УДК 334.024; 338.28

М.В. Тихомирова, аспирант Академии управления при Президенте Республики Беларусь
gromkovoinova@rambler.ru

О РАЗДЕЛЕНИИ РИСКОВ И ПРОБЛЕМ В СТРУКТУРЕ ЭЛЕКТРОННОГО ГОСУДАРСТВА

Создание и развитие структур и процессов электронного государства меняет характер взаимодействия государства и общества (Настельс, М. Информационная эпоха: Экономика, общество и культура / М. Настельс. – М., 2000. – 167 с.). В Беларуси эта проблема решается в рамках Государственной программы развития цифровой экономики и информационного общества на 2016 − 2020 годы (постановление Совета Министров Респ. Беларусь, 23 марта 2016 г., № 235). Однако, как показывает зарубежный опыт, оказание электронных услуг органами государственного управления порождает ряд не только положительных эффектов, но и формирует проблемы и риски. Сошлемся на административный опыт ЕС (Reorganization of government bask offices for better electronic public services-europian best practices, January 2004, DG Information Society, European Commission [Электронный ресурс]. – URL: http: //www.europa.eu.int/egovernment_research), а также научные исследования (Банасиковска, Я. Система отношений государства и общества в сфере государственных услуг в условиях цифровой экономики : дис. … д-ра экон. наук : 08.00.01 / Я. Банасиковска. – М., 2017. – 396 л.). С учетом зарубежного опыта в рамках белорусской модели государственного управления предлагается четко разделить эти две категории.

Риски связывают в первую очередь с неблагоприятными явлениями, порождаемыми несанкционированным использованием информационно-коммуникативными технологиями (ИКТ). Источником рисков при этом являются действия третьих лиц. Примерами таких явлений служат риски несанкционированного доступа к личным данным, частной жизни и коммерческой тайне получателей услуг; риски присвоения чужих имущественных и личных неимущественных прав посредством доступа в систему под чужим именем; мошенничество с использованием ИКТ; риски уничтожения или искажения информации в результате сбоев в системе или целенаправленной вирусной атаки и др. Перечень подобных примеров можно продолжить.

Под *проблемами* понимают неблагоприятные последствия для социально-экономического развития страны, порожденные новыми фор-

мами организации деятельности. Они вытекают не из преднамеренного противоправного поведения тех или иных лиц, а из характера и особенностей самой применяемой технологии. К числу примеров можно отнести цифровое неравенство пользователей, принадлежащих к разным поколениям, социальным группам, административно-территориальным единицам; электронную зависимость пользователей соответствующих услуг (привыкание к использованию электронных средств связи, хранения и обработки информации, электронных помощников, развлекательных систем); возможность оказания деструктивного информационно-психологического воздействия и др.

В приведенной ниже таблице систематизированы и разделены основные риски и проблемы, связанные с формированием и развитием системы государственных электронных услуг.

Таблица 3

Основные проблемы и риски системы государственных электронных услуг

№	Проблемы и риски	Категория	Источник
1.	Несанкционированный доступ к информации	Риск	Третьи лица
2.	Присвоение чужих прав	Риск	
3.	Уничтожение (искажение) информации	Риск	
4.	Цифровое неравенство пользователей	Проблема	Технологии
5.	Электронная зависимость	Проблема	

В целях внедрения и поддержки стабильного функционирования системы государственных электронных услуг (снижения как рисков, так и издержек) необходимы комплексные и целенаправленные усилия органов государственного управления. Перечислим основные меры, принимаемые на практике органами государственного управления в Республике Беларусь:

совершенствование законодательства и правоприменительной практики в области спецификации и защиты прав потребителей электронных услуг;

совершенствование организационной структуры государственного управления;

повышение доступности и прозрачности информации, направленное на смягчение проблемы асимметрии информации;

снижение издержек рентоориентированного поведения представителей власти;

издержки, связанные с преодолением последствий неверных решений, и т. д.

Сделаем некоторые выводы. На современном этапе развития экономики наблюдается широкое проникновение ИКТ в социальные технологии. Система государственных электронных услуг представляет собой комплекс услуг, предоставляемых государственными органами в соответствии с их компетенциями по запросу граждан, организаций или других государственных органов с помощью использования ИКТ посредством транзакций обмена. Внедрение системы государственных электронных услуг изменяет принципы отношений между государством, гражданами и предпринимателями. Граждане и организации получают более широкий доступ к информации о государстве, административных процессах, организациях и действиях конкретных представителей государства. В результате смягчается проблема асимметрии информации между участниками процессов, растет открытость органов власти, создаются условия для более действенного общественного контроля над деятельностью отдельных государственных служащих. Использование ИКТ при оказании государственных электронных услуг уменьшает большую часть транзакционных издержек. В то же время порождаются новые виды затрат и издержек: идентификации пользователей, защиты имени, защиты личной информации, интерпретации информации, потери (искажения) информации и др. В целом система государственных электронных услуг повышает эффективность государственного и местного управления, укрепляет доверие между государством, публичными образованиями, гражданами и организациями предпринимателей, стимулирует развитие экономики страны. В то же время оказание государственных электронных услуг порождает новые социальные проблемы и технологические риски, для преодоления которых необходимы совместные целенаправленные усилия общества и государства.

УДК 340.113:004

О.А. Федоренко, младший научный сотрудник лаборатории по проблемам противодействия преступности Национальной академии внутренних дел (г. Киев, Украины)
Kseniya25@ukr.net

ИНТЕРНЕТ ВЕЩЕЙ КАК УЯЗВИМОЕ МЕСТО ДЛЯ ДЕСТРУКТИВНЫХ ДЕЙСТВИЙ КИБЕРПРЕСТУПНИКОВ

В настоящее время современный мир информационных технологий требует постоянного взаимодействия между своими компонентами. Однако люди имеют ограниченное время, внимание и точность. Все это означает, что человек – не лучший инструмент по сбору данных. В таких

условиях концепция коммуникации между устройствами предусматривает выполнение определенных действий вообще без вмешательства человека. Как следствие – вопрос разработки и внедрения технологий Интернет вещей активно обсуждается в Украине еще с конца XX в.

Понятие «Интернет вещей» (англ. Internet of things, IoT) рассматривается как сеть разнообразных объектов, увеличивается от промышленных устройств к потребительским товарам и услугам, которые могут обмениваться информацией и выполнять свои задачи.

Интернет вещей стремительно растет. По данным исследования консалтинговой компании, специализирующейся на рынках информационных технологий, Gartner по всему миру было 6,4 млрд подключенных вещей в 2016 г., что на 30 % выше, чем в 2015 г. В 2016 г. 5,5 млн новых вещей подключались к Интернету вещей ежедневно. С таким темпом, по прогнозу Gartner, к 2020 г. количество достигнет 20,8 млрд подключенных вещей.

Некоторые другие аналитические агентства выражают еще более оптимистичные прогнозы и предрекают 50 млрд подключенных устройств.

Высокий уровень неоднородности в сочетании с широкой гаммой систем IoT, как ожидается, увеличит число угроз безопасности владельцев устройств, которые все чаще используются для взаимодействия людей, машин и вещей в любой вариации. Традиционные меры обеспечения безопасности и конфиденциальности не могут быть применены к технологиям IoT, в частности, из-за их ограниченной вычислительной мощности.

Кроме того, большое количество подключенных устройств порождает проблему массовости. В то же время для достижения признания со стороны пользователей необходимо в обязательном порядке обеспечить соблюдение безопасности, конфиденциальность и модели доверия, которые подходят для контекста IoT. Для предотвращения несанкционированного доступа пользователей (т. е. людей и устройств) к системе должны использоваться механизмы аутентификации и авторизации, гарантированная безопасность, конфиденциальность и целостность персональных данных. По персональным данным пользователей и информации должны обеспечиваться защита и конфиденциальность, прежде всего потому, что устройства имеют к ней доступ и способны ей управлять (например, сведения о привычках пользователей).

Для Интернета вещей стоят сложные проблемы обеспечения безопасности по сравнению с теми, которые характерны для сетей связи. К ним добавляются возможные проблемы масштабируемости сети, вызванные мало предполагаемым объемом передачи данных от большого числа узлов, ненадежность программного обеспечения и т. п.