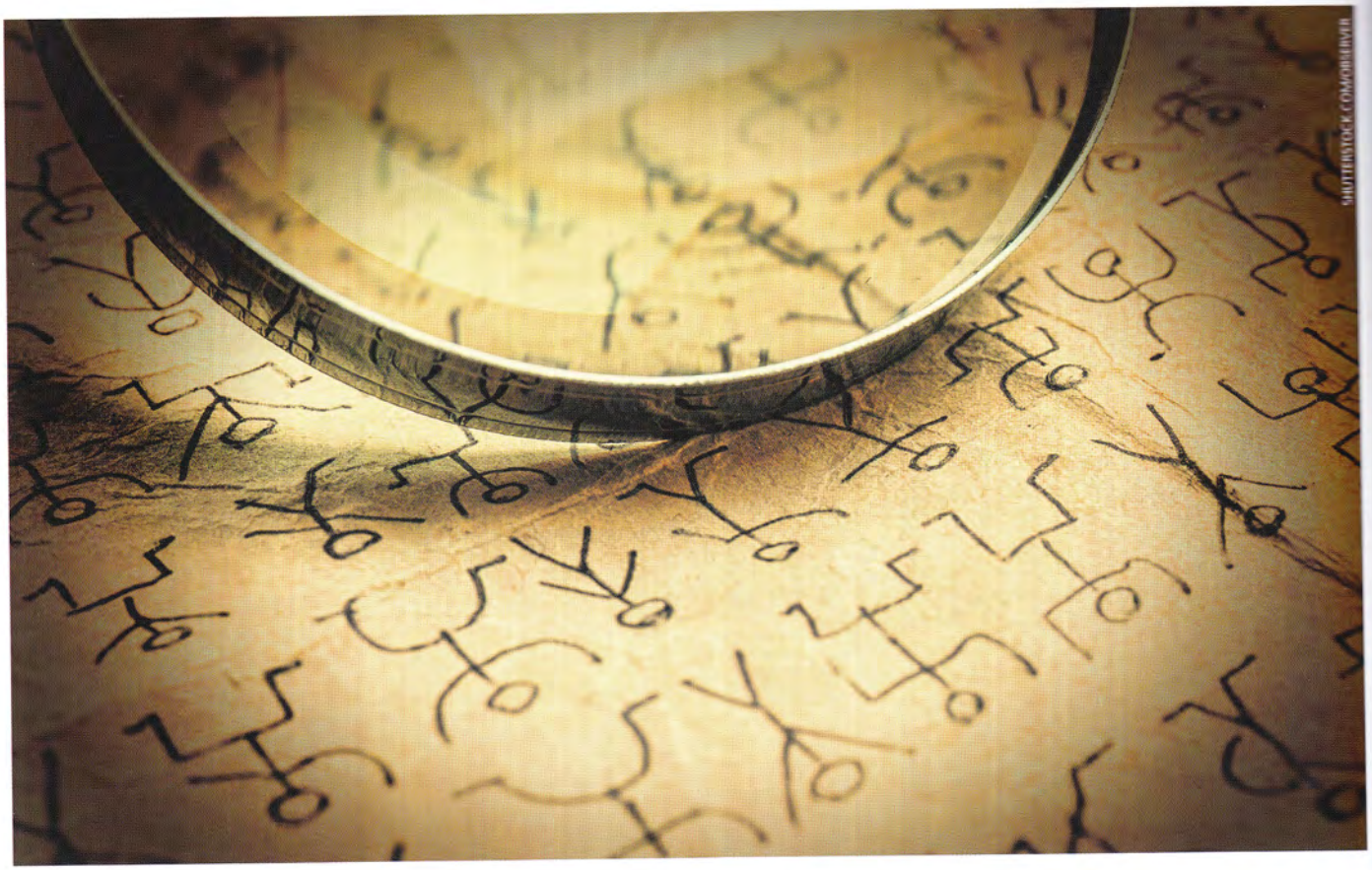
ЕСТЬ РЕШЕНИЕ

Сертификация СКЗИ – да / нет / может быть



Вторая половина июля 2016 года прошла в обсуждении закона Яровой и связанного с ним извещения (комментария) ФСБ России «по вопросу использования несертифицированных средств кодирования (шифрования) при передаче сообщений в информационно-телекоммуникационной сети “Интернет”».

Если Вас по счастливой случайности обсуждение данного вопроса обошло стороной, то кратко изложу проблему, касающуюся использования СКЗИ. Мы будем обсуждать только эту часть, не касаясь других аспектов закона.

Событие первое

В КОАП внесены изменения, в том числе в ч. 1 ст. 13.6 КОАП. Сейчас указанная статья выглядит следующим образом:

«Использование в сетях связи… несертифицированных средств кодирования (шифрования) при передаче сообщений в… сети "Интернет", если законодательством предусмотрена их обязательная сертификация, – влечет наложение административного штрафа … на юридических лиц – от шестидесяти тысяч до трехсот тысяч рублей с конфискацией несертифицированных средств связи либо без таковой.»

Штраф в 300 000 руб., а также потенциальная возможность конфискации средств связи является достаточным основанием обратить внимание на указанную статью и разобраться, насколько это касается «моей» организации. Сама мысль о возможной конфискации средств шифрования (криптошлюза), которые обеспечи-

ВЛАДИМИР ЖУРАВЛЕВ,
заведующий кафедрой юридических проблем защиты конфиденциальной информации
Учебного центра «Информзащита»

вают взаимодействие с филиалами и сторонними организациями, огорчает значительно сильней штрафа.

Соответственно возникает вопрос: в каких случаях необходимо использовать сертифицированные средства защиты?

Эксперты устроили жаркий спор и перебрали почти все виды тайн, начиная от фаворита – персональных данных, заканчивая банковской и даже коммерческой тайной, разве что тайну исповеди не упоминали.

Событие второе

ФСБ России опубликовал на своем сайте разъяснения, в каких случаях требуется использовать сертифицированные средства защиты. Действующую версию ответа можно посмотреть (следует отметить, что это уже вторая версия извещения, про первую поговорим ниже).

В заключительном абзаце извещения отражена главная мысль:

«Обязательной сертификации средств кодирования (шифрования) при передаче сообщений в информационно-телекоммуникационной сети Интернет, массово применяемых для защиты сведений, не составляющих государственную тайну, в том числе в абонентских устройствах и базовых станциях мобильной связи, компьютерах, оборудовании информационно-телекоммуникационной сети Интернет, на соответствие требованиям по безопасности информации не требуется».

Событие третье

Специалисты ИБ и т. п. устроили «холивар» на тему как трактовать данное заявление.

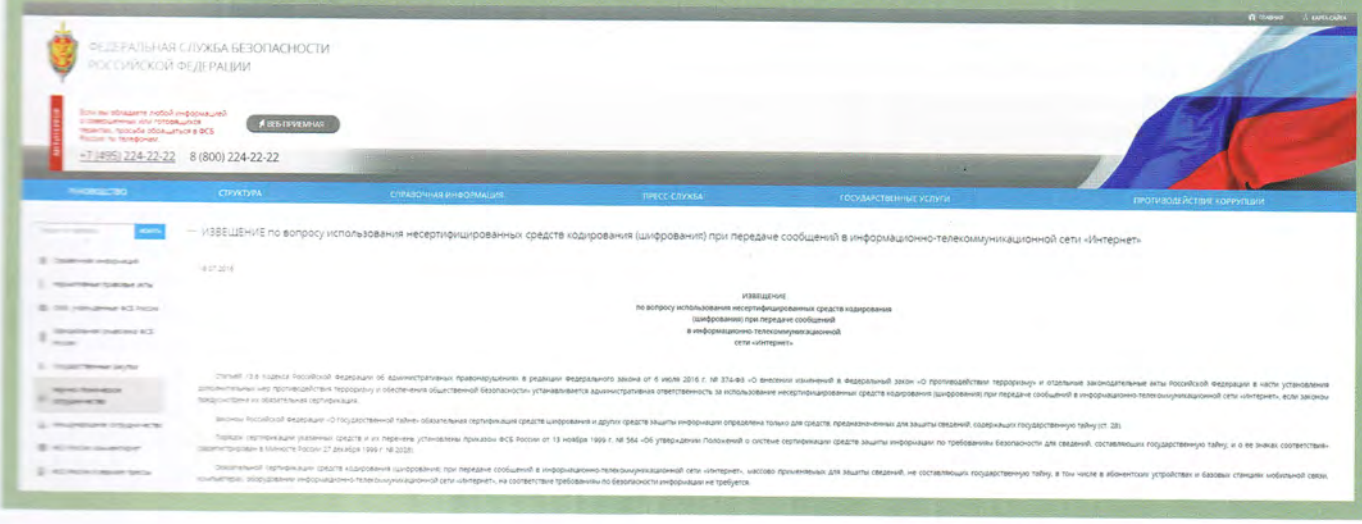
Условно можно выделить несколько вариантов трактовки извещения: «Оптимистический» и «Пессимистические».

- Оптимисты. ФСБ России прямо указала, что сертификация средств шифрования (кодирования) необходима только для защиты государственной тайны. Во всех остальных случаях сертификация не требуется. Остальное домыслы. Версия простая, понятная и выгодная для бизнеса.
- Пессимисты. Тут можно выделить несколько вариантов обоснований.

а. В ФСБ России забыли о другом законодательстве, том числе о своем Приказе от 10 июля 2014 года № 378 *«Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Пра-*

Эксперты устроили жаркий спор и перебрали почти все виды тайн, начиная от фаворита – персональных данных, заканчивая банковской и даже коммерческой тайной, разве что тайну исповеди не упоминали

ФСБ России опубликовал на своем сайте разъяснения (http://www.fsb.ru/fsb/science/single.htm%21id%3D10437738%40fsbResearchart.html)



вительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Для большей ясности следует отметить, что в первоначальной версии «разъяснений» второй абзац звучал немного по-другому:

«Законодательством Российской Федерации обязательная сертификация средств шифрования и других средств защиты информации определена только для средств, предназначенных для защиты сведений, содержащих государственную тайну (статья 28 Закона Российской Федерации "О государственной тайне")».

Разъяснения первоначально охватывали все законодательство, а не только Федеральный закон «О государственной тайне».

Позиция данной группы пессимистов была основана на том, что если в других Федеральных законах и не сказано напрямую о необходимости сертификации, то в выпущенных в исполнение этих ФЗ нормативных актах такая обязанность закреплена.

Самым простым примером для рассмотрения является ФЗ № 152 «О персональных данных».

В указанном ФЗ нет упоминаний об обязательной сертификации, однако есть ст. 19 ч. 2 п. 3, в которой сказано:

Самым простым примером для рассмотрения является ФЗ № 152 «О персональных данных»

П.3 Ч.2 СТ.19 ФЗ № 152 «О ПЕРСОНАЛЬНЫХ ДАННЫХ»
«Обеспечение безопасности персональных данных достигается, в частности:
3) Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации»

ПОСТАНОВЛЕНИИ ПРАВИТЕЛЬСТВА 1119
«ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ»
п.13 ч. «г»
«Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз»

ПРИКАЗ ФСБ РОССИИ ОТ 10.07.2014 № 378 П.9. Ч «В»
Выполнение требования (указанного выше, - примечание автора) достигается путем:
«использования для обеспечения требуемого уровня защищенности персональных данных при их обработке в информационной системе СКЗИ класса КС1 и выше»

«Обеспечение безопасности персональных данных достигается, в частности:

- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации»;

Аналогичное требование есть и в Постановлении правительства 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и в Приказе № 378 ФСБ России от 10.07.2014 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» сказано, что для выполнения указанного требования необходимо использовать СКЗИ класса КС1 и выше (п.9 ч. «в»). Таким образом, получается, что для исполнения требований ФЗ № 152 «О персональных данных» необходимо использовать сертифицированные СКЗИ.

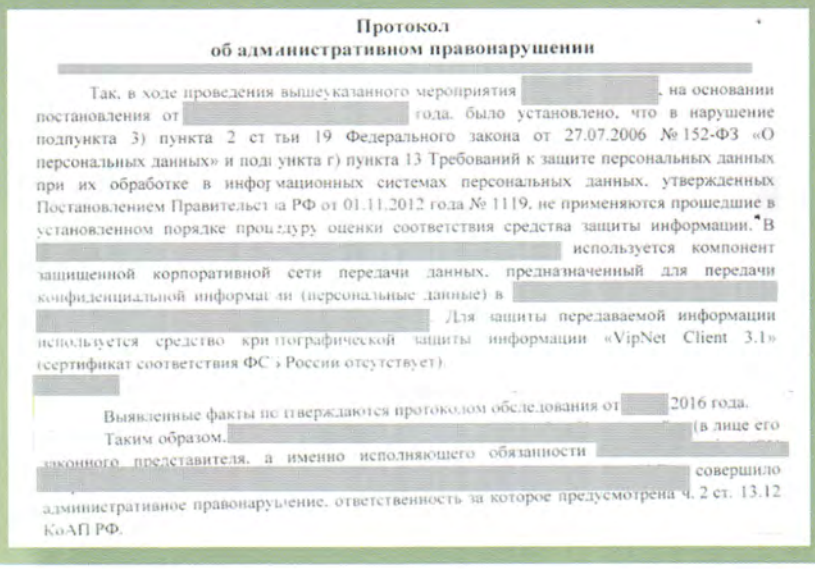
b. Дела говорят громче слов (Сложившаяся практика важнее комментария). При проверках ФСБ России отсутствие сертифицированных СКЗИ при защите ПДн уже фактически трактуется как нарушение.

Несколько примеров из блога Сергея Борисова: http://sborisov.blogspot.ru/2016/07/blog-post_20.html

Использование СКЗИ без сертификата ФСБ трактуется как ч. 2 ст. 13.12 КОАП РФ *«Использование несертифицированных … средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну)».*

Второй пример еще веселее. Работа с СКЗИ с истекшим сроком дей-

Первый пример из блога Сергея Борисова



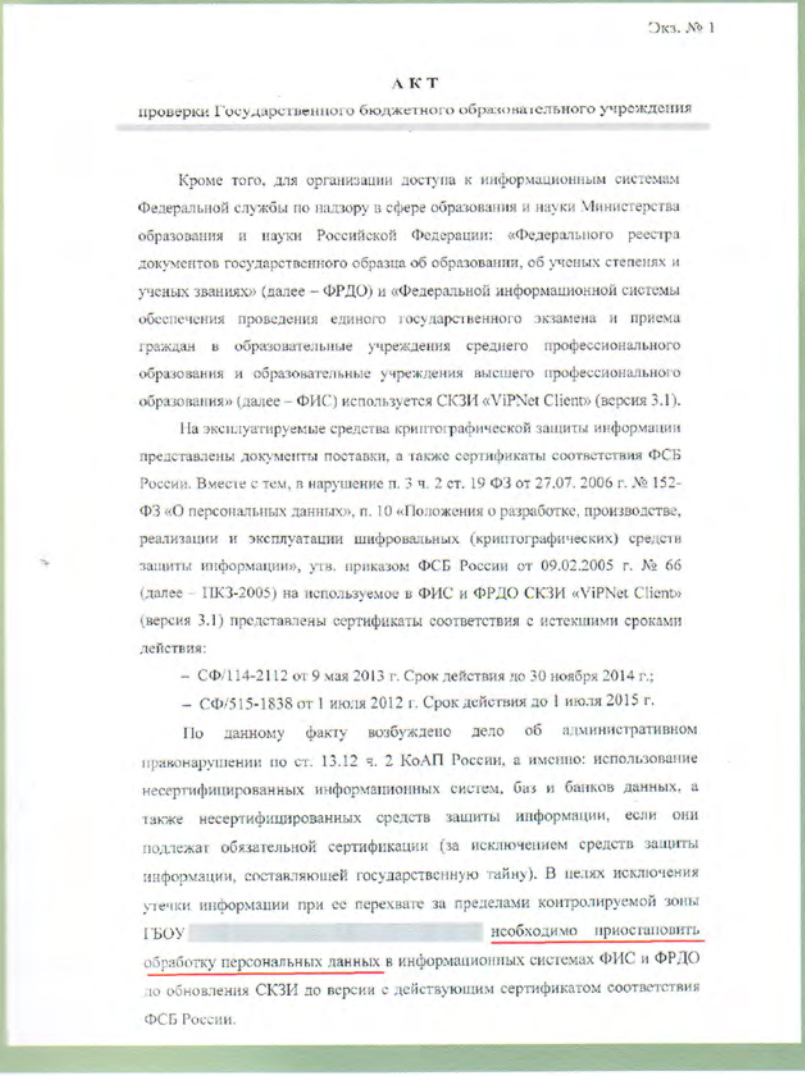
Протокол
об административном правонарушении

Так, в ходе проведения вышеуказанного мероприятия [redacted], на основании постановления от [redacted] года, было установлено, что в нарушение подпункта 3) пункта 2 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и подпункта г) пункта 13 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 года № 1119, не применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации. В [redacted] используется компонент защищенной корпоративной сети передачи данных, предназначенный для передачи конфиденциальной информации (персональные данные) в [redacted]. Для защиты передаваемой информации используется средство криптографической защиты информации «VipNet Client 3.1» (сертификат соответствия ФСБ России отсутствует).

Выявленные факты подтверждаются протоколом обследования от [redacted] 2016 года.

Таким образом, [redacted] (в лице его законного представителя, а именно исполняющего обязанности [redacted]) совершило административное правонарушение, ответственность за которое предусмотрена ч. 2 ст. 13.12 КоАП РФ.

Второй пример из блога Сергея Борисова



Экз. № 1

АКТ

проверки Государственного бюджетного образовательного учреждения

Кроме того, для организации доступа к информационным системам Федеральной службы по надзору в сфере образования и науки Министерства образования и науки Российской Федерации: «Федерального реестра документов государственного образца об образовании, об ученых степенях и ученых званиях» (далее – ФРДО) и «Федеральной информационной системы обеспечения проведения единого государственного экзамена и приема граждан в образовательные учреждения среднего профессионального образования и образовательные учреждения высшего профессионального образования» (далее – ФИС) используется СКЗИ «ViPNet Client» (версия 3.1).

На эксплуатируемые средства криптографической защиты информации представлены документы поставки, а также сертификаты соответствия ФСБ России. Вместе с тем, в нарушение п. 3 ч. 2 ст. 19 ФЗ от 27.07. 2006 г. № 152-ФЗ «О персональных данных», п. 10 «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утв. приказом ФСБ России от 09.02.2005 г. № 66 (далее – ПКЗ-2005) на используемое в ФИС и ФРДО СКЗИ «ViPNet Client» (версия 3.1) представлены сертификаты соответствия с истекшими сроками действия:

– СФ/114-2112 от 9 мая 2013 г. Срок действия до 30 ноября 2014 г.;
– СФ/515-1838 от 1 июля 2012 г. Срок действия до 1 июля 2015 г.

По данному факту возбуждено дело об административном правонарушении по ст. 13.12 ч. 2 КоАП России, а именно: использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну). В целях исключения утечки информации при ее перехвате за пределами контролируемой зоны ГБОУ [redacted] необходимо приостановить обработку персональных данных в информационных системах ФИС и ФРДО до обновления СКЗИ до версии с действующим сертификатом соответствия ФСБ России.

ствия сертификата трактуется также по ст. 13.12 ч. 2 КОАП РФ, а вот последствия интереснее, тут речь идет не о банальном штрафе даже в 300 000 руб. *«В целях исключения утечки информации при ее перехвате за приделами контролируемой зоны… необходимо приостановить обработку персональных данных …до обновления до версии с действующим сертификатом ФСБ России».*

Обратите внимание, что речь идет об образовательном учреждении. Если это не Академия ФСБ России/МВД/Министерства обороны, то я слабо представляю себе реального нарушителя, который будет перехватывать ПДн при их передаче по зашифрованному каналу. Намного привлекательнее «слушать трафик, передаваемый при заказе авиа/жд билетов» по «https:».

с. «Нео, ложки нет!» (Матрица). В ночь на 22 июля 2016 г. в разъяснениях ФСБ (по указанному выше адресу) произошли изменения. Поменяли всего одно слово, (об этом было указано в начале статьи) и вместо

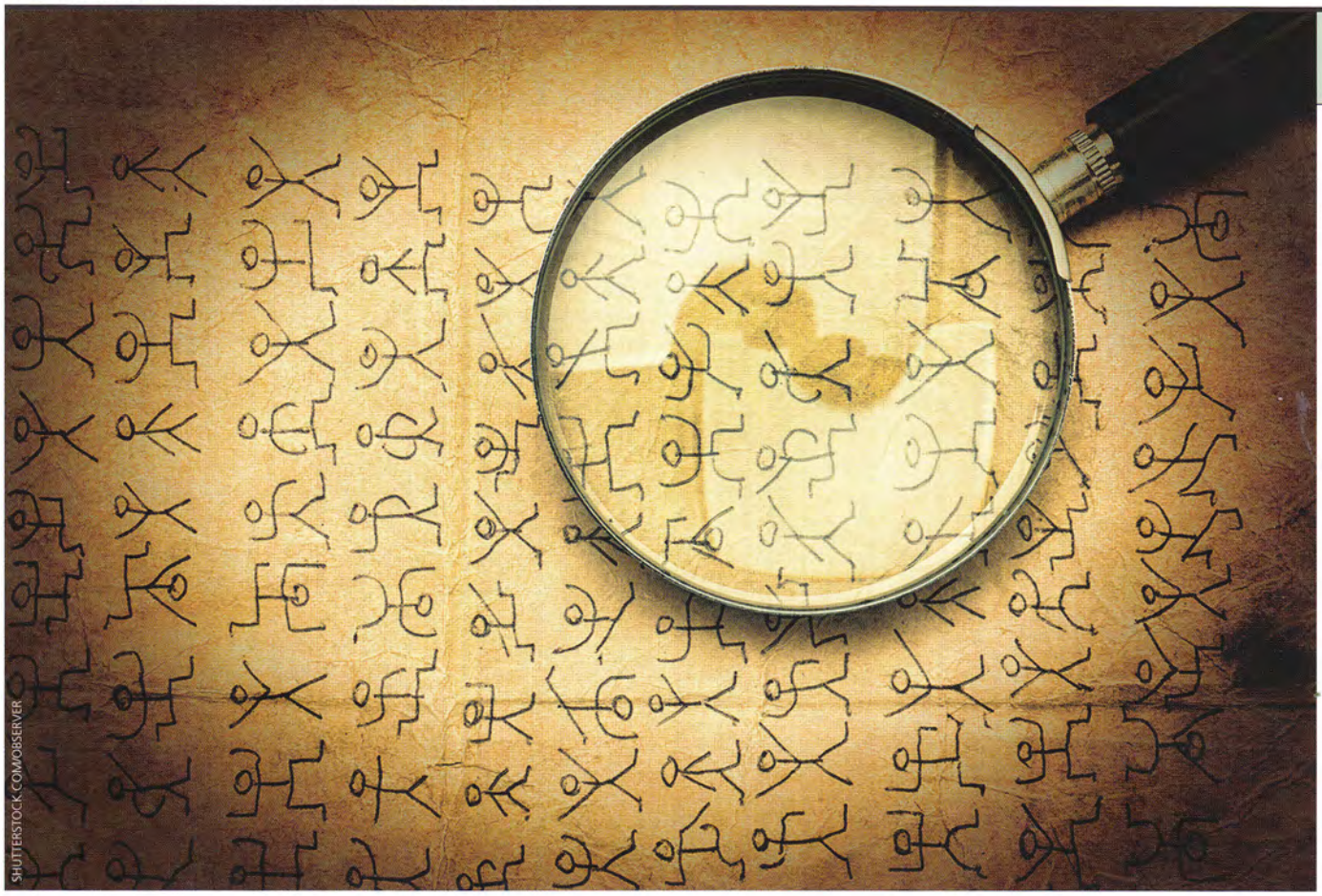
«Законодательством Российской Федерации обязательная сертификация средств шифрования и других средств защиты информации определена только для средств, предназначенных для защиты сведений, содержащих государственную тайну (статья 28 Закона Российской Федерации "О государственной тайне")».

Стало

«Законом Российской Федерации "О государственной тайне" обязательная сертификация средств шифрования и других средств защиты информации определена только для средств, предназначенных для защиты сведений, содержащих государственную тайну (ст.28).»

Таким образом, получается, что остальное «законодательство» (пресловутые ПДн) в рамках данного извещения не рассматривалось.

Учитывая, что для защиты ПДн в соответствии с Приказом № 378 ФСБ России может использоваться только СКЗИ



класса КС 1 и выше, нет оснований отказываться от сертификации.

Вместо вывода

ФСБ сделал очевидный вывод про обязательную сертификацию СКЗИ для государственной тайны, не сообщив ничего нового и не ответив на действительно интересующий всех вопрос.

П.С.

Представьте ситуацию, что молодой человек встает на одно колено перед своей любимой и спрашивает: «Выйдешь ли ты за меня замуж?», – но вместо ответа (да/нет/дай подумать) получает цитату из семейного кодекса ст. 10 «Заключение брака». Он смотрит на нее непонимающим взглядом и думает: «Может она меня бросила?»

Разница только в том, что ФСБ России – это настоящие мужчины, и они нас не бросят.

П.С.С.

Использование только сертифицированного СКЗИ для всех видов тайн, или даже только для ПДн, чрезвычайно сложная задача и на настоящем этапе фактически не выполнимая, несмотря на «новый закон».

ФСБ сделал очевидный вывод про обязательную сертификацию СКЗИ для государственной тайны, не сообщив ничего нового и не ответив на действительно интересующий всех вопрос

Немного позитива

Новое – это хорошо забытое старое! Требованию использовать на территории РФ только «разрешенные» СКЗИ уже 21 год.

Кому интересно, перечитайте действующий *«Указ Президента РФ от 03.04.1995 № 334 "О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации"»*.

Вам особенно понравятся:

- п. 2. Все СКЗИ, включая электронную подпись, должны иметь соответствующий сертификат. Государственные заказы на предприятиях, нарушающих данный пункт, запрещены.
- п. 5. Таможне принять меры по недопущению «ввоза» иностранного СКЗИ без лицензии.
- п. 6. Контрразведке и МВД усилить контроль за юридическими и физическими лицами, нарушающими данный указ.
- п. 7. Прокуратуре усилить контроль. ●