Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

Для данной комплексной модели уязвимости информационных объектов справедливо выполнение условия:

$$\exists\left(v_{k^{\otimes}} \in V^{\otimes}\right)\ \exists\left(Y=\{y_i\}\right)\left(R_1^{\bullet}=\left\{r_{c_1}^{\bullet}=\langle y_i, v_{k^{\otimes}}, a_j\rangle\right\}, \mathbf{r}_{\mathbf{c_1}}^{\otimes}=\left(\mathbf{y_i}\ \mathbf{v_{k^{\otimes}}}\mathbf{a_j}\right)\neq \mathbf{0}\right),\ i=\overline{1,I}, j=\overline{1J}.$$

Таким образом, задача формализации процесса информационного противоборства может быть решена. С целью развития теоретических основ информационного противоборства методика ее решения может корректироваться в рамках предложенного подхода, а предложенная комплексная модель уязвимости информационных объектов может быть использована для проведения оценки и ранжирования уязвимостей информационных объектов, определения степени их опасности в статическом режиме, разработки комплексного показателя, характеризующего уязвимость информационных объектов как элемент безопасности.

Список литературы

1. Гриняев, С. Н. Информационная война в ходе агрессии США, Великобритании и их союзников против Ирака. / С. Н. Гриняев. // Аналитический доклад. Центр стратегических оценок и прогноза. – М., 2010. – 118 с.

2. Гриняев, С. Н. Поле битвы – киберпространство: теория, приемы, средства, методы и системы ведения информационной войны / С. Н. Гриняев. – Минск: Харвест, 2004. – 448 с.

3. Гриняев, С. Н. Война в четвертой сфере / С. Н. Гриняев. // Независимое воен. обозрение. – №42. – 2000.

4. Рудаков, А. Б. Стратегия информационной войны / А. Б. Рудаков. // АТЕНЕЙ. – М.: 2003. – 145 с.

5. Горевич, Б. Н, Эльяс, В. П. Проблема оценки эффективности функционирования сложноформализуемых систем военного назначения. / Б. Н Горевич, В. П. Эльяс. // С-Пб.: ВМИРЭ им. А.С. Попова. Прикладные вопросы военно-морской радиоэлектроники. 2008.

ДОВЕРЕННАЯ ТРЕТЬЯ СТОРОНА: РЕАЛИИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Д.В. МОСКАЛЕВ

Республиканское унитарное предприятие «Национальный центр электронных услуг»

Современный мир стремится к взаимодействию в электронном виде. В различных областях жизнедеятельности общества – будь то здравоохранение, образование или бизнес, банковская или социальная сфера – для информационного взаимодействия применяются электронные документы, подлинность и целостность которых подтверждается электронной цифровой подписью (далее – ЭЦП). ЭЦП позволяет создавать электронные документы, имеющие юридическую силу на территории определенного государства.

Вместе с тем в основе применяемых электронных цифровых подписей различных государств лежит несколько существенных отличий:

различные криптографические алгоритмы,

различия в законодательстве,

различные подходы к защите информации,

различные системы сертификации (экспертизы) средств криптографической защиты информации.

Для построения трансграничного электронного взаимодействия на межгосударственном уровне следует установить необходимый уровень доверия к электронным документам.

На сегодняшний день существуют три основных подхода в части признания документов с иностранной электронной подписью:

концепция Доверенной третьей стороны (далее – ДТС);

возможный отказ от собственных правил и принятие стандарта одной из сторон единым стандартом системы;

поддержка криптографических реализаций всех участников в конкретном сервисе (обмен средствами электронной цифровой подписи).

Концепция ДТС является единственным оптимальным решением, как с технической точки зрения, так и со стороны правовых норм. Именно этот механизм позволяет участникам оставаться в правовом поле в сфере электронной подписи своей страны, не принимая чужие и не навязывая свои правила другим государствам [1].

ДТС нацелена на сохранение в разных странах собственного пространства доверия, но при этом будет обеспечивать возможность трансграничного обмена электронными документами. При этом данная технология не отрицает и не подменяет существующие национальные технологии, а дополняет их.

Каждый «игрок» живет в отношении электронной подписи по своим правилам, со своими алгоритмами, в своем правовом пространстве, но при этом существует и механизм проверки, который позволяет доверять документы с электронными подписями одной страны – в другой.

Каким образом можно установить, что иностранная подпись действительно легитимна и «соответствует нормам иностранного права»?

Например, для обеспечения доверия при электронном взаимодействии в рамках Евразийского экономического союза в каждом государстве создается доверенная третья сторона (независимый посредник или служба), которая всегда будет в курсе текущих изменений в законодательстве той страны, подпись из которой она проверяет, и которая будет выдавать юридически правомочное, составленное по нормам страны, в юрисдикции которой она находится, заключение о действительности электронной подписи из другого государства.

Данная концепция предполагает существование в каждой из взаимодействующих сторон своего центра (той самой Доверенной третьей стороны, который, будучи аккредитован в своей стране, в соответствии со своими национальными правилами, не только уполномочен проверить действительность сертификата (получен ли он законно, не скомпрометирован ли, не отозван ли, не утерян ли т.д.) и электронной подписи под документом, но и выдавать квалифицированную справку (квитанцию) о результатах такой проверки (что проверялось, когда проверялось, результаты проверки). Каждая такая квитанция подписывается ЭЦП ДТС, производившей проверку. Это означает, что, например, белорусская ДТС, подтвердившая законность и действительность ЭЦП на документе, присланном из другого государства – несет полную юридическую ответственность за результаты такой проверки. В случае возникновения спорных ситуаций, данная квитанция может служить юридически значимым доказательством того, что данный документ был подписан в соответствии со всеми юридическими нормами страны подписанта.

Таким образом, применение сервиса ДТС позволяет:

повысить удобство обмена электронными документами (далее – ЭД), подписанными электронной цифровой подписью различных государств;

повысить уровень надежности и защищенности трансграничного межгосударственного информационного взаимодействия;

разрешать спорные вопросы, возникающие между участниками межгосударственных информационных процессов.

В соответствии с Указом Президента Республики Беларусь от 8 ноября 2011 года № 515 «О некоторых вопросах развития информационного общества в РБ» (с изменениями, внесенными Указом от 15.03.2016 года № 98) республиканское унитарное предприятие «Национальный центр электронных услуг» назначено национальным оператором доверенной третей стороны по признанию подлинности электронных документов при межгосударственном электронном взаимодействии [2].

Использование технологии ДТС позволяет использовать имеющуюся в государстве инфраструктуру открытых ключей без дополнительной ее модернизации при межгосударственном электронном взаимодействии. Но, с другой стороны, это накладывает существенные меры по определению и обеспечению ответственности за совершаемые действия субъектами такого взаимодействия.

Основными задачами ДТС являются [1]:

осуществление легализации (подтверждение подлинности) ЭД и ЭЦП субъектов информационного взаимодействия в фиксированный момент времени;

обеспечение проверки ЭЦП отправителя, выбранной в соответствии с законодательством государства, в юрисдикции которого находится этот отправитель;

обеспечение гарантий доверия в международном (трансграничном) обмене ЭД;

обеспечение правомерности применения ЭЦП в исходящих и (или) входящих ЭД в соответствии с законодательством Республики Беларусь и государства, по которому оператор ДТС оказывает услуги.

Среди возможных областей для использования сервисов ДТС, кроме межгосударственного электронного документооборота, выделяют электронную торговлю, государственные закупки, телемедицину, дистанционное образование, фондовый рынок, мобильные платежные системы, электронные библиотеки и многое другое.

НЦЭУ осуществляет работу по развитию ДТС в двух основных направлениях:

1. В декабре 2016 года введена в постоянную эксплуатацию автоматизированная информационная система доверенной третьей стороны Республики Беларусь (ДТС-Беларусь) для коммерческого использования.

2. В рамках развития интегрированной информационной системы ЕАЭС создается сервис ДТС национального сегмента РБ интегрированной системы.

ДТС для коммерческого использования.

Типовая схема взаимодействия ДТС-Беларусь РБ и ДТС иностранного государства для коммерческого использования приведена на рисунке 1.

Для проверки иностранного ЭД Клиент посредством веб-интерфейса ДТС формирует и направляет в ДТС электронный запрос с приложением ЭД, подлежащего проверке на подлинность. Доступ к веб-интерфейсу ДТС осуществляется через личный кабинет единого портала электронных услуг (далее – портал) ОАИС или по выделенномуVPN-каналу.

Перечень иностранных государств и их УЦ, по которым ДТС-Беларусь оказывает услуги в зависимости от страны происхождения ЭД, размещается на сайте НЦЭУ.

Ознакомиться с работой ДТС-Беларусь можно по ссылке https://nces.by/pki/news-dts.

На сегодняшний день успешно проведено тестирование и осуществляется взаимодействие ДТС-Беларусь с ДТС Республики Казахстан (РГП «Государственная техническая служба» Министерства информации и коммуникаций Республики Казахстан).

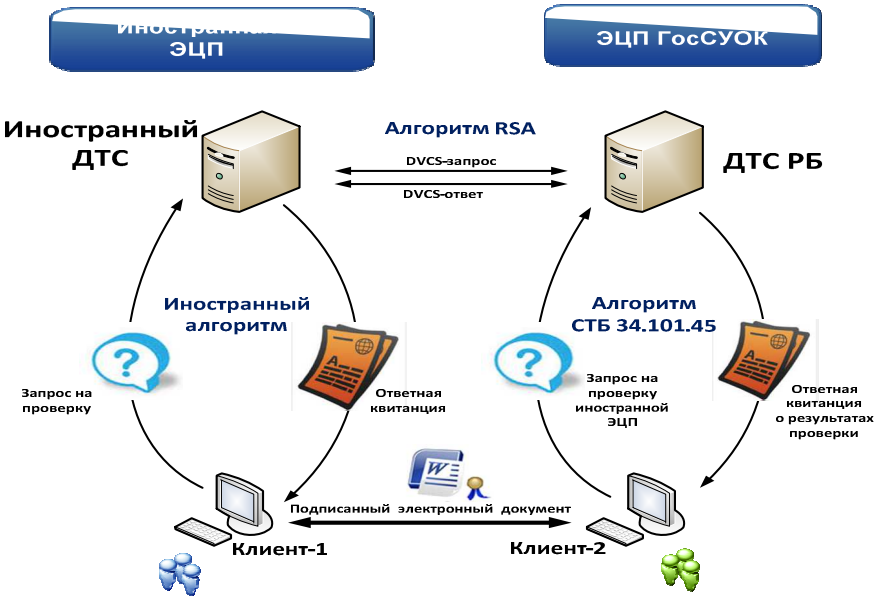

Рис. 1 – Типовая схема взаимодействия ДТС при коммерческом использовании

Сервис ДТС национального сегмента РБ интегрированной информационной системы ЕАЭС.

В соответствии с законодательством государств-членов Евразийского экономического союза (далее соответственно – государства-члены, Союз) документ в электронном виде, подписанный соответствующей законодательству электронной цифровой подписью (электронной подписью) (далее – ЭЦП), признается электронным документом (далее – ЭД), равным по юридической силе аналогичному документу на бумажном носителе, заверенному подписью (подписью и печатью) составителя такого документа.

При этом в государствах-членах в соответствии с их законодательством обеспечение юридической силы ЭД и организация защищенного документооборота построены на гарантиях их подлинности и целостности посредством применения национальных криптографических методов и средств [5].

Государства-члены, включая Республику Беларусь (далее – РБ), используют национальные стандарты криптографических алгоритмов создания и проверки ЭЦП. Применяемые органами государственной власти государств-членов способы реализации криптографических алгоритмов между собой несовместимы, что обусловлено различными подходами к обеспечению информационной безопасности.

Обеспечение трансграничного обмена имеющими юридическую силу ЭД в интегрированной информационной системе Евразийского экономического союза (далее – интегрированная система) реализуется на основе применения создаваемой службы доверенной третьей стороны (далее – ДТС) интегрированной системы [1].

Служба ДТС интегрированной системы состоит из сервисов ДТС национальных сегментов и сервиса ДТС Евразийской экономической комиссии (далее – ЕЭК), в совокупности образуя ядро трансграничного пространства доверия [4].

Сервисы ДТС национального сегмента Республики Беларусь (далее – ДТС-Беларусь-ЕЭК) является составной частью этой интегрированный системы.

Сервисы ДТС-Беларусь взаимодействуют с интеграционным шлюзом интеграционного сегмента РБ, который входит в состав интеграционной платформы интегрированной системы, через который осуществляется взаимодействие с национальными сегментами других государств-членов и сегментом Комиссии. Отправители (получате-

ли) при подписании и проверке ЭЦП используют криптографические стандарты, принятые на уровне соответствующего государства-члена. Для применения в Комиссии используются криптографические стандарты, определенные решением Комиссии. При взаимодействии сервисов службы ДТС между собой используется согласованный криптографический стандарт (стандарт службы ДТС), определенный для этих целей решением Комиссии.

ДТС оказывают участникам межгосударственного информационного обмена услуги по проверке ЭЦП отправителя в криптографическом стандарте юрисдикции отправителя с подписанием квитанции как результата такой проверки. Электронный документ с результатом положительной проверки ДТС признается в юрисдикции получателя равнозначным электронному документу, подписанному собственной ЭЦП отправителя на основе нормы о признании ЭЦП, выданных в соответствии с нормами иностранного права. Инфраструктура ДТС (подсистемы/программно-аппаратные комплексы) должна быть размещена во всех национальных сегментах и интегрированном сегменте (ДТС Комиссии) интегрированной системы.

Компонентами обеспечения юридической силы ЭД национального сегмента РБ являются [4-6]:

удостоверяющий центр службы ДТС ЕЭК;

ДТС-Беларусь-ЕЭК (сервис подтверждения подлинности, сервис штампов времени, сервис хранения данных);

республиканский удостоверяющий центр Государственной системы управления открытыми ключами.

Для создания инфраструктуры сервисов ДТС интеграционного сегмента РБ интегрированной системы оператору ДТС-Беларусь-ЕЭК НЦЭУ передано программное обеспечение (далее – ПО) типовой службы ДТС интеграционного сегмента ЕЭК интегрированной системы в соответствии с «Порядком передачи программного обеспечения интеграционного сегмента Евразийской экономической комиссии интеграционной информационной системы Евразийского экономического союза и его использования», утвержденным Решением Коллегии ЕЭК от 26.01.2016 № 10.

Схема электронного документооборота в интегрированной информационной системе ЕАЭС приведена на рисунке 2.

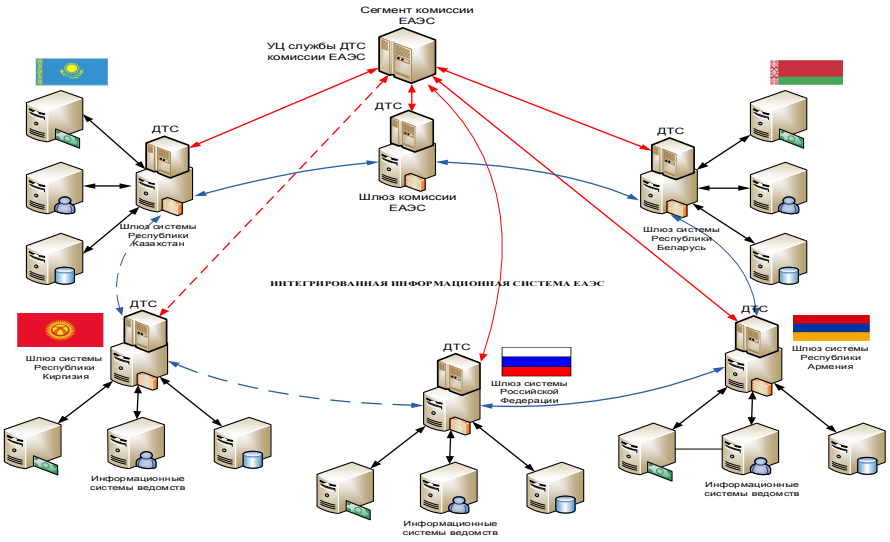

Рис. 2 – Схема электронного документооборота
в интегрированной информационной системе ЕАЭС

В соответствии со Стратегией развития трансграничного пространства доверия (на 9 лет) [3], предусмотрено три этапа:

1. 1 этап (до 2018 года) – должно обеспечиваться развитие трансграничного пространства доверия для осуществления полноценного межгосударственного электронного взаимодействия. На данном этапе:

формируются требования к правовому, организационному и техническому обеспечению, составу и характеристикам сервисов трансграничного пространства доверия при межгосударственном информационном взаимодействии государств-членов на основе службы доверенной третьей стороны, которые закрепляются актами государств-членов и органов Союза (принимаются нормативные правовые и нормативно-технические акты, разрабатываются документы организационного характера);

создаются интеграционные шлюзы и программно-аппаратные комплексы доверенных третьих сторон государств-членов и Комиссии;

с использованием службы доверенной третьей стороны обеспечивается подтверждение подлинности электронной цифровой подписи (электронной подписи) на электронных документах при реализации общих процессов в рамках Союза;

прорабатываются вопросы, связанные с поэтапным формированием и выполнением государствами-членами согласованных требований в области криптографической защиты трансграничного пространства доверия;

проводятся подготовительные мероприятия по масштабированию трансграничного пространства доверия для взаимодействия с международными организациями и государствами, не являющимися членами Союза.

Субъектами электронного взаимодействия на данном этапе должны стать должностные лица и сотрудники органов государственной власти государств-членов, должностные лица и сотрудники органов Союза.

Приоритетом в реализации настоящей Стратегии на данном этапе должно стать обеспечение возможности для всех органов государственной власти государств-членов использовать преимущественно электронные документы, подписанные электронными цифровыми подписями (электронными подписями).

2. 2 этап (до 2020 года) – при условии согласования совместных подходов государств-членов к формированию правового, технического и организационного обеспечения трансграничного пространства доверия и на основе поэтапного выполнения государствами-членами согласованных требований в области криптографической защиты трансграничного пространства доверия должна быть обеспечена возможность электронного взаимодействия физических и юридических лиц между собой, а также с органами государственной власти государств-членов при нахождении физических и юридических лиц на территориях своих государств.

3. 3 этап (до 2024 года) – при условии согласования совместных подходов государств-членов к формированию правового, технического и организационного обеспечения трансграничного пространства доверия и на основе поэтапного выполнения государствами-членами согласованных требований в области защиты информации трансграничного пространства доверия должны начать формироваться межгосударственный институт электронного нотариата на основе службы доверенной третьей стороны и другие межгосударственные сервисы электронных услуг, в том числе в области трудовой миграции, которые вовлекут в процесс электронного взаимодействия в рамках трансграничного пространства доверия физических лиц.

На этом этапе должны быть созданы правовые, организационные и технические условия для обеспечения формирования института электронного нотариата на основе

службы доверенной третьей стороны и разработаны требования к организации взаимодействия с электронными торговыми площадками в рамках трансграничного пространства доверия.

Список литературы

1. Решение Совета Коллегии Евразийской экономической комиссии от 18 сентября 2014 г. № 73 «О Концепции использования при межгосударственном информационном взаимодействии сервисов и имеющих юридическую силу электронных документов».

2. Указ Президента Республики Беларусь от 08.11.2011 г. № 515 «О некоторых вопросах развития информационного общества в Республике Беларусь» (с изм. от 15.03.2016 № 98).

3. Стратегия развития трансграничного пространства доверия, утверждена решением Коллегии ЕЭК от 27.09.2016 № 106.

4. Положение об обмене ЭД при трансграничном взаимодействии органов государственной власти государств – членов ЕЭС между собой и с ЕЭК, утвержденное решением Коллегии Комиссии от 28.09.2015 № 125.

5. Правила электронного обмена данными в интегрированной информационной системе внешней и взаимной торговли, утвержденные решением Коллегии Евразийской экономической комиссии от 27 января 2015 г. № 5.

КОНЦЕПТУАЛЬНЫЕ ПОДХОДЫ К РАЗВИТИЮ ТЕОРИИ И ПРАКТИКИ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

С.И. ПАСКРОБКА, Ю.Е. КУЛЕШОВ

Белорусский государственный университет информатики и радиоэлектроники

Анализ концептуального уровня развития теории и практики информационного противоборства развитых государств и степени подготовленности их вооруженных сил к информационному противоборству показал, что они имеют значительные наработки как в степени теоретического осмысления роли и места информационного противоборства в достижении политических и военных целей государств, так и в практике его организации и ведения.

Теория информационного противоборства получила мощное развитие после создания современных методов военной системологии, используя которые, можно быстро найти уязвимые места в системах управления, связи, компьютерного обеспечения и разведки противника и, выводя их из строя, резко повысить эффективность своих действий в других видах противоборства.

Поэтому выявление проблем и противоречий, а также наиболее эффективных направлений развития теории информационного противоборства, форм и способов его ведения с учетом развития современных средств информационного противоборства представляется первостепенной задачей современной белорусской военной науки.

В свою очередь развитие теоретических основ информационного противоборства, важнейшими элементами которого являются законы, закономерности и принципы его ведения, создает необходимую методологическую базу для выработки научно обоснованных рекомендаций и обоснованных руководящих документов по организации и ведению информационного противоборства.

Развитие теоретических основ информационного противоборства и методологии оценки его эффективности, исследование информационного аспекта строительства,