УДК 004.056

УДОСТОВЕРЯЮЩИЕ ЦЕНТРЫ КАК ИНФРАСТРУКТУРА СОВРЕМЕННОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЦИФРОВЫЕ БАРЬЕРЫ

© 2004 Г. Э. Афанасьев

Информационно-аналитический департамент ЦСИ ПФО

Анализируется наиболее значимая проблема в области информатизации, связанная с новыми административными барьерами – цифровыми барьерами, которые возникли из-за технологических и организационных рассогласований. Выделяются несколько типов цифровых барьеров: непроницаемые границы между различными ведомствами, между регионами России и международные цифровые границы.

Предлагаются пути преодоления существующих барьеров.

Еще несколько лет назад главным лейтмотивом развития информационного общества было преодоление цифрового неравенства. Один из наиболее глобальных документов по информационно-коммуникационным технологиям (ИКТ), Окинавская хартия, посвящена именно задаче преодоления цифрового неравенства. С 2000 года, когда представители стран большой восьмерки подписали этот документ, ситуация полностью изменилась. Сейчас наиболее значимая проблема в области информатизации связана с новыми административными барьерами – цифровыми барьерами, которые возникли из-за технологических и организационных рассогласований. Основная задача повышения экономического роста в России – задача удвоения ВВП – может быть выполнена только при условии обеспечения свободного перемещения всех видов ресурсов: денег, товаров, людей и информации.

Можно выделить несколько типов цифровых барьеров, возникших в процессе информатизации: это непроницаемые границы между различными ведомствами, между регионами России и международные цифровые границы. Эта классификация основана на итогах 23 встреч, которые провел автор за последний месяц в регионах Приволжского федерального округа. Как член рабочей группы по удостоверяющим центрам, автор готовит доклад, в котором будет отражен согласованный региональный и окружной взгляд на весь комплекс задач, связанный с преодолением цифровых барьеров и полномасштабным внедрением электронной цифровой подписи (ЭЦП).

Говоря о межведомственных цифровых барьерах, имеется в виду ситуация, при которой данные в электронной форме, выработанные в одном ведомстве, могут быть юридически оправданно переданы в электронном виде и рассмотрены в другом. Беседы с госслужащими, ответственными за информатизацию в региональных министерствах и ведомствах, показали, что сейчас ключевая задача в вопросе преодоления цифровых барьеров – обеспечение легитимной идентификации, а не шифрование данных. В госорганах очень редко возникает потребность зашифровать файл при передаче через электронную почту. Широко принятые в мире системы защиты пользователей, данных и прикладных программ стандарта PKI (Publik Key Infrastructure) – инфраструктура открытых ключей – с точки зрения практического использования – это в первую очередь идентификация, а не шифрование.

Цифровые барьеры, как межведомственные, так и межрегиональные, не являются следствием или издержками «неправильной» информатизации. Напротив, их появление закономерно и есть конкретное воплощение инновационных барьеров.

Если сосредоточиться на задаче построения инфраструктуры ЭЦП, то причины рассогласования лежат в несовместимости технологических платформ. Необходимо выделить три составляющих информационной системы: прикладное программное обеспечение (ПО), криптографию, сертификаты ЭЦП. В задаче построения единой эффективной системы цифрового обмена есть несколько уровней: согласование стандартов ПО,

криптоплатформ и стандартов сертификатов на открытые ключи.

Продолжение линии «изолированной» информатизации разных территорий и ведомств, усиления цифровых барьеров ведет к информационному, а значит и ресурсному «тромбофлебиту». Задержки и заторы в движении информации влекут за собой сложности в перемещении всех остальных видов ресурсов. Несогласованность политики внедрения ЭЦП имеет также и краткосрочный отрицательный финансовый результат, состоящий в дублировании траты государственных денег на параллельное создание десятков ведомственных удостоверяющих центров и выдачу наборов ЭЦП одним и тем же юридическим лицам. Речь идет о ситуации, когда юридическое лицо для взаимодействия с разными госорганами использует разные криптосредства и учитывается в десятке внутренних удостоверяющих центров. Типовая попытка «договориться» между ведомствами выглядит так. Одно ведомство предлагает другому: установите у себя то средство, которое есть у нас, и будем обмениваться данными. Но второе ведомство уже также потратило средства на построение своей системы и не намерено начинать все с нуля. Для пользователя ситуация оборачивается тем, что он обременен дополнительным «налогом» на приобретение специфичных средств для общения с каждым ведомством.

Все эти проблемы являются следствием принятия ведомственной модели построения удостоверяющих центров. Дело уже не в правильности действий отдельных участников, а в самом принципе. Усиление барьеров в этом случае неизбежно. Предлагается альтернативная модель – окружная. В рамках этой модели работают крупные удостоверяющие центры, поддержанные президентской линией власти в округе, которые, во-первых, не продвигают никакие отдельные криптоалгоритмы и, во-вторых, работают исключительно с сертификатами ЭЦП, не принимая на себя никаких других функций. Подход к выбору модели важен и потому, что если госведомства между собой не договорятся, то это отразится на пользователях государственных услуг и повлечет за собой падение престижа госсектора в целом. Результатом серии встреч в ПФО стала предварительная договоренность о пилотном проекте по обмену данными с использованием сертификатов окружного удостоверяющего центра. С информацией о проекте можно познакомиться по адресу www.ekey.ru.

CERTIFICATION CENTRES AS THE INFRASTRUCTURE OF MODERN INFORMATION SECURITY AND DIGITAL BARRIERS

© 2004 G. E. Afanasiev

Information Analysis Department of Information Insurance Centre, Privolzhsky Federal District

The paper analyses the most important problem in the area of information connected with new administrative barriers – digital barriers which came into existence due technological and organizational mismatches. Several types of digital barriers are isolated: impenetrable, borders between different departments, between Russia's regions and international digital borders.

Ways of overcoming existing barriers are proposed.