CNews FORUM 2017:
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЗАВТРА

Об обеспечении доверия к сервисам безопасности при реализации электронного взаимодействия в финансовой сфере

Конечная цель реализации мер безопасности

Повышение потребительских свойств защищаемого сервиса, а именно:

→ Удобство использования сервиса

→ Безопасность при использовании сервиса

Применительно к системам ДБО это означает сохранность денег

Применительно к системам электронного взаимодействия это означает контроль над правами на объект и сохранность ресурсов

Утрата любого свойства безопасности означает потерю доверия к сервису безопасности

Что такое свидетельство доверия [ИСО/МЭК 15408-1]

2.4 доверие (assurance):

→ Выполнение соответствующих действий или процедур для обеспечения уверенности в том, что оцениваемый объект соответствует своим целям безопасности.

→ Основание для уверенности в том, что сущность отвечает своим целям безопасности.

2.16 свидетельство доверия (assurance evidence): Документированные результаты, представленные данными, полученными при анализе доверия к оцениваемому объекту, включая отчеты (обоснования) в поддержку утверждения о доверии.

Какие сервисы безопасности необходимы конечному потребителю?

- Доверие к системе и сервису, позволяющее без изъятий вступать в гражданско-правовые отношения с использованием типовых электронных инструментов взаимодействия
- Равные условия доступа к цифровым сервисам для всех граждан страны, исключение «цифрового неравенства», географического фактора и удаленности субъектов от точек доступа к сервисам
- Возможность переложить свою «головную боль», возникающую при хранении и обработке электронных документов, на надежного провайдера этих услуг
- Возможность пользоваться сервисами УКЭП, желательно бесплатно и без хранения ключа подписи «в собственном кармане»

Что подрывает доверие к сервисам безопасности ?

НА БЫТОВОМ УРОВНЕ	НА ПРАВОВОМ УРОВНЕ
Информация о хищениях денег и собственности, зачастую излагаемая гипертрофировано	Утрата аутентичности данных
Запуганность людей непонятными для них, а значит, неконтролируемыми угрозами (кибератаками, хакерами, вирусами и т.д.)	Утрата легитимности сервиса безопасности по формальному признаку (окончание срока действия сертификата, аттестата на объект, лицензии на вид деятельности, окончание поддержки)
Некачественная работа предоставленного сервиса,(отказы, ошибки, неточная информация, утрата информации)	Сбои в работе СКД –СУД, нарушение конфиденциальности
Недостаточно надежная аутентификация личности	Слабый уровень доверия к сервису аутентификации
Факты мошенничества, с которыми сталкиваются люди или слышали о них	Сбои и недостатки в работе систем защиты, дающие возможность оспорить легитимность совершаемых операций

Электронный документ - автономный объект защиты

Электронный документ (совместно с его метаданными), являясь самостоятельным юридическим объектом, с точки зрения информационной безопасности также представляет собой самостоятельный, если точнее – автономный объект защиты, для которого должны быть обеспечены следующие приоритеты безопасности и требования сохранности:

- → должна быть обеспечена целостность (идентичность, аутентичность документа). Приоритет является абсолютным и должен быть обеспечен на всех этапах жизненного цикла документа;
- → должна быть обеспечена доступность документа на всех этапах жизненного цикла документа. Правила предоставления доступа к документу со временем могут изменяться в зависимости от его статуса;
- → должна быть обеспечена конфиденциальность документа. Требования к отнесению документа к категории конфиденциальных могут изменяться со временем;
- → должна быть обеспечена сохранность документа на всем жизненном цикле и защищенность от неконтролируемого уничтожения.

Основной фактор, позволяющий использовать электронный документ в системе правоотношений - это возможность придания ему в случае необходимости юридической силы на всем протяжении жизненного цикла, или с точки зрения права обеспечить необходимый уровень доверия.

Доверие к документу возникает только в том случае, когда обеспечивается его аутентичность, что подразумевает обеспечение идентичности (идентификации) и целостности электронного документа, естественно также на всем протяжении его жизненного цикла.

ТЕХНИЧЕСКИЕ, ТЕХНОЛОГИЧЕСКИЕ И ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ОСНОВАНИЯ ВОЗНИКНОВЕНИЯ И СОХРАНЕНИЯ ДОВЕРИЯ К ЭЛЕКТРОННОМУ ДОКУМЕНТУ

ТЕХНИЧЕСКИЕ, ТЕХНОЛОГИЧЕСКИЕ И ОРГАНИЗАЦИОННЫЕ СЕРВИСЫ:

- Идентификации, аутентификации и авторизации субъекта
- Электронной подписи, электронной печати, электронной метки времени
- Обеспечения доверия к web-сервису
- Доверенной доставки документов потребителю
- Конфиденциальности
- Обеспечения целостности документа и его метаданных
- Сохранности документов на всем сроке его жизненного цикла
- Выполнения требований хранения, обеспечения катастрофоустойчивости и безопасности
- Аудит и сертификация технических систем

Меры, обеспечивающие доверие к электронному документу

Организационно-правовые основания для возникновения и сохранения доверия к электронному документу

Что может быть использовано в качестве свидетельств доверия

При наличии уже действующих гарантий со стороны государства и хорошо налаженной системы контроля со стороны государственных регуляторов (или по их поручению), в качестве свидетельств доверия могут быть использованы имеющиеся документы, подтверждающие заявленные свойства безопасности.

В качестве таких свидетельств, (по аналогии со свидетельствами аудита), могут выступать:

1. Перечень реализованных исходных технических и организационных требований, на основании которых построена система защиты.
2. Положительные заключения о результатах проверки (аудита, контроля) этих требований с указанием сроков проведения контроля и очередных сроков проверки.
3. Сведения об используемых средствах безопасности, согласно заранее сформированному списку разрешенных применению средств и программных продуктов, наличие действующих сертификатов безопасности, сроки их действия.
4. Наличие действующих свидетельств аттестации объектов по требованиям безопасности, сроки их окончания.
5. Наличие соответствующих действующих лицензий (свидетельств по аккредитации) организаций на право обработки и хранения электронных документов, возможно – устанавливающих право на архивное хранение.

Какие документы могут быть использованы в качестве свидетельств доверия

Официальный, актуальный по дате отчет по результатам оценки соответствия организации требованиям защиты информации, содержащий заключение о соответствии уровня защиты организации установленным требованиям. Для организаций кредитно-финансовой сферы - не ниже 0,85.

Перечень средств защиты информации с действующими сертификатами на них. Сведения о наличии сертификатов на средства электронной подписи включаются в сертификат ключа проверки подписи.

Лицензия по технической защите конфиденциальной информации, с указанием установленных для СЭВ видов лицензированной деятельности, выданная организации - участнику электронного взаимодействия на финансовом рынке.

Лицензия, по предоставлению телематических услуг связи, выданная организации, как организатору системы доверенной передачи сообщений (требует нормативно-правового оформления).

Свидетельство об аккредитации организации на выполнение деятельности, связанной с долговременным хранением электронных документов (требует нормативно-правового оформления).

Оформление свидетельств доверия

Опора, при подготовке свидетельств доверия к техническим средствам и системам обеспечения безопасности и защиты информации, на действующие государственные системы контроля, сертификации аккредитации и лицензирования.

Это позволяет обеспечить достаточное качество контроля и обеспечить наиболее высокий уровень доверия, гарантируемый государством.

При этом, вся необходимая информация в отношении отчетов по результатам оценки соответствия требованиям защиты информации, сертификатов средств защиты, лицензий, выданных организациям, сроков их действия, причин отзыва лицензий хранится в централизованных базах данных государственных регуляторов и может быть легко проверена.

В случае необходимости, по запросу могут быть предоставлены официальные выписки, в том числе и в форме электронного документа.

Где и каким образом хранить эту информацию

Наиболее целесообразным является присоединение этой информации к самому электронному документу, что позволяет в этом случае наиболее оперативно использовать эту информацию для подтверждения уровня доверия к нему.

Такая информация может быть помещена в метаданные документа, обработанного в конкретной системе и корректироваться по мере перемещения документа из хранилища в хранилище, а также по мере измерения статус самих свидетельств.

Однако следует сократить избыточность информации, присоединяемой к документу, так как для признания свидетельства доверия легитимным, следует иметь только его реквизиты и сроки действия. Это существенно уменьшает объем присоединяемых данных, но всегда дает возможность по имеющимся реквизитам обратится к централизованно хранящемуся в базе данных первоисточнику.

ТЕРРИТОРИЯ БЕЗОПАСНОСТИ

Курило Андрей Петрович
Главный эксперт

+7 495 777 75 77
kap@rnt.ru

РОССИЙСКИЕ НАУКОЁМКИЕ ТЕХНОЛОГИИ