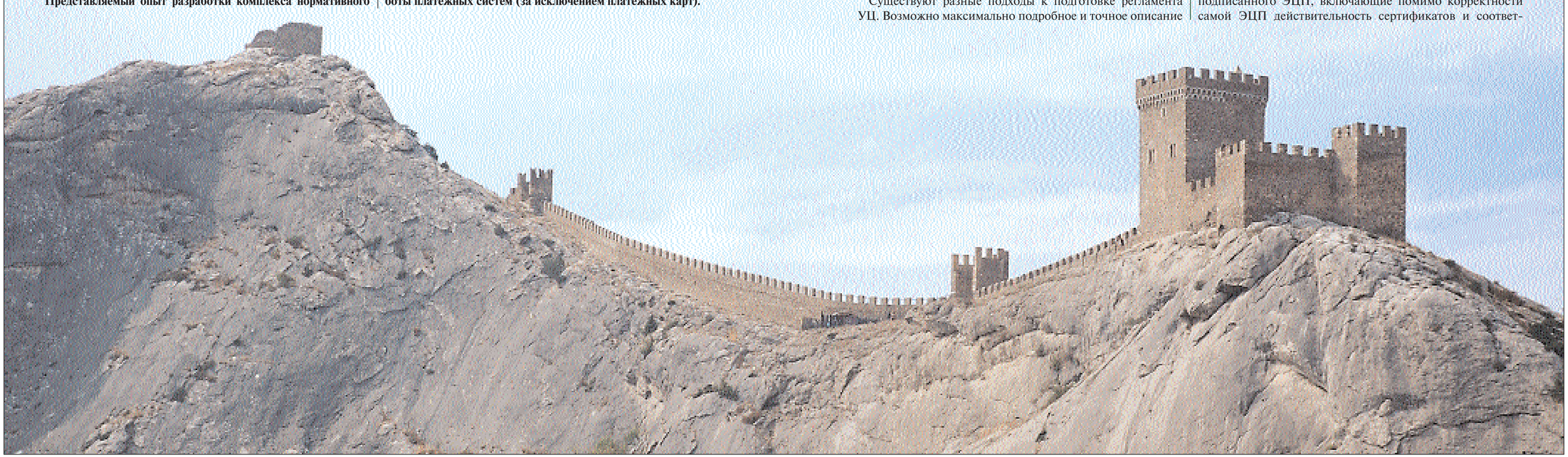
■ **Евгения ЯНАУЭР,**
ведущий специалист Отдела сопровождения информационной безопасности – Удостоверяющего центра управления информационной безопасности Департамента безопасности ОАО «Россельхозбанк»

КАК ЗА КАМЕННОЙ СТЕНОЙ

ОПЫТ НОРМАТИВНОГО ОБЕСПЕЧЕНИЯ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ И ПРИМЕНЕНИЯ СРЕДСТВ ЭЦП В ДЕЯТЕЛЬНОСТИ БАНКА

Юридическую значимость электронного документооборота в корпоративных и внешних информационных системах обеспечивает работа Удостоверяющего центра (далее – УЦ) и применение средств ЭЦП. Представляемый опыт разработки комплекса нормативного обеспечения PKI-инфраструктуры был наработан в сфере банковской деятельности. В том числе – обеспечения юридически значимого электронного документооборота внутри организации, дистанционного банковского обслуживания и работы платежных систем (за исключением платёжных карт).



Юридически значимый электронный документооборот в организации обеспечивается при помощи инфраструктуры открытых ключей (PKI-инфраструктуры). При её формировании большое значение придаётся разработке и применению комплекса нормативно-распорядительной и эксплуатационной документации, в том числе для конкретных бизнес-процессов. В этом процессе необходимо выполнять требования к ЭЦП и средствам защиты информации, предъявляемые федеральным законодательством и государственными регуляторами, нормы отечественных и международных стандартов, учесть ряд рекомендаций. В то же время следует учитывать специфику конкретной организации и корпоративного бизнеса.

НАЧИНАЯ С ГЛАВНОГО

В «Россельхозбанке» первым этапом создания нормативного обеспечения инфраструктуры открытых ключей и применения средств ЭЦП явилась разработка регламента Удостоверяющего центра, основополагающего при формировании PKI-инфраструктуры. Этот документ содержит описание процедур и действий – полный перечень операций Удостоверяющего центра и субъектов информационного обмена при выдаче и управлении сертификатами.

Существуют разные подходы к подготовке регламента УЦ. Возможно максимально подробное и точное описание процедур и действий. В таком случае регламент может содержать закрытую служебную информацию, что может усложнить создание защищенного информационного обмена с применением средств ЭЦП организации (в том числе УЦ) с внешними клиентами и контрагентами.

Поэтому при нормативном документировании корпоративной PKI-инфраструктуры «Россельхозбанком» был использован противоположный метод. Разрабатываемый регламент УЦ определял лишь общие принципы исполнения функций и условия получения услуг пользователями PKI-инфраструктуры. Вот их перечень:

- функциональные требования жизненного цикла сертификатов ключей подписи (далее – сертификатов), определяющие условия и правила их выдачи, управления и применения;
- организационные, эксплуатационные, физические и технические меры обеспечения безопасности закрытой ключевой информации, в том числе порядок действий её владельца в случае компрометации ключа подписи;
- перечень политик сертификатов, используемых Удостоверяющим центром и условия применения сертификатов в информационных системах организации для каждой политики;
- условия действительности электронного документа, подписанного ЭЦП, включающие помимо корректности самой ЭЦП действительность сертификатов и соответ-

ствующих ключей подписи как самого подписанта, так и уполномоченного лица, выдавшего ему сертификат;

- порядок разрешения споров и конфликтов, связанных с применением ЭЦП, и позиционирование УЦ в качестве третьей доверенной стороны для взаимодействующих сторон.

При таком подходе регламент УЦ не должен являться документом, определяющим договорные отношения с конкретным пользователем услуг. Регламент в виде перечня условий может быть приложением к договору об организации защищенного информационного обмена.

Руководствуясь таким подходом, в шаблоне регламента УЦ были выделены следующие разделы:

- основные функции УЦ;
- права и обязанности УЦ и Субъектов информационного обмена;
- ответственность УЦ и Субъектов информационного обмена;
- условия конфиденциальности;
- порядок предоставления и пользования услугами УЦ:
  - регистрация Субъектов информационного обмена;
  - изготовление сертификата ключа подписи Субъекту информационного обмена;
  - аннулирование (отзыва) сертификата ключа подписи;
  - приостановление действия сертификата ключа подписи;
  - возобновление действия сертификата ключа подписи;
  - проверка подлинности ЭЦП в электронных документах;
  - плановая смена ключей уполномоченного лица УЦ и Субъектов информационного обмена;
  - внеплановая смена ключей уполномоченного лица УЦ и Субъектов информационного обмена;
  - действия владельца сертификата ключа подписи при компрометации его закрытого ключа.

При этом порядок предоставления и использования сервисов УЦ не затрагивает внутренние процессы информационного взаимодействия между подразделениями, обеспечивающими предоставление услуг конечному пользователю. Определяются лишь предназначенные для пользователя процедуры и сроки их выполнения.

ПРЕГРАДА ХАОСУ

Вместе с тем для описания внутренних процедур и действий по обеспечению деятельности УЦ и предоставлению его услуг целесообразно разработать так называемый «внутренний регламент» УЦ. А для сотрудников организации – участников информационного обмена – порядок обеспечения информационной безопасности при применении средств ЭЦП.

Разработка «внутреннего регламента» УЦ стала вторым этапом нормативного обеспечения инфраструктуры открытых ключей и применения средств ЭЦП в деятельности банка. Этот документ призван обеспечивать единый процесс выдачи и управления сертификатами, контролируемый на всех этапах. Когда в информационном обмене участвует несколько подразделений организации необходимо также соблюдение функций идентификации владельцев сертификатов. Подразделения могут участвовать в обеспечении функционирования УЦ в силу распределения полномочий, а также по территориальному признаку – при обращении клиентов в филиалы организации в регионах.

Без должного нормативного обеспечения деятельность УЦ может стать хаотичной и неконтролируемой. Особенно в крупной организации, структуры которой территориально и функционально распределены, клиент-ориентированный бизнес исключает централизацию прямого взаимодействия субъектов информационного обмена с УЦ, а создание системы из нескольких УЦ невозможно по финансовым причинам.

Так называемый «внутренний регламент» УЦ в «Россельхозбанке» был разработан в формате регламента взаимодействия подразделений, который определяет:

- зоны ответственности подразделений в процессе обеспечения деятельности УЦ;
- конкретные функции и порядок их выполнения всеми участниками процесса;
- меры обеспечения безопасности передачи между подразделениями конфиденциальной информации субъектов информационного обмена, включая ключевые носители с временной ключевой информацией.

«Внутренний регламент» УЦ описывает процедуры следующих разделов:

- регистрации Субъекта информационного обмена;
- изготовления сертификата ключа подписи Субъекта информационного обмена;
- аннулирования (отзыва) сертификата ключа подписи;
- приостановления действия сертификата ключа подписи;
- возобновления действия сертификата ключа подписи;
- проверки подлинности ЭЦП в электронных документах.

Каждый из разделов для всех участников процесса – от работника банка, непосредственно взаимодействующего с клиентом, до ИТ-подразделения и собственно УЦ – описывает конкретные задачи, а также сроки и условия обеспечения информационной безопасности в процессе их выполнения.

И НЕСПЕЦИАЛИСТ СПРАВИТСЯ

В ходе третьего этапа были разработаны документы, регламентирующие порядок обеспечения информационной безопасности при применении средств ЭЦП.

Формирование PKI-инфраструктуры предполагает применение средств ЭЦП не только специалистами по информационной защите, но и широким кругом сотрудников, многие из которых недостаточно подготовлены к соблюдению сопутствующих правил безопасности. Кроме того, методы обеспечения информационной безопасности и применения средств ЭЦП могут реализовываться различными способами в информационных системах организации.

Поэтому для обеспечения информационной безопасности организации и выполнения соответствующих требований государственных регуляторов недостаточно общих мер обеспечения безопасности закрытой ключевой информации, сформулированных в Регламенте УЦ. Следует дополнительно для каждой информационной системы прописать порядок обеспечения информационной безопасности при применении средств ЭЦП. При условии его неукоснительного соблюдения все «электронные подписанты» могут чувствовать себя в полной информационной безопасности – как за каменной стеной.

В документе, регламентирующем порядок обеспечения информационной безопасности при применении средств ЭЦП, должны быть прописаны следующие процедуры:

- назначение и учет лиц, допущенных к работе со средствами ЭЦП;
- обращение с ключевыми носителями;
- обеспечение безопасной среды функционирования средств ЭЦП, включая антивирусную защиту соответствующих АРМ;
- восстановление информации, в том числе при аварийной ситуации.

РЕГЛАМЕНТ ПРЕВЫШЕ ВСЕГО

Таким образом, создание корпоративной PKI-инфраструктуры помимо организационных и технических мероприятий должно сопровождаться разработкой следующих нормативных документов:

1. Регламента УЦ – основного нормативного документа, регулирующего деятельность PKI-инфраструктуры. Его положения могут лишь уточняться, детализироваться или дополняться другими документами, но не подменять его требования и не противоречить им.

2. Документы PKI-инфраструктуры, определяющие обеспечение юридически значимого защищенного электронного документооборота в корпоративных и внешних информационных системах. Одновременно они должны предусматривать возможности контролировать исполнение требований обеспечения его информационной безопасности как со стороны непосредственного участника процесса, так и со стороны подразделения безопасности организации, его администраторов.

* * *

Описанное нормативное обеспечение корпоративной PKI-инфраструктуры направлено на построение безопасной работы с криптографическими ключами и сертификатами, ключевыми носителями, СКЗИ, организацию контроля этой работы. Благодаря этому процедура разбора инцидентов в сфере информационной безопасности упрощается и становится прозрачной.