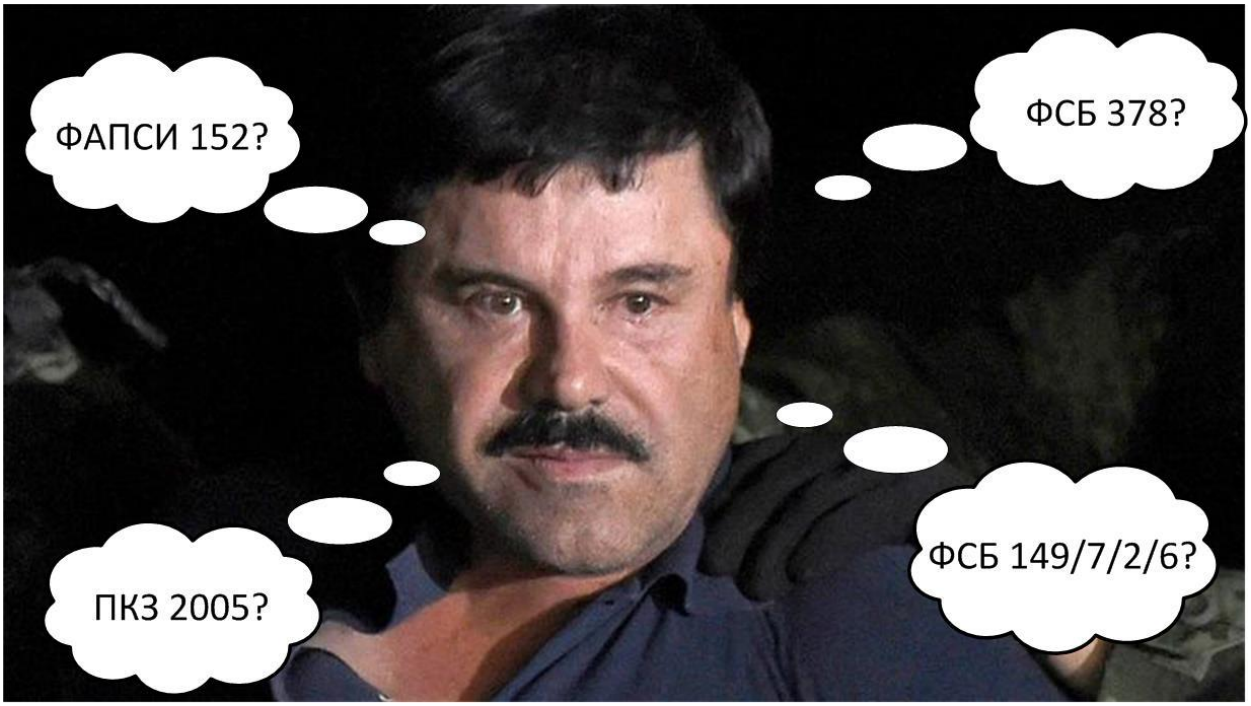
Разбираемся с российской криптографической нормативкой… на примере ареста наркобарона



Мексиканский наркобарон Хоакин Гусман Лоэра (Эль Чапо)

Не так давно в СМИ промелькнула статья о том, что мексиканского наркобарона Эль Чапо арестовали из-за того, что его IT-шник слил криптоключи в ФБР, а те в свою очередь смогли расшифровать и прослушать его телефонные переговоры.

Давайте пофантазируем и представим, что наркобарон, IT-шник и все, все, все жили бы в России…

Представили? А теперь разберем, какими законами и как регулировалось бы применение криптозащиты в данном фантасмагорическом случае.

Об истории и главных действующих лицах поподробнее

© кадр из к/ф «Банды Нью-Йорка»

Наркобарон Эль Чапо нанял 21-летнего колумбийского IT-специалиста Кристиана Родригеса, чтобы тот создал для него систему зашифрованной мобильной связи, через которую можно было бы общаться с подельниками, не опасаясь прослушки со стороны спецслужб.

Родригес подобную систему создал и, судя по описанию, она представляла собой VoIP телефонию с шифрованием трафика. Клиенты системы устанавливались на мобильные телефоны бандитов, после чего тем «достаточно было набрать 3 добавочных цифры», чтобы разговаривать, не опасаясь прослушки.

После внедрения системы Родригес ее сопровождал, а также занимался другими IT-проектами (например, организовал прослушку жены Эль Чапо), повинуясь воле наркобарона.

Спустя некоторое время Родригеса завербовало ФБР и тот… по версии SecurityLab.ru слил ключи шифрования… или по версии New York Times «установил на зашифрованную сеть записывающее оборудование, которое отсылало в ФБР в полночь копии всех переговоров Эль Чапо».

В двух словах это все. Теперь перейдем к разбору законов.

Лицензирование

© скриншот из игры «Герои меча и магии»

Наша история начинается с того, что Эль Чапо нанял Родригеса на разработку системы защищенной связи.

С точки зрения пп. 1 п. 1 ст. 12 Федерального закона от 04.05.2011 N 99-ФЗ «О лицензировании отдельных видов деятельности» у Родригеса, для того чтобы реализовать контракт с Эль Чапо, должна быть лицензия «на криптографию».

Если у Родригеса подобной лицензии нет, и он вязлся за работу, то за это ему в соответствии со ст. 13.13 КоАП РФ грозит административная, а в соответствии ст. 171 УК РФ уголовная ответственность.

Лицензия «на криптографию» правильно называется — ***лицензией на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)***. Далее для простоты будем использовать неправильное, но более понятное и короткое название — лицензия «на криптографию».

В соответствии с Постановлением Правительства РФ от 21.11.2011 N 957 «Об организации лицензирования отдельных видов деятельности» выдачей лицензий «на криптографию» занимается ФСБ России.

Процедура получения лицензии и лицензионные требования к Родригесу описаны в Постановлении Правительства РФ от 16.04.2012 N 313 (ред. от 18.05.2017) «Об

утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

При этом Родригесу мало «просто получить» лицензию, в ней должны быть перечислены соответствующие разрешенные виды деятельности, полный перечень которых приведен в Приложении к Постановлению Правительства РФ от 16.04.2012 N 313. В зависимости от состава разрешенных видов деятельности к Родригесу будут предъявляться различные лицензионные требования, начиная от ценза по образованию, заканчивая доступом к гостайне.

С учетом того Родригес занимался не только разработкой системы, но также ее внедрением и сопровождением, то навскидку в его лицензии должны присутствовать следующие виды деятельности (нумерация в соответствии с Постановлением Правительства РФ от 16.04.2012 N 313):

3. Разработка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.
4. Разработка средств изготовления ключевых документов.
5. Модернизация шифровальных (криптографических) средств.
6. Модернизация средств изготовления ключевых документов.
7. Производство (тиражирование) шифровальных (криптографических) средств.
9. Производство защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.
10. Производство средств изготовления ключевых документов.
12. Монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации.
14. Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.
15. Монтаж, установка (инсталляция), наладка средств изготовления ключевых документов.
16. Ремонт шифровальных (криптографических) средств.
18. Ремонт, сервисное обслуживание защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.
19. Ремонт, сервисное обслуживание средств изготовления ключевых документов.
20. Работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).
21. Передача шифровальных (криптографических) средств, за исключением

шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации.
23. Передача защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем.
24. Передача средств изготовления ключевых документов.

Сразу отметим, что использование шифрования в собственных целях в России не лицензируется и соответственно никакой лицензии «на криптографию» Эль Чапо не требуется.

Далее будем считать, что лицензия «на криптографию» с соответствующими видами деятельности у Родригеса есть.

Разработка и производство

© Internet картинки

В соответствии с лицензионными требованиями, а именно пп. б п.6 Постановления Правительства РФ от 16.04.2012 N 313 Родригес в своей работе обязан руководствоваться выпущенными ФСБ России соответствующими нормативно-методическими документами, основным среди которых является Приказ ФСБ РФ от 09.02.2005 N 66 (ред. от 12.04.2010) «Об утверждении «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (Зарегистрировано в Минюсте РФ 03.03.2005 N 6382)" (далее ПКЗ-2005).

В соответствии с этим документом процесс создания системы защищенной мобильной связи состоит из следующих этапов:

1. Разработка.
2. Производство.
3. Распространение. *Не смотря на то, что Родригес делал заказную/кастомную разработку, процесс ее передачи заказчику трактуется как распространение.*

Все эти этапы подразумевают тесное сотрудничество с ФСБ России и согласование технических заданий и документации на выпускаемую систему.

Эксплуатация системы защищенной мобильной связи

© Internet картинки

Будем считать, что эксплуатация системы защищенной мобильной связи — это зона ответственности Эль Чапо. Родригес в этом участвует лишь в качестве тех. поддержки.

Из описания истории Эль Чапо мы помним, что система создавалась для защиты от прослушки со стороны правоохранительных органов. Данное основание слабо коррелируется с действующим законодательством, поэтому примем, что цель эксплуатации системы: «защита информации для личных и семейных нужд». При такой цели эксплуатации на Эль Чапо не накладывается никаких ограничений, и он может делать с системой все, что хочет, и как хочет.

Для нашей статьи это слишком просто и не интересно.

По материалам расследования установлено, что в телефонных разговорах Эль Чапо давал команды на дачу взяток и подкуп чиновников и скорее всего называл их имена, фамилии и другую личную информацию, то есть персональные данные (далее — ПДн).

Давайте представим, что Эль Чапо, прочитав Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», понял, что является оператором ПДн, и что на самом деле использует ПДн не для личных нужд, а в предпринимательской деятельности, и что по закону обязан их защищать.

Криптографическая защита персональных данных

© Internet картинки

Поскольку во время телефонных переговоров ПДн передаются в открытом виде через сеть связи общего пользования, Эль Чапо подумал и решил, что велик риск перехвата ПДн злоумышленниками, и, следовательно, информацию нужно шифровать.

Для криптографической защиты персональных данных, в соответствии с

- Приказом ФСБ от 10 июля 2014 года N 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 Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»
- «Методическими рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России (N 149/7/2/6-432 от 31.03.2015)

Эль Чапо должен построить модель нарушителя, на основании которой определить требуемый класс средства криптографической защиты. Поскольку Эль Чапо опасается спец.служб, то ему нужно средство защиты максимального класса — **КА**.

Эль Чапо открыл перечень сертифицированных ФСБ России криптосредств и, не найдя ничего подходящего, обратился к Родригесу. Тут наша история, как и многие проекты в ИБ, делает петлю, и мы вновь возвращаемся к этапу разработки. Не вдаваясь в подробности, будем считать, что Родригес подобное криптосредство сделал и сертифицировал в ФСБ на соответствующий класс.

Поскольку Эль Чапо защищает персональные данные, то требования ПКЗ-2005 являются для него обязательными к исполнению. Ничего сверхъестественного в этих требованиях

нет, и фактически они лишь заставляют Эль Чапо соблюдать требования технической документации на систему, которые Родригес подготовил и согласовал с ФСБ России.

Кроме указанных выше документов, Эль Чапо обязан руководствоваться «Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ от 13 июня 2001 года N 152 (в простонародье — ФАПСИ 152).

По данному документу Эль Чапо необходимо будет выстроить внутренние процессы, связанные с эксплуатацией криптосредств, среди которых можно выделить:

- организацию обучения и допуска бандитов к использованию оборудования защищенной мобильной связи (по науке — допуск пользователей к самостоятельному использованию криптосредств);
- поэкземплярный учет программных клиентов системы и криптоключей;
- организацию режимных помещений, в которых будет проводиться техническое обслуживание телефонов и формирование криптоключей;
- и др.

Вывоз защищенных мобильных телефонов за границу

© Internet картинки

Поскольку Эль Чапо вел «международный бизнес», защита связи при общении с иностранными «партнерами» была бы для него не менее актуальна, чем защита переговоров внутри страны. Для этого, как ни крути, ему потребовалось бы передать

иностранцам либо софт для своей системы мобильной связи, либо телефон с уже установленными и настроенными программными клиентами.

И то, и другое по российскому законодательству трактуется как вывоз шифровальных (криптографических) средств за границу и, в соответствии с Положением о ввозе на таможенную территорию Евразийского экономического союза и вывозе с таможенной территории Евразийского экономического союза шифровальных (криптографических) средств (Приложение N 9 к Решению Коллегии Евразийской экономической комиссии от 21 апреля 2015 г. N 30), ограничивается (за исключением использования для личных нужд, но это не наш случай).

Перед прохождением таможни Эль Чапо должен был бы получить разрешение на вывоз, которые бывают двух видов:

1. Нотификация
2. Лицензирование

Нотификация — упрощенная форма разрешений на ввоз/вывоз — применяется для «ослабленной» или «бытовой» криптографии. Перечень средств, подпадающих под нотификацию, определен в Приложении N 4 к Положению о ввозе на таможенную территорию Евразийского экономического союза и вывозе с таможенной территории Евразийского экономического союза шифровальных (криптографических) средств (Приложение N 9 к Решению Коллегии Евразийской экономической комиссии от 21 апреля 2015 г. N 30)

Поскольку система защищенной мобильной связи Эль Чапо имеет класс криптографической защиты **КА**, то нотификацией он не обойдется, и ему придется получать лицензию на вывоз. Для этого он должен будет пройти квест, задание на который описано в Решении Коллегии Евразийской экономической комиссии от 06.11.2014 N 199 (ред. от 19.04.2016) «Об Инструкции об оформлении заявления на выдачу лицензии на экспорт и (или) импорт отдельных видов товаров и об оформлении такой лицензии и Инструкции об оформлении разрешения на экспорт и (или) импорт отдельных видов товаров», и далеко не факт, что он сможет это сделать…

Заключение

Надеюсь, что на данном фантасмагоричном примере вы смогли получить общие представления об основных направлениях регулирования криптографии в Российской Федерации. Для дальнейшего развития рекомендую ознакомиться с перечнем основных законодательных и нормативно-правовых актов, регулирующих ИБ в России.

Disclimer. *Автор, как и все прогрессивное человечество, решительно осуждает незаконную торговлю наркотиками и другую преступную деятельность. Солнце, воздух и вода — наши лучшие друзья.*