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

щенности информации, а на оценку качества реализации процессов, связанных с созданием, внедрением и функционированием системы защиты информации организации. Снижение временных затрат на проведение аудита связано со следующими причинами, обуславливающими уменьшение количества нормативных и правовых коллизий при реализации названного процесса: корректный выбор круга лиц из числа сотрудников аудируемой организации; точное определение перечня анкетных вопросов для сотрудников аудируемой организации; корректные планирование и определение очередности проведения аудита системы менеджмента защиты информации в организациях электросвязи (в случае выполнения задачи по проведению аудита в нескольких организациях одновременно).

Список литературы

1. О некоторых мерах по обеспечению безопасности критически важных объектов информатизации : Указ Президента Респ. Беларусь, 25 окт. 2011 г., № 486 // Нац. реестр правовых актов Респ. Беларусь. – 2011. – № 121. – 1/13026.

2. Об утверждении Инструкции о порядке проведения внешнего контроля за обеспечением безопасности критически важных объектов информатизации : Приказ Оперативно-аналитического центра при Президенте Респ. Беларусь 30 апр. 2012 г., № 42 // Нац. реестр правовых актов Респ. Беларусь. – 2012. – № 52. – 7/2003.

3. Бойправ, В.А. Принципы реализации методики аудита системы менеджмента защиты информации в организациях электросвязи / В.А. Бойправ, Л.Л. Утин // Доклады БГУИР. – 2016. – № 6 (100). – С. 94–99.

НОРМАТИВНО-ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ РЕСПУБЛИКИ БЕЛАРУСЬ

А.В. ДЕНИСЕВИЧ

Оперативно-аналитический центр при Президенте Республики Беларусь

В настоящее время по оценке Международного союза электросвязи Республика Беларусь по итоговому индексу развития информационно-коммуникационных технологий поднялась с 52 места в 2011 г. на 31-е в 2016 г. среди 175 стран. За данный период в Беларуси создан базовый комплекс электронного правительства, в который входят такие компоненты как: общегосударственная автоматизированная информационная система, система межведомственного электронного документооборота, Государственная система управления открытыми ключами проверки электронной цифровой подписи, единое расчетное информационное пространство. Завершено строительство Республиканского центра обработки данных. Осуществляется информатизация здравоохранения, образования, социально-трудовой сферы. Основной задачей внедрения ИКТ в реальном секторе экономики является повышения эффективности управления полным циклом производства, создание интегрированных информационных систем, осуществляющих управление ресурсами предприятия. Развитие информатизации в Республике Беларусь приведет к появлению новых угроз национальной безопасности в информационной сфере, с которыми уже столкнулись страны с высоким индексом развития ИКТ. Объекты в отношении которых могут быть реализова-

ны угрозы информационной безопасности, представлены в различных сферах деятельности (энергетика, промышленность).

Примером этого может выступать компьютерная атака, совершенная в Германии на металлургическом предприятии, злоумышленникам удалось удаленно вывести из строя доменную печь, что привело к поломке и простою производства. Доступ к печи хакеры получили, заразив вредоносным программным обеспечением офисную сеть. В декабре 2015 года на Украине зафиксирована компьютерная атака на энергетическую систему. Злоумышленнику удалось получить несанкционированный доступ к системе управления компании «Прикарпатье облэнерго», специализирующейся на передаче и снабжении электроэнергией потребителей в западной Украине. На протяжении нескольких часов область и сам город остались без энергоснабжения (без электричества остались более 200 тысяч человек).

В соответствии с Концепцией национальной безопасности Республики Беларусь одним из основных национальных интересов в информационной сфере является обеспечение надежности и устойчивости функционирования критически важных объектов информатизации. Основными потенциальными либо реально существующими угрозами национальной безопасности являются нарушение функционирования критически важных объектов информатизации. В информационной сфере внутренними источниками угроз национальной безопасности являются несовершенство системы обеспечения безопасности критически важных объектов информатизации. В связи с планомерным развитием информатизации в Республике Беларусь возрастает количество информационных систем функционирующих в системе ЖКХ, здравоохранения, образования, банковского сектора (в том числе предоставляющие услуги процессинга), финансового сектора, энергетики, промышленности, торговли, транспорта и коммуникаций, связи и информатизации подверженных в информационной сфере. Данный факт говорит о важности и необходимости регулирования в области обеспечения информационной безопасности критически важных объектов информатизации Республики Беларусь.

В настоящее время для обеспечения безопасности критически важных объектов информатизации (далее — КВОИ) используется следующее законодательство:

«Положение об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации», утверждено Указом Президента РБ от 25 октября 2011 г. № 486. Положение устанавливается порядок отнесения объектов информатизации к критически важным и обеспечения безопасности КВОИ.

«Положение о Государственном реестре критически важных объектов информатизации», утверждено Приказом Оперативно-аналитического центра при Президенте РБ 20.12.2011 № 96. Положение определяется порядок включения объектов информатизации в Государственный реестр КВОИ, ведения реестра, исключения объектов информатизации из реестра, а также предоставления сведений из него.

Приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 30.04.2012 № 42 утверждена «Инструкция о порядке проведения внешнего контроля за обеспечением безопасности критически важных объектов информатизации». В инструкции устанавливается порядок проведения внешнего контроля за обеспечением безопасности КВОИ.

Приказом Оперативно-аналитического центра при Президенте Республики Беларусь 17.07.2013 № 47, был утвержден и введен в действие технический кодекс установившейся практики (ТКП 483-2013) «Информационные технологии и безопасность.

Безопасная эксплуатация и надежное функционирование критически важных объектов информатизации. Общие требования». ТКП устанавливает требования по обеспечению безопасности КВОИ.

Порядок обеспечения безопасности КВОИ, который включает в себя: отнесение ОИ к КВОИ в соответствии с перечнем отраслевых критериев; классификацию КВОИ; реализацию комплекса мероприятий по созданию системы безопасности КВОИ.

Обязанности по обеспечению безопасного функционирования КВОИ возлагаются на его владельца. Классификация КВОИ проводится в соответствии с СТБ 34.101.52-2016 «Информационные технологии. Методы и средства безопасности. Критически важные объекты информатизации. Классификация» (вступил в силу с 01.04.2017).

ИЗМЕНЕНИЕ СТБ 34.101.8-2006 «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. МЕТОДЫ И СРЕДСТВА БЕЗОПАСНОСТИ. ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНЫХ ПРОГРАММ И АНТИВИРУСНЫЕ ПРОГРАММНЫЕ СРЕДСТВА. ОБЩИЕ ТРЕБОВАНИЯ

Д.И. ЖУКОВА, О.Ю. КОНДРАХИН, Д.В. ШУЛЯК

Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»

С 1 января 2014 г. введен в действие технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY), утвержденный постановлением Совета Министров Республики Беларусь от 15 мая 2013 г. № 375 (далее - регламент).

Соответствие средств защиты информации (СЗИ) требованиям регламента обеспечивается либо выполнением требований, непосредственно приведенных в регламенте, либо выполнением требований взаимосвязанных с ним нормативно-правовых актов, перечисленных в приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 17 декабря 2013 г. № 94 «О перечне технических нормативных правовых актов, взаимосвязанных с техническим регламентом ТР 2013/027/BY».

Согласно указанному Приказу программные средства защиты от воздействия вредоносных программ и антивирусные программные средства, выпускаемые в обращение на рынке должны выполнять требования СТБ 34.101.8-2006 «Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования» (далее – стандарт) (пункты 6.2, и (или) 6.3, и (или) 6.4).

В стандарте устанавливаются три типа программных средств защиты от воздействия вредоносных программ и антивирусных программных средств (ПСЗВВП и АПС).

ПСЗВВП и АПС первого типа после запуска по запросу пользователя должны обнаруживать изменения элементов объектов информационных технологий;

ПСЗВВП и АПС второго типа после запуска по запросу пользователя должны обеспечивать проверку элементов объекта информационных технологий на наличие вредоносных программ (ВП) и обезвреживание обнаруженных ВП;