_2021.04.29_77.

При заполнении аттестата соответствия выделенного помещения в пункте 1 в сведениях «Наименование требований по защите информации, на соответствии которым проводилась аттестация» необходимо использовать «Приказ-282-от-30.08.2002».

Представить разработанные варианты технического паспорта и аттестата соответствия выделенного помещения для рассматриваемого объекта информатизации преподавателю для проверки в форме отчета по практической работе.

5. Контрольные вопросы

1. Опишите состав аттестационных испытаний выделенного помещения.
2. Укажите структурные элементы «Аттестата соответствия» на выделенное помещение.
3. Опишите порядок проведения специального обследования выделенного помещения на соответствие требованиям безопасности информации.
4. Порядок проведения оформления результатов специального обследования выделенного помещения на соответствие требованиям безопасности информации.
5. Дайте характеристику составу заключения аттестационной проверки выделенного помещения.
6. Опишите структуру аттестата соответствия выделенного помещения.

Литература

1. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. – М.: Горячая линия – Телеком, 2005, с. 416.
2. Приказ ФСТЭК РФ от 29 апреля 2021 г. N 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».
3. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Государственной технической комиссии при Президенте РФ от 30 марта 1992 г.).

4. Приказ ФСТЭК РФ от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

5. Требования к защите персональных данных при их обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 1 ноября 2012 г. №1119).

6. Приказ ФСТЭК РФ от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Тема 8.

Практическое занятие №8

Цель занятия:

1. Закрепление теоретических знаний по вопросам аттестационных испытаний объектов информатизации.
2. Получение практических навыков по вопросам аккредитации испытательных лабораторий и органов сертификации средств защиты информации по требованиям безопасности информации.
3. Совершенствование навыков анализа процессов при аттестации объектов информатизации по требованиям безопасности информации и формулировки выводов.

Формируемые компетенции: ПК-3, ПК-6

Время – 4 ч.

1. Подготовка к занятию

1. Ознакомиться с заданием на практическую работу.
2. Ознакомиться с программой практической работы.

2. Распределение времени занятия:

Всего: 180 мин

Вступительная часть 5 мин

Проверка готовности студентов к занятию 15 мин

Основная часть 150 мин

Заключительная часть 10 мин

3. Программа практической работы

Основная часть

1. Понятие аккредитации предприятий в качестве органов по сертификации средств защиты информации – 30 мин.
2. Порядок аккредитации предприятия – 50 мин.
3. Контроль и надзор за деятельностью аккредитованных испытательных лабораторий и органов сертификации – 70 мин.

4. Методические указания студентам по подготовке и проведению практического занятия

4.1. При подготовке к занятию

В период подготовки к практическому занятию студенты получают в соответствии с указаниями преподавателя необходимую литературу в библиотеке университета и изучают учебные материалы темы №5 «Аккредитации органов сертификации (испытательных лабораторий) средств

защиты информации по требованиям безопасности информации», используя 1у [1, с.99-102; 2-4], а также конспект лекций.

1. Понятие аккредитации предприятий в качестве органов по сертификации средств защиты информации

1.1. Настоящее Положение устанавливает основные принципы аккредитации юридических лиц - предприятий, организаций и учреждений (далее предприятий) в качестве испытательных лабораторий и органов по сертификации средств защиты информации в системе сертификации средств защиты информации по требованиям безопасности информации.

1.2. Положение об аккредитации испытательных лабораторий разработано в соответствии с Законом Российской Федерации "О сертификации продукции и услуг", Постановлением Правительства Российской Федерации "О сертификации средств защиты информации", основании "Системы сертификации ГОСТ Р", "Правил по проведению сертификации в Российской Федерации", "Положения о сертификации средств защиты информации по требованиям безопасности информации", "Положения о государственном лицензировании деятельности в области защиты информации". А также дополняется на основе новых указов и приказов, среди них Указ Президента Российской Федерации от 9 марта 2004 г. № 314 Гостехкомиссия России преобразована в Федеральную службу по техническому и экспортному контролю (ФСТЭК России) и приказ от 3 апреля 2018 г. N 55 «ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ О СИСТЕМЕ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ» (в ред. Приказов ФСТЭК России от 05.08.2021 N 121, от 19.09.2022 N 172) и Федеральный закон от 28.12.2013 N 412-ФЗ «ОБ АККРЕДИТАЦИИ В НАЦИОНАЛЬНОЙ СИСТЕМЕ АККРЕДИТАЦИИ» с редакцией от 24 июля 2023 года. Положение от 25 ноября 1994 года действует до сих пор.

1.3. Аккредитация предприятия в качестве органа по сертификации средств защиты информации по требованиям безопасности информации (далее - орган по сертификации) является официальным признанием его технической

компетентности и независимости от разработчиков, изготовителей (поставщиков) и заказчиков (потребителей) испытываемых средств защиты информации для организации и проведения испытаний в соответствии с требованиями стандартов или иных нормативных документов.

Аккредитация предприятия в качестве испытательной лаборатории может являться официальным признанием только ее технической компетентности в проведении испытаний. При этом, испытания для целей сертификации допускается проводить лишь под контролем представителей органа по сертификации соответствующих средств защиты информации.

Аккредитация производится только при наличии у указанных органов и лабораторий лицензий на соответствующие виды деятельности.

1.4. При аккредитации предприятия ему выдается Аттестат аккредитации (Приложения 1, 2) с указанием области аккредитации. Срок действия Аттестата аккредитации не должен превышать пяти лет. Но в связи с принятием Федерального закона от 28.12.2013 № 412-ФЗ «ОБ АККРЕДИТАЦИИ В НАЦИОНАЛЬНОЙ СИСТЕМЕ АККРЕДИТАЦИЙ» с редакцией от 24 июля 2023, в статье 18, пункт 1 сказано, что аккредитация в национальной системе аккредитации является бессрочной

1.5. Требования аккредитации, установленные настоящим документом, являются общими для всех видов испытаний средств защиты информации.

При необходимости, они могут быть дополнены другими требованиями, исходя из специфики деятельности конкретного предприятия.

1.6. Аккредитацию предприятий осуществляет Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России), но в связи с Указом Президента Российской Федерации от 9 марта 2004 г. № 314 Гостехкомиссия России преобразована в Федеральную службу по техническому и экспортному контролю (ФСТЭК России). По приказу от 3 апреля 2018 г. N 55 «ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ О СИСТЕМЕ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ» (в ред. Приказов

ФСТЭК России от 05.08.2021 N 121, от 19.09.2022 N 172). В пункте 5, участниками системы сертификации ФСТЭК России являются:

- федеральный орган по сертификации;
- организации, аккредитованные ФСТЭК России в качестве органа по сертификации;
- организации, аккредитованные ФСТЭК России в качестве испытательной лаборатории;
- изготовители средств защиты информации

2. Порядок аккредитации предприятия

2.1. Аккредитация предусматривает следующие этапы:

- рассмотрение документов, представленных предприятием;
- проверка предприятия комиссией, определяемой федеральный орган по сертификации;
- принятие решения об аккредитации по результатам проверки;
- оформление, регистрация и выдача Аттестата аккредитации.

2.2. Предприятие, претендующее на аккредитацию, должно подать заявку на аккредитацию (Приложения 3, 4). Одновременно с заявкой направляется проект Положения об органе по сертификации или испытательной лаборатории с заявляемой областью аккредитации (Приложение 5).

В случае аккредитации предприятия в качестве испытательной лаборатории средств защиты информации к заявке дополнительно прикладывается паспорт испытательной лаборатории (Приложение 6) и анкета - опросник (Приложение 7).

2.3. После рассмотрения представленных материалов создается комиссия по проверке предприятия. Состав комиссии формируется из специалистов территориальных по сертификации, отраслевых, региональных центров по защите информации, других организаций и предприятий, компетентных в области защиты информации, и утверждается руководителем ФСТЭК России.

2.4. Проверка проводится на соответствие фактического состояния предприятия представленным документам и на его способность выполнять заявленные функции.

По результатам проверки комиссия составляет акт (в случае испытательной лаборатории средств защиты информации форма акта приведена в Приложении 8), который подписывается членами комиссии и представляется для ознакомления руководителю аккредитуемого предприятия.

2.5. Решение об аккредитации предприятия принимается после рассмотрения всей полученной информации о состоянии этого предприятия и его готовности к аккредитации.

Аккредитованное предприятие вносится органом сертификации в государственный реестр системы и ему выдается Аттестат аккредитации. Порядок повторной аккредитации устанавливается в зависимости от результатов контроля и может проводиться по полной или сокращенной процедуре, устанавливаемой в каждом конкретном случае.

2.7. Аккредитация в дополнительной области.

2.7.1. Орган по сертификации, испытательная лаборатория, претендующие на расширение своей области аккредитации, направляют заявку на аккредитацию в дополнительной области (Приложения 3, 4).

К заявке прилагаются:

- сведения о дополнительной области аккредитации;
- дополнения к Паспорту (Приложение 5).

2.7.2. Аккредитация может проводиться по полной или сокращенной программе, устанавливаемой в каждом конкретном случае.

3. Контроль и надзор за деятельностью аккредитованных испытательных лабораторий и органов сертификации

3.1. Контроль может осуществляться путем:

- периодических проверок;

- предоставления предприятием регулярной информации о качестве проводимых им испытаний, о результатах периодических внутренних проверок системы обеспечения качества испытаний, о претензиях клиентов и т.д.;

- любых других действий контрольного характера, которые могут обеспечить уверенность в том, что предприятие в течение срока действия Аттестата аккредитации соответствует требованиям, предъявленным к нему при аккредитации.

3.2. Условия контроля для каждого предприятия определяются в соответствующем Положении об органе по сертификации (испытательной лаборатории) при принятии решения по его аккредитации.

3.3. Расходы на проведение всех видов работ по аккредитации предприятий в качестве испытательных лабораторий и органа по сертификации, по осуществлению контроля и надзора за их деятельностью оплачиваются заявителями в порядке, установленном органом сертификации России по согласованию с Министерством финансов Российской Федерации.

При подготовке к практическому занятию студентам рекомендуется ответить на контрольные вопросы.

Контрольные вопросы:

1) Аккредитация предприятия в качестве органа по сертификации средств защиты информации по требованиям безопасности информации (далее - орган по сертификации) является официальным признанием его технической компетентности и независимости от разработчиков, изготовителей (поставщиков) и заказчиков (потребителей) испытываемых средств защиты информации для организации и проведения испытаний в соответствии с требованиями стандартов или иных нормативных документов.

2) Аккредитация предприятия в качестве испытательной лаборатории может являться официальным признанием только ее технической компетентности в проведении испытаний. При этом, испытания для целей сертификации допускается проводить лишь под контролем представителей

органа по сертификации соответствующих средств защиты информации. Аккредитация производится только при наличии у указанных органов и лабораторий лицензий на соответствующие виды деятельности.

3) В случае аккредитации предприятия в качестве испытательной лаборатории средств защиты информации к заявке дополнительно прикладывается паспорт испытательной лаборатории (Приложение 6) и анкета - опросник (Приложение 7)

4) При аккредитации предприятия ему выдается Аттестат аккредитации (Приложения 1, 2) с указанием области аккредитации. Срок действия Аттестата аккредитации не должен превышать пяти лет.

5) Контроль может осуществляться путем:

- периодических проверок;
- предоставления предприятием регулярной информации о качестве проводимых им испытаний, о результатах периодических внутренних проверок системы обеспечения качества испытаний, о претензиях клиентов и т.д.;
- любых других действий контрольного характера, которые могут обеспечить уверенность в том, что предприятие в течение срока действия Аттестата аккредитации соответствует требованиям, предъявленным к нему при аккредитации.

6) Аккредитация предприятия может быть досрочно отменена в следующих случаях: - несоответствие предприятия требованиям, предъявляемым к аккредитованным предприятиям; - самостоятельное решение аккредитованного предприятия о досрочном прекращении действия аккредитации. Предприятие может в течение 15 дней опротестовать решение по любым вопросам аккредитации в Госарбитраже России.

Порядок проведения занятия

Во время проведения занятия преподаватель осуществляет опрос студентов и определяет их готовность к занятию.

Затем студенты последовательно усваивают учебные вопросы, касающиеся порядка аккредитации предприятий, контроля и надзора за деятельностью аккредитованных предприятий, лично отрабатывают

контрольные вопросы практического занятия. При необходимости неясные вопросы обсуждаются в группе под руководством преподавателя.

По окончании занятия студенты оформляют отчет и представляют его на подпись преподавателю.

5. Контрольные вопросы

1. Дайте определение аккредитации предприятия в качестве органа по сертификации средств защиты информации.
2. Дайте определение аккредитации предприятия в качестве испытательной лаборатории.
3. Порядок аккредитации предприятия в качестве органа по сертификации (испытательной лаборатории) средств защиты информации.
4. На какой срок выдается аттестат аккредитации?
5. Виды контроля за деятельностью аккредитованных предприятий.
6. Перечислите случаи, в которых аккредитация может быть досрочно аннулирована.

Литература

1. Снытников А.А. Лицензирование и сертификация в области защиты информации. – М.: Гелиос АРВ, 2013.
2. Приказ ФСТЭК от 3 апреля 2018 г. N 55 «ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ О СИСТЕМЕ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ».
3. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Утверждены приказом ФСТЭК России от 25 декабря 2017 г. №239 (в ред. приказа ФСТЭК России от 9 августа 2018 г. № 138).

Тема 9.

Практическое занятие №9

Цель занятия:

1. Изучить теоретические сведения о защите речевой информации от утечки по акустическому техническому каналу.
2. Изучить работу программно-аппаратного комплекса «СПРУТ-МИНИ-А».
3. Получить практические навыки исследования и анализа ВТСС на наличие в них акустических каналов утечки конфиденциальной речевой информации.

Формируемые компетенции: ПК-3, ПК-6

Время – 4 ч.

1. Программа исследований:

1. Теоретические сведения о защите речевой информации от утечки по акустическому техническому каналу	30 мин
2. Изучение работы программно-аппаратного комплекса «СПРУТ-МИНИ-А»	30 мин
3. Проведение исследований и анализ ВТСС на наличие в них акустических каналов утечки конфиденциальной речевой информации	75 мин
4. Оформление и защита отчета о практической работе у преподавателя	30 мин
Проверка выполнения практической работы	5 мин
Заключительная часть	5 мин

2. Оборудование:

1. Комплекс контроля эффективности речевой информации «СПРУТ-МИНИ-А»
2. ЭВМ с ОС Windows XP / Windows 7 с установленным СМПО «Спрут-мини v 3.2»
3. «СОНАТА-АВ»

3. Основные теоретические сведения

В зависимости от физической природы возникновения информационных сигналов, среды распространения акустических колебаний и способов их перехвата, каналы утечки информации также можно разделить на акустические, виброакустические, оптико-электронные.

В акустическом канале утечки информации средой распространения речевых сигналов является воздух, и для приёма (перехвата) сигнала (перехвата) используются органы слуха человека, либо первичные преобразователи – воздушные микрофоны (в том числе направленные), которые соединяются с усилительными и звукозаписывающими устройствами. Эти же первичные преобразователи применяются в аппаратуре контроля ТКУИ. Общее построение средства разведки и средства контроля едино и включает в свой состав усилители сигналов с выхода первичного преобразователя, различного рода фильтры и средства регистрации (записи) сигналов.

Таблица 1 - Возможности технических средств акустической речевой разведки

Вид разведки	Аппаратура	Дальность	Особенности применения
Акустическая (речевая) разведка	Оптико-электронная (лазерная)	150-250м	При благоприятных метеоусловиях: диффузное отражение в пределах прямой видимости
		1 км	Узконаправленное отражение
	Направленные микрофоны	150-250м	Возимая и носимая - эпизодически при благоприятной обстановке
	Электронные стетоскопы	До 1 м	кирпичная стена
		До 10 м	бетонная стена

Вариант существования ТКУИ без применения технических средств перехвата в нормативной документации носит условное наименование «Непреднамеренное прослушивание». Непреднамеренное прослушивание относится к единственному исключению среди набора наиболее вероятных ТКУИ, так как принято, что оно может осуществляться и внутри контролируемой зоны (КЗ).

В рамках сегодняшних подходов различают два подвида ТКУИ с применением технических средств разведки (для акустической информации):

- прямой перехват, то есть в режиме «реал тайм», с прямым прослушиванием сигнала на выходе средства перехвата;
- отложенную обработку сигнала, подразумевающую его запись с последующей шумоочисткой, математической обработкой и т.д., повышающими вероятность правильного восстановления информации.

4. Работа программно-аппаратного комплекса «СПРУТ-МИНИ-А»

4.1 Назначение и состав программного аппаратного комплекса «СПРУТ-МИНИ-А».

Комплекс контроля эффективности защиты речевой информации «Спрут-мини-А» предназначен для проверки выполнения норм эффективности защиты речевой информации от утечки по акустическому, виброакустическому каналам, а также за счет НЧ наводок на токопроводящих элементах ограждающих конструкций, электроакустических преобразований в линиях ТСПИ и за счет побочных электромагнитных излучений от технических средств в речевом диапазоне. Комплекс обеспечивает измерение акустического давления, виброускорения, а также уровней побочных электромагнитных излучений и наводок (ПЭМИН) от технических средств в речевом диапазоне и производит автоматизированную оценку показателей эффективности защиты речевой информации.

В состав комплекса входят:

1. Многоканальный сигнальный концентратор СПРУТ-МЗ 1 шт.
2. Блок формирования тестовых акустических сигналов СПРУТ-ГЗ 1 шт.
3. Акустическая система 1 шт.
4. Микрофон ЕСМ-8000 с держателем в кейсе 1 шт.
5. Кабель подключения микрофона к концентратору СПРУТ-МЗ (ХГК-XLR) 1 шт.
6. Кабель подключения микрофона к концентратору СПРУТ-МЗ (ХГВ-XLR) защищенный 1 шт.

7. Тренога для микрофона 1 шт.
8. Штанга для микрофона 2 шт.
9. Акселерометр AP98-100 (AP2037-100) с принадлежностями 1 шт.
10. Кабель подключения акселерометра к изделию СПРУТ-МЗ (10-32 - ВМС) 1 шт.
11. Кабель подключения изделий СПРУТ-МЗ и СПРУТ-ГЗ к управляющей
12. ПЭВМ (ОЗВ 2.0 АМ/ВМ) 1 шт.
13. Кабель подключения акустической системы к блоку СПРУТ-ГЗ (ВСА -
14. ВСА) 1 шт.
15. Гальванический контакт подключения несимметричных линий, тип А
16. (ВМС — «Крокодил») 1 шт.
17. Гальванический контакт подключения несимметричных линий, тип В
18. (ВМС — «Клеммный зажим») 1 шт.
19. Т- коннектор для подключения к разъему ВМС 1 шт.
20. Заглушка на разъем ВМС с сопротивлением 600 Ом 1 шт.
21. Компакт диск с программным обеспечением СПРУТ-МИНИ-А, 1 шт.
22. Зарядные устройства изделий СПРУТ-МЗ и СПРУТ-ГЗ 2 шт.
23. Сумка для хранения и переноски аппаратуры (пи. 1-18) 1 шт.

4.2 Принцип работы программно-аппаратного комплекса «СПРУТ-МИНИ-А».

Сигнальный концентратор (СПРУТ-МЗ) принимает электрические сигналы от датчиков, усиливает их, преобразует в цифровую форму и передает в управляющий компьютер. Он имеет три независимых канала, каждый из которых содержит точные усилители, управляемые программно, устройства питания датчиков и активные НЧ фильтры. Концентратор может работать в централизованном и автономном режимах. В централизованном режиме он работает под управлением компьютера, обрабатывающего результаты измерений в реальном времени. В автономном режиме он функционирует без подключения к компьютеру, записывает измеряемые сигналы в запоминающее устройство для их последующей обработки с использованием компьютера. Управление

концентратором в автономном режиме производится с использованием клавиатуры, расположенной на передней панели.

Генератор (СПРУТ-ГЗ) формирует тестовые акустические сигналы различных уровней. Тестовые сигналы могут быть шумовыми, гармоническими или речеподобными. Тестовые сигналы нужны для проверки выполнения норм по защите речевой информации.

5. Исследование и анализ ВТСС на наличие в них акустических каналов утечки конфиденциальной речевой информации.

5.1 Исходное положение оборудования.



Рисунок 1 – Исходное положение комплекса «СПРУТ-МИНИ-А» при исследовании акустического канала утечки информации

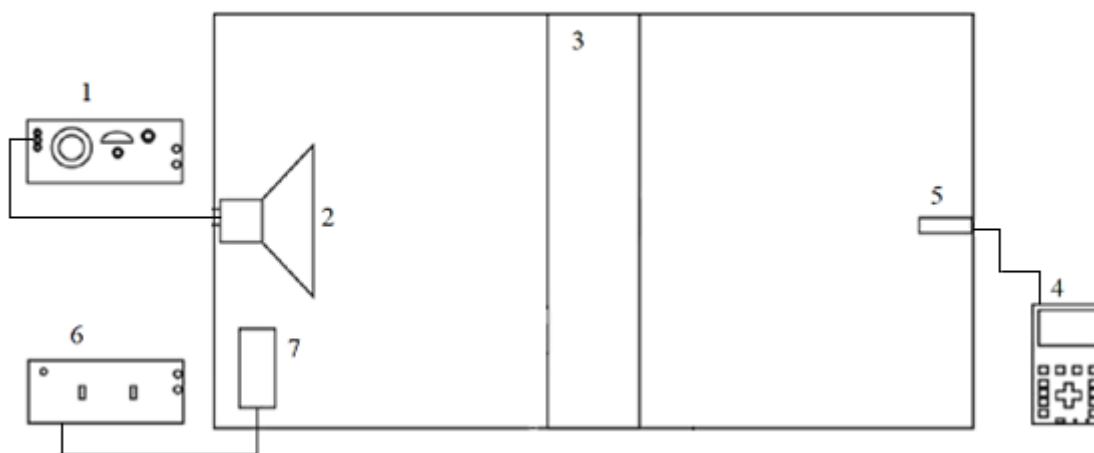


Рисунок 2 – Лабораторный стенд

Состав лабораторного стенда: 1 – генератор (СПРУТ-ГЗ); 2 – акустическая система; 3 – стена; 4 – сигнальный концентратор (СПРУТ-МЗ); 5 - микрофон ЕСМ-8000; 6 – прибор «Соната-АВ»; 7 – акустический излучатель «Соната-АВ».

Акустическая система (2) должна быть подключена к генератору СПРУТ-ГЗ (1) к каналу «АС»; микрофон ЕСМ-8000 (5) подключается к сигнальному концентратору СПРУТ-МЗ (4) к 3-му каналу. Прибор «Соната-АВ» и акустические излучатели «Соната-АВ» находятся в подключенном и готовым к работе состоянии в «Аудитории 505».

5.2 Методика исследований.

1. Собрать комплекс «СПРУТ-МИНИ-А» как показано на рисунках 1,2, для этого:

- 1) Достать из сумки элементы комплекса
- 2) Запустить на ПЭВМ среду виртуализации с Windows XP
- 3) Из папки «СМПО «Спрут-мини» установить на виртуальную машину файл «setup.exe».

4) Включить зарядные устройства изделий СПРУТ-МЗ и СПРУТ-ГЗ в сеть питания и подключить их к МЗ и ГЗ соответственно.

5) С помощью кабеля (USB 2.0 – АМ/ВМ) подключите концентратор СПРУТ-МЗ к управляющей ПЭВМ, на котором заранее запустите СМПО «Спрут-мини».

6) Включите концентратор. На экране должна включиться подсветка и высветиться название изделия.

7) Переведите СПРУТ-МЗ в режим работы по USB. Для этого, нажатием кнопки «Mode», перейдите в меню выбора режима работы:

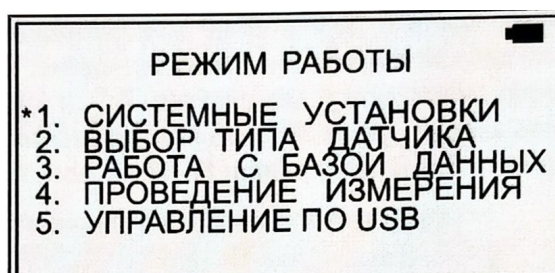


Рисунок 3 – Режимы работы СПРУТ-М3

- 8) С помощью стрелок выберите режим работы «Управление по USB».
- 9) В экране программы в левом нижнем углу должен появиться статус «СИГНАЛ – ЕСТЬ», это свидетельствует об успешном подключении СПРУТ-М3.
- 10) Кнопкой «выбора канала» выберите «Акустический канал» и далее «Разборчивость речи».
- 11) Подключите акустическую систему ко входу «АС» в СПРУТ-Г3.
- 12) Направьте акустическую систему к теоретическому каналу утечки информации, подложив под нее шумоизолирующую подкладку (идет в комплекте с микрофоном)
- 13) Подключите микрофон ЕСМ-8000 к каналу 1 в СПРУТ-М3
- 14) Включите генератор (СПРУТ-Г3). На экране должны высветиться режимы работы генератора.

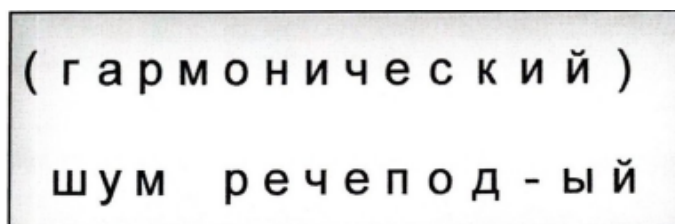


Рисунок 4 – Режимы работы СПРУТ-Г3

- 15) С помощью кнопок «▶», «◀» выбрать режим «речеподобный».



Рисунок 5 – Рабочее окно СПРУТ-Г3

- 16) Для воспроизведения/отключения «речеподобного» сигнала на акустической системе используется кнопка «out».

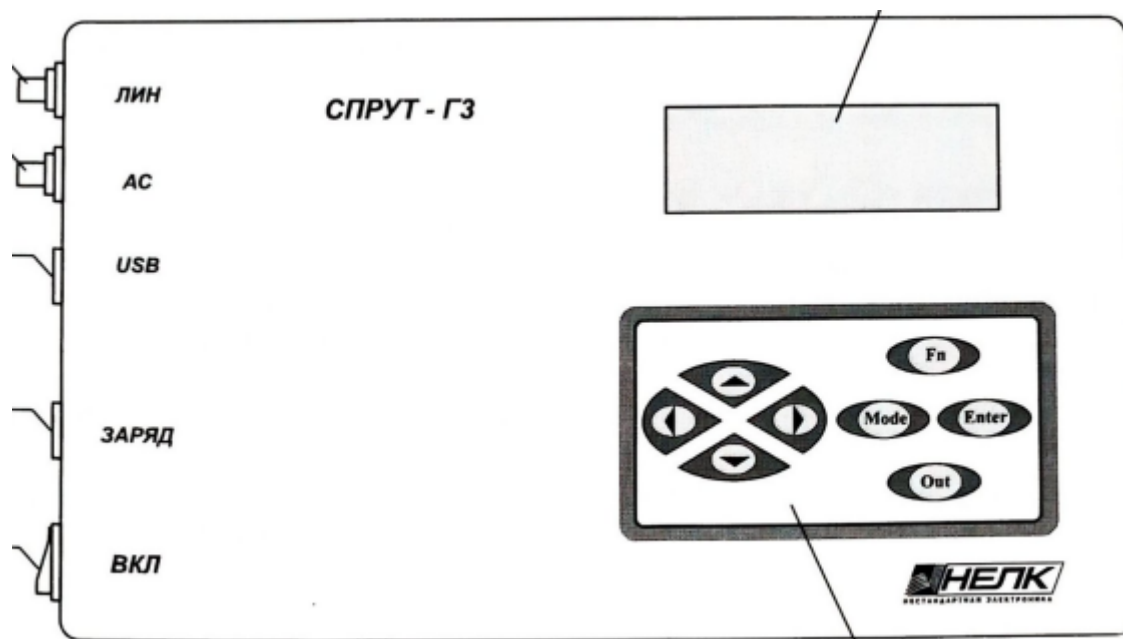


Рисунок 6 – Общий вид, расположение и назначение органов управления и индикации СПРУТ-ГЗ

17) Установите уровень тестового сигнала в пределах от 20 до 30 относительных единиц уровня.

18) Для возврата к выбору режимов работ СПРУТ-ГЗ используется кнопка «mode».

19) Начать исследование разборчивости речи через акустический канал утечки информации, определить контрольные точки для проверяемого помещения, согласно сведениям из комплекта эксплуатационной документации «СПРУТ-МИНИ-А»:

а. Для защищаемого помещения «Аудитория 505» были определены следующие контрольные точки:

I.Внутри помещения.

II.За дверью.

III.За стеной.

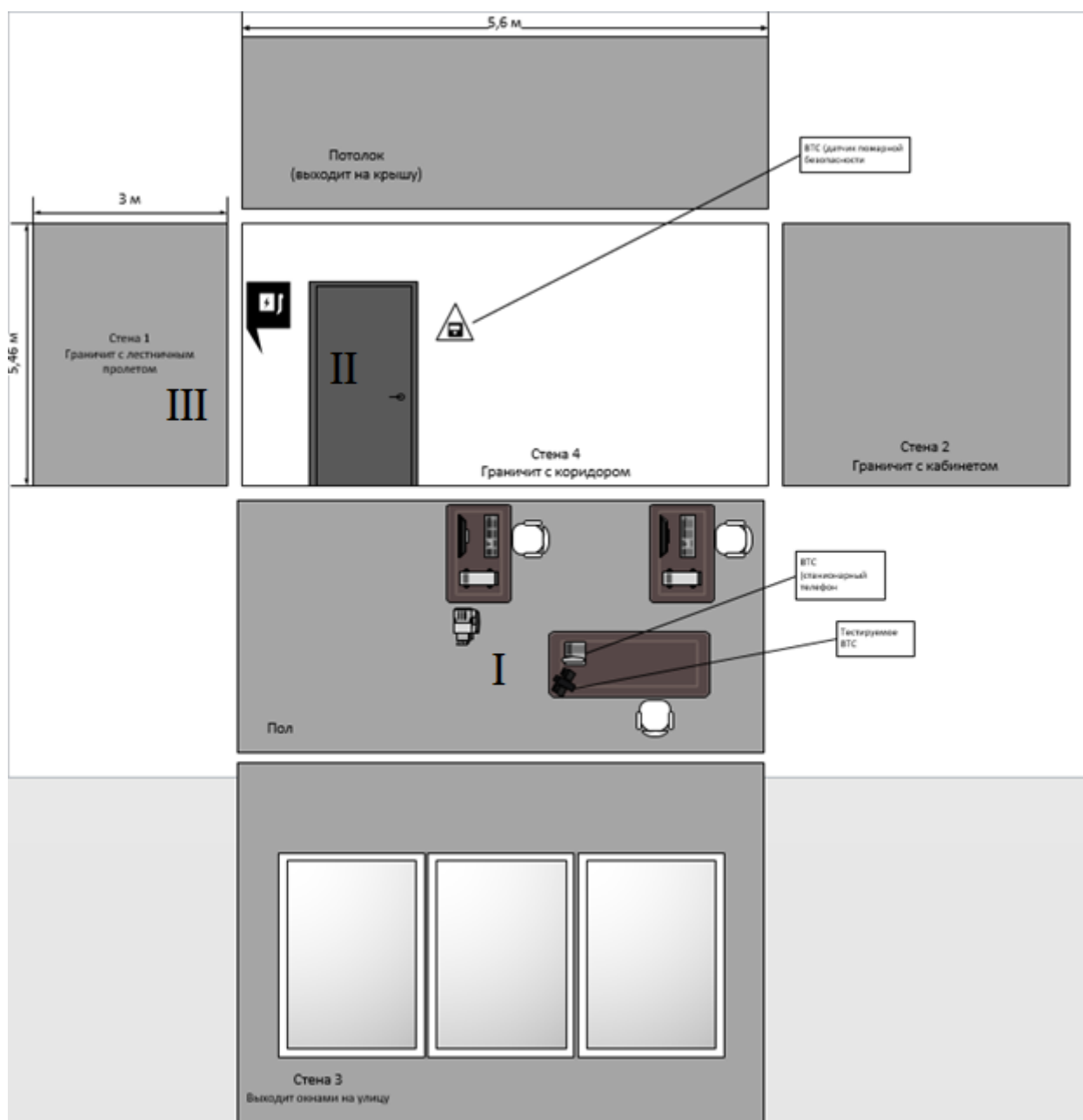


Рисунок 7 – План-схема «Аудитории 505»

б. Измерения будут проводится для следующих режимов:

- I. Без сигнала.
- II. Речеподобный сигнал.
- III. Речеподобный сигнал + Средство защиты «Соната-АВ».

20) Установите микрофон ЕСМ-8000 в контрольной точке (I), выполните тестовое снятие в режиме (I).

21) Нажатием на кнопку «СИГНАЛ» (кнопка старта измерения информативного сигнала) осуществляется измерение и загрузка данных сигнала из сигнального концентратора «СПРУТ-МЗ». При этом на экране спектрограмм

контролируемых сигналов отображается спектр зеленого цвета.

22) Нажатием на кнопку «ШУМ» (кнопка старта измерения фонового сигнала) осуществляется измерение и загрузка данных фона. При этом на экране спектрограмм контролируемых сигналов отображается спектр голубого цвета.

23) Нажатием на кнопку «С+Ш» (кнопка старта измерения суммарного информативного сигнала и фонового шума) осуществляется измерение и загрузка данных суммарного информативного и фонового сигнала из сигнального концентратора «СПРУТ-МЗ». При этом на экране спектрограмм контролируемых сигналов отображается спектр красного цвета.

24) Нажатием на кнопку «САЗ» (кнопка старта измерения суммарного уровня сигнала средства активного зашумления) осуществляется измерение и загрузка данных сигнала средства активного зашумления из сигнального концентратора «СПРУТ-МЗ». При этом на экране спектрограмм контролируемых сигналов отображается спектр желтого цвета.

25) После проведения цикла измерений активизируется кнопка расчета результатов контроля. При нажатии на кнопку расчет главной экранной формы осуществляется переход к экранной форме, представленной на рисунке 8.

Значения уровней сигнала в октавных полосах				Расчетные значения	
тестовый сигнал	помеха (ш/м)	сигнал + помеха	САЗ	отношение сигнал/помеха	R октавный
250 Гц: 80,01 дБ	30,06 дБ	35,45 дБ	48,00 дБ	c/n: -28,042 дБ	0,000001482
500 Гц: 80,92 дБ	30,49 дБ	37,03 дБ	44,00 дБ	c/n: -22,979 дБ	0,000108500
1000 Гц: 80,10 дБ	30,11 дБ	40,00 дБ	43,00 дБ	c/n: -22,570 дБ	0,000811500
2000 Гц: 80,92 дБ	30,24 дБ	42,76 дБ	50,00 дБ	c/n: -32,410 дБ	0,000172800
4000 Гц: 80,01 дБ	30,85 дБ	35,95 дБ	48,00 дБ	c/n: -40,665 дБ	0,000014530

Название контрольной точки: первая

☐ Средства ЗУ
☒ Средства АЗ
☐ учет 7 октав

R интегральный = 0,001106673
W = 0,003398574

Сохранить протокол
Назад

Рисунок 8 - Экранная форма просмотра результатов оценки разборчивости речи для акустического и виброакустического контроля

26) Сохраните протокол о проведенном исследовании.

27) Повторите пункты с 20-26 для контрольных точек (I-III) и режимов (I-

III) (каждой точке соответствуют все режимы, исключение – контрольная точка (I) – для нее исследуется только режим (I).

5.3 Проведение исследований и анализ результатов

Контрольная точка (I):

Режим работы (I) – Без сигнала

Таблица 2 - Результаты определения отношений "сигнал/шум" в октавных полосах в контрольной точке № (I)

F полосы, Гц	Lш, дБ	Lс+ш, дБ	Lс, дБ	Lасз, дБ	Ei
250 Гц	39,30	40,00	31,50	-	19,00
500 Гц	44,40	44,80	34,80	-	11,00
1 кГц	47,50	47,20	37,50	-	3,54
2 кГц	49,40	49,20	39,40	-	-3,14
4 кГц	35,60	36,30	27,80	-	9,14

Таблица 3 - Результаты расчета значения показателя противодействия акустической речевой разведке в контрольной точке № (I)

F полосы, Гц	Ri	R	W
250 Гц	0,015895	0,362856	0,959
500 Гц	0,048589		
1 кГц	0,065653		
2 кГц	0,068514		
4 кГц	0,164204		

Вывод (контрольная точка I): таким образом, $W = 0,959 = 95,9\%$ свидетельствует о том, что класс качества разборчивости речи – высший, то есть присутствует понимание передаваемой речи без малейшего напряжения внимания.

Контрольная точка (II):**Режим работы (I) – Без сигнала**

Таблица 4 - Результаты определения отношений "сигнал/шум" в октавных полосах в контрольной точке № (II)

F полосы, Гц	Lш, дБ	Lс+ш, дБ	Lс, дБ	Lасз, дБ	Ei
250 Гц	48,80	39,00	38,80	-	18,60
500 Гц	49,80	39,90	39,80	-	19,70
1 кГц	39,10	41,50	37,80	-	27,60
2 кГц	32,10	34,10	29,70	-	24,60
4 кГц	29,80	27,00	19,80	-	15,50

Таблица 5 - Результаты расчета значения показателя противодействия акустической речевой разведке в контрольной точке № (II)

F полосы, Гц	Ri	R	W
250 Гц	0,015578	0,773419	0,848
500 Гц	0,081295		
1 кГц	0,187057		
2 кГц	0,280746		
4 кГц	0,208742		

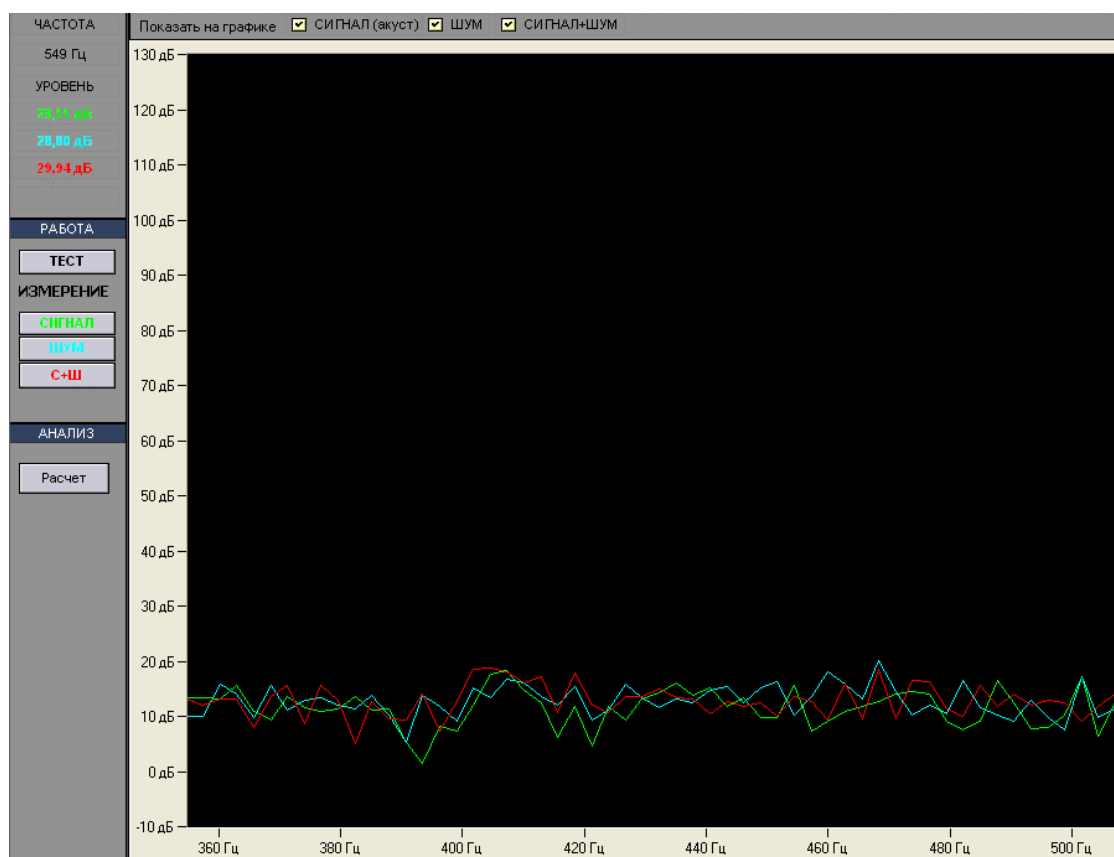


Рисунок 9 – Спектрограмма (контрольная точка – П, режим работы – I)

Режим работы (II) – Речеподобный сигнал.

Таблица 6 - Результаты определения отношений "сигнал/шум" в октавных полосах в контрольной точке № (II)

F полосы, Гц	Lш, дБ	Lс+ш, дБ	Lс, дБ	Lасз, дБ	Ei
250 Гц	36,10	35,70	26,10	-	19,90
500 Гц	30,50	32,60	28,50	-	31,10
1 кГц	26,50	27,50	20,50	-	27,40
2 кГц	24,80	29,00	26,90	-	33,00
4 кГц	23,30	34,70	34,40	-	40,60

Таблица 7 - Результаты расчета значения показателя противодействия акустической речевой разведке в контрольной точке № (II)

F полосы, Гц	Ri	R	W
250 Гц	0,016771	0,869674	0,849
500 Гц	0,110214		
1 кГц	0,186727		
2 кГц	0,296307		
4 кГц	0,259654		

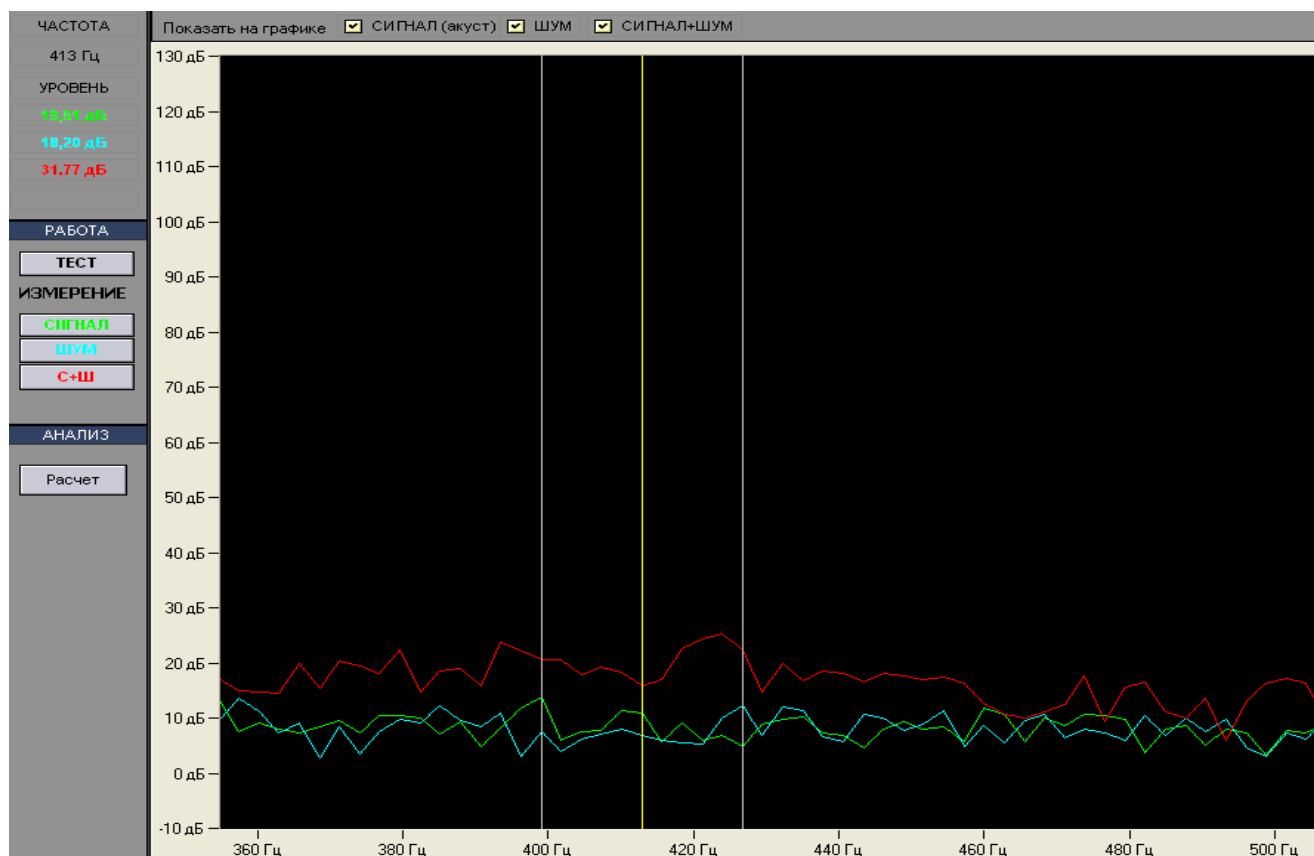


Рисунок 10 – Спектрограмма (контрольная точка – II, режим работы – II)

Режим работы (III) – Речеподобный сигнал + Система защиты

«Соната-АВ».

Таблица 8 - Результаты определения отношений "сигнал/шум" в октавных полосах в контрольной точке № (II)

F полосы, Гц	Lш, дБ	Lс+ш, дБ	Lс, дБ	Lсз, дБ	Ei
250 Гц	35,50	36,00	26,60	0,00	20,90
500 Гц	36,20	35,90	26,20	0,00	19,90
1 кГц	27,70	28,90	22,50	0,00	28,30
2 кГц	26,50	25,90	16,50	0,00	19,00
4 кГц	25,00	24,60	15,00	0,00	17,40

Таблица 9 - Результаты расчета значения показателя противодействия акустической речевой разведке в контрольной точке № (II)

F полосы, Гц	Ri	R	W
250 Гц	0,017784	0,764151	0,816
500 Гц	0,082152		
1 кГц	0,188622		
2 кГц	0,256535		
4 кГц	0,219058		

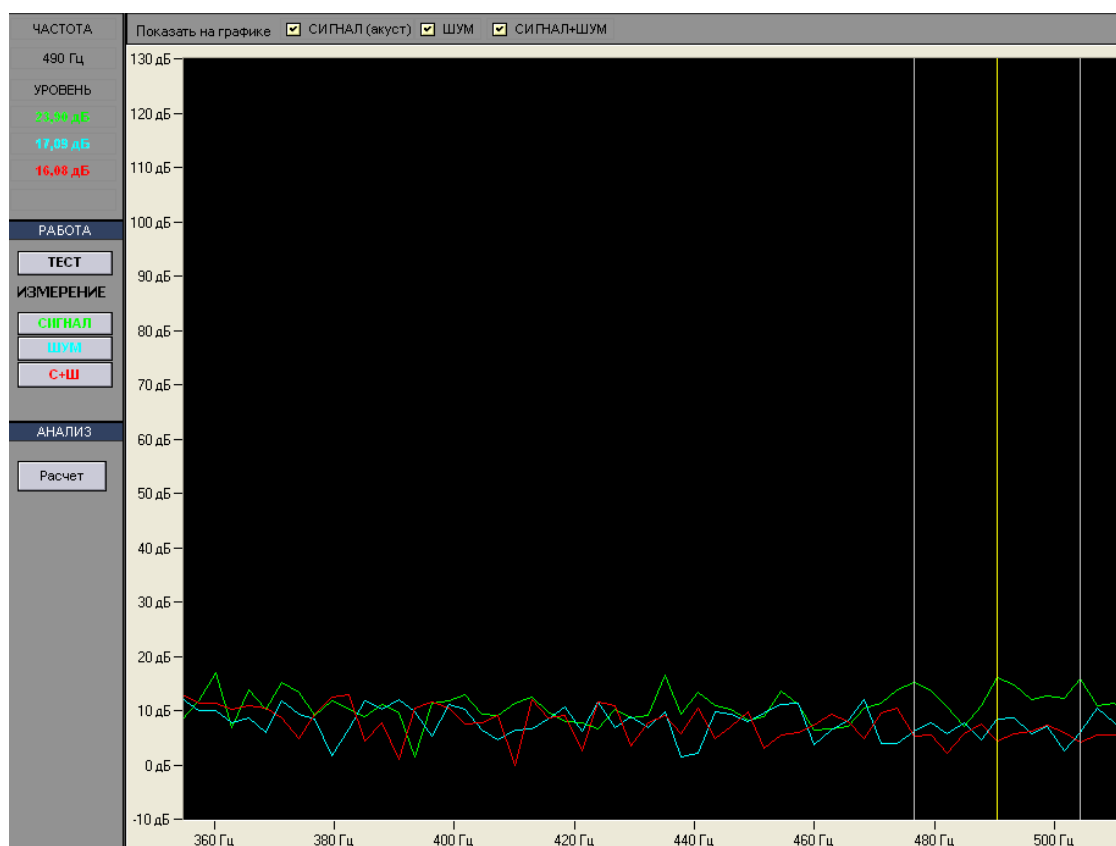


Рисунок 11 – Спектрограмма (контрольная точка – II, режим работы – III)

Вывод (контрольная точка II): в результате анализа разборчивости речи в режимах I-III, было обнаружено, что коэффициенты разборчивости оказались примерно равными. Это может быть связано с тем, что среда, через которую проходит речь, представляет собой сложную структуру, такую как стена, которая может в равной степени влиять на качество речи во всех трех режимах. Использование вибродатчика для измерения через стену может также вносить дополнительные сложности, поскольку вибрации могут быть затуханы или искажены материалами стены. Это может объяснить, почему разборчивость речи остается примерно одинаковой во всех трех режимах, несмотря на различия в настройках. Эти выводы подчеркивают важность учета характеристик среды при оценке и оптимизации систем передачи речи.

Контрольная точка (III):**Режим работы (I) – Без сигнала**

Таблица 10 - Результаты определения отношений "сигнал/шум" в октавных полосах в контрольной точке № (III)

F полосы, Гц	Lш, дБ	Lс+ш, дБ	Lс, дБ	Lасз, дБ	Ei
250 Гц	34,90	41,30	40,20	0,00	38,50
500 Гц	31,60	36,00	34,10	0,00	34,80
1 кГц	27,70	28,50	20,90	0,00	27,90
2 кГц	25,10	29,10	26,90	0,00	33,60
4 кГц	26,10	30,50	28,60	0,00	27,50

Таблица 11 - Результаты расчета значения показателя противодействия акустической речевой разведке в контрольной точке № (III)

F полосы, Гц	Ri	R	W
250 Гц	0,028613	0,879599	0,921
500 Гц	0,114753		
1 кГц	0,187824		
2 кГц	0,296758		
4 кГц	0,251650		

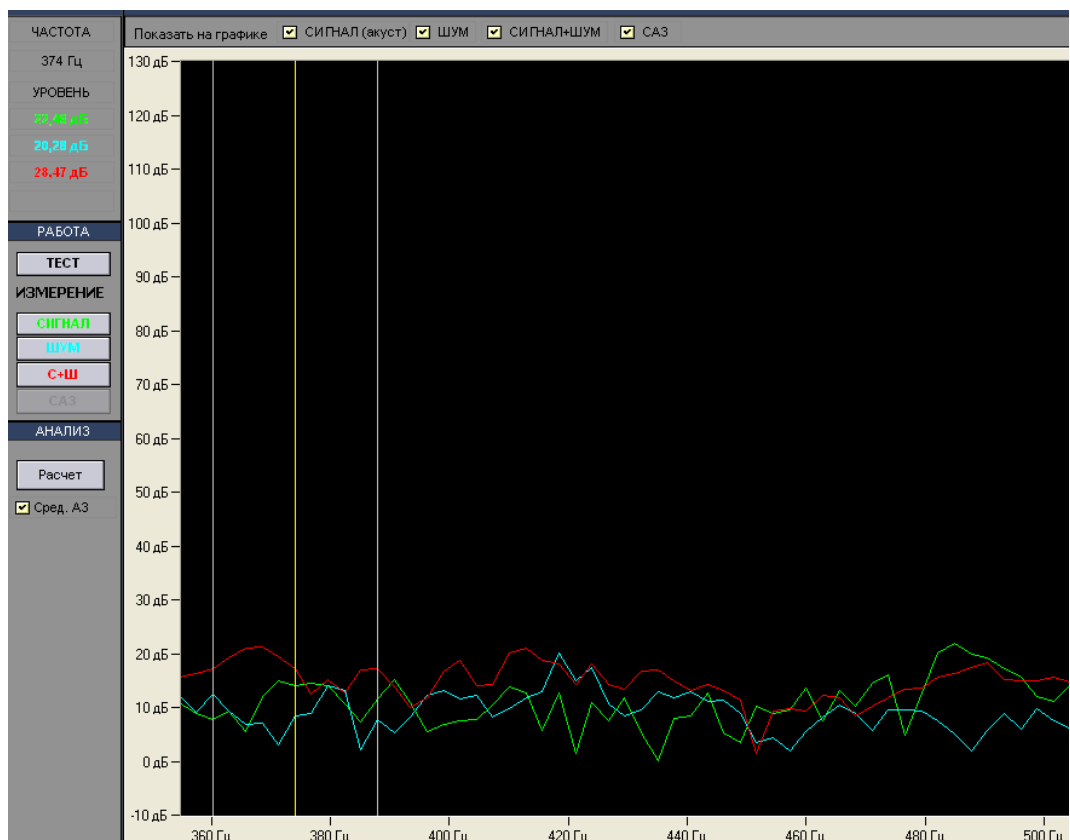


Рисунок 12 – Спектрограмма (контрольная точка – III, режим работы – I)

Режим работы (II) – Речеподобный сигнал

Таблица 12 - Результаты определения отношений "сигнал/шум" в октавных полосах в контрольной точке № (III)

F полосы, Гц	Lш, дБ	Lс+ш, дБ	Lс, дБ	Lасз, дБ	Ei
250 Гц	31,60	38,10	37,00	-	36,60
500 Гц	27,90	30,60	27,20	-	36,20
1 кГц	25,10	26,10	19,00	-	29,50
2 кГц	24,10	25,80	20,80	-	28,70
4 кГц	22,30	24,60	20,60	-	29,20

Таблица 13 - Результаты расчета значения показателя противодействия акустической речевой разведке в контрольной точке № (III)

F полосы, Гц	Ri	R	W
250 Гц	0,028073	0,879649	0,911
500 Гц	0,115919		
1 кГц	0,190767		
2 кГц	0,290785		
4 кГц	0,254107		

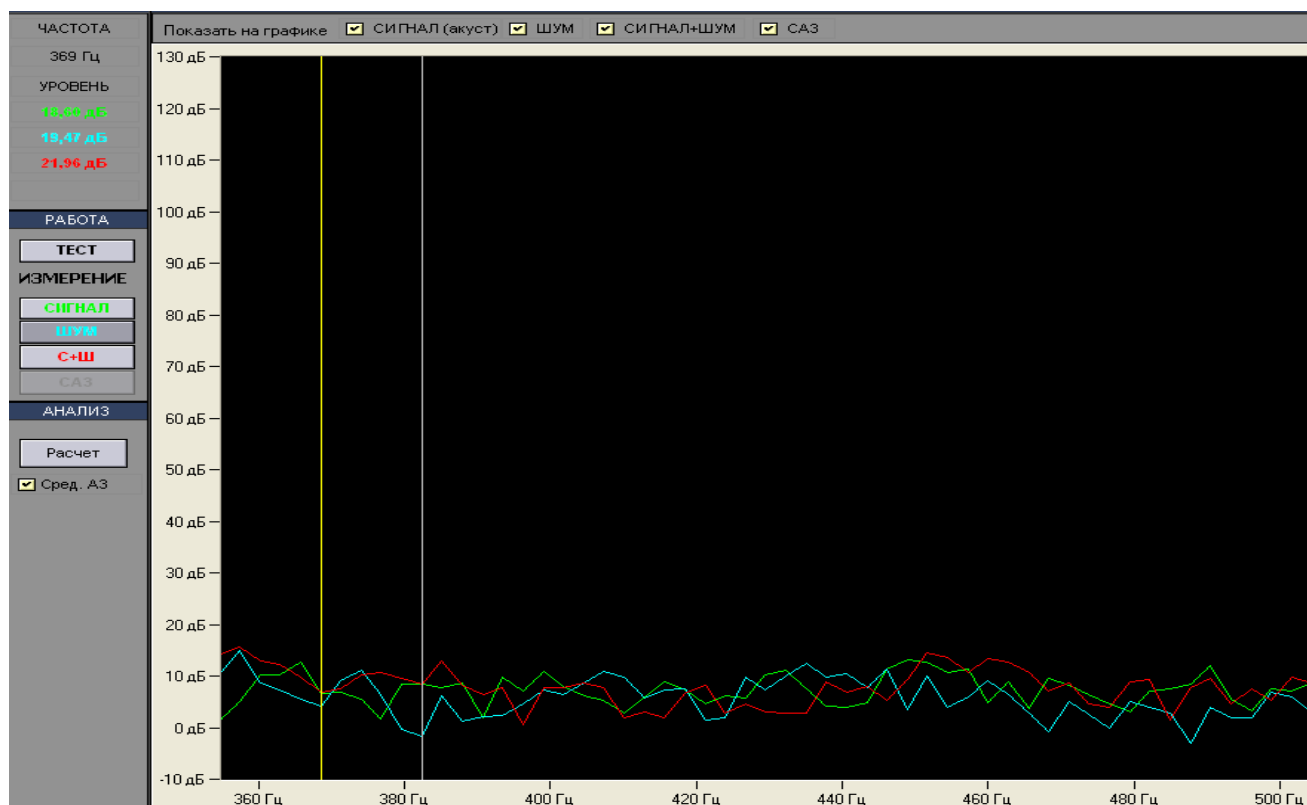


Рисунок 13 – Спектрограмма (контрольная точка – III, режим работы – II)

Режим работы (III) – Речеподобный сигнал + Система защиты

«Соната-АВ».

Таблица 14 - Результаты определения отношений "сигнал/шум" в октавных полосах в контрольной точке № (III)

F полосы, Гц	Lш, дБ	Lс+ш, дБ	Lс, дБ	Lасз, дБ	Ei
250 Гц	44,00	53,30	52,80	0,00	23,90
500 Гц	58,80	58,80	48,80	0,00	-5,30
1 кГц	51,40	52,10	44,10	0,00	1,12
2 кГц	46,90	47,70	40,00	0,00	0,71
4 кГц	47,30	47,40	29,00	0,00	-14,40

Таблица 15 - Результаты расчета значения показателя противодействия акустической речевой разведке в контрольной точке № (III)

F полосы, Гц	Ri	R	W
250 Гц	0,020508	0,194105	0,832
500 Гц	0,006863		
1 кГц	0,052065		
2 кГц	0,099981		
4 кГц	0,014688		

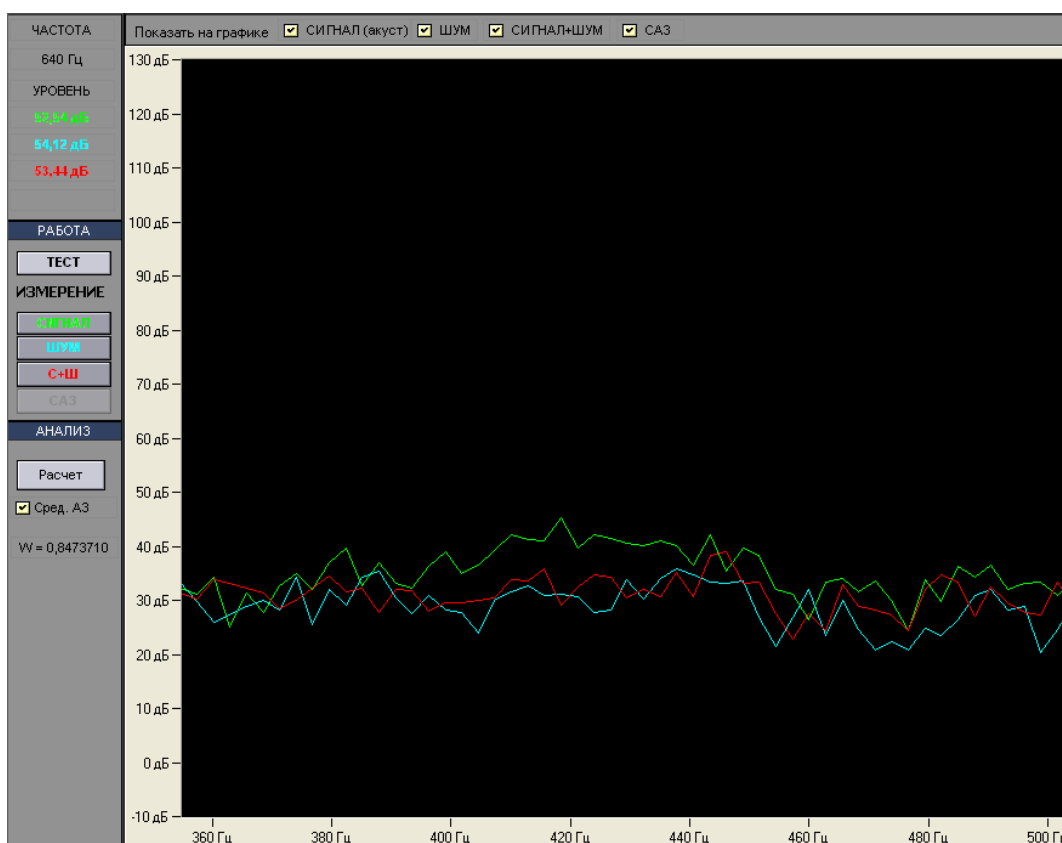


Рисунок 14 – Спектрограмма (контрольная точка – III, режим работы – III)

Вывод (контрольная точка III): при сравнении разборчивости речи в режимах I-III, было обнаружено, что включение генератора СПРУТ-ГЗ приводит к улучшению разборчивости речи. Это может быть связано с тем, что генератор помогает усилить и уточнить звуковые сигналы, делая речь более ясной и понятной. Однако, когда была включена система защиты «Соната-AB», разборчивость речи резко снижается. Это может быть связано с тем, что данное устройство, хотя и уменьшает фоновый шум, может также случайно подавлять некоторые важные аспекты речевого сигнала, что ведет к снижению качества речи. Несмотря на эти различия, разборчивость речи режимах I, II соответствуют классу качества – I, что означает, что передаваемую речь можно понять без затруднений. Разборчивость речи режима работы III соответствует классу качества разборчивости речи – II – понимание передаваемой речи с напряжением внимания без переспросов и повторений – происходит из-за включения системы защиты «Соната-AB», то есть повышению уровня шума. Это говорит о том, что,

несмотря на вариации в разборчивости речи при различных настройках, распознавание речи остается достаточно высоким, что свидетельствует о легкости съема злоумышленником информации по акустическому каналу утечки информации.

ОБЩИЙ ВЫВОД:

В процессе выполнения работы успешно достигнуты следующие цели:

1. Изучение теории и практики акустических измерений.
2. Освоение работы с программно-аппаратным комплексом «СПРУТ-МИНИ-А».
3. Приобретение практических навыков оценки результатов акустических измерений с использованием комплекса «СПРУТ-МИНИ-А».

В ходе исследования разборчивости речи через акустический канал утечки информации было выявлено, что разборчивость речи в режимах I-III примерно одинакова. Это свидетельствует о эффективности системы в обеспечении ясности речи, независимо от выбранного режима. Включение генератора способствует улучшению разборчивости речи, в то время как включение шумогенератора (система защиты «Соната-АВ») может создавать дополнительный фоновый шум, который может влиять на разборчивость речи. Это объясняет, почему разборчивость речи остается примерно одинаковой во всех трех режимах, несмотря на различия в настройках.

На основе полученных результатов можно предложить следующие рекомендации для дальнейшей работы:

1. Провести дополнительную оптимизацию настроек генератора и шумогенератора для максимизации качества речи.
2. Учитывать характеристики среды при проектировании и настройке системы.
3. Провести дополнительные исследования и тестирование в различных условиях.
4. Обеспечить регулярный мониторинг и обслуживание системы.
5. Обучить пользователей правильному использованию и настройке системы, включая работу с шумогенератором.

Литература

1 Воробьев Л.В., Давыдов А.В., Щербина Л.П. Системы и сети передачи информации: учебное пособие для студентов высших учебных заведений. – М.: Издательский центр «Академия», 2009.

2 Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии протоколы: учебник для вузов. - СПб.: Питер, 2010.

3 Системы и сети передачи информации. М.В. Гаранин и др. Учебное пособие. – М.: "Радио и связь", 2001 г.

Контрольные вопросы

1. Какие основные типы технических каналов утечки информации вы знаете?

2. Что такое акустический канал утечки информации и каковы его основные характеристики?

3. Какие методы защиты от утечки информации через акустические каналы вы можете назвать?

4. Что такое “непреднамеренное прослушивание” и в каких условиях оно может происходить?

5. Что такое прямой перехват и отложенная обработка сигнала в контексте акустической информации?

6. Какие последствия могут быть от утечки информации через акустические каналы?

7. Каковы основные принципы работы программно-аппаратного комплекса «СПРУТ-МИНИ-А» в области акустических измерений?

8. Какие функции выполняет комплекс контроля эффективности защиты речевой информации «Спрут-мини-А»?

9. Что такое прибор СПРУТ-МИНИ-А и для чего он используется?

Отчет о выполнении практического занятия

Отчет оформляется согласно образцу:

Отчет по практическому занятию № _

Тема: Запишите тему занятия

Цель: Запишите цели занятия

Оборудование: Запишите используемое оборудование и программное обеспечение

Ход занятия:

Описание теоретической и практической части занятия, схемы, графики, таблицы согласно содержанию занятия по разделам:

1. Теоретическая часть

Указываются основные теоретические сведения об изучаемом явлении, приборе, законе или устройстве

2. Практическая часть

Описывается ход практической части занятия. Изображаются необходимые схемы, чертежи, графики, записываются результаты измерений и исследований.

Вывод: Основные выводы по практической части занятия, обоснование полученных результатов измерений, достигнуты ли цели занятия, совпадают ли полученные в эксперименте значения с теоретическими данными.

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для обучающихся по организации и проведению самостоятельной работы
по дисциплине «Защита объектов критической информационной инфраструктуры»
для студентов направления подготовки

10.03.01 «Информационная безопасность»

Направленность (профиль):

«Организация и технологии защиты информации (по отрасли или в сфере профессиональной
деятельности)»

Ставрополь,
2026

СОДЕРЖАНИЕ

Введение

Общая характеристика самостоятельной работы студента

Технологическая карта самостоятельной работы студента

Порядок выполнения самостоятельной работы

Список рекомендуемой литературы

ВВЕДЕНИЕ

Учебная дисциплина «Защита объектов критической информационной инфраструктуры» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Основной *целью* дисциплины «Защита объектов критической информационной инфраструктуры» является обеспечение студентов теоретическими знаниями и практическими навыками, необходимыми для проведения работ по аттестации объектов информатизации по требованиям безопасности информации, а также работ по оценке защищенности информации от утечки по техническим каналам и от несанкционированного доступа.

Задачами изучения дисциплины является формирование у студентов знаний в области:

- информационного законодательства РФ и международного законодательства в области защиты информации;
- организации государственного лицензирования в области защиты информации;
- организации системы сертификации и аттестации объектов информатизации.

1. Общая характеристика самостоятельной работы студента

Самостоятельная работа включает те разделы курса, которые не получили достаточного освещения на лекциях по причине ограниченности лекционного времени и большого объема изучаемого материала.

Методическое обеспечение самостоятельной работы по дисциплине состоит из:

- 1) Определения учебных вопросов, которые студенты должны изучить самостоятельно;
- 2) Подбора необходимой учебной литературы, обязательной для проработки и изучения;
- 3) Поиска дополнительной научной литературы, к которой студенты могут обращаться по желанию, если у них возникает интерес в данной теме;
- 4) Определения контрольных вопросов, позволяющих студентам самостоятельно проверить качество полученных знаний;
- 5) Организации консультаций преподавателя со студентами для разъяснения вопросов, вызвавших у обучающихся затруднения при самостоятельном освоении учебного материала.

Самостоятельная работа студента – это особым образом организованная деятельность, включающая в свою структуру такие компоненты, как:

- уяснение цели и поставленной учебной задачи;
- четкое и системное планирование самостоятельной работы;
- поиск необходимой учебной и научной информации;
- освоение собственной информации и ее логическая переработка;
- использование методов исследовательской, научно-исследовательской работы для решения поставленных задач;
- выработка собственной позиции по поводу полученной задачи;
- представление, обоснование и защита полученного решения;
- проведение самоанализа и самоконтроля

К основным видам самостоятельной работы студентов относится:

- работа с понятийным аппаратом;
- конспектирование первоисточников;
- проектирование фрагментов исследовательской деятельности;

- анализ научных исследований по психологической проблематике;
- подготовка научного проекта по теме.

Контроль знаний студентов включает формы текущего и итогового контроля. Текущий контроль осуществляется в процессе изучения курса и включает в себя оценку работы студентов на практических занятиях (круглый стол, собеседование, групповые научные проекты, тестирование), а также подготовку домашнего задания.

2. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций, индикатора(ов)	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
5 семестр					
ИД-3 ПК-3 ИД-2 ПК-6	Подготовка к практическому занятию	Собеседование	12.00	2.00	14.00
ИД-3 ПК-3 ИД-2 ПК-6	Подготовка к лекции	Конспект	12.00	2.00	14.00
ИД-3 ПК-3 ИД-2 ПК-6	Подготовка доклада	Доклад	10.00	2.00	12.00
ИД-3 ПК-3 ИД-2 ПК-6	Самостоятельное изучение литературы	Конспект	5.00	2.00	7.00
ИД-3 ПК-3 ИД-2 ПК-6	Самостоятельное выполнение заданий по заданным темам.	Конспект. Письменный отчет	5.00	2.00	7.00
Итого за 5 семестр			44.00	10.00	54.00
Итого			44.00	10.00	54.00

3. Порядок выполнения самостоятельной работы

3.1 Методические рекомендации по изучению теоретического материала

Комплексное изучение предлагаемой студентам учебной дисциплины «Защита объектов критической информационной инфраструктуры» предполагает овладение материалами лекций, учебников, программы, творческую работу студентов в ходе проведения практических занятий, а также систематическое выполнение заданий для самостоятельной работы.

В ходе лекций раскрываются основные вопросы в рамках рассматриваемых тем, делаются акценты на наиболее сложные и интересные положения изучаемого материала,

которые должны быть приняты студентами во внимание. Материалы лекций являются основой для подготовки студентов к практическим занятиям.

Работа с конспектом лекций

Просмотрите конспект сразу после занятий. Отметьте материал конспекта лекций, который вызывает затруднения для понимания. Попробуйте найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю.

Каждую неделю отводите время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам и тестам.

Выполнение практических занятий по дисциплине «Защита объектов критической информационной инфраструктуры»

На первом занятии получите у преподавателя задания по курсу, планы подготовки к практическим занятиям. Обзаведитесь всем необходимым методическим обеспечением.

Перед практическими занятиями изучите теорию вопроса, предполагаемого к исследованию, ознакомьтесь с опытом других исследователей в этом направлении.

Целью практических работ является:

- закрепление методов приложения теории к решению практических задач анализа и синтеза психологического знания;
- проверка уровня понимания студентами вопросов, рассмотренных на лекциях и по учебной литературе, степени и качества усвоения материала;
- обучение навыкам освоения методики эксперимента и работы с нормативно-справочной литературой;
- восполнение пробелов в пройденной теоретической части курса и оказание помощи в его усвоении.

3.2 Методические рекомендации по конспектированию первоисточников

Изучение и анализ литературных источников является обязательным видом самостоятельной работы студентов. Изучение литературы по избранной теме имеет своей задачей проследить характер постановки и решения определенной проблемы различными авторами, аргументацию их выводов и обобщений, провести анализ и систематизировать полученный материал на основе собственного осмысления с целью выяснения современного состояния вопроса.

Проработка отобранного материала обязательно должна идти с одновременным ведением записей прочитанного и своих замечаний. Запись может иметь как форму конспекта, так и выписок, а также картотеку положений, тезисов, идей, методик, что в дальнейшем облегчит классификацию и систематизацию полученного материала. Такого рода записи являются лучшим способом накопления и первичной обработки материал, одной из обязательных форм организации умственного труда.

Планом удобно пользоваться при подготовке к устному выступлению по выбранной теме. Каждый пункт плана должен раскрывать одну из сторон избранной темы, а весь план должен охватывать ее целиком.

Тезисы предполагают сжатое изложение основных положений текста в форме утверждения или отрицания. Они являются более совершенной формой записей и представляют основу для дискуссии. К тому же их легко запомнить.

Конспектирование – процесс мысленной переработки и письменной фиксации информации, в виде краткого изложения основного содержания, смысла какого-либо текста.

Результат конспектирования – запись, позволяющая конспектирующему немедленно или через некоторый срок с нужной полнотой восстановить полученную информацию. Конспект в переводе с латыни означает «обзор». По существу его и составлять надо как обзор, содержащий основные мысли текста без подробностей и второстепенных деталей. Конспект носит индивидуализированный характер: он рассчитан на самого автора и поэтому может оказаться малопонятным для других.

Для того чтобы осуществлять этот вид работы, в каждом конкретном случае необходимо грамотно решить следующие задачи:

1. Сориентироваться в общей композиции текста (уметь определить вступление, основную часть, заключение).
2. Увидеть логико-смысловую канву сообщения, понять систему изложения автором информации в целом, а также ход развития каждой отдельной мысли.
3. Выявить «ключевые» мысли, т. е. основные смысловые вехи, на которые «нанизано» все содержание текста.
4. Определить детализирующую информацию.
5. Лаконично сформулировать основную информацию, не перенося на письмо все целиком и дословно.

Во всяком научном тексте содержится информация 2-х видов: основная и вспомогательная. Основной является информация, имеющая наиболее существенное значение для раскрытия содержания темы или вопроса. К ней относятся: определения научных понятий, формулировки законов, теоретических принципов и т. д. Назначение вспомогательной информации – помочь читателю лучше усвоить предлагаемый материал. К этому типу информации относятся разного рода комментарии. Основную – записываем как можно полнее, вспомогательную, как правило, опускаем. Содержание конспектирования составляет переработка основной информации в целях ее обобщения и сокращения. Обобщить – значит представить ее в более общей, схематической форме, в виде тезисов, выводов, отдельных заголовков, изложения основных результатов и т. п. Читая, мы интуитивно используем некоторые слова и фразы в качестве опорных. Такие опорные слова и фразы называются ключевыми. Ключевые слова и фразы несут основную смысловую и эмоциональную нагрузку содержания текста.

Выбор ключевых слов – это первый этап смыслового свертывания, смыслового сжатия материала.

Важными требованиями к конспекту являются наглядность и обозримость записей и такое их расположение, которое давало бы возможность уяснить логические связи и иерархию понятий.

По форме конспекты подразделяются на формализованные и графические.

1. Формализованные (все записи вносятся в заранее подготовленные таблицы).

Это удобно, во-первых, при конспектировании материалов, когда перечень характеристик описываемых предметов или явлений более или менее постоянен, во-вторых, при подготовке единого конспекта по нескольким источникам. Особенно если есть необходимость сравнения отдельных данных. Разновидностью формализованного конспекта является запись, составленная в форме ответов на заранее подготовленные вопросы, обеспечивающие исчерпывающие характеристики однотипных предметов или явлений.

2. Графические (элементы конспектируемой работы располагаются в таком виде, при котором видна иерархия понятий и взаимосвязь между ними).

По каждой работе может быть не один, а несколько графических конспектов, отображающих книгу в целом и отдельные ее части. Ведение графического конспекта - наиболее совершенный способ изображения внутренней структуры книги, а сам этот процесс помогает усвоению ее содержания.

Можно выделить следующие основные **типы конспектов: плановый, текстуальный, сводный, тематический.**

Плановый – легко получить с помощью предварительно сделанного плана произведения, каждому вопросу плана отвечает определенная часть конспекта:

а) вопросно-ответный (на пункты плана, выраженные в вопросительной форме, конспект дает точные ответы);

б) схематичный плановый конспект (отражает логическую структуру и взаимосвязь отдельных положений).

Текстуальный – это конспект, созданный в основном из цитат.

Сводный конспект – сочетает выписки, цитаты, иногда тезисы; часть его текста может быть снабжена планом.

Тематический – дает более или менее исчерпывающий ответ (в зависимости из числа привлеченных источников и другого материала, например, своих же записей) на поставленный вопрос – тему: обзорный; хронологический.

Роль конспекта – чисто учебная: он помогает зафиксировать основные понятия и положения первичного текста и в нужный момент их воспроизвести, например, при написании реферата или подготовке к экзамену.

Способы конспектирования.

- **Тезисы** – это кратко сформулированные основные мысли, положения изучаемого материала. Тезисы лаконично выражают суть читаемого, дают возможность раскрыть содержание. Приступая к освоению записи в виде тезисов, полезно в самом тексте отмечать места, наиболее четко формулирующие основную мысль, которую автор доказывает (если, конечно, это не библиотечная книга). Часто такой отбор облегчается шрифтовым выделением, сделанным в самом тексте.

- **Линейно-последовательная запись текста.** При конспектировании линейно – последовательным способом целесообразно использование плакатно-оформительских средств, которые включают в себя следующие:

- сдвиг текста конспекта по горизонтали, по вертикали;
- выделение жирным (или другим) шрифтом особо значимых слов;
- использование различных цветов;
- подчеркивание;
- заключение в рамку главной информации.

- **Способ «вопросов – ответов».** Он заключается в том, что, поделив страницу тетради пополам вертикальной чертой, конспектирующий в левой части страницы самостоятельно формулирует вопросы или проблемы, затронутые в данном тексте, а в правой части дает ответы на них.

Одна из модификаций способа «вопросов – ответов» - таблица, где место вопроса занимает формулировка проблемы, поднятой автором (лектором), а место ответа – решение данной проблемы. Иногда в таблице могут появиться и дополнительные графы: например, «мое мнение» и т. п.

- **Схема с фрагментами** – способ конспектирования, позволяющий ярче выявить структуру текста, - при этом фрагменты текста (опорные слова, словосочетания, пояснения всякого рода) в сочетании с графикой помогают созданию рационально - лаконичного конспекта.

- **Простая схема** – способ конспектирования, близкий к схеме с фрагментами, объяснений к которой конспектирующий не пишет, но должен уметь давать их устно. Этот

способ требует высокой квалификации конспектирующего. В противном случае такой конспект нельзя будет использовать.

- **Параллельный способ** конспектирования. Конспект оформляется на двух листах параллельно или один лист делится вертикальной чертой пополам и записи делаются в правой и в левой части листа.

Однако лучше использовать разные способы конспектирования для записи одного и того же материала.

Комбинированный конспект – вершина овладения рациональным конспектированием. При этом умело используются все перечисленные способы, сочетая их в одном конспекте (один из видов конспекта свободно перетекает в другой в зависимости от конспектируемого текста, от желания и умения конспектирующего). Именно при комбинированном конспекте более всего проявляется уровень подготовки и индивидуальность студента.

Принципы составления конспекта прочитанного.

1. Записать все выходные данные источника: автор, название, год и место издания. Если текст взят из периодического издания (газеты или журнала), то записать его название, год, месяц, номер, число, место издания.

2. Выделить поля слева или справа, можно с обеих сторон. Слева на полях отмечаются страницы оригинала, структурные разделы статьи или книги (названия параграфов, подзаголовки и т. п.), формулируются основные проблемы. Справа – способы фиксации прочитанной информации.

Один из видов чтения – углубленное – предполагает глубокое усвоение прочитанного и часто сохранение информации в целях последующего обращения к ней. Эффективность такого чтения повышается, если прочитанное зафиксировано не только в памяти, но и на бумаге. Психологи утверждают, что записанное лучше и полнее усваивается, прочнее откладывается в памяти. Установлено, что если прочитать 1000 слов и затем записать 50, подытоживающих прочитанное, то коэффициент усвоения будет выше, чем, если прочитать 10000 слов, не записав ни одного. Кроме того, при записи прочитанного формируется навык свертывания информации. И, наконец, чередование чтения и записывания уменьшает усталость, повышает работоспособность и производительность умственного труда.

1. Резюмирование.

Резюме – краткий итог прочитанного, содержащий его оценку. Резюме характеризует основные выводы книги, главные итоги.

Выбор языковых средств для построения резюме-выводов подчинен основной задаче свертывания информации: минимум языковых средств – максимум информации. Это обычно одно – три четких, кратких, выразительных предложения, раскрывающих, по мнению автора, самую суть описываемого объекта.

2. Аннотация.

Аннотация – краткая обобщенная характеристика печатной работы (книги, статьи), включающая иногда и его оценку. Это наикратчайшее изложение содержания первичного документа, дающее общее представление о теме.

Основное ее назначение – дать некоторое представление о книге (статье, научной работе) с тем, чтобы рекомендовать ее определенному кругу читателей или воспользоваться своими записями при выполнении работы исследовательского, реферативного характера. Поэтому аннотации не требуются изложения содержания произведения, в ней лишь перечисляются вопросы, которые освещены в первоисточнике (содержание этих вопросов не раскрывается). Аннотация отвечает на вопрос: «О чем говорится в первичном тексте?», дает представление только о главной теме и перечне вопросов, затрагиваемых в тексте первоисточника.

Текст аннотации не стандартизирован. В научной литературе можно встретить различные требования к составлению аннотаций. Например, текст справочной аннотации может включать следующие сведения:

- тип и название аннотируемого документа (монография, диссертация, сборник, статья и т. п.)
- задачи, поставленные автором аннотируемого документа
- метод, которым пользовался автор (эксперимент, сравнительный анализ, компиляция других источников)
- принадлежность автора к определенной научной школе или направлению
- структуру аннотируемого документа
- предмет и тему произведения, основные положения и выводы автора
- характеристику вспомогательных иллюстративных материалов, дополнений, приложений, справочного аппарата, включая указатели и библиографию.

Практические задания, выполняемые на практических занятиях

Тема №1. Организационные основы аттестации объектов информатизации по требованиям безопасности информации

Типовые задачи:

Задания базового уровня:

1. Общая характеристика методов проведения испытаний.
2. Перечислить организационно-технические требования по защите информации.
3. Перечислить требования, выдвигаемые объекту, по защите информации от утечки по каналам ПЭМИН

Задания повышенного уровня:

1. Проверить объект (объект выбирается самостоятельно) на соответствие организационно-техническим требованиям по защите информации, требованиям по защите информации от утечки по каналам ПЭМИН, требованиям по защите информации от НСД, требованиям по защите информации от утечки по акустическим каналам.

Тема 2. Государственная система защиты информации

Типовые задачи:

Задания базового уровня:

1. Перечислить требования, выдвигаемые объекту, по защите информации от НСД.

2. Перечислить требования, выдвигаемые объекту, по защите информации от утечки по акустическим каналам.

Задания повышенного уровня:

3. Покажите на примере права и обязанности лицензиатов.

4. Покажите на примере порядок проведения лицензирования и контроля за деятельностью лицензиатов.

Тема 3. Содержание и порядок проведения аттестации объекта информатизации по требованиям безопасности информации Типовые задачи:

Задания базового уровня:

1. Каковы функции ФСТЭК в области сертификации средств защиты информации?

2. Каковы функции органов сертификации средств защиты информации?

3. Каковы функции испытательных лабораторий (центров).

4. Каковы функции заявителей?

Задания повышенного уровня:

5. Покажите на примере виды и схемы сертификации средств защиты информации.

6. Покажите на примере порядок проведения сертификации средств защиты информации.

Тема 4. Мероприятия при аттестации объектов информатизации на соответствие требованиям безопасности информации.

Типовые задачи:

Задания базового уровня:

1. Какая документация представляется органу по аттестации?

2. Содержание заключения аттестационной проверки помещения.

3. Содержание протокола аттестационных испытаний помещения.

4. Содержание аттестата соответствия на объект информатизации.

5. Какие помещения подлежат обязательной аттестации?

Задания повышенного уровня:

1. Покажите на примере цель и содержание специальных обследований и проверок.

2. Покажите на примере порядок проведения измерения и оценки уровней защищенности.

Тема 5. Классификация автоматизированных систем по уровню их защищенности.

Типовые задачи:

Задания базового уровня:

1. Особенности классификации автоматизированных систем по уровню их защищенности.

2. Классификации автоматизированных систем персональных данных по уровню их защищенности.

3. Классификации автоматизированных систем критической информационной инфраструктуры по уровню их защищенности.

Задания повышенного уровня:

4. Покажите на примере порядок присвоения класса автоматизированной системе персональных данных по уровню их защищенности.

5. Покажите на примере порядок присвоения класса автоматизированной системе критической информационной инфраструктуры по уровню их защищенности.

Тема 6. Разработка, структура, оформление и утверждение программ и методик аттестационных испытаний объектов информатизации

Типовые задачи:

Задания базового уровня:

1. Содержание программ аттестационных испытаний объектов информатизации.
2. Содержание методик аттестационных испытаний объектов информатизации.
3. Содержание заключения аттестационной проверки объекта информатизации.
4. Содержание протокола аттестационных испытаний объекта информатизации.

Задания повышенного уровня:

5. Покажите на примере содержание программы аттестационных испытаний объекта информатизации.
6. Покажите на примере содержание методики аттестационных испытаний объекта информатизации.

Тема 7. Формирование требований по защите информации на объектах информатизации

Типовые задачи:

Задания базового уровня:

1. Виды аттестации помещений по требованиям безопасности информации.
2. Какие помещения подлежат обязательной аттестации?
3. Порядок проведения аттестации помещений по требованиям безопасности информации.

Задания повышенного уровня:

4. Покажите на примере содержание заключения аттестационной проверки помещения.
5. Покажите на примере содержание протокола аттестационных испытаний помещения.

Тема 8. Методы проверок и испытаний, применяемые при проведении аттестационных испытаний

Типовые задачи:

Задания базового уровня:

1. Дайте определение аккредитации предприятия в качестве органа по сертификации средств защиты информации.
2. Дайте определение аккредитации предприятия в качестве испытательной лаборатории.
3. Порядок аккредитации предприятия в качестве органа по сертификации (испытательной лаборатории) средств защиты информации.
4. На какой срок выдается аттестат аккредитации?

Задания повышенного уровня:

5. Покажите на примере порядок контроля за деятельностью аккредитованных предприятий.
6. Покажите на примере случаи, в которых аккредитация может быть досрочно аннулирована.

Тема 9. Меры по защите информации на объекте информатизации. Использование средств защиты информации

Типовые задачи:

Задания базового уровня:

1. Кто осуществляет руководство деятельностью испытательной лаборатории?

2. Чем должна располагать испытательная лаборатория для проведения сертификационных испытаний?
3. Перечислите задачи испытательной лаборатории.
4. Перечислите функции испытательной лаборатории.
5. Какие документы готовит испытательная лаборатория по окончании сертификационных испытаний?

Задания повышенного уровня:

6. Покажите на примере обязанности испытательной лаборатории.
7. Покажите на примере какими помещениями должна располагать испытательная лаборатория.

Список рекомендуемой литературы

1. Основная литература

1. Рагозин, Ю. Н. Инженерно-техническая защита информации на объектах информатизации : учебное пособие / Ю. Н. Рагозин ; под редакцией Т. С. Кулаковой. — Санкт-Петербург : Интермедия, 2019. — 216 с. — ISBN 978-5-4383-0182-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/95271.html>
2. Фомин, Д. В. Информационная безопасность : учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 54 с. — ISBN 978-5-4487-0298-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/77320.html>

2. Дополнительная литература

1. Мониторинг и аудит информационной безопасности : учеб.-метод. пособие : специальность 090103 - Организация и технология защиты информации / сост. Д. В. Якушев ; М-во образования и науки Рос. Федерации, ФГБОУ ВПО "Ставроп. гос. ун-т". - Ставрополь : Изд-во СГУ, 2011. - 69 с. - Библиогр.: с. 66-67
2. Уродовских, В. Н. Управление рисками предприятия : учеб. пособие для вузов / В. Н. Уродовских. - Москва : Вузовский учебник : ИНФРА-М, 2014. - 167, [1] с. : ил. ; 22. - (Вузовский учебник). - Гриф: Доп. УМО. - Библиогр.: с. 155-156. - ISBN 978-5-9558-0158-2. - ISBN 978-5-16-004107-0

3. Интернет-ресурсы

1. Белов Е.Б. Основы информационной безопасности. Учебное пособие для вузов/Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2006, - 544 с. – Доступно: <http://www.alleng.ru/d/comp/comp51.htm>
2. Воройский Ф. С. Информатика. Энциклопедический словарь-справочник: введение в современные информационные и телекоммуникационные технологии в терминах и фактах. - М.: ФИЗМАТЛИТ, 2016. - 768 с. – Доступно: <http://physics-for-students.ru/bookpc/informatika/slovar.zip>
3. Информатика: Практикум по технологии работы на компьютере /Под ред. Н.В. Макаровой. - 3-е изд., перераб. - М.: Финансы и статистика, 2015. - 256 с. – Доступно: http://physics-for-students.ru/bookpc/informatika/makarova_3.zip
4. Могилев А. В., Пак Н. И., Хеннер Е. К. Информатика: Учеб. Пособие для студ. пед. вузов. / Под ред. Е. К. Хеннера. – М.: Изд. центр «Академия», 2014. – 848 с. – Доступно:

http://physics-for-students.ru/bookpc/informatika/mogilev_uchebn.zip

5. Могилев А. В. Практикум по информатике: Учеб. пособие для студ. высш. учеб. заведений / А.В.Могилев, Н.И.Пак, Е.К.Хеннер; Под ред. Е.К.Хеннера. – 2-е изд., стер. – М.: Издательский центр «Академия», 2015. – 608 с. – Доступно: http://physics-for-students.ru/bookpc/informatika/mogilev_praktik.zip

6. Романова Ю.Д. Информатика и информационные технологии. Конспект лекций: учеб.пособие / Ю.Д. Романова, И.Г. Лесничная. – 2-е изд., перераб. и доп. – М.: Эксмо, 2013, – 320 с. – Доступно: http://physics-for-students.ru/bookpc/informatika/romanova_2.rar

7. Симонович С.В. Информатика. Базовый курс. 2-е издание / Под ред. С. В. Симоновича. – СПб.: Питер, 2014. – 640 с. – Доступно: http://physics-for-students.ru/bookpc/informatika/kurs_informat.rar

8. Савельев А. Я. Основы информатики: Учеб.для вузов. – М.: Изд-во МГТУ им. Н. Э. Баумана, 2014. – 328 с. – Доступно: <http://physics-for-students.ru/bookpc/informatika/saveliev.zip>

9. Соболев Б.В. Информатика: учебник/ Б.В. Соболев [и др.] – Изд. 3-е, дополн. и перераб. – Ростов н/Д: Феникс, 2013. – 446 с. – Доступно: <http://physics-for-students.ru/bookpc/informatika/Sobol.rar>

10. Степанов А.Н. Информатика: учебник для вузов. – 4-е изд. – СПб.: Питер, 2016. – 684 с. – Доступно: <http://physics-for-students.ru/bookpc/informatika/stepanov.rar>

4. Программное обеспечение

1. программное обеспечение: MicrosoftOffice или OpenOffice, файловый менеджер Far, архиватор WinRAR, AdobeAcrobatReader или FoxITReader;
2. утилиты обнаружения вторжений, сетевые сканеры, сканеры безопасности;
3. программы тестового контроля Iren.

5. Материально-техническое обеспечение дисциплины

1. Лекционная аудитория, оборудованная электронной доской;
2. Компьютерный класс из расчета одна ПЭВМ на одного человека.
3. Автоматизированная система оценки защищённости помещений от утечки информации по вибрационному и акустическому каналам ШЕПОТ.
4. Автоматизированная система оценки защищённости технических средств от утечки информации по каналу ПЭМИН СИГУРД