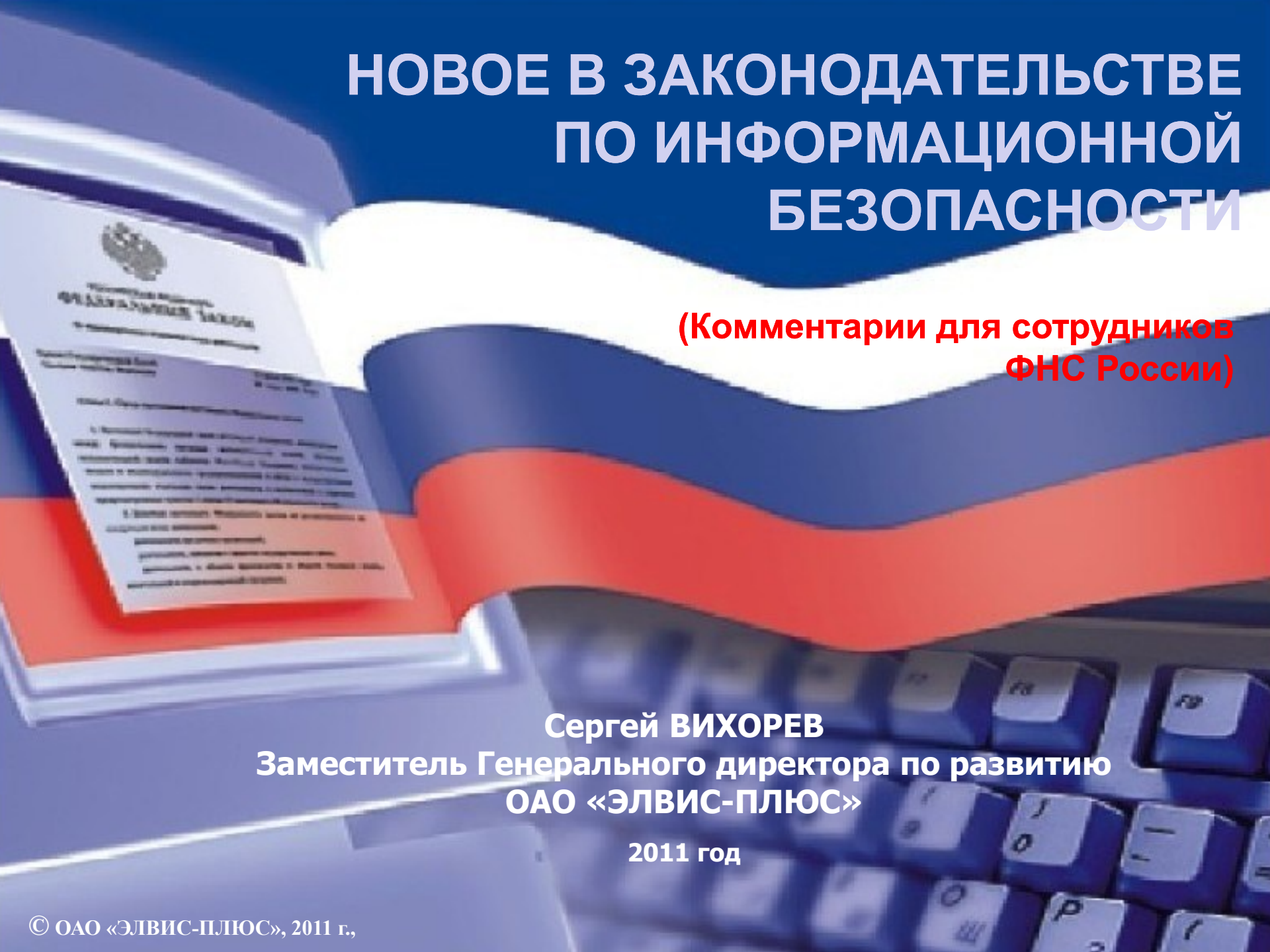
НОВОЕ В ЗАКОНОДАТЕЛЬСТВЕ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(Комментарии для сотрудников ФНС России)



Сергей ВИХОРЕВ
Заместитель Генерального директора по развитию
ОАО «ЭЛВИС-ПЛЮС»

2011 год

«…Что было,
что будет,
чем сердце успокоится….»

ВНИМАНИЕ!

Материалы, изложенные в данной презентации рассматривают только основные аспекты проблемы безопасности информации и не претендуют на полноту анализа изменений российского законодательства

ЭЛВИС-ПЛЮС

ВОПРОСЫ ПРЕЗЕНТАЦИИ

- Новые законодательные акты 2007-2011 годы
- Новые указания Правительства РФ
- Нормативные документы регуляторов
- Обобщенная структура нормативной базы

ЭЛВИС-ПЛЮС

ПРОЛОГ

В 2007 – 2011 годы законодательство РФ в области информационной безопасности усиленно совершенствовалось.

За этот период издано:

- 4 новых Федеральных закона
- 8 Распоряжений и Постановлений Правительства РФ
- Большое количество подзаконных актов, изданных уполномоченными органами государственной власти

В соответствии с Концепцией национальной безопасности законодательство совершенствовалось в направлении:

- ***реализации конституционных прав и свобод граждан***
- ***защиты отечественной информационной инфраструктуры***
- ***интеграции России в мировое информационное пространство***

ЭЛВИС-ПЛЮС

ФЕДЕРАЛЬНЫЕ ЗАКОНЫ

ЭЛВИС-ПЛЮС

НОВЫЕ ЗАКОНОДАТЕЛЬНЫЕ АКТЫ

за период 2007-2011 годы

ФЕДЕРАЛЬНЫЙ ЗАКОН № 8-ФЗ, 2009 г
«Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»

ФЕДЕРАЛЬНЫЙ ЗАКОН № 108-ФЗ, 2010 г
«О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»

ЭЛВИС-ПЛЮС

ФЕДЕРАЛЬНЫЙ ЗАКОН № 8-ФЗ, 2009 г

Об обеспечении доступа к информации о деятельности государственных органов

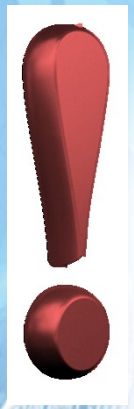
Закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» напрямую не касается проблем обеспечения безопасности информации, однако именно этот закон породил необходимость издания целой цепочки подзаконных актов, в том числе и вопросам защиты информации

Наиболее важное для защиты информации –
Постановление Правительства РФ от 24.11.2009 г. № 953
«Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти»

Казалось бы закон из смежной области права, но влияет на требования к защите информации

ЭЛВИС-ПЛЮС

ВАЖНОЕ ЗАМЕЧАНИЕ



Решения и действия (бездействие) государственных органов, их должностных лиц, нарушающие право на доступ к информации о деятельности государственных органов могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд.

Виновные должностные лица и служащие несут дисциплинарную, административную, гражданскую и уголовную ответственность.

Убытки от таких действий (бездействий) подлежат возмещению в соответствии с гражданским законодательством РФ

Получается, что общедоступная информация на официальном сайте государственного органа должна быть всегда доступна и целостна – а это задачи защиты информации

ЭЛВИС-ПЛЮС

ФЕДЕРАЛЬНЫЙ ЗАКОН № 108-ФЗ, 2010 г.

О внесении изменений в КоАП

Ст. 5.39. Неправомерный отказ в предоставлении информации, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации – штраф **от 1 до 3 тыс**. руб.

Ст.13.27.1. Нарушение требований к технологическим, программным и лингвистическим средствам обеспечения пользования сайтами госорганов – штраф **от 3 до 5 тыс**. руб.
Ст. 13.27.2. Неразмещение в сети «Интернет» информации о деятельности госорганов – штраф **от 3 до 5 тыс.** руб.

Ст. 13.28.1. Нарушение порядка предоставления информации о деятельности госорганов, содержащей сведения ограниченного доступа – штраф **от 3 до 5 тыс**. руб.
Ст. 13.28.2. Незаконное взимание платы за предоставление информации о деятельности госорганов – штраф должностных лиц **от 3 до 5 тыс**. руб.

ЭЛВИС-ПЛЮС

НОВЫЕ ЗАКОНОДАТЕЛЬНЫЕ АКТЫ

за период 2007-2011 годы

ФЕДЕРАЛЬНЫЙ ЗАКОН № 63-ФЗ, 2011 г.

«Об электронной подписи»

ЭЛВИС-ПЛЮС

ФЕДЕРАЛЬНЫЙ ЗАКОН № 63-ФЗ, 2011 г.

Об электронной подписи

Закон «Об электронной подписи»
пришел на смену устаревшему Федеральному закону 2002 года № 1-ФЗ «Об электронной цифровой подписи»,
который утратит силу 01.07.2012 года
Закон кардинально изменил понятие электронной подписи, максимально приблизив его к международным нормам.

Изменение в правовом регулировании вызвано тем, что старый закон не позволял использовать в электронном документообороте более простые виды электронных подписей (не основанные на технологии ассиметричного шифрования), что ставило их за рамки правового регулирования.

Поменялось не только название закона, но полностью изменилась его концепция

ЭЛВИС-ПЛЮС

ФЕДЕРАЛЬНЫЙ ЗАКОН № 63-ФЗ, 2011 г.

Об электронной подписи

Признание электронных документов равнозначных обычным (ст. 6):

- **Простая и неквалифицированная электронная подпись:**

  только в случаях, установленных законами, иными нормативными актами или соглашением между участниками электронного взаимодействия, предусматривающего порядок проверки электронной подписи

- **Усиленная квалифицированная электронная подпись:**

  в любом кроме случая, когда законом или иным нормативным актом установлено требование о составлении документа исключительно на бумажном носителе, при этом, такая подпись признается действительной до тех пор, пока решением суда не установлено иное.

Закон допускает получение ЭП от имени юридических лиц или государственных органов.

ЭЛВИС-ПЛЮС

НОВЫЕ ЗАКОНОДАТЕЛЬНЫЕ АКТЫ

за период 2007-2011 годы

ФЕДЕРАЛЬНЫЙ ЗАКОН № 152-ФЗ, 2006 г.

«О персональных данных»

(в редакции ФЗ № 261-ФЗ, 2011 г.)

ЭЛВИС-ПЛЮС

ФЕДЕРАЛЬНЫЙ ЗАКОН № 152-ФЗ, 2006 г.

О персональных данных (в редакции ФЗ № 261-ФЗ, 2011 г.)

В новой редакции Закона «О персональных данных» уточнена сфера его действия используемые в нём основные понятия.

Существенно уточнены принципы и условия обработки персональных данных.

Существенно переработаны нормы, регламентирующие права и обязанности оператора, взаимоотношения оператора и субъекта персональных данных, вопросы трансграничной передачи персональных данных, а также меры по обеспечению безопасности персональных данных при их обработке в ИСПДн

По своей сути, хотя концепция закона не изменилась, он получил существенно новое наполнение

ЭЛВИС-ПЛЮС

ФЕДЕРАЛЬНЫЙ ЗАКОН № 152-ФЗ, 2006 г.

О персональных данных (в редакции ФЗ № 261-ФЗ, 2011 г.)

Существенно уточнен понятийный аппарат Закона (ст. 3):

персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн)

В ходе судебного процесса по вопросу об опеке над девочкой был произведен нейропсихиатрический анализ ее состояния, в ходе которого был представлен ее рисунок, характеризующий ее семью. Рисунок содержал информацию о ее состоянии и то, что она думала о членах семьи. Тем самым, он мог быть оценен, как содержащий «персональные данные». Рисунок и вправду раскрывал информацию, относящуюся к ребенку (состояние ее здоровья с психиатрической точки зрения), а также о поведении отца и матери. Как результат, родители могли настаивать на их праве доступа к такой специфической информации.

Пример из Мнения Рабочей группы 136 № 4/2007 О понятии «персональные данные»

Значительно расширено понятие «персональные данные»

ЭЛВИС-ПЛЮС

ФЕДЕРАЛЬНЫЙ ЗАКОН № 152-ФЗ, 2006 г.

О персональных данных (в редакции ФЗ № 261-ФЗ, 2011 г.)

Хотя в Законе в прямую не сказано, но, по смыслу, введено понятие «обработчик» (ст. 6):

Оператор вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн на основании поручения оператора. Такое лицо обязано соблюдать принципы и правила обработки ПДн, но не обязано получать согласие субъекта ПДн. Ответственность перед субъектом ПДн за действия указанного лица несет оператор.

Поручение оператора (договор) должно содержать:

- *перечень действий (операций) с ПДн, которые будут совершаться*
- *цели обработки,*
- *обязанность соблюдать конфиденциальность ПДн*
- *обязанность обеспечивать безопасность ПДн при их обработке*
- *требования к защите обрабатываемых ПДн*

Даны существенные условия договора с «обработчиком»

ЭЛВИС-ПЛЮС

ФЕДЕРАЛЬНЫЙ ЗАКОН № 152-ФЗ, 2006 г.

О персональных данных (в редакции ФЗ № 261-ФЗ, 2011 г.)

Полностью переписана статья, определяющая порядок обеспечения безопасности ПДн (ст. 19):

Оператор обязан принимать необходимые правовые, организационные и технические меры для защиты ПДн.

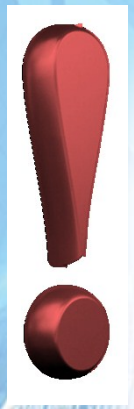
Обеспечение безопасности ПДн достигается:

- *определением угроз безопасности ПДн при их обработке*
- *применением организационных и технических мер защиты ПДн*
- *применением прошедших оценку соответствия СЗИ*
- *оценкой эффективности мер до ввода в эксплуатацию ИСПДн*
- *учетом машинных носителей ПДн*
- *обнаружением фактов НСД к ПДн и принятием мер*
- *восстановлением модифицированных или уничтоженных ПДн*
- *установлением правил доступа к ПДн*
- *контролем за принимаемыми мерами по обеспечению безопасности*

Организационные и технические меры должны соответствовать уровню установленному защищенности.

ЭЛВИС-ПЛЮС

ВАЖНОЕ ЗАМЕЧАНИЕ



Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки ПДн, установленных законом, а также требований к защите ПДн, установленных в соответствии с законом, подлежит возмещению в соответствии с законодательством Российской Федерации.

Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Теперь имеется возможность применить ст. 151 ГК РФ!

ЭЛВИС-ПЛЮС

ФЕДЕРАЛЬНЫЙ ЗАКОН № 152-ФЗ, 2006 г.

О персональных данных (в редакции ФЗ № 261-ФЗ, 2011 г.)

Новая редакция Закона предполагает издание ряда подзаконных актов, в том числе Постановлений Правительства РФ, устанавливающих:

1. Порядок получения в форме электронного документа согласия субъекта ПДн на обработку его ПДн в целях предоставления государственных и муниципальных услуг
2. Перечень мер, направленных на обеспечение выполнения обязанностей операторами, являющимися государственными или муниципальными органами
3. Уровни защищенности ПДн при их обработке в ИСПДн в зависимости от угроз безопасности этих данных
4. Требования к защите ПДн при их обработке в ИСПДн, исполнение которых обеспечивает установленные уровни защищенности ПДн
5. Требования к материальным носителям биометрических ПДн и технологиям хранения таких данных вне ИСПДн
6. Порядок согласования моделей угроз безопасности ПДн с ФСБ России и ФСТЭК России
7. Перечень видов деятельности, при которых обработка ПДн в ИС, не являющихся государственными ИСПДн, подлежат контролю ФСБ России и ФСТЭК России

ЭЛВИС-ПЛЮС

ФЕДЕРАЛЬНЫЙ ЗАКОН № 152-ФЗ, 2006 г.

О персональных данных (в редакции ФЗ № 261-ФЗ, 2011 г.)

А также документов уполномоченных государственных органов:

1. Перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, обеспечивающих адекватную защиту прав субъектов ПДн. (Роскомнадзор)
2. Моделей актуальных угроз безопасности ПДн, при их обработке в ИСПДн, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания ПДн, характера и способов их обработки (государственные органы в пределах своей компетенции)
3. Состав и содержание требований к защите ПДн для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн (ФСБ России, ФСТЭК России)
4. Административный регламент осуществления государственной функции по контролю и надзору за соответствием обработки ПДн требованиям Закона «О персональных данных» (Роскомнадзор)
5. Административный регламент осуществления государственной функции контроля и надзора за выполнением организационных и технических мер по обеспечению безопасности ПДн, при их обработке в ИСПДн (ФСБ России, ФСТЭК России)

ЭЛВИС-ПЛЮС

НОВЫЕ ЗАКОНОДАТЕЛЬНЫЕ АКТЫ

Основные выводы из анализ изменений в законодательстве РФ

Анализ изменений законодательной базы показывает, что:

- Законодательно вводятся новые категории субъектов правоотношений
- Субъекты наделяются определенными правами по отношению к ИР
- Обеспечение ИБ направлено на защиту интересов субъектов
- Изменяется концепция применения электронной подписи
- Вводится обязательная защита открытых общедоступных ИР
- Развивается система межведомственного взаимодействия
- Вводится понятие базовых информационных ресурсов
- Усиливается контроль и надзор за выполнением требований по защите
- Усиливается ответственность за невыполнение требований по доступу и защите информации

ЭЛВИС-ПЛЮС

Распоряжения и Постановления Правительства РФ

ЭЛВИС-ПЛЮС

НОВЫЕ ПОДЗАКОННЫЕ АКТЫ

за период 2007-2011 годы

В период 2007-2011 года нормотворческая деятельность Правительства РФ в области информационных технологий проходила под эгидой Концепции формирования в Российской Федерации Электронного Правительства (Распоряжение Правительства РФ от 06.05.2008 г. № 632-р).

Издаваемые Правительством РФ Распоряжения и Постановления были направлены на создание защищенной инфраструктуры, обеспечивающей взаимодействие органов государственной власти между собой (межведомственной сети обмена данными, защищенного межведомственного электронного документооборота), а также организацию предоставления государственных услуг в электронной форме (развитие систем доступа граждан к информации госорганов, определение требования к ИБ сайтов госорганов, предоставление государственных услуг с использованием Интернет.

ЭЛВИС-ПЛЮС

РАСПОРЯЖЕНИЕ ПРАВИТЕЛЬСТВА РФ № 632-р

Концепция формирования в РФ электронного правительства

Концепция предполагает необходимость:

- ✓ Использовать при оказании государственных услуг Интернет
- ✓ Определить нормативно-технические требования по ИБ
- ✓ Создать защищенную систему межведомственного ЭДО
- ✓ Создать единую межведомственную сеть обмена данными
- ✓ Использовать современные средства идентификации
- ✓ Использовать при взаимодействии электронную подпись
- ✓ Обеспечить конфиденциальность при оказании услуг
- ✓ Обеспечить юридическую значимость электронных сообщений

Все три составляющие ИБ: обеспечение целостности, доступности и конфиденциальности нашли отражение в Концепции.

ЭЛВИС-ПЛЮС

РАСПОРЯЖЕНИЕ ПРАВИТЕЛЬСТВА РФ № 1403-р

Технические требования к организации взаимодействия СМЭДО с ИС госорганов

Система межведомственного ЭДО обеспечивает защищенный обмен электронными сообщениями, в том числе, содержащими служебную тайну. Требования по ИБ включают:

- ✓ ОС типа Windows XP Professional Russian и Secure Pack Rus 1.0
- ✓ Применение антивирусного ПО типа Kaspersky Business Space Security
- ✓ Применение электронного замка типа Соболь-PCI (DS-1996)
- ✓ Применение сертифицированных СЗИ
- ✓ Обязательную аттестацию АРМ на которых размещены шлюзы

Требования по защите информации и мероприятия по их выполнению, а также конкретные средства защиты должны определяться и уточняться в зависимости от установленного класса защищенности на основании разрабатываемой модели угроз и действий нарушителя

Предусмотрено максимальное использование программно-технических средств, имеющихся в госорганах

ЭЛВИС-ПЛЮС

РАСПОРЯЖЕНИЕ ПРАВИТЕЛЬСТВА РФ № 654-р

О базовых государственных информационных ресурсах

Базовые государственные ИР – ресурсы, содержащие идентификаторы, позволяющие получить сведения о лице и (или) об объекте, необходимые для предоставления государственных услуг. Обладатели Базовых ИР обеспечивают:

- ✓ Непрерывный доступ через СМВЭВ получения идентификаторов
- ✓ Достоверность, полноту и актуальность предоставляемых сведений
- ✓ Размещение на сайтах информацию о базовых ресурсах
- ✓ Внесение в базовые ресурсы идентификаторов, используемых при предоставлении государственных или муниципальных услуг

Использование при оказании государственных услуг идентификаторов позволяет обезличивать ПДн субъектов. Такими идентификаторами служат СНИЛС (для граждан) и ИНН (для организаций).

Это Распоряжение направлено на обезличивание сведений при оказании государственных услуг.

ЭЛВИС-ПЛЮС

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ № 424

Об особенностях подключения государственных ИС к ИТКС

При подключении информационных систем общего пользования (ИСОП) госорганов, к ИТКС, доступ к которым не ограничен определенным кругом лиц, оператор обязан обеспечить (п.1):

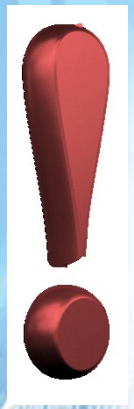
- ✓ защиту информации от уничтожения, изменения, блокирования доступа
- ✓ постоянный контроль возможности доступа неограниченного круга лиц
- ✓ восстановление информации, измененной или уничтоженной из-за НСД
- ✓ использовать СЗИ, прошедших оценку соответствия (в том числе в установленных случаях сертификацию)

Требования по защите информации, содержащейся в информационных системах общего пользования разрабатывают ФСБ России и ФСТЭК России в пределах своей компетенции. (п.3)

Системы общего пользования – федеральные государственные ИС, используемые для реализации полномочий госорганов и содержащие сведения, обязательные для размещения в сети Интернет.

ЭЛВИС-ПЛЮС

ВАЖНОЕ ЗАМЕЧАНИЕ



Операторы связи обязаны обеспечивать информационную безопасность при подключении информационных систем общего пользования к информационно-телекоммуникационным сетям.

Узаконено разделение ответственности в обеспечении защиты информации между оператором ИС и оператором связи.

ЭЛВИС-ПЛЮС

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ № 953

Об обеспечении доступа к информации о деятельности Правительства РФ и ФОИВ

Постановление определяет требования к технологическим, программным и лингвистическим средствам обеспечения пользования официальным сайтом Правительства РФ в сети Интернет. Такие средства должны обеспечивать:

- ✓ доступ пользователей к информации на основе общедоступного ПО
- ✓ ведение электронных журналов учета операций
- ✓ ежедневное копирование информации на резервный носитель
- ✓ восстановление информации после неправомерных действий с ней
- ✓ защиту ИР от уничтожения, модификации и блокирования доступа к ним
- ✓ защиту от неправомерных действий в отношении размещенных ИР
- ✓ хранение информации, размещенной на сайте, в течение 5 лет

Впервые говорится о необходимости защиты открытой общедоступной информации. Основные направления: обеспечение целостности и доступности информации

ЭЛВИС-ПЛЮС

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РФ № 697

О единой системе межведомственного электронного взаимодействия (СМЭВ)

СМЭВ создается для информационного взаимодействия при предоставлении государственных услуг и исполнении государственных функций в электронной форме и обеспечивает:

- ✓ доступ к электронным сервисам взаимодействующих ИС госорганов
- ✓ фиксацию времени передачи, целостности и подлинности сообщений
- ✓ централизованные БД и классификаторы для взаимодействующих ИС
- ✓ защиту информации от НСД, искажения и блокирования

Особенности использования СМЭВ и подключения к ней ИС госорганов и организаций определяются соглашением с Минкомсвязи России

Технические требования к взаимодействию ИС в единой СМЭВ определяются Минкомсвязи России

ЭЛВИС-ПЛЮС

НОВЫЕ ДОКУМЕНТЫ ГОСУДАРСТВЕННЫХ ОРГАНОВ

за период 2007-2011 годы

СОВМЕСТНЫЙ 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»

ЭЛВИС-ПЛЮС

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

Требования по защите информации, содержащейся в ИСОП

В ИСОП должны использоваться средства (п.17):

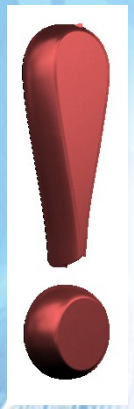
- ✓ защиты от неправомерных действий (СЗИ, СКЗИ, ЭП)
- ✓ обнаружения вирусов и вредоносного ПО
- ✓ контроля доступа к информации
- ✓ обнаружения компьютерных атак
- ✓ фильтрации и блокирования сетевого трафика, в том числе МЭ
- ✓ записи и хранения сетевого трафика при обращении к ИР ИСОП
- ✓ защиты от воздействий на технические средства и ПО ИСОП
- ✓ резервирования технических и программных средств ИСОП
- ✓ дублирования носителей и массивов информации
- ✓ мониторинга защищенности ИСОП

Введение в эксплуатацию ИСОП осуществляется только после направления оператором уведомления о ее готовности к эксплуатации и соответствии настоящим Требованиям.

Защиту информации в ИСОП обеспечивает оператор (п.10).

ЭЛВИС-ПЛЮС

ВАЖНЫЕ ЗАМЕЧАНИЯ



Используемые в ИСОП средства:

должны пройти обязательную сертификацию, при этом:

- **для ИСОП I класса – в ФСБ России**
- **для ИСОП II класса – в ФСБ и ФСТЭК по компетенции**

Уведомления о готовности к эксплуатации и соответствии ИСОП требованиям направляются:

- **для ИСОП I класса – в ФСБ России**
- **для ИСОП II класса – во ФСТЭК России**

К I классу относятся ИСОП в случае, если нарушение целостности и доступности информации, содержащейся в них, может привести к возникновению угроз безопасности РФ.

ЭЛВИС-ПЛЮС

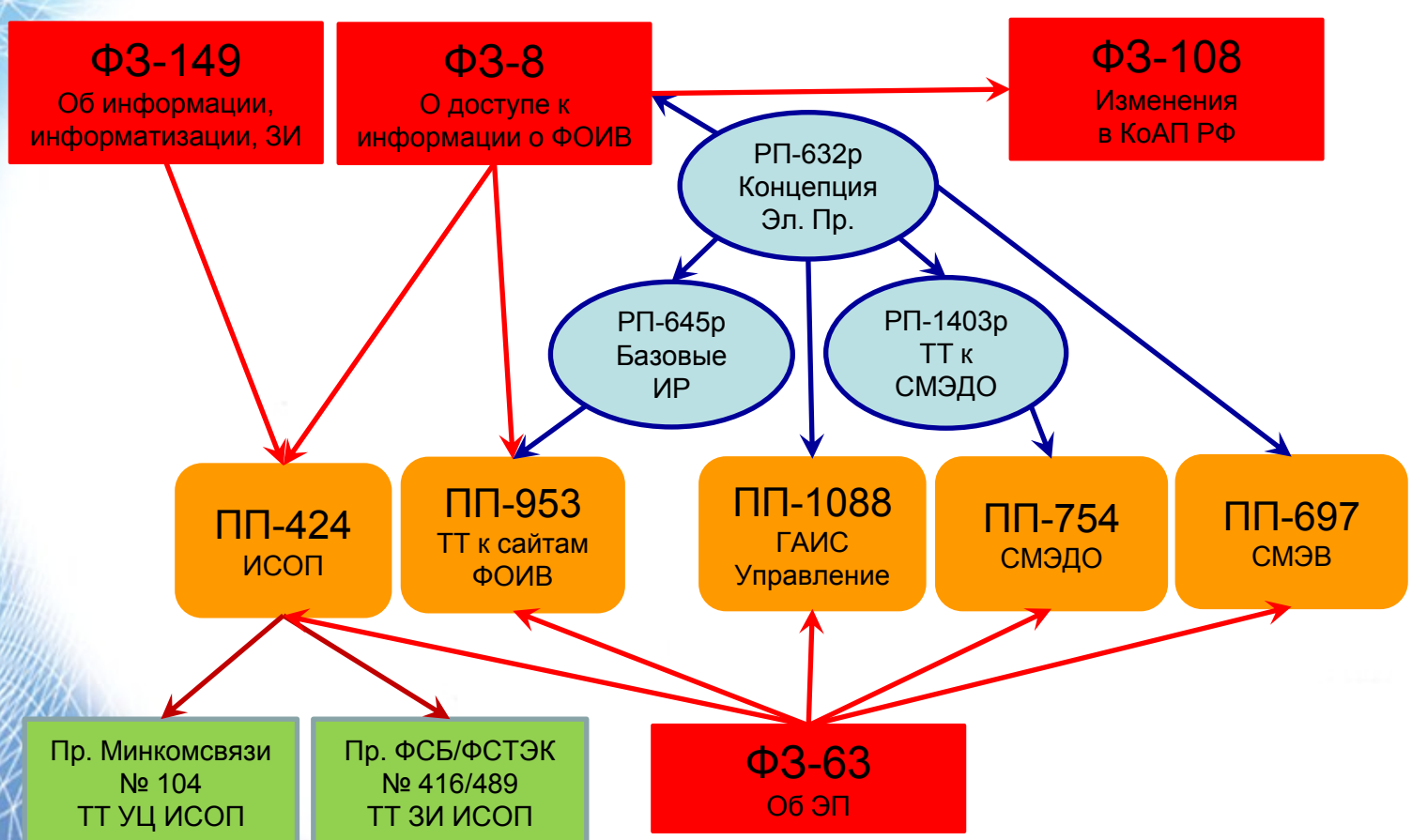
ОБОБЩЕННАЯ СТРУКТУРА

нормативно-правовой базы по информационной безопасности за период 2007-2011 годы

ЭЛВИС-ПЛЮС

СТРУКТУРА НОРМАТИВНОЙ БАЗЫ

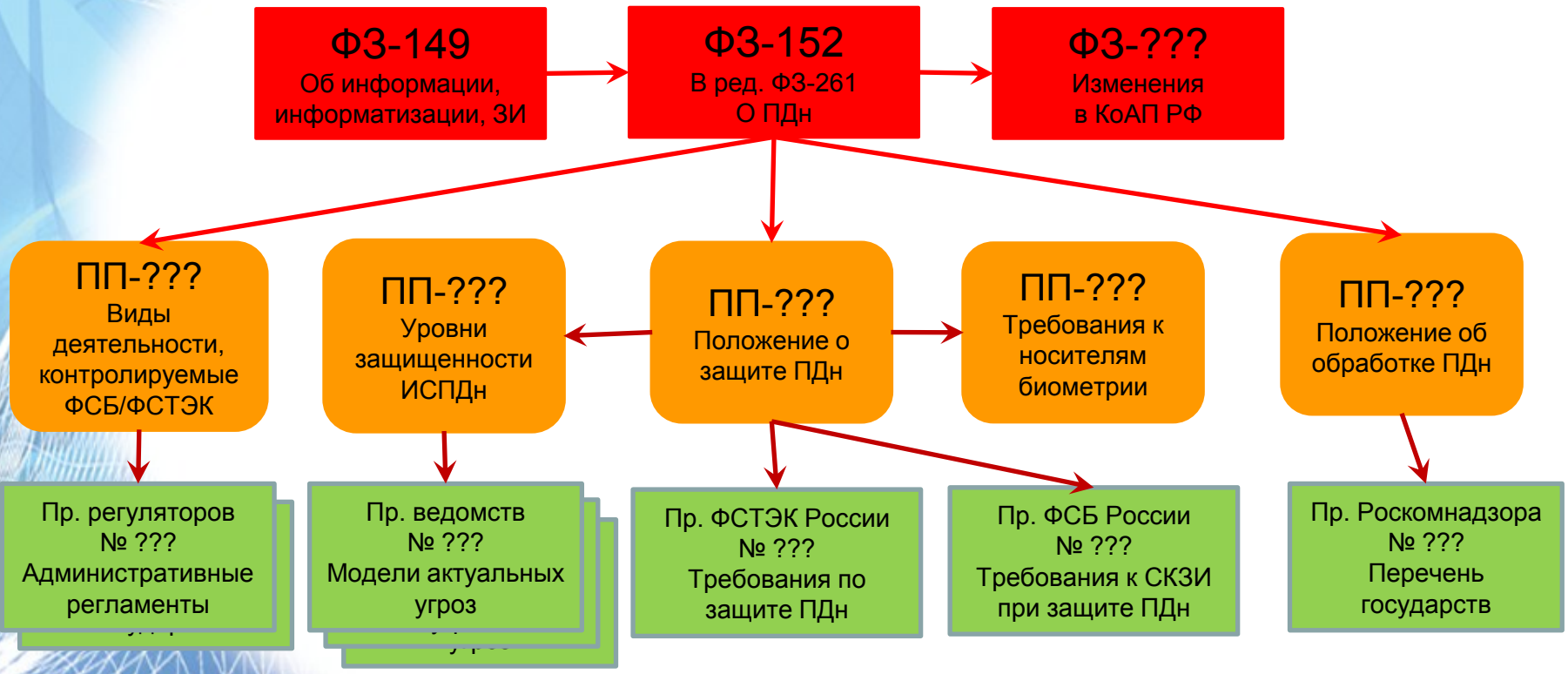
Вопросы электронного правительства и госуслуг



ЭЛВИС-ПЛЮС

СТРУКТУРА НОРМАТИВНОЙ БАЗЫ

Вопросы обработки персональных данных (предположение)



ЭЛВИС-ПЛЮС

Спасибо за внимание !

124460, Москва, Зеленоград,
Проезд 4806, д.5, стр. 23,
Тел. (495)276-0211,
e-mail: vsv@elvis.ru
http://www.elvis.ru