УДК 004.056.53

ПРОЕКТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ «ЭЛЕКТРОННОЕ ПРАВИТЕЛЬСТВО» В РЕСПУБЛИКЕ БЕЛАРУСЬ

Николаенко Владимир Лаврентьевич кандидат технических наук, доцент, Белорусский Государственный Университет Информатики и Радиоэлектроники, Минск (Беларусь)

Савенко Андрей Геннадьевич инженер, Белорусский Государственный Университет Информатики и Радиоэлектроники, Минск (Беларусь)

Матвеев Андрей Владимирович инженер, Белорусский Государственный Университет Информатики и Радиоэлектроники, Минск (Беларусь)

Аннотация: Показана проблема в области информационной безопасности, которая возникает при разработке проекта «Электронное правительство» в Республике Беларусь. Кратко проанализированы основные угрозы информационной безопасности и мероприятия по их парированию.

Abstract: The problem in the field of information security, which arises in the development of the project "Electronic Government" in the Republic of Belarus, is shown. Briefly analyzed are the main threats to information security and measures for their parrying.

Ключевые слова: «Электронное правительство»; информационная безопасность; угрозы информационной безопасности; защита информации.

Key words: "Electronic government"; Information Security; threats to information security; data protection.

«Электронное правительство» представляет собой сложный комплекс аппаратно-программных средств и документов организационного обеспечения, позволяющих осуществлять

взаимодействие между органами государственного и местного управления, а также самоуправления, гражданами и субъектами коммерческой деятельности [1] и предполагает три направления взаимодействия:

1. G2B/B2G (governmenttobusiness, государство – бизнес/бизнес – государство),
2. G2G (government to government, государство – государство),
3. G2C/C2G (governmenttocitizens, государство – граждане/граждане – государство).

В Беларуси работы по проекту «Электронное правительство» ведутся в соответствии с Национальной стратегией устойчивого социально-экономического развития Республики Беларусь на период до 2030 года [2].В докладе анализируются угрозы информационной безопасности для публичных точек доступа к интернету (ПТДкИ) в местных органах власти (направление взаимодействия G2C/C2G) [3] и в системе электронного документооборота(СЭД) «SMBUSINESS», внедрение которой в Академии управления при Президенте Республики Беларусь позволило Академии управления снизить трудозатраты, получать деловую информацию в стандартизованном виде, ускорить процесс согласования и подписания документа(направление взаимодействия G2G).

Основные угрозы информационной безопасности и способы их парирования в ПТДкИ. К ним относятся, во-первых, стандартные угрозы для ЛВС точки, во-вторых, проблемы с идентификацией и аутентификацией граждан, обращающихся к местным органам власти. Для парирования выделенных угроз в докладе предлагаются стандартные мероприятия –защита информации в сети и ЭЦП.

Основные угрозы информационной безопасности и способы их парирования в СЭД.К этому классу относятся, во-первых, стандартные угрозы для аппаратно-программной части СЭД (компьютеры и сервера локальной вычислительной сети и другого

оборудования). На них и на методах их парирования останавливаться не будем – они общеизвестны. Во-вторых, это проблемы с идентификацией и аутентификациейпользователей СЭД с помощью ЭЦП. Часть из них была решена созданием республиканского центра инфраструктуры открытых ключей [4] с использованием программно-технического комплекса «Штрих-код». Оставшаяся часть проблем, возникающих при использовании ЭЦП в СЭД, может быть решена с помощью правильно разработанной политики информационной безопасности СЭД, которая должна содержать следующие разделы: 1) ОПРЕДЕЛЕНИЕ ЦЕЛЕЙ ПОЛИТИКИ (обеспечение функционирования СЭД и изложение основных понятий в данной области, 2) ФУНКЦИИ ЭЦП (авторизация, защита интересов получателя документа – приемника, защита интересов подписывающего лица – передатчика).

Вывод. Показана проблема в области информационной безопасности, которая возникает при разработке проекта «Электронное правительство» в Республике Беларусь. Кратко проанализированы основные угрозы информационной безопасности и мероприятия по их парированию.

Список используемых источников:

1. Вечер, Л. С. Государственная служба: Курс лекций. – Минск: Академия управления при Президенте Республики Беларусь, 2005. – 233 с.

2. Национальная стратегия устойчивого социально-экономического развития Республики Беларусь на период до 2030 года (одобрена Президиумом Совета Министров Республики Беларусь 10 февраля 2015 г.) // Экономический бюллетень научно-исследовательского экономического института Министерства экономики Республики Беларусь. – 2015. – № 4 (214). – С. 2–99.

3.Дедюля, П. А., Гончар, С. Е. Угрозы информационной

безопасности для публичных точек доступа к интернету в местных органах власти // Современные средства связи: материалы XX Междунар. науч.-техн. конф., 14–15 окт. 2015 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2015. – 326 с. – С. 176–177.

4 Абламейко, С. В. и др. Обеспечение информационной безопасности в системе предоставления государственных информационных услуг // Тезисы докл. 5-й белорусско-российской НТК «Технические средства защиты информации», Нарочь, 28 мая–1 июня 2007 года). – Минск: БГУИР, 2007. – С. 7.