**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Петербургский государственный университет путей сообщения**

**Императора Александра I»**

**(ФГБОУ ВО ПГУПС)**

Факультет «Автоматизация и интеллектуальные технологии»

Кафедра «Информатика и информационная безопасность»

Лабораторная работа № 1

по дисциплине

«Информационная безопасность автоматизированных транспортных систем»

«*Изучение требований к защите информации и обеспечению безопасности автоматизированных и информационных систем*»

|  |  |  |
| --- | --- | --- |
| **Выполнил обучающийся**  Курс 5  Группа КИБ-012 | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись, дата | Г. Е. Груздев |
|  |  |  |
| **Проверил** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись, дата | А.А. Корниенко |

Санкт-Петербург

2024

**Цель выполнения лабораторной работы:**

Изучение и сравнительный анализ руководящих документов ФСТЭК России, устанавливающих требования к защите информации (ЗИ) и обеспечению безопасности АС, ИС и значимых объектов КИИ.

**Определение и краткое описание объекта защиты:**

1. ГИС - государственные информационные системы - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов (ФЗ-149 ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ).

Государственные системы бывают федеральные и региональные. Федеральные государственные системы создаются на основании федерального закона или же акта федерального государственного органа. Региональные государственные системы создаются на основании законов субъектов или же акта регионального государственного органа.

1. ИСПДн - информационные системы персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств» (ФЗ-152 О ПЕРСОНАЛЬНЫХ ДАННЫХ). То есть ИСПДн — это любые системы компаний, в которых хранится и обрабатывается чья-либо персональная информация: собственных сотрудников или клиентов.
2. АСУ ТП — это система, состоящая из персонала и совокупности оборудования с программным обеспечением, использующихся для автоматизации функций этого самого персонала по управлению промышленными объектами: электростанциями, котельными, насосными, водоочистными сооружениями, пищевыми, химическими, металлургическими заводами, нефтегазовыми объектами и т.д. и т.п.

**Основные этапы предъявления требований (мероприятия) при организации ЗИ и мероприятия при формировании требований к защите информации в АС, ИС**

### ****1. Организация защиты информации (ЗИ)****

#### ****Общие этапы:****

1. **Назначение ответственного лица:**
   * Определение подразделения или должностного лица, ответственного за организацию и выполнение мер защиты информации.
2. **Привлечение лицензированных организаций:**
   * Для выполнения работ по защите информации (например, аттестация, аудит, проектирование).
3. **Обеспечение защиты информации сертифицированными средствами:**
   * Использование средств, прошедших процедуру оценки соответствия по требованиям безопасности.

#### ****Мероприятия:****

1. Установление перечня объектов защиты:
   * Информация, программное обеспечение, технические средства, средства защиты информации.
2. Определение состава и содержания организационных и технических мер:
   * Разграничение доступа, антивирусная защита, регистрация событий безопасности и др.
3. Реализация защиты на всех этапах жизненного цикла:
   * Проектирование, внедрение, эксплуатация, модернизация, вывод из эксплуатации.
4. Формирование организационно-распорядительных документов:
   * Политики информационной безопасности, инструкции по реагированию на инциденты.

### ****2. Формирование требований к защите информации****

#### ****Общие этапы:****

1. **Анализ нормативных и правовых требований:**
   * Федеральные законы, ГОСТы, ведомственные приказы.
2. **Классификация информационной системы:**
   * Установление уровня защищенности системы (класс защищенности, уровень значимости информации).
3. **Определение угроз безопасности информации:**
   * Учет внешних и внутренних угроз, использование банка данных угроз ФСТЭК.
4. **Разработка модели угроз:**
   * Описание угроз, уязвимостей, сценариев реализации угроз и их последствий.

#### ****Мероприятия:****

1. **Принятие решения о необходимости защиты:**
   * Оценка задач и целей информационной системы.
   * Выявление критической информации, нарушение безопасности которой может привести к ущербу.
2. **Формирование требований к системе защиты:**
   * Установление требований к мерам защиты (организационным и техническим).
   * Определение целей, задач защиты, перечня нормативных актов.
3. **Разработка технического задания:**
   * Включение требований к защите в ТЗ на создание или модернизацию системы.
4. **Согласование требований с ГОСТами:**
   * Использование стандартов (например, ГОСТ 34.602, ГОСТ Р 51583) для определения формата и содержания требований.
5. **Адаптация требований:**
   * Учет специфики системы, масштабов и особенностей эксплуатации.

### ****Примеры мероприятий для АС и ИС:****

#### ****Для автоматизированных систем (АС):****

1. Разделение на уровни управления:
   * Операторский (верхний), автоматический (средний), ввод/вывод данных (полевой).
2. Проектирование системы защиты:
   * Определение субъектов и объектов доступа, выбор методов управления доступом.
3. Внедрение и аттестация системы защиты:
   * Макетирование, тестирование, опытная эксплуатация, приемочные испытания.

#### ****Для информационных систем (ИС):****

1. Определение уровня защищенности персональных данных:
   * Применение постановления Правительства РФ №1119.
2. Реализация базового набора мер безопасности:
   * Идентификация и аутентификация, антивирусная защита, регистрация событий.
3. Обеспечение доступности и целостности информации:
   * Резервное копирование, защита каналов связи.

**Сравнительный анализ процедур классификации и направленности требований, а также количества классов защищенности для государственных информационных систем (ГИС), информационных систем персональных данных (ИСПДн) и автоматизированных систем управления технологическими процессами (АСУ ТП)**

### ****1. Процедуры классификации и их направленность****

| **Система** | **Основания классификации** | **Цель классификации** |
| --- | --- | --- |
| **ГИС** | Уровень значимости обрабатываемой информации и потенциальный ущерб в случае нарушения конфиденциальности, целостности или доступности. | Определение требований к защите информации в зависимости от ее значимости и масштаба системы. |
| **ИСПДн** | Количество субъектов персональных данных и возможные последствия нарушения их прав. | Защита персональных данных от неправомерного доступа, изменения, уничтожения или распространения. |
| **АСУ ТП** | Уровень риска для жизни и здоровья людей, окружающей среды, а также критичность технологических процессов. | Обеспечение безопасности и стабильности функционирования критически важных объектов. |

### ****2. Количество классов защищенности****

| **Система** | **Количество классов защищенности** | **Критерии классификации** |
| --- | --- | --- |
| **ГИС** | 3 класса (К1, К2, К3) | Значимость информации и масштабы информационной системы (федеральный, региональный, объектовый). |
| **ИСПДн** | 4 уровня защищенности (1, 2, 3, 4) | Потенциальный ущерб субъектам данных, уровень актуальных угроз, объем и значимость обрабатываемых данных. |
| **АСУ ТП** | 3 класса (1-й, 2-й, 3-й) | Критичность объектов и процессов, возможные последствия нарушения безопасности информации. |

### ****3. Направленность классификации****

| **Система** | **Основные аспекты направленности классификации** |
| --- | --- |
| **ГИС** | Направлена на защиту государственных интересов, предотвращение утечек информации, поддержание целостности и доступности информации. |
| **ИСПДн** | Сосредоточена на обеспечении прав граждан на конфиденциальность персональных данных и защите информации от несанкционированного доступа. |
| **АСУ ТП** | Ориентирована на предотвращение нарушений в технологических процессах, которые могут привести к авариям, угрозам для жизни, здоровья и экологии. |

### ****Ключевые отличия****

1. **ГИС:**
   * Классы защищенности основаны на масштабе и уровне значимости информации.
   * Основная направленность — защита государственных информационных ресурсов.
2. **ИСПДн:**
   * Уровни защищенности зависят от количества субъектов персональных данных и характера обрабатываемой информации.
   * Цель — защита персональных данных, включая предотвращение утечек и несанкционированного доступа.
3. **АСУ ТП:**
   * Классы классифицируются по критичности объектов и потенциальным рискам для общества и окружающей среды.
   * Фокус на предотвращении катастроф и поддержании устойчивой работы критических объектов.

**Перечень, краткая характеристика и процедуры выбора требуемых мер защиты информации в ГИС, результаты сравнительного анализа требуемых мер защиты информации и обеспечения безопасности ГИС, ИСПДн, АСУ ТП**

### ****1. Перечень и краткая характеристика мер защиты информации в ГИС****

| **Мера защиты** | **Краткая характеристика** |
| --- | --- |
| **Идентификация и аутентификация** | Обеспечение уникальной идентификации пользователей и систем, проверка подлинности при доступе к системе. |
| **Управление доступом** | Регулирование прав и привилегий пользователей, разграничение доступа к данным и ресурсам в соответствии с ролями. |
| **Регистрация событий безопасности** | Фиксация действий пользователей, событий в системе и анализ их для обнаружения инцидентов. |
| **Антивирусная защита** | Обнаружение, предотвращение и устранение вредоносного ПО. |
| **Контроль целостности** | Выявление изменений в информации или системе, которые могли быть вызваны несанкционированным доступом. |
| **Обеспечение доступности** | Меры для предотвращения отказов в обслуживании, использование резервирования данных и оборудования. |
| **Обнаружение и предотвращение атак** | Использование систем предотвращения вторжений (IPS/IDS) для обнаружения попыток нарушения безопасности. |
| **Защита технических средств** | Физическая защита оборудования и предотвращение несанкционированного доступа к носителям информации. |
| **Обеспечение безопасности передачи данных** | Шифрование данных, защита каналов связи от перехвата и анализа. |

### ****2. Процедуры выбора требуемых мер защиты информации в ГИС****

1. **Определение класса защищенности:**
   * Установление класса защищенности системы на основе масштаба и уровня значимости обрабатываемой информации (К1, К2, К3).
2. **Анализ угроз безопасности:**
   * Оценка актуальных угроз в контексте системы, учет внутреннего и внешнего нарушителей.
3. **Формирование модели угроз:**
   * Выявление уязвимостей системы, определение сценариев реализации угроз.
4. **Выбор базового набора мер:**
   * Использование нормативных документов для определения минимальных обязательных мер защиты.
5. **Адаптация базового набора мер:**
   * Учет особенностей инфраструктуры и требований, исключение мер, не применимых к конкретной системе.
6. **Уточнение мер защиты:**
   * Дополнение базового набора специфическими мерами, необходимыми для защиты системы.
7. **Проведение аттестации системы:**
   * Проверка соответствия реализованных мер установленным требованиям.

### ****3. Сравнительный анализ мер защиты в ГИС, ИСПДн и АСУ ТП****

| **Критерий** | **ГИС** | **ИСПДн** | **АСУ ТП** |
| --- | --- | --- | --- |
| **Основная цель** | Защита государственных информационных ресурсов. | Обеспечение конфиденциальности и защиты прав субъектов персональных данных. | Обеспечение стабильности и безопасности технологических процессов. |
| **Идентификация и аутентификация** | Уникальные учетные записи для пользователей и систем. | Уникальные учетные записи для субъектов и объектов обработки данных. | Учет идентификаторов пользователей и оборудования на всех уровнях управления. |
| **Управление доступом** | Разграничение доступа по ролям, контроль действий пользователей. | Управление правами доступа к персональным данным, разграничение прав по необходимости. | Контроль доступа на уровне всех сегментов системы (полевой, автоматический, диспетчерский). |
| **Регистрация событий** | Логирование действий пользователей и изменений в системе. | Логирование операций с персональными данными, анализ событий безопасности. | Журналирование действий, связанных с технологическими процессами и их состоянием. |
| **Антивирусная защита** | Использование сертифицированного антивирусного ПО. | Выявление и устранение угроз вредоносного ПО. | Проверка ПО на целостность и выявление вредоносных программ, влияющих на управление. |
| **Контроль целостности** | Проверка целостности системных файлов и баз данных. | Обеспечение неизменности персональных данных. | Выявление несанкционированных изменений в данных или управляющих программах. |
| **Обеспечение доступности** | Резервное копирование и аварийное восстановление. | Резервирование персональных данных, защита от отказов. | Использование отказоустойчивых систем и резервирования на уровне оборудования. |
| **Физическая защита** | Оборудование защищенных помещений для серверов и рабочих станций. | Защита помещений, где обрабатываются персональные данные. | Обеспечение контролируемых зон для оборудования и защиты технических каналов утечки. |

**Вывод**

1. **Общие принципы защиты:**  
   Все системы — ГИС, ИСПДн и АСУ ТП — основываются на идентификации и аутентификации, управлении доступом, контроле целостности, регистрации событий безопасности и других базовых мерах защиты.
2. **Специфика систем:**
   * **ГИС:** Основной акцент на масштабе и значимости обрабатываемой информации. Требования к защите ориентированы на государственные интересы и предотвращение утечек информации.
   * **ИСПДн:** Фокус на защите конфиденциальности персональных данных и прав субъектов. Используются дополнительные меры для минимизации последствий утечки данных.
   * **АСУ ТП:** Ориентированы на предотвращение техногенных катастроф и обеспечение безопасности процессов. Классификация и меры защиты зависят от риска для людей и окружающей среды.
3. **Различия в классификации:**
   * ГИС и АСУ ТП используют трехуровневую классификацию.
   * ИСПДн включает четыре уровня защищенности, что обусловлено объемом данных и характером угроз.
4. **Меры защиты:**  
   Меры защиты во многом пересекаются, однако их реализация и акцент зависят от целей системы. Для ГИС важна масштабность, для ИСПДн — защита данных пользователей, для АСУ ТП — стабильность технологических процессов.
5. **Регулирование:**  
   Все системы регулируются приказами ФСТЭК и ГОСТами, но в ИСПДн и АСУ ТП уделяется больше внимания узкоспециализированным требованиям.

### ****Перечень использованных информационных источников****

1. **Федеральный закон № 152-ФЗ от 27 июля 2006 г.** «О персональных данных».
2. **Федеральный закон № 187-ФЗ от 26 июля 2017 г.** «О безопасности критической информационной инфраструктуры Российской Федерации».
3. **Приказ ФСТЭК России № 17 от 11 февраля 2013 г.** «Требования к защите информации в государственных информационных системах».
4. **Приказ ФСТЭК России № 21 от 18 февраля 2013 г.** «Организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах».
5. **Приказ ФСТЭК России № 31 от 14 марта 2014 г.** «Требования к защите информации в автоматизированных системах управления производственными и технологическими процессами».
6. **Приказ ФСТЭК России № 239 от 25 декабря 2017 г.** «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры».
7. **Постановление Правительства РФ № 1119 от 1 ноября 2012 г.** «Требования к защите персональных данных при их обработке в информационных системах персональных данных».