Максим ОСОКИН,
анонимный эксперт «BIS Journal»

ДЛЯ ИНФОРМАЦИОННОЙ ЗАЩИТЫ БАНКИ ВСЁ ЧАЩЕ ПРЕДПОЧИТАЮТ ЗАКУПАТЬ ПРОФЕССИОНАЛЬНЫЕ РЕШЕНИЯ

НЕ ВРЕМЯ САМОДЕЛКИНЫХ

Закупки банками специального оборудования и программного обеспечения для информационной защиты – дело довольно новое. Хотя на рынке уже работают десятки поставщиков такого специализированного оборудования, некоторые банки ещё удовлетворяет работа по старинке. Но резонов экономить на информационной безопасности остаётся всё меньше. Довольствоваться придумками собственных самоделкиных на базе стандартного «железа» и софта можно, лишь пока не грянет гром.

Ещё совсем недавно лишь самые дальновидные и осторожные руководители банков заблаговременно выстраивали контуры защиты в ожидании бума кибер-преступности

ВТОРЖЕНИЕ «СЕРЫХ ХАЛАТОВ»

Бережливость банкиров можно понять. Создание банками на стыке сфер ответственности служб безопасности и IT-подразделений структур информационной безопасности, которые и выступают покупателями специализированных решений, – дело довольно новое. Повсеместной привычки к этому пока нет, что в свою очередь не может не тормозить развитие рынка предложений. Но отчаиваться не стоит, давайте вспомним недавнее прошлое и проанализируем тенденцию.

В начале 2000-х годов информационная защита банков находилась в зачаточном состоянии. Занимались этими вопросами, как правило, сотрудники IT-служб и работали на базе стандартных персональных компьютеров и рабочих серверов, сетевого оборудования, на платформе операционной системы Windows-98. Испуг после аферы начала 1990-х с фальшивыми авизо, когда мошенники легко уводили на сторону миллиарды рублей, поулёгся. Применения при банковских расчётах элементарных технических средств криптографии на некоторое время казалось достаточным.

Немногие руководители банков прислушивались к прогнозам появления интернет-банкинга, других «нетрадиционных» способов расширения спектра услуг и клиентской базы. Также не все верили предупреждениям о возможных новых угрозах. Лишь самые дальновидные и осторожные внимали предостережениям экспертов о грядущем буме киберпреступности, заблаговременно выстраивали контуры защиты. Еще кто-то предохранялся от злоупотреблений со стороны «людей в серых халатах», необоснованных вторжений недобросовестных работников правоохранительных органов.

Случаи инициатив по укреплению информационной защиты «снизу», со стороны персонала банков, нередки. Энтузиастов на

Дмитрий ЛЕВИЕВ,
Председатель Совета
НП «Партнерство специалистов
по информационной безопасности»

ТОКЕНЫ НА ВЫБОР

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ЭЛЕКТРОННЫХ ТОКЕНОВ ВТОРОГО ПОКОЛЕНИЯ ДЛЯ ПОСТРОЕНИЯ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА НА БАЗЕ КВАЛИФИЦИРОВАННОЙ УСИЛЕННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ

В современном Банке системы «Банк-Клиент» давно перешагнули грань информационных систем для управления счетом и стали полноценной системой электронного документооборота между Банком и Клиентом. Принятие Федерального закона об электронной подписи, постепенное внедрение анализа операционного риска, а также Комплекса Стандартов Банка России заставляет по новому взглянуть на эксплуатируемые системы «Банк-Клиент» с целью минимизации риска и стоимости владения с улучшением качества обслуживания и уменьшением требований, по возможности, к рабочему месту Клиента.

Современная система «Банк-Клиент» представляет собой трёхступенчатую систему, состоящую из сервера приложения, системы управления ключевой информации и клиентских рабочих мест. Сервер приложения и система управления ключевой информации располагаются в Банке и часто называются серверной частью системы «Банк-Клиент», рабочие места операционных сотрудников Банка и клиентов

Отечественную разработку – металлический чёрный ящик ценой в несколько сотен «зеленых», чёрный в буквальном смысле, с острыми гранями, почти мгновенно начисто уничтожал информацию с десятка кассет – отыскали через интернет

местах хватает, но доказывать руководству обоснованность дополнительных расходов им приходилось долго и с трудом, зачастую безуспешно. Редки удачные ситуации, когда ответственный за информационную безопасность не только проявлял неформальный интерес к новым решениям, но и занимал в банковской иерархии достаточно влиятельный пост, чтобы добиваться одобрения предлагаемых мер, не всегда дешевых.

ЧЁРНЫЙ НЕ ПО НАЗВАНИЮ

Безусловно, главным стимулирующим фактором наращивания банковских расходов на обеспечение информационной защиты являются официальные требования государственных регуляторов: новые законы, стандарты, требования, нормативные акты в рекомендательной или обязывающей, категоричной форме. В начале 2000-х годов государство от банков почти ничего такого относительно параметров информационной безопасности не требовало.

Один из моих собеседников смог припомнить переломный момент, когда в его банке решились на первую закупку специализированного решения. Это был, конечно, примитив, зато очень функциональный, и, главное, начало было положено. Банк приобрёл устройство для быстрого уничтожения информации на кассетах магнитных лент стримеров.

Задача была актуальной: в те времена ещё не было широкополосных сетей, сети каждого из офисов банка работали автономно, резервные копии рабочей информации серверов сохранялись на таких кассетах. Чтобы обезопасить эту информацию от несанкционированного доступа, по окончании рабочего дня курьеры по определённой схеме объезжали все офисы, забирали все кассеты и привозили в архив.

Представляете, сколько времени нужно было стирать информацию традиционными способами и какова надёжность операции? Тут-то и возникла идея приобрести отечественную разработку, которую отыскали через Интернет. Металлический чёрный ящик ценой в несколько сотен «зелёных», чёрный в буквальном смысле, с острыми гранями, почти мгновенно начисто уничтожал информацию с десятка кассет.

Поле работ по информационной защите и потребности в новых решениях расширяются по мере роста высокотехнологичного сектора банковской деятельности.

Существенным сдвигам способствуют официальные разрешения удобных и эффективных новшеств. Особенно когда высокотехнологичные нововведения существенно облегчают, ускоряют и удешевляют делопроизводство.

РАСХОД КАРМАН НЕ ТЯНЕТ

Приведу пример: когда в обязательном порядке требовалось хранить бумажные копии бухгалтерских документов, среднестатистическому банку на эти нужды требовались ежедневно несколько пачек бумаги формата А4. Прибавьте сюда расходы на тонер, печати, чернила и амортизацию принтеров, а также непосредственные трудозатраты сотрудников.

Разрешение Центробанка РФ в начале 2000-х хранить электронные копии документов казалось бы упростило и удешевило для банков хранение бухгалтерских документов. Но и тут было не все так гладко. Дело в том, что документы Центробанка РФ (и тот документ не исключение) зачастую сформулированы таким образом: как бы тот или иной банк не пытался соответствовать требованиям ре-

системы могут быть выполнены в виде тонких и толстых клиентов.

Согласно ФЗ об электронной подписи в сертификате электронной подписи должны содержаться данные, отнесенные в соответствии с ФЗ о персональных данных к персональным данным. Согласно п.7.7. Стандарта Банка России при построении содержащих персональные данные систем электронного документооборота, защищенных с использованием шифровальных (криптографических) средств, необходимо применять средства криптографической защиты информации (далее СКЗИ) не ниже класса КС2.

На рабочем месте Клиента при использовании широко распространенных СКЗИ необходимо использовать средства защиты, перечисленные в ***Таблице 1***.

Таблица 1. ТРЕБОВАНИЯ К СРЕДСТВАМ ЗАЩИТЫ ПРИ ИСПОЛЬЗОВАНИИ СКЗИ КЛАССА КС2

№№	КриптоПро CSP	Криптоком 3.2	МАГПро CSP
	версия 3.6 R2		
1.	АПМДЗ Соболь 2.0/2.1	АПМДЗ Соболь 2.0/2.1	АПМДЗ Соболь 2.0/2.1
2.	АПМДЗ Соболь 3.0	АПМДЗ Соболь 3.0	АПМДЗ Соболь 3.0
3	АПМДЗ Аккорд-АМДЗ	АПМДЗ Аккорд-АМДЗ	АПМДЗ Аккорд-АМДЗ

Использование перечисленных в ***Таблице 1*** средств защиты создает большие неудобства для клиентов, особенно руководителей клиентов – юридических лиц, которые в большинстве используют мобильные компьютеры.

Альтернативой использования АПМДЗ является использование токенов второго поколения без возможности извлечения закрытого (секретного) ключа и формирование электронной подписи и сеансовых ключей шифрования непосредственно на самом устройстве. Сравнительные характеристики токенов, отвечающих требованиям Стандарта Банка России приведены в ***Таблице 2***.

Все приведенные в ***Таблице 2*** токены являются в понимании ПП9575 средствами криптографической защиты информации, и их передача Клиентам Банком должна проводится на основании лицензии на распространение СКЗИ по адресам, указанной в данной лицензии. Это требование необходимо учитывать при формировании внутренней нормативно-правовой базы эксплуатации систем «Банк-Клиент».

Реализация средства электронной подписи на клиентском месте в понимании ФЗ об электронной подписи и формирования защищенного канала взаимодействия с серверной частью системы требует применения единого комплекса программных и программно-аппаратных средств, состоящих из прикладного программного обеспечения, позволяющего создать и отобразить перед подписанием документ, программного СКЗИ для формирования защищенного канала связи и хэш-функции подписываемого документа и собственно токена.

Согласно требованиям ФЗ об электронной подписи средства электронной подписи должны пройти оценку соответствия в системе сертификации ФСБ России в виде контроля встраивания по процедуре, предусмотренной ПКЗ-20056 и эксплуатационной документации на используемые СКЗИ на основании согласованного с ФСБ России Технического задания на построение информационной системы «Банк-Клиент», защищенного с использованием шифровальных (криптографических) средств.

Для выполнения требований, предъявляемых к системе управления ключевой информации для квалифицированной усиленной подписи, необходимо использовать сертифицированные ФСБ России Удостоверяющие центры.

Единой методики подсчёта расходов на информационную безопасность банков нет, но сюда необходимо включать расходы на зарплату специа-листам, оборудование, программные продукты, а также приплюсовать часть ежегодных затрат на аудиторские услуги

гулятора, всегда найдется «крючок», за который могут зацепиться проверяющие.

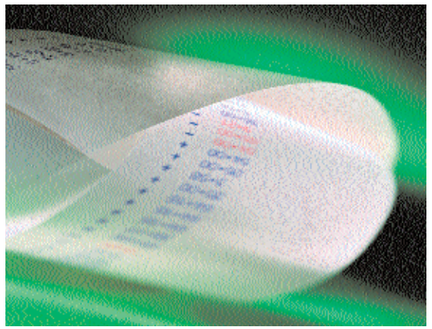
Поэтому далеко не все банки решились перейти на новые технологии, справедливо полагая, что «шутки» с государственным регулятором могут выйти боком. И только после того, как в конце 2009 года ЦБ наконец-то издал документ, в котором были четко прописаны организационные и технические требования по осуществлению хранения документов в электронном виде, многие банки незамедлительно приступили к реализации этой идеи.

Теперь материальные затраты на архив документов одного банковского дня сводятся к цене двух (с учетом резервного дубля) болванок оптических дисков.

Взаимодействие с Центральным каталогом кредитных историй – ЦККИ – и ещё пятью крупнейшими частными бюро кредитных историй ставит перед банками задачу защиты персональных данных от несанкционированного использования. В ходе повседневной работы банков с этими организациями встают вопросы защиты информации, передаваемой по общедоступным каналам связи. И здесь требуется решение задачи по установлению подлинности электронных документов, которое осуществляется с использованием современных криптографических средств, сертифицированных в полном соответствии с законом.

ЭКОНОМИЯ НЕ БЕЗОПАСНА

Все вышесказанное, разумеется, относится и к повсеместно используемой услуге «Клиент-Банк». Услуги банков по предоставлению гарантий исполнения обязательств импортера в адрес таможенных органов также предполагают информационную защиту документооборота. Как мы



видим, подразделениям информационной защиты работы, конечно, каждый раз прибавляется, но тем убедительнее становится необходимость их существования и выделения средств на их оснащение.

Расходы на информационную безопасность «среднего банка» оценить довольно сложно, т.к. все «средние банки» разные, да и единой методики подсчета затрат не выработано, тем не менее, опрошенные специалисты склоняются к тому, что эти затраты неуклонно растут. Сюда необходимо включать расходы на зарплату специалистам, а также на оборудование и программные продукты. В какой-то степени сюда можно приплюсовать часть ежегодных затрат на аудиторские услуги.

Оценка надёжности информационной защиты банка, произведенная аудиторами из компании «большой четверки», влетает в

Таблица 2. СРАВНИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ ТОКЕНОВ

№№	Наименование параметра	Рутокен ЭЦП	eToken ГОСТ	Магистра 1.2	Магистра 1.3	MS_Key1.
1.		*Форм-фактор технического средства*				
1.1.	Usb-ключ тип А	В стандартном корпусе красного цвета	В стандартной корпусе синего цвета	Стандартный корпус Rutoken	Стандартный корпус Rutoken	Стандартный корпус
1.2.	Usb-ключ тип А с выбором нанесением логотипа	При заказе более 1000 штук	При заказе более 1000 штук	Нет	Нет	Нет
1.3.	Смарт-карта ISO 7816	Нет	В стандартном корпусе	Нет	Нет	Нет
1.4.	Смарт-карта ISO 7816 для полно цветной печати	Нет	При заказе от 1000 штук	Нет	Нет	Нет
1.5.	Смарт-карта ISO 7816 с полноцветной печатью	Нет	При заказе от 1000 штук	Нет	Нет	Нет
2.	*Наличие сертификатов*					
2.1.	ФСБ России на СКЗИ	Сертификат №СФ/124-1674 ФСБ России	Сертификат № СФ/124-1671 ФСБ России	Сертификат на криптоядро	Сертификат на криптоядро	Сертификат на криптоядро
3.	*Класс СКЗИ*	*КС2*	*КС2*	*КС2**	*КС2**	*КС2**
4.	*Интерфейсы и стандарты, реализуемые аппаратно*					
4.1.	PKCS#11 версии 2.30	Да	да	Нет	Нет	Да
4.2.	Microsoft CryptoAPI	Да	Да	Нет	Нет	Нет
4.3.	PC/SC	Да	да	Нет	Нет	Нет
4.4.	Сертификаты X.509 v3, SSL v3, IPSec/IKE	Да	да	Нет	Нет	Нет
4.5.	Microsoft CCID	Да	да	Нет	Нет	Нет
4.6.	ISO/IEC 7816-12	Да	Да	Да	Да	Нет
5.	*Поддерживаемые криптографические алгоритмы с указанием реализуемых функций*					
5.1.	ГОСТ Р 34.10-2001	Генерация ключевых пар импорт ключевых пар, формирование и проверка электронной цифровой подписи	Генерация ключевых пар формирование и проверка электронной цифровой подписи	Выработка и проверка эцп, аутентификация, выработка ключевой пары, генерация сессионного ключа	Выработка и проверка эцп, аутентификация, выработка ключевой пары, генерация сессионного ключа	Да
5.2.	ГОСТ Р 34.11-94	Вычисление значения хэш-функции	Вычисление значения хэш-функции	Вычисление значения хэш-функции	Вычисление значения хэш-функции	Нет
5.3.	ГОСТ 28147-89	Генерация и импортирование ключей шифрования, зашифрование и расшифрование данных в режимах простой замены гаммирования иаммирования с обратной связью, вычисление и проверка имитовставки	Зашифрование /расшифрование блоков данных, вычисление имитовставки	Шифрование, имитовставка, аутентификация, защищенный обмен сообщениями, генерация сессионного ключа	Шифрование, имитовставка, аутентификация, защищенный обмен сообщениями, генерация сессионного ключа ключа	Да
5.4.	RFC4357	Да	Да	Нет	Нет	Нет данных
5.5.	Генерация случайных чисел	Да	Да	Нет данных	Нет данных	Нет данных
5.6.	Поддержка алгоритма RSA	С ключами длиной до 2048 бит	Нет	Выработка и проверка ЭЦП, аутентификация, выработка ключевой пары с длиной ключа 1024 бит	Выработка и проверка ЭЦП, аутентификация, выработка ключевой пары с длиной ключа 1024 бит	Нет данных

Класс Удостоверяющего центра не должен быть ниже требования к СКЗИ, т.е. не ниже КС2. Перечень сертифицированных Удостоверяющих центров класса не ниже КС2 приведен в ***Таблице 3***.

Для проверки электронной подписи и формирования защищенного канала взаимодействия сервера приложения системы «Банк-Клиент» должны использоваться сертифицированные СКЗИ в исполнении не ниже КС2. Для выполнения указанных требований на Сервер приложений устанавливается АПМДЗ, а также используются межсетевой экран, средства защиты от несанкционированного доступа и антивирусное средство защиты согласно требованиям эксплуатационной документации на используемое СКЗИ.

Построение системы «Банк-Клиент» с квалифицированной электронной подписью является хорошо структурированным процессом с жестким алгоритмом выполнения требования и этапов. Качественное выполнение всех этапов позволяет получить эффективную и безопасную информационную систему, соответствующую требованиям действующего законодательства РФ.

Перечень литературы

1. Федеральный закон «Об электронной подписи» № 63-ФЗ от 06 апреля 2011 года.

2. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения «СТО БР ИББС-1.0-2010» (принят и введен в действие Распоряжением Банка России № Р-705 от 21 июня 2010 года).

3. Д.Левиев. Информационная система современного банка сегодня. Журнал Connect! Мир Связи № 11 2008 г.

«копеечку», вполне сравнимую по величине со всеми остальными расходами банка на информационную безопасность. Сегодня, в начале 2010-х, общие расходы на информационную безопасность «среднего банка» оцениваются в 2,5–3,5 млн рублей в год. В том числе 1,5–2 млн рублей на зарплату специалистам и 1–1,5 млн рублей на оборудование и программные продукты.

ДЕСЯТЬ ЛЕТ СПУСТЯ

Сегодня, 10 лет спустя, нормальный среднестатистический банк не может не обойтись без некоего минимума решений в сфере информационной защиты. Обязательно закупается такое специализированное оборудование с криптозащитой, как маршрутизаторы и коммутаторы. Чаще всего предпочитают продукцию «законодателя мод» – фирмы Cisco Systems. Пусть дорого, зато надёжно. Есть и прочие вендоры, более приемлемые по цене, но менее надёжные при переходе к решению не вполне стандартных задач. В любом случае не мешает поинтересоваться, есть ли у продавцов лицензии ФСБ на поставки такого оборудования.

Что касается программных инструментов, то в настоящее время на рынке представлено достаточно много вполне функциональных и при этом недорогих решений российских разработчиков, например, продукты компании «Крипто-ПРО», позволяющие обеспечить наиболее типичные потребности банков в области защиты информации.

Тем не менее для бедных и жадных банкиров пока ещё остаётся простор пробовать своих сотрудников в качестве «самоделкиных». Пусть ухищряются защищать каналы связи на базе платформы Linux, генерируют собственные микрокоды, перепрошивают обычные Wi-Fi-маршрутизаторы. Однако таких возможностей остаётся всё меньше, информационная защита банков всё больше выстраивается в самостоятельную отрасль и специализируется.

Ширятся перечень и объём банковских услуг, потенциально уязвимых для информационных атак. Растут перечень и уровень соответствующих угроз. Государственные регуляторы формулируют стандарты и прочие требования к информационной защите банков. Вендорами создаются новые технические решения, на рынке складывается круг их поставщиков. Контур замыкается: формируется полноценный закупщик – специализированные подразделения информационной защиты банков, обеспеченные бюджетами. Время «самоделкиных» близится к концу.

* * *

Представленные наблюдения не претендуют на всесторонний анализ состояния и динамики рынка решений по информационной защите банков. За этим нужно обращаться к профессиональным маркетологам, которые и методику разработают, и исследование проведут, и результаты проанализируют, и сделают выводы. Разумеется, оценив услуги пропорционально трудозатратам, плюс некая норма прибыли... Здесь же аккумулирован практический опыт работы подразделений информационной защиты «средних банков», обсуждаемый в ходе постоянного общения с достаточно квалифицированными коллегами.

Таблица 2. СРАВНИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ ТОКЕНОВ (продолжение)

№№	Наименование параметра	Рутокен ЭЦП	eToken ГОСТ	Магистра 1.2	Магистра 1.3	MS_Key1.
5.7.	DES/3DES	Нет	Нет	Аутентификация, шифрование, MAC, защищенный обмен сообщениями	Аутентификация, шифрование, MAC, защищенный обмен сообщениями	Нет данных
5.8.	SHA-1	Нет	Нет	Вычисление хэш-функции	Вычисление хэш-функции	Нет данных
6.	Объем доступной защищенной памяти	64 Кбайта	72 Кбайта	66Кбайт	Нет данных	Нет данных
7.	Возможность установки дополнительного модуля Flash-памяти	Есть для USB-ключей объем 4 ГБайт при заказе от 100 штук	Есть для USB-ключей объем 1/2/4 ГБайт при заказе от 100 штук	Нет	Нет	Нет данных
8.	Возможность установки модуля генератора одноразовых паролей	Нет	Есть для USB-ключей при заказе от 100 штук	Нет	Нет	Нет данных
9.	Возможность встраивания радио-меток (RFID)	Есть для USB-ключей при заказе от 100 штук	Есть для USB-ключей при заказе от 100 штук	Нет	Нет	Нет данных
10.	Комплект драйверов	С сайта разработчика	eToken PKI Client 4.55 и выше с сайта разработчика	Поставляется разработчику прикладного решения	Поставляется разработчику прикладного решения	Поставляется разработчику прикладного решения
11.	*Поддерживаемые операционные системы и среды*					
11.1.	Microsoft Windows 2000	Нет	Нет	Да	Да	Да
11.2.	Microsoft Windows XP	Да	Да	Да	Да	Да
11.3.	Microsoft Windows 2003	Да	Да	Да	Да	Да
11.4.	Microsoft Windows Vista	Да	Да	Да	Да	Да
11.5.	Microsoft Windows 7	Да	Да	Да	Да	Да
11.6.	Microsoft Windows 2008	Да	Да	Да	Да	Да
11.7.	MacOS X (RISC)	Да	Да	Нет	Нет	Нет данных
11.8.	MacOS X (Intel)	Да	Да	Нет	Нет	Нет данных
11.9.	Linux Suse	Да	Да	Нет	Нет	Нет данных
11.10.	Linux RedHat	Да	Да	Нет	Нет	Нет данных
11.11.	Linux Ubuntu	Да	Да	Нет	Нет	Нет данных
12.	Комплект разработчика	Rutoken Developer's Kit с сайта разработчика	eToken ГОСТ SDK с сайта разработчика	Поставляется по запросу	Поставляется по запросу	Нет данных

** Законченное функциональное изделие выполняется по Техническому заданию, согласованному с ФСБ России*

Таблица 3. ПЕРЕЧЕНЬ СЕРТИФИЦИРОВАННЫХ ФСБ РОССИИ УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ КЛАССА НЕ НИЖЕ КС2 (по состоянию на 15 апреля 2011 года)

№№	Наименование Продукта	Класс Удостоверяющего центра, номер сертификата
1.	«Стандарт-КИ УЦ»	КВ2 , СФ/128-1165
2.	«Программно-аппаратный комплекс «Удостоверяющий центр корпоративного уровня ViPNet КС2"	КС2, СФ/128-1269
3.	«Программно-аппаратный комплекс «Удостоверяющий центр корпоративного уровня ViPNet КС3"	КС3, СФ/128-1270
4.	«Удостоверяющий центр ВТБ», версия 1.0	КС2, СФ/128-1284
5.	Программно-аппаратный комплекс "Юнисерт-ГОСТ», версия 2	КС2, СФ/128-1307
6.	«Notary-PRO», версии 2.6	КС2, СФ/128-1351
7.	«Верба-сертификат МВ», версия 2.0	КС2, СФ/128-1500
8.	«Сигнатура-сертификат», версия 3.5	КС2, СФ/128-1506
9.	«КриптоПро УЦ», версия 1.4)	КС2, СФ/128-1557

4. Федеральный закон «О персональных данных» № 152-ФЗ от 27 июля 2006 г.

5. Постановление Правительства РФ «Об утверждении Положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами» № 957 от 29 декабря 2007 года, вместе с:

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

6. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005). Утверждено приказом ФСБ России № 66 от 9 февраля 2005 года, зарегистрировано в Минюсте РФ под № 6382 03 марта 2005 года.