Обзор изменений в области персональных данных. Стало ли проще?

Николай Конопкин,
заместитель директора департамента
внедрения и консалтинга

НОВЫЕ И ОТМЕНЕННЫЕ ДОКУМЕНТЫ

Новые документы

- **Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных.** Приказ ФСТЭК России от 5.02.2010 №58 зарегистрирован в Минюсте России 19.02.2010 №16456
- **Решение ФСТЭК России от 5 марта 2010 г.** Утверждено первым заместителем директора ФСТЭК России

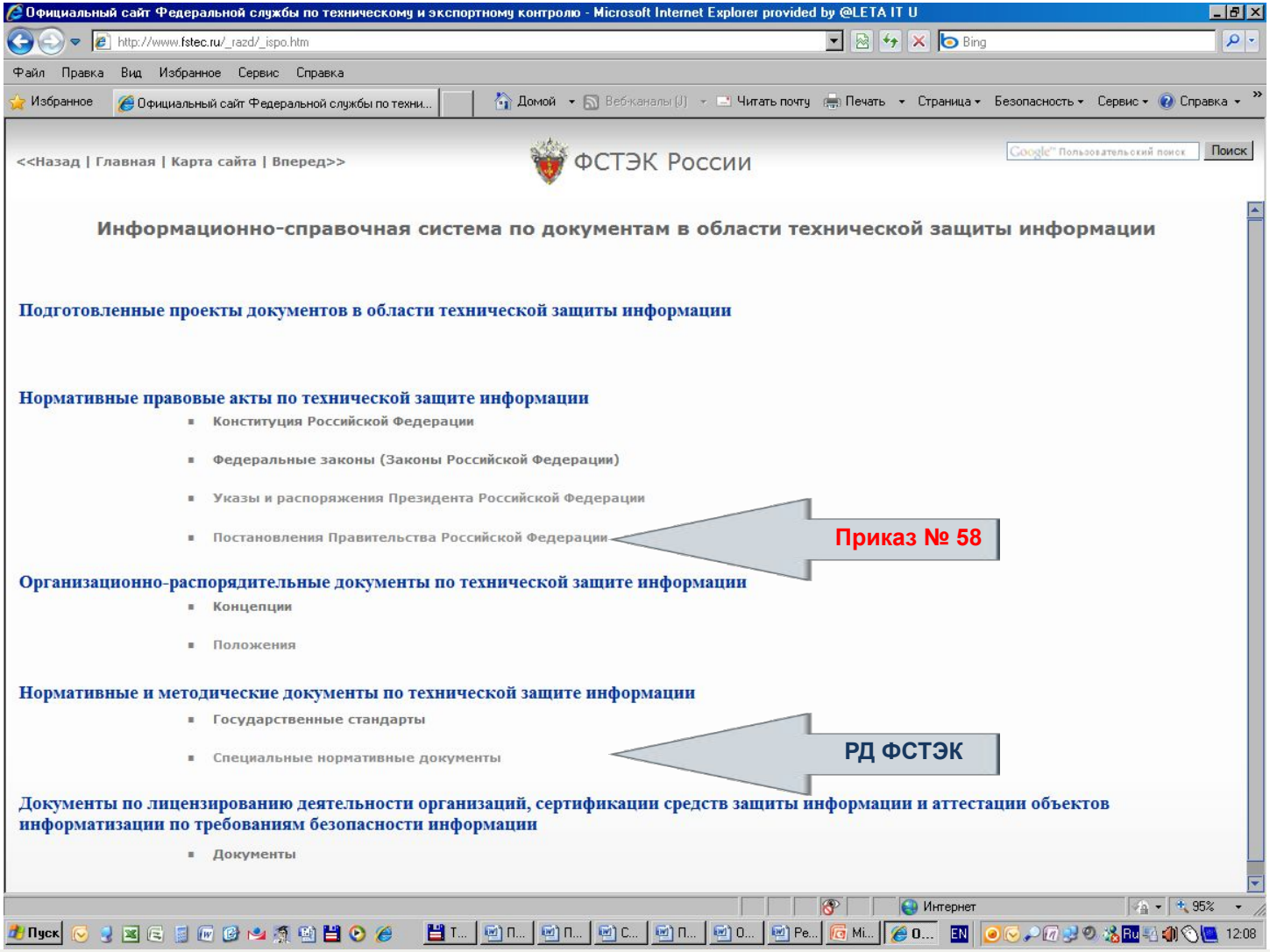
Отмененные документы

- **Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных,** утвержденные заместителем директора ФСТЭК России 15 февраля 2008 г.
- **Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных,** утвержденные заместителем директора ФСТЭК России 15 февраля 2008 г.

Не применять с 15 марта 2010 г.
для обеспечения безопасности персональных данных при их обработке
в информационных системах персональных данных

НОВОЕ МЕСТО ДОКУМЕНТОВ НА САЙТЕ ФСТЭК РОССИИ

http://www.fstec.ru/_razd/_ispo.htm



Новое в структуре документа

I. Общие положения

Основные способы защиты

См. п. 1.2:
К методам и способам защиты информации в информационных системах относятся:

- методы и способы защиты информации от несанкционированного доступа
- методы и способы защиты информации от утечки по техническим каналам

Помнить о целях защиты!

1.5. Выбранные и реализованные методы и способы защиты информации в информационной системе должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных при их обработке в информационных системах в составе создаваемой оператором (уполномоченным лицом) системы защиты персональных данных.

Новое в структуре методов и способов защиты… Но не в составе

II. Методы и способы защиты информации от несанкционированного доступа

Общие для всех ИСПДн

Пункт 2.1.:

- реализация разрешительной системы допуска ...;
- ограничение доступа пользователей в помещения… ;
- разграничение доступа …;
- регистрация действий ..., контроль …;
- учет и хранение съемных носителей информации ...;
- резервирование …, дублирование …;
- **использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия**;
- использование защищенных каналов связи;
- размещение технических средств … в пределах охраняемой территории;
- организация физической защиты …;
- предотвращение внедрения … вредоносных программ …

Пункт 2.2.:

Методы и способы защиты информации от несанкционированного доступа … в зависимости от класса информационной системы определяются оператором (уполномоченным лицом) **в соответствии с приложением к настоящему Положению**

Новое в структуре методов и способов защиты… Но не в составе

II. Методы и способы защиты информации от несанкционированного доступа

Дополнительные

2.1+
- 2.4. При взаимодействии ИСПДн с сетями международного информационного обмена (Интернет)
- 2.5. При подключении государственных информационных систем к Интернет

Указ 351

2.1&2.4+
- 2.6. При подключение ИСПДн к Интернет (сети связи общего пользования) с целью получения общедоступной информации
- 2.7. При удаленном доступе к ИСПДн через Интернет (сети связи общего пользования)

2.1&2.4+

2.1&2.4+
- 2.8. При межсетевом взаимодействии отдельных ИСПДн через Интернет (сети связи общего пользования)
- 2.9. При межсетевом взаимодействии отдельных ИСПДн разных операторов через Интернет (сети связи общего пользования)

2.1&2.4+

Новое в структуре методов и способов защиты… Но не в составе

II. Методы и способы защиты информации от несанкционированного доступа

Об антивирусной защите

2.3. В информационных системах, имеющих подключение к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования), или при функционировании которых предусмотрено использование съемных носителей информации, используются средства антивирусной защиты

О криптографии

2.10. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) применения технических средств

О межсетевых экранах

2.11. Подключение информационной системы к информационной системе другого класса или к информационно-телекоммуникационной сети международного информационного обмена (сети связи общего пользования) осуществляется с использованием межсетевых экранов

О сертификации

2.12. Программное обеспечение средств защиты информации, применяемых в информационных системах 1 класса, проходит контроль отсутствия недекларированных возможностей.
Необходимость проведения контроля отсутствия недекларированных возможностей программного обеспечения средств защиты информации, применяемых в информационных системах 2 и 3 классов, определяется оператором (уполномоченным лицом)

О главном

2.13. В зависимости от особенностей обработки персональных данных и структуры информационных систем могут разрабатываться и применяться другие методы защиты информации от несанкционированного доступа, **обеспечивающие нейтрализацию угроз безопасности персональных данных**.

Новое в структуре методов и способов защиты… Но не в составе

III. Методы и способы защиты информации от утечки по техническим каналам

- 3.1. Защита речевой информации и информации, представленной в виде информативных электрических сигналов и физических полей, осуществляется в случаях, когда … являются актуальными угрозы …, определенные на основе методических документов…
- 3.2. Для исключения утечки персональных данных за счет побочных электромагнитных излучений и наводок в информационных системах 1 класса могут применяться следующие методы и способы защиты информации…
- 3.3. В информационных системах 2 класса … используются средства вычислительной техники, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости…
- 3.4. При применении в информационных системах … голосового ввода … для информационной системы 1 класса реализуются методы и способы защиты акустической (речевой) информации
- 3.5. Размещение устройств … осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные

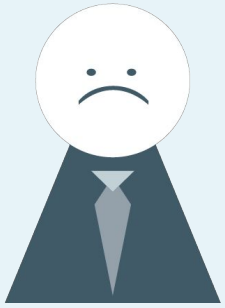
Приложение к Положению о методах и способах защиты информации в информационных системах персональных данных

МЕТОДЫ И СПОСОБЫ
ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА
В ЗАВИСИМОСТИ ОТ КЛАССА ИНФОРМАЦИОННОЙ СИСТЕМЫ

- В информационных системах 4 класса целесообразность их применения определяются оператором (уполномоченным лицом)
- ИСПДн 3 класса (однопользовательские, многопользовательские с равными и разными правами доступа):
  а) управление доступом
  б) регистрация и учет
  в) обеспечение целостности
- Межсетевое взаимодействие ИСПДн 3 класса
- Для ИСПДн 2 класса соответствуют ИСПДн 3 класса при соответствующих режимах и правах доступа пользователей
- Межсетевое взаимодействие ИСПДн 2 класса
- ИСПДн 1 класса (однопользовательские, многопользовательские с равными и разными правами доступа)
  а) управление доступом
  б) регистрация и учет
  в) обеспечение целостности
- Межсетевое взаимодействие ИСПДн 1 класса
- Требования к анализу защищенности, обнаружению вторжений и контролю отсутствия НДВ

Отрицательные плюсы и положительные минусы

- Устранение препятствий, связанных с согласованием в Минюсте
- Уменьшение объёма и улучшение структуры документа
- Снижение уровня требований к отдельным подсистемам защиты
- Повышение практической применимости документа
- Изъятие требований по аттестации и декларированию соответствия
- Отсутствие требований по применению сертифицированных средств защиты
- Изъятие требований по лицензированию деятельности



- Отсутствие внятного описания процесса классификации ИСПДн
- Возврат к дискуссии о классификации специальных ИСПДн
- Пересмотр хода и результатов проектов по созданию СЗПДн
- Изъятие требований по аттестации и декларированию соответствия
- Отсутствие требований по применению сертифицированных средств защиты
- Изъятие требований по лицензированию деятельности

Решение принимается на основании федерального законодательства, указов Президента Российской Федерации, постановлений Правительства и нормативно-правовых актов федеральных органов исполнительной власти

Отрицательные плюсы и положительные минусы

И тем не менее…

«Методы и способы…», раздел 2:

Межсетевые экраны, которые обеспечивают выполнение указанных выше функций, *[МЭ, применяемые в ИСПДн 3 класса]* применяются в распределенных информационных системах 2 и 1 классов при их разделении на отдельные части.

При разделении информационной системы при помощи межсетевых экранов на отдельные части системы для указанных частей системы может устанавливаться более низкий класс, чем для информационной системы в целом.

Вопросы уже возникают:

- ИСПДн 1 и 2 класса можно защищать с помощью МЭ 5 класса?

  Только при условии выполнения требований разделов 3 и 4 к МЭ ИСПДн 2 и 1 классов

- Можно присвоить отдельной части системы более низкий класс при наличии классификационных признаков ИСПДн более высокого класса?

  Только при наличии у выделенного сегмента классификационных признаков ИСПДн более низкого класса

Нельзя ли попроще?

Подсистема управления доступом

<table>
<tr><th rowspan="4">Меры и способы защиты</th><th colspan="9">Наличие требования для ИСПДн соответствующего класса (документы 2008 г. / документ 2010 г.)</th></tr>
<tr><th colspan="3" rowspan="2">Однопользовательские</th><th colspan="6">Многопользовательские</th></tr>
<tr><th colspan="3">С равными правами доступа</th><th colspan="3">С разными правами доступа</th></tr>
<tr><th>3 кл.</th><th>2 кл.</th><th>1 кл.</th><th>3 кл.</th><th>2 кл.</th><th>1 кл.</th><th>3 кл.</th><th>2 кл.</th><th>1 кл.</th></tr>
<tr><td>Идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов</td><td colspan="3">Да</td><td colspan="3">Нет</td><td colspan="3">Да</td></tr>
<tr><td colspan="9">Требования идентичны</td></tr>
<tr><td>Идентификация и проверка подлинности пользователя при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов</td><td colspan="3">Нет</td><td colspan="3">Да</td><td colspan="3">Нет</td></tr>
<tr><td colspan="9">Требования идентичны</td></tr>
<tr><td>Осуществление идентификации терминалов, технических средств обработки ПДн, узлов ИСПДн, каналов связи, внешних устройств ИСПДн по их логическим адресам (номерам)</td><td colspan="4">Нет</td><td colspan="2">Да</td><td colspan="3">Нет</td></tr>
<tr><td colspan="9">Ранее действовало для ИСПДн 1 и 2 классов с равными правами доступа.
Теперь требование с ИСПДн 2 класса снято. Действует для ИСПДн 1 класса как с равными, так и с разными правами доступа.</td></tr>
<tr><td>Осуществление идентификации программ, томов, каталогов, файлов, записей, полей записей по именам</td><td colspan="4">Нет</td><td colspan="2">Да</td><td>Нет</td><td colspan="2">Да</td></tr>
<tr><td colspan="9">Ранее действовало для всех многопользовательских ИСПДн 1 и 2 классов.
Теперь требование с ИСПДн 2 класса снято</td></tr>
<tr><td>Осуществление контроля доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа</td><td colspan="8">Нет</td><td>Да</td></tr>
<tr><td colspan="9">Ранее действовало для многопользовательских ИСПДн 1 и 2 классов с разными правами доступа.
Теперь требование с ИСПДн 2 класса снято</td></tr>
</table>

ОБЯЗАТЕЛЬНО ЛИ ПРОВОДИТЬ ОЦЕНКУ СООТВЕТСТВИЯ?

СТР-К: Объекты информатизации должны быть аттестованы по требованиям безопасности информации в соответствии с нормативными документами Гостехкомиссии России … (п.2.17);

ГОСТ Р 51583-2000: Применение автоматизированной системы в защищенном исполнении для обработки защищаемой информации разрешается только после ее аттестации на соответствие требованиям безопасности информации (п.5.3);

«Основные мероприятия»: К1, К2 - сертификация (аттестация); К3 - декларирование соответствия (п. 3.11).

- Формально исключены требования к соответствию вида оценки классу ИСПДн, включая аттестацию и декларирование соответствия
- **Реализованные методы и способы защиты должны обеспечить нейтрализацию угроз!!!**

Что говорит ФЗ «О техническом регулировании»?

Федеральный закон от 27 декабря 2002 г. № 184-ФЗ

Ст. 7, часть 3: Оценка соответствия проводится в формах

- государственного контроля (надзора),
- аккредитации,
- испытания,
- регистрации,
- подтверждения соответствия,
- приемки и ввода в эксплуатацию,

Ст. 23, часть 1: Обязательное подтверждение соответствия проводится только в случаях, установленных соответствующим техническим регламентом, и **исключительно на соответствие требованиям технического регламента**

Ст. 5, часть 1: В случае отсутствия требований технических регламентов в отношении… продукции (работ, услуг), используемой в целях защиты сведений … относимых к … информации ограниченного доступа, … обязательными являются требования …, установленные федеральными органами исполнительной власти, являющимися в пределах своей компетенции государственными заказчиками оборонного заказа, и (или) государственным контрактом.

ОБЯЗАТЕЛЬНО ЛИ ПРОВОДИТЬ ОЦЕНКУ СООТВЕТСТВИЯ?

Что говорят действующие нормы?

- Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор или уполномоченное лицо — Постановление №781-2007 г., п. 10
- Мероприятия по обеспечению безопасности ПДн в ИСПДн включают в себя… проверку готовности СЗИ … **с составлением заключений** — Постановление №781-2007 г., п. 12
- Результаты оценки соответствия оцениваются в ходе экспертизы, осуществляемой ФСТЭК России и ФСБ России в пределах их полномочий — Постановление №781-2007 г., п. 18

Выводы:

- Аттестаты на ИСПДн могут не выдаваться
- Наличия Заключения с выводом о выполнении установленных требований достаточно для начала обработки ПДн
- Различия в процедурах оценки соответствия ИСПДн различных классов отсутствуют
- Оператор самостоятельно или с привлечением уполномоченного лица обязан проводить оценку соответствия как обязательное мероприятие по обеспечению безопасности ПДн

Ничего принципиально не изменилось!!!

ОБЯЗАТЕЛЬНО ЛИ ПРИМЕНЯТЬ СЕРТИФИЦИРОВАННЫЕ СРЕДСТВА ЗАЩИТЫ?

СТР-К: Для защиты конфиденциальной информации используются **сертифицированные** по требованиям безопасности информации технические средства защиты информации (п.2.16).

«Основные мероприятия…»: СЗИ, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая **сертификацию** на соответствие требованиям по безопасности информации (п. 3.3).

- Формально исключены требования по применению сертифицированных средств защиты
- **Реализованные методы и способы защиты должны обеспечить нейтрализацию угроз!!!**

Что говорит ФЗ «О техническом регулировании»?

Федеральный закон от 27 декабря 2002 г. № 184-ФЗ

Ст. 2, абз. 19: **Сертификация** - форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов или условиям договоров.

Ст. 20, ч. 3: **Обязательное** подтверждение соответствия осуществляется в формах:

- принятия декларации о соответствии (декларирование соответствия);
- обязательной сертификации.

Исключительно на соответствие требованиям технического регламента!!!
(ст. 23, ч.1)

Ст. 5, часть 1!!!

ОБЯЗАТЕЛЬНО ЛИ ПРИМЕНЯТЬ СЕРТИФИЦИРОВАННЫЕ СРЕДСТВА ЗАЩИТЫ?

Что говорят действующие нормы?

- Средства защиты информации, применяемые в ИС, в установленном порядке проходят процедуру оценки соответствия — Постановление №781-2007 г., п. 5
- Методы и способы защиты информации от НСД: … использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия… — «Положение о методах…», п. 2.1
- Программное обеспечение средств защиты информации, применяемых в информационных системах 1 класса, проходит контроль отсутствия НДВ — «Положение о методах…», п. 2.12
- Для информационных систем 1 класса применяется ПО СЗИ, соответствующее 4 уровню контроля отсутствия НДВ — «Методы и способы…», п. 7

Выводы:

- Основанием для обязательной сертификации является ФЗ «О техническом регулировании», согласно которому в отсутствие принятого технического регламента ФСТЭК России правомочна устанавливать соответствующие требования
- В новом Положении напрямую говорится лишь о сертификации на соответствие 4 уровню контроля отсутствия НДВ средств защиты информации, используемых в ИСПДн 1 класса
- Прочие средства защиты должны также проходить процедуру оценки соответствия, одной из форм которой является сертификация («на ТУ»)

Ничего принципиально не изменилось!!!

ОБЯЗАТЕЛЬНО ЛИ ПОЛУЧАТЬ ЛИЦЕНЗИИ?

«Основные мероприятия…»: … Операторы ИСПДн при проведении мероприятий по обеспечению безопасности ПДн (конфиденциальной информации) при их обработке в ИСПДн 1,2 и 3 (распределенные системы) классов должны получить лицензию (п. 3.14).

- Формально исключены требования по получению лицензий ФСТЭК России
- Почему аналогичные нормы никогда не включались в методические документы ФСБ?

Облегчение?
- Не надо иметь лицензии никому?

Ужесточение!
- Лицензии должны получать все!

Федеральный закон от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности»

Статья 4. Критерии определения лицензируемых видов деятельности
К лицензируемым видам деятельности относятся виды деятельности, осуществление которых может повлечь за собой нанесение ущерба правам, законным интересам, здоровью граждан, обороне и безопасности государства, культурному наследию народов Российской Федерации и регулирование которых не может осуществляться иными методами, кроме как лицензированием

Статья 17. Перечень видов деятельности, на осуществление которых требуются лицензии
ч. 1: Лицензированию подлежат следующие виды деятельности:

- ... деятельность по техническому обслуживанию шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации;
- разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем …
- деятельность по технической защите конфиденциальной информации…

ОБЯЗАТЕЛЬНО ЛИ ПОЛУЧАТЬ ЛИЦЕНЗИИ?

Лицензирование в системе ФСТЭК России

Постановление Правительства РФ от 15 августа 2006 г. № 504
«О лицензировании деятельности по технической защите конфиденциальной информации»

Под **технической защитой конфиденциальной информации** понимается комплекс мероприятий и **(или) услуг** по ее защите от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней (пункт 2)

Лицензирование в системе ФСБ России

Постановление Правительства РФ от 29 декабря 2007 г. N 957
"Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами"

- Положение о лицензировании деятельности по распространению шифровальных (криптографических) средств;
- Положение о лицензировании деятельности по техническому обслуживанию шифровальных (криптографических) средств;
- Положение о лицензировании предоставления услуг в области шифрования информации;
- Положение о лицензировании разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

Выводы:

- ФСТЭК России имеет право требовать получения лицензий на деятельность по ТЗКИ не только от организаций, оказывающих услуги, но и от операторов, **проводящих мероприятия** по защите информации от НСД в собственных целях
- Лицензионные требования и условия для операторов ПДн чрезмерно завышены

Ничего принципиально не изменилось!!!

КОНТАКТНАЯ ИНФОРМАЦИЯ

Конопкин Николай Иванович
Заместитель директора департамента внедрения и консалтинга
Моб. тел.: +7 (903) 194-3300
e-mail: NKonopkin@leta.ru

LETA IT-company
109129, Россия, Москва, ул. 8-я Текстильщиков, д.11, стр. 2
Тел./факс: +7 (495) 921-1410
Единая служба сервисной поддержки: + 7 (495) 921-1410
www.leta.ru