Управление
ФСТЭК России по Сибирскому федеральному округу

ЩЕКЛАЧЕВ
Иван Владимирович

«Система нормативных правовых актов, устанавливающих требования по организации и обеспечению безопасности информации»

Основные принципы организации защиты информации

Угрозы безопасности информации:

- Угрозы безопасности информации ограниченного доступа, **содержащей ГТ**
- Угрозы безопасности информации, ограниченного доступа, **не содержащей ГТ**

Объекты защиты:

- **информационные (автоматизированные) системы различного назначения;**
- **помещения, для проведения закрытых совещаний;**
- **средства изготовления и размножения документов;**
- **ключевые системы информационной инфраструктуры**

Организационные и технические мероприятия по ЗИ

Система документов по ЗИ:

нормативно-правовые акты Российской Федерации, нормативно-правовые, руководящие и методические документы ФСТЭК России, регулирующие вопросы защиты информации, ограниченного доступа:

- **содержащей сведения, составляющие ГТ**
- **не содержащей сведений, составляющие ГТ**

149-ФЗ «Об информации, информационных технологиях и о защите информации»

Объект правового регулирования – информация
(сведения (сообщения, данные) независимо от формы их представления

в зависимости от категории доступа информация подразделяется на:

информацию ограниченного доступа
(доступ ограничен федеральными законами)

- содержит сведения, составляющие государственную тайну
- не содержит сведений, составляющих государственную тайну (конфиденциальная информация)

общедоступная информация

- общеизвестные сведения и иная информация, **доступ** к которой **не ограничен**

свойства информации, которые подлежат защите:

- **конфиденциальность**
- **доступность**
- **целостность**

Государственное регулирование в области защиты информации

ФЗ-149 «Об информатизации, информационных технологиях и о защите информации»

ч.1. ст. 16 **149-ФЗ**:
Государственное регулирование отношений в сфере защиты информации осуществляется **путем установления требований о защите информации**

ч.2 ст. 16 **149-ФЗ:**
Требования о защите информации, содержащейся в ГИС, **устанавливаются** федеральным органом исполнительной власти в области противодействия техническим разведкам и технической защиты информации, в пределах его полномочий – **ФСТЭК России**

ч.5 ст. 16 **149-ФЗ:**
При создании и эксплуатации государственных информационных систем используемых в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям

149-ФЗ «Об информации, информационных технологиях и о защите информации»

ИНФОРМАЦИОННАЯ СИСТЕМА

- Информация
- Технология
- Технические средства

- **Государственные ИС**
  - **Федеральные ИС**
  - **Региональные ИС**
- **Муниципальные ИС**
- **Иные ИС**

Система документов по ТЗИ ограниченного доступа в ИС, не содержащей сведений, составляющих ГТ

ФЗ «О персональных данных» (152-ФЗ)

Постановление Правительства Российской Федерации

№ 1119

«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Документы ФСТЭК России по ОБИ ПДн в ИСПДН

«Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

(утверждены приказом ФСТЭК России **от 18.02.2013 № 21**)

Нормативные правовые акты и руководящие документы, регулирующие вопросы предотвращения НСД к персональным данным при их обработке в информационных системах персональных данных

Методические документы, регулирующие вопросы по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Система документов по ОБ ПДн при их обработке в ИСПДн

Постановление Правительства Российской Федерации
от 1.11.2012 **№ 1119**

«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Устанавливает

- **типы актуальных угроз** для информационной системы, обрабатывающей ПДн **(3 типа)**
- **требования к защите персональных данных** при их обработке в информационных системах персональных данных
- **уровни защищенности персональных данных (4 уровня)**

ФСТЭК России

Приказ от 18.02.2013 № 21
«Об утверждении состава и содержания организационных и технических мер по ОБ ПДн при их обработке в ИСПДн»

I. Общие положения

II. Состав и содержание мер по обеспечению персональных данных

Приложение
Состав и содержание мер по обеспечению персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных
(определяются исходя из актуальных угроз ПДн и уровня защищённости ПДн при их обработке в ИСПДн)

Выбор мер по обеспечению безопасности ПДн в ИСПДн

Уровни защищенности ПДн (постановление Правительства РФ № 1119) + **Перечень актуальных угроз ПДн**

Выбор мер ОБ ПДн в ИСПДн (приказ ФСТЭК России № 21)

Выбор базового набора мер по обеспечению безопасности (ОБ) ПДн в ИСПДн, в соответствии с установленным уровнем защищенности ПДн

Адаптация базового набора мер по ОБ ПДн в ИСПДн, с учетом структурно-функциональных характеристик ИСПДн

Уточнение адаптированного базового набора мер по ОБ ПДн в ИСПДн, с учетом не выбранных ранее мер, нейтрализующие все угрозы ПДн

Дополнение адаптированного базового набора мер для выполнения требований по ОБ ПДн в ИСПДн, установленных иными нормативно-правовыми актами

Набор мер по защите ПДн в ИСПДн

Компенсирующие меры (при необходимости)

Методические документы ФСТЭК России по определению актуальных угроз безопасности ПДн, при их обработке в ИСПДн

ФЗ «О персональных данных» (152-ФЗ)

БАЗОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Утверждена заместителем директора ФСТЭК России **15.02.2008**

Утверждена заместителем директора ФСТЭК России **14.02.2008**

МЕТОДИКА ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Документы используются :

- **операторами персональных данных** (**ПДн**) - в ходе работ по определению актуальных угроз ПДн при их обработке в информационных системах персональных данных (ИСПДн);
- **органами государственной власти** субъектов РФ, **Банком России**, органами государственных внебюджетных фондов, иными государственными органами – при разработке нормативных правовых актов, которые определяют угрозы безопасности ПДн, актуальные при их обработке в ИСПДн

Система документов по ТЗИ ограниченного доступа в ГИС, не содержащей сведений, составляющих ГТ

ФЗ «Об информации, информационных технологиях и о защите информации» (149-ФЗ)

Документы ФСТЭК России по защите информации в ГИС

«Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (утверждены приказом ФСТЭК России от **11.02.2013 № 17**)

Нормативные правовые акты и руководящие документы, регулирующие вопросы предотвращения НСД к информации в государственных информационных системах

Методические документы, регулирующие вопросы по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

Действие указанных документов распространяется и на муниципальные информационные системы, если иное не предусмотрено законодательством Российской Федерации о местном самоуправлении

Классификация ГИС (приложение 1 к приказу ФСТЭК России № 17)

Уровень значимости информации

+

Масштаб информационной системы

Класс ГИС

К1 – первый класс защищенности ИС

К2 – второй класс защищенности ИС

К3 – третий класс защищенности ИС

К4 - четвертый класс защищенности ИС

Определение уровня значимости информации в ГИС

Степень ущерба ≡ нарушение свойств безопасности информации:

- **«конфиденциальность»**
- **«целостность»**
- **«доступность»**

Уровень значимости информации

ВЫСОКИЙ	хотя бы для одного из свойств … делена **высокая степень ущерба**
СРЕДНИЙ	хотя бы для одного из свойств безопасности информации определена **средняя степень ущерба** и нет ни одного свойства, для которого определена высокая степень ущерба
НИЗКИЙ	для всех свойств безопасности информации определены **низкие степени ущерба**
МИНИ-МАЛЬНЫЙ	если обладателем информации (заказчиком) и (или) оператором **степень ущерба** от нарушения свойств безопасности информации **не может быть определена**, но при этом информация подлежит защите

Определение масштаба информационной системы

Масштаб информационной системы

	Критерии
федеральная	**ИС функционирует на территории РФ** (в пределах федерального округа) и имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях
региональная	**ИС функционирует на территории субъекта РФ** и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях
объектовая	**ИС функционирует на объектах одного федерального органа государственной власти**, органа государственной власти субъекта РФ, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях

Работы по определению угроз безопасности информации в ГИС

БАЗОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

- оценка возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей;
- анализ возможных уязвимостей ГИС;
- анализ возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности)

МЕТОДИКА ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Итог:

Модель угроз безопасности информации в ГИС:

- описание ГИС;
- описание угроз безопасности информации в ГИС;
- описание возможностей нарушителя (модель нарушителя);
- возможные уязвимости ГИС;
- способы (сценарии) реализации угроз безопасности информации в ГИС;
- последствия от нарушения свойств информации (целостности, доступности, конфиденциальности) и штатного режима функционирования ГИС

Выбор мер защиты информации в ГИС

Модель угроз безопасности информации в ГИС + **Класс Защищенности ГИС**

Выбор мер ЗИ:

Выбор базового набора мер по защите информации, соответствующего установленному классу защищенности информационной системы

Адаптация базового набора мер по защите информации к структурно-функциональным характеристикам информационной системы

Уточнение адаптированного базового набора мер защиты информации с целью блокирования (нейтрализации) актуальных угроз безопасности информации

Дополнение адаптированного базового набора мер для выполнения требований по защите информации, установленных иными нормативно-правовыми актами

Набор мер по защите информации в ГИС

Компенсирующие меры (при необходимости)

Требования Указа Президента РФ от 17.03.2008 г. № 351

ИНФОРМАЦИОННЫЕ СИСТЕМЫ (ИС), ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ (ИТКС), средства вычислительной техники (СВТ)

(применяемые для хранения, обработки или передачи информации, содержащей сведения, составляющие **государственную тайну**, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие **служебную тайну**)

Указ Президента РФ
от 17.03.2008 **№ 351**

«О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»

1. **Подключение указанных ИС, ИТКС и СВТ к трансграничным сетям не допускается.**
2. **При необходимости** такое подключение производится только с использованием специально предназначенных для этого **СЗИ**, в том числе **шифровальных (криптографических)** средств, прошедших в установленном законодательством РФ порядке сертификацию в **ФСБ России** и (или) получивших подтверждение соответствия в **ФСТЭК России**.
3. **Выполнение данного требования является обязательным** для операторов ИС, владельцев ИТКС и (или) СВТ

Система документов по ТЗИ в ИС общего пользования

ИНФОРМАЦИЯ в информационных системах общего пользования

(Перечни сведений для обязательного размещения в сети Интернет в форме открытых данных (постановление Правительства РФ **24.11.2009 г. N 953,** распоряжение Правительства РФ **от 10 июля 2013 г. N 1187-р**)

Целостность

Доступность

149-ФЗ

Постановление Правительства РФ
от 18.05.2009 г. **№ 424**

«Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям»

ПРИКАЗ Минкомсвязи России
от 25.08.2009 г. № 104

«Об утверждении требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования»

ПРИКАЗ ФСБ России и ФСТЭК России от 31.08.2010 г. № 416/489

«Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»

Спасибо за внимание