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

СЕКЦИОННЫЕ ЗАСЕДАНИЯ

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

НОРМАТИВНЫЕ ТРЕБОВАНИЯ И ПРАКТИКА АТТЕСТАЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

И.Е. АМЕЛИШКО

Общество с ограниченной ответственностью «Лайт Вел Организейшн»

Основными нормативными правовыми документами, определяющими порядок создания и аттестации систем защиты информации информационных систем, являются:

Закон Республики Беларусь от 10.11.2008 № 455-З (ред. от 11.05.2016) «Об информации, информатизации и защите информации»;

Положение о технической и криптографической защите информации в Республике Беларусь, утверждено Указом Президента Республики Беларусь от 16.04.2013 № 196 «О некоторых мерах по совершенствованию защиты информации»;

Положение о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утверждено приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 № 62 (в редакции приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 16.01.2015 № 3);

Положение о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утверждено приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 № 62 (в редакции приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 16.01.2015 № 3);

Положение о порядке криптографической защиты информации в государственных информационных системах, информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, и на критически важных объектах информатизации, утверждено приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 № 62.

Положения о порядке технической защиты информации и криптографической защиты информации я включил в этот список так как в них определены требования к документам и порядок выполнения мероприятий при проектировании, разработке и создании системы защиты информации, анализ которых проводится при проведении аттестации.

В соответствии с требованиями законодательства для защиты информации в информационных системах создается система защиты информации, включающая комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

Аттестация системы защиты информационной системы является тем механизмом, который должен ответить на вопросы достаточности реализованных организационных и технических мер и гарантировать защищенность информации ограниченного распространения, обрабатываемой в информационной системе.

В 2009 году постановлением Совета Министров Республики Беларусь № 675 было утверждено Положение об аттестации систем защиты информации, которое определяло порядок аттестации систем защиты информации, используемых при обработке информации, распространение и (или) предоставление которой ограничено, а также информации, содержащейся в государственных информационных системах.

Данным положением было определено, что для проведения аттестации должна разрабатываться программа аттестации, содержащая перечень работ и их продолжительность, методики испытаний, перечень используемой контрольной аппаратуры и тестовых средств, а также перечень привлекаемых аккредитованных испытательных лабораторий по требованиям безопасности информации.

Таким образом, присутствовало нормативное требование о проведении испытаний системы защиты информации и оформлении их результатов с привлечением квалифицированных специалистов аккредитованных испытательных лабораторий.

Более поздним документом – Положением о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утвержденным приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 № 62 (в редакции приказа ОАЦ от 16.01.015 № 3), требования о разработке методик испытаний и привлечении к испытаниям аккредитованных испытательных лабораторий были исключены.

И вот здесь возникает коллизия, когда в соответствии с требованиями законодательства при оценке продуктов информационных технологий по требованиям безопасности в одном случае (при испытании средств защиты безопасности) требуется проведение испытаний в аккредитованных испытательных лабораториях по методикам, согласованным с органом по сертификации – ОАЦ, а в других (при испытаниях систем защиты) – требования о проведении испытаний есть, а о порядке их проведения – отсутствуют.

Причем вопрос проведения испытаний актуален также и для организаций, которые проводят аттестацию силами аттестационной комиссии, назначенной приказом (решением) руководителя организации. Достаточна ли квалификация и уровень подготовленности специалистов, включенных в комиссию, имеются ли у нее для решения задач аттестации, в том числе для проведения испытаний системы защиты.

В настоящее время по данным информации из реестра лицензий ОАЦ насчитывается 33 организации имеющих право на проведение аттестации систем защиты информации информационных систем и лишь 12 из них имеют испытательные лаборатории. Следует также принимать во внимание область аккредитации испытательных лабораторий, так как оценивать качество встраивания средств криптографической защиты информации и правильность выполнения криптографических операций способны только специалисты с соответствующим образованием. Вместе с тем, известны факты, когда для участия в конкурсе на аттестацию системы защиты с применением СКЗИ, заявлялись организации, не имеющие не только испытательной лаборатории, но даже хотя бы одного специалиста в области криптографии.

Рассматривая вопрос квалификации специалистов возникает проблема проверки подготовки кадров и распределения ответственности персонала за организацию и обеспечение выполнения требований по защите информации.

Единый квалификационный справочник должностей служащих (ЕКСД) «Выпуск 1 ЕКСД. Должности служащих для всех видов деятельности» предъявляет следующие квалификационные требования администратору баз данных, администратору сервера (web-, файл-, почтового и др.), администратору сетей (администратору системному) (без категории): высшее профессиональное (математическое, инженерно-математическое,

техническое) образование и стаж работы в должностях по специальности, замещаемых специалистами с высшим профессиональным образованием, не менее 3 лет.

Вместе с тем, в НПА отсутствует ссылка на необходимость учитывать выше названные требования, либо какие-нибудь другие при проверке квалификации кадров в ходе аттестации, что может использоваться недобросовестными аттестующими.

Также, учитывая международную практику при оценке защищенности информационных систем целесообразно было бы проводить тесты на проникновение (пентесты), которые могли бы подтверждать состоятельность системы защиты в межаттестационный период. Причем целесообразно было бы установить периодичность их проведения (например, в платежной системе PSI DSS, тесты на проникновение проводятся, как правило, один раз в квартал) для систем защиты информации это мог бы быть один год. Можно также предусмотреть проведение пентестов в случае выявления уязвимостей как в самой системе, так и в средствах защиты, входящих в ее состав. По результатам выполнения тестов на проникновение принимать решение о необходимости модернизации системы защиты либо о продолжении ее эксплуатации.

Важным признаком испытаний является задание определенных условий испытаний. Они могут быть реальными или моделируемыми. Условия испытаний (ГОСТ 16504-81) – совокупность воздействующих факторов и (или) режимов функционирования объекта при испытаниях.

Таким образом с целью создания условий воспроизводимости и повторяемости результатов испытаний одной или несколькими испытательными лабораториями, а также для обеспечения достоверности материалов при проведении расследований инцидентов информационной безопасности необходима фиксация топологии и архитектуры информационных систем и систем защиты информации. С этой же целью в паспортах на рабочие места, на которых осуществляется администрирование информационной системы и системы защиты информации, а также обработка защищаемой информации, должны быть указаны установленное программное обеспечение и приложения.

Подводя краткие итоги можно сказать, что для обеспечения единообразного подхода к проведению аттестации и для того, чтобы выданный аттестат был документом, действительно подтверждающим соответствие системы защиты требованиям НПА и ТНПА необходимо:

выработать требования к порядку разработки и, возможно, согласования методик проведения испытаний систем защиты информации, а также непосредственно проведения испытаний, проведения межаттестационных испытаний (пентестов);

для сокращения времени проведения аттестации для вновь создаваемых систем предусмотреть совмещение приемочных испытаний и испытаний, проводимых в рамках аттестации;

нормативно определить минимальные квалификационные требования к персоналу (администраторам IT систем, администраторам (специалистам) информационной безопасности). Возможно, отражать требования к квалификации персонала в задании по безопасности;

предусмотреть представление заявителем на аттестацию документов, фиксирующих топологию и архитектуру информационной системы и системы защиты информации, а также паспортов на рабочие места.

Список литературы

1. Закон Республики Беларусь от 10.11.2008 № 455-З (ред. от 11.05.2016) «Об информации, информатизации и защите информации», «Национальный реестр правовых актов Республики Беларусь», 08.09.2010, № 212, 1/11914.

2. Положение о технической и криптографической защите информации в Республике Беларусь, утвержденное Указом Президента Республики Беларусь от 16.04.2013 № 196 «О некоторых мерах по совершенствованию защиты информации», Национальный правовой Интернет-портал Республики Беларусь, 18.04.2013, 1/14225.

3. Положение о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, утверждено приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 № 62 (в редакции приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 16.01.2015 № 3), Национальный реестр правовых актов Республики Беларусь, Национальный правовой Интернет-портал Республики Беларусь, 10.09.2013, 7/2561.

КВАНТОВЫЙ МЕТОД КОНТРОЛЯ НЕСАНКЦИОНИРОВАННЫХ ПОДКЛЮЧЕНИЙ К ОПТОВОЛОКОННЫМ ЛИНИЯМ СВЯЗИ

О.К. БАРАНОВСКИЙ, А.О. ЗЕНЕВИЧ, О.Ю. ГОРБАДЕЙ, С.А. ГАИБОВ

Белорусская государственная академия связи

Оптоволоконные линии связи зарекомендовали себя в качестве надежной среды передачи, обеспечивающей реализацию высоких скоростей передачи данных. В настоящее время для решения задач обеспечения конфиденциальности передаваемой информации используют алгоритмы криптографической защиты. В ряде случаев решение задачи контроля отсутствия несанкционированных подключений к линиям связи не может быть выполнено традиционными способами.

Сложность обнаружения несанкционированного съема информации с оптической линии связи связана с развитием безразрывных способов подключения к оптическому волокну, использующих нарушение закона полного внутреннего отражения оптического излучения в волокне. Перехват оптического излучения злоумышленником реализовывается пассивным или активным способами съема данных, что приводит к частичной или полной потере мощности оптического излучения, несущего информацию о каждом отдельном бите сообщения, в результате увеличивается число ошибок приема. Однако применение злоумышленником компенсационного способа съема данных не влияет на качество передачи данных современных систем связи и может быть не обнаружено [1].

Как показано в работах [2,3], наиболее эффективными являются методы контроля отсутствия несанкционированных подключений к каналу связи, основанные на регистрации изменения состояния фотонов на выходе оптического волокна в случае подключения злоумышленника по сравнению со штатным режимом работы линии связи.

Вместе с тем перспективными являются квантовые методы, использующие статистический характер оптического излучения. Добавление контрольного квантового сигнала в общий информационный сигнал, передаваемый по оптоволоконной линии связи, позволит гарантированно решить задачу обнаружения несанкционированного подключения путем учета физических эффектов, связанных с процессами генерации, переноса и регистрации отдельных квантов света.

Учтем, что при компенсационном способе съема оптического излучения с боковой поверхности оптического волокна возникает временная задержка в распространении информационного сигнала или его части по сравнению со штатным режимом работы. Минимальная задержка в таком случае будет являться суммой времен прохождения фотоном расстояния от места его вывода из оптического волокна до места детектирования, погло-