фикате открытого ключа или в списке отозванных сертификатов открытых ключей неверных сведений, несвоевременного включения отзываемого сертификата открытого ключа в список отозванных сертификатов открытых ключей, отсутствия доступа к списку отозванных сертификатов открытых ключей).

14. Завершение работ по вводу в постоянную эксплуатацию службы Доверенной третьей стороны Республики Беларусь и организации взаимодействия с:

ДТС государств-членов Евразийского Экономического Союза (ЕАЭС);

ДТС государств-членов Европейского Союза (ЕС).

ВОПРОСЫ ОБЕСПЕЧЕНИЯ КАЧЕСТВА ОЦЕНОК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ю. И. ИВАНЧЕНКО, И. С. ХРИПОВИЧ

Существующие на сегодняшний день методологии оценки уровня защищенности информации, информационных ресурсов и информационных систем сводятся к оценке соответствия (серия стандартов ISO 1700), а в Республике Беларусь – к подтверждению соответствия (Закон Республики Беларусь «Об оценке соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации», ст. 7 и 8) нормативно установленным требованиям. Такой подход подразумевает, что соответствующие требования, будучи выполненными, обеспечивают надлежащий уровень безопасности.

Анализ источников требований и методологий их формирования показывает невозможность формирования объективной, высококачественной и в то же время универсальной совокупности требований охватывающей весь комплекс мероприятий по обеспечению информационной безопасности организации, а отсюда и соответствующей ее оценки. Важнейшими источниками требований являются правовые и технические нормы, что позволяет обеспечить высокое качество и обязательность применения требований. Но использование нормативных правовых актов с целью повышения качества и легитимации требований не решает задачи, поскольку вступают в игру новые факторы, связанные с особенностями формирования национального законодательства и технического регулирования.

Невозможность закрыть все вопросы обеспечения информационной безопасности собственными силами, без привлечения средств, происхождение которых не вызывает доверия, и международных стандартов, осложняет положение.

В настоящее время, особенно в быстро меняющихся областях, к которым относится и область информационных технологий, этот подход вызывает все большее неудовлетворение. Причинами этого являются: невозможность оперативной актуализации нормативных актов, устанавливающих адекватные текущему времени требования; многообразие особенностей объектов оценки, которые невозможно отразить в нормативных актах; сильное влияние на процессы оценивания человеческого фактора и др.

Но ключевой вопрос при этом – соответствие самих требований современным представлениям о требуемом (приемлемом) уровне безопасности оцениваемых объектов. Вновь возникает задача оценки, но уже нового объекта (совокупности требований), весьма неоднозначному критерию – некоторому (приемлемому) уровню. Таким образом, вся цепочка операций от определения приемлемого уровня до собственно оценки соответствия в каждом своем звене содержит погрешность, поскольку в значительной степени строится не на формальных выводах или расчетах, а на основе субъективных факторов и качественных оценок. Но если обратиться к началу цепочки, то очевидно, что наиболее приемлемым критерием определения приемлемого уровня информационной безопасности, с которого начинается и формирование

требований, в настоящее время является возможный ущерб – риск информационной безопасности. В качестве примера даже для государственных секретов определяющим является тяжесть последствий, которые наступили или могут наступить, размер вреда, другими словами, ущерб, который может быть причинен в результате их разглашения или утраты. Таким образом, оценка риска информационной безопасности может быть использована для оценки уровня защищенности организации, системы, ресурса и т. д. Можно использовать и термин «оценка соответствия» на основе оценки риска, если заранее определиться со значением критичного недопустимого риска.

Если пользоваться оценками рисков в денежном выражении, то это может оказаться универсальным критерием оценки уровня обеспечения информационной безопасности вне зависимости от применяемых правовых или технических норм. Последние в этом случае становятся не целью, а средством, в том числе получения конкурентных преимуществ.

ОСОБЕННОСТИ РАЗРАБОТКИ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА ДОВЕРЕННЫХ ЦЕНТРОВ ОБЕСПЕЧЕНИЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Д. А. КОМЛИКОВ, А. Н. ГАВРИЧЕНКО

На сегодняшний день очень остро стоит проблема организации трансграничного обмена электронными документами и оказания электронных услуг. Проблема заключается в создании доверенной инфраструктуры, содержащей центры доверенных сервисов, используемых информационными системами (ИС), юридическими и физическими лицами при трансграничном взаимодействии. При этом доверенные сервисы не должны зависеть от используемых средств электронной цифровой подписи (ЭЦП) или национального законодательства и стандартов в области ЭЦП.

Технические концепции доверенной третьей стороны (ДТС) изложены в международных рекомендациях ITU-T X.842, определяющих требования по использованию и управлению услугами доверенной третьей стороны.

Единое пространство доверия представляет собой свод нормативных правовых, национальных и межгосударственных актов, а также технических условий для обеспечения юридической значимости электронного взаимодействия.

С технической точки зрения Единое пространство доверия представляет собой совокупность систем доверенных сервисов ДТС и доверенных удостоверяющих центров (УЦ).

Основными функциями центров ДТС при трансграничном обмене электронными документами между сторонами являются:

- проверка действительности ЭЦП на электронном сообщении (документе);
- проверка валидности сертификата;
- выработка штампа времени, связанного с проверкой, и отправки квитанции, подписанной ЭЦП центра ДТС.

С целью решения проблем организации трансграничного обмена электронными документами и оказания электронных услуг Государственное предприятие «НИИ ТЗИ» выполнило опытно-конструкторскую работу (ОКР) «Разработка программно-аппаратного комплекса доверенных центров обеспечения электронного документооборота». Основанием для выполнения ОКР являлась программа Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на основе высоких технологий» на 2011–2015 гг., утвержденная постановлением Совета Министров Союзного государства от 20.04.2012 № 6.

Результатом выполнения ОКР является программно-аппаратный комплекс «Доверие», реализующий функции доверенной третьей стороны (ПАК-ДТС).