3.5. АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

Косенко В.В.,
кандидат наук по государственному управлению
Харьковский региональный институт государственного управления Национальной академии государственного управления при Президенте Украины
Онищенко Ю.М.,
кандидат наук по государственному управлению
Харьковский национальный университет внутренних дел
Мельников А.А.
аспирант кафедры экономической кибернетики и управления экономической безопасностью
Харковский национальный университет радиоэлектроники

Электронное правительство – это система взаимодействия власти и общества на основе сочетания внутренней правительственной и внешней общественной инфраструктуры через властные Интернет-представительства (порталы), что расширяет доступность государственно-управленческих услуг в сети Интернет и сокращает сроки их предоставления [2].

Чтобы побудить гражданина использовать услуги электронного правительства, важно, чтобы люди доверяли государственным службам и имели гарантии защиты информации и конфиденциальности. Однако, с точки зрения гражданина, правительство представляется, как единое целое и поэтому недостатки в безопасности работы любой правительственной структуры будут рассматриваться как провал всей государственной системы защиты информации. Поэтому процесс защиты информационной безопасности всех правительственных ведомств должен рассматривается как жизненно важный и необходимый вопрос.

Сетевая и информационная безопасность является предпосылкой информационного общества, как определённо в документах Европейской комиссии [4].

Структура безопасности электронного правительства (ЭП) состоит из основных трёх элементов: люди, процессы и технологии. Поэтому безопасность электронного правительства может быть в широком смысле представлена следующим образом (рис. 1).

Существуют различные технические и физические проблемы, влияющие на безопасность информационной защиты электронного правительства [5,6]. Рассмотрим некоторые из них.

Интернет-инфраструктура. Здесь необходимо отметить основные составляющие безопасности:

– стабильность – это возможность гарантировать, что система функционирует в соответствии со своим регламентом, а также способность

обеспечить уверенность пользователей системы уникальных идентификаторов в том, что это именно так;

– отказоустойчивость представляет собой способность системы уникальных идентификаторов эффективно противостоять / выдерживать / переживать злонамеренные атаки и другие разрушающие события без ущерба и без прекращения выполняемых системой функций [2].

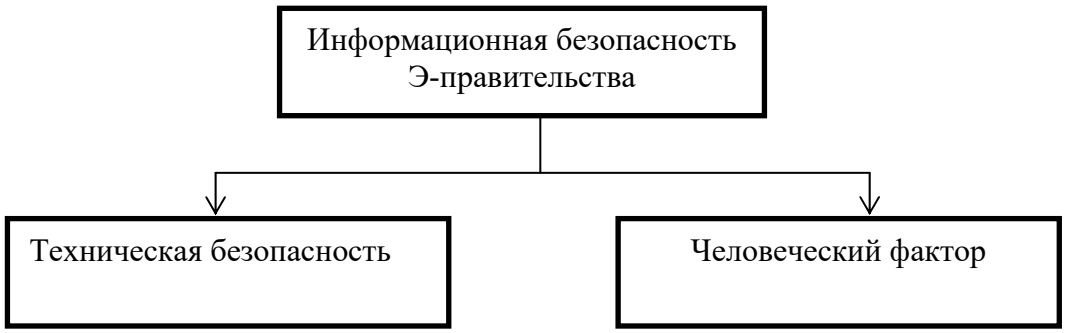

Рис. 1. Проблемы безопасности электронного правительства

Идентификация. Обеспечение безопасности участника процесса с точки зрения уникальной идентификации. При анализе использования механизмов идентификации для целей ЭП важен не столько выбор типа идентификатора, сколько обоснование того, какие именно услуги можно предоставить гражданину, который идентифицировался тем или иным способом.

Электронная аутентификация. Требуется высоконадёжная система индивидуальной идентификации, как для граждан, так и для государственных учреждений. Для этих целей используется инфраструктура открытых ключей (PKI – Public Key Infrastructure) – набор средств (технических, материальных, людских и т. д.), распределённых служб и компонентов, в совокупности используемых для поддержки криптозадач на основе закрытого и открытого ключей. PKI – это технология, которая была признана лучшей электронной аутентификацией для электронного правительства.

Типы данных. Данные и информационные ресурсы классифицируются на основе риска несанкционированного доступа. Высокий риск потери данных классифицируется как конфиденциальный, и соответственно им требуется более высокий уровень защиты, в то время как данные с более низким риском, возможно, обозначенные как «внутренние», требуют пропорционально меньшей защиты.

Контроль доступа включает в себя проблемы идентификации, аутентификации и авторизации. Во избежание вмешательства извне необходимо использовать механизмы контроля доступа для получения информации от системы и ее пользователей.

Отказ от доступа к данным вне диапазона (Out-of Band Data Denial of Service). Атака злоумышленников на 139 порт данных. Порт 139 используется сеансовой службой NetBIOS, которая активизирует браузер поиска других

компьютеров, службы совместного использования файлов и службу сервера. Это приводит к тому, что компьютер под управлением ОС Windows теряет сеть.

Вредоносные программы (malware). Это могут быть различные скрипты, активный контент, код и другое программное обеспечение, специально предназначенное для нанесения вреда либо уничтожения компьютерной системы, что может привести к непредвиденным последствиям в работе системы.

Снифферы. Сетевой сниффер (sniffer) пакетов представляет собой прикладную программу, которая перехватывает все пакеты, проходящие по сети и передаваемые через определённый, заданный домен. Этот сетевой анализатор, используется специалистами для диагностики сетевых проблем. Однако этот инструмент также может быть использован злоумышленником для сбора логинов и паролей в сети.

Угрозы каналов связи. Трудно гарантировать, что каждый узел в Интернете, через который проходят сообщения (пакеты) является безопасным.

Угрозы для сервера. Сервер является одной из основных составляющих сети. Для предотвращения таких угроз используется брандмауэр (firewall) – программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами. Firewall обеспечивает проверку всех соединений между сетью организации и Internet на соответствие политике безопасности данной организации.

Кроме того в работе электронного правительства выделяют три основных вида угроз информационной безопасности: угрозы конфиденциальности – несанкционированный доступ к данным; угрозы целостности – несанкционированная модификация, дополнение или уничтожение данных; угрозы доступности – ограничение или блокирование доступа к данным (например, невозможность подключится к серверу с базой данных в результате DDoS-атаки) [1].

Обмен информацией между государственными учреждениями всегда должен рассматривается как определённый риск. Однако понимания и устранения этих угроз только с технической точки зрения явно недостаточно. Поэтому проблемы информационной безопасности электронного правительства также должны решаться с учётом человеческого фактора.

Интероперабельность – это способность продукта или системы, интерфейсы которых полностью открыты, взаимодействовать и функционировать с другими продуктами или системами без каких-либо ограничений доступа и реализации. Отсутствие интероперабельности из-за семантики, отсутствия стандартов, различных систем классификации влияет на эффективность работы систем электронного правительства.

Удобство использования (Юзабилити) сосредоточено на создании приложений, программ и услуг, которые могут быть легко использованы гражданами. Удобство использования системы не сводится только к тому,

насколько её легко эксплуатировать. В соответствии со стандартами серии ISO 9241 эту характеристику следует понимать более широко, учитывая личные цели пользователя, его эмоции и ощущения, связанные с восприятием системы, а также удовлетворённость работой.

Политика безопасности представляет собой совокупность документированных руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые регулируют управление, защиту и распределение ценной информации. Этот план должен сопровождаться оценкой уровня эффективности электронного правительства. В целях сохранности и защиты персональных данных пользователей используются все необходимые технические и организационно-правовые меры защиты их от неправомерного доступа. Любая защитная мера есть компромисс между снижением рисков и удобством работы пользователя. При этом любое применение любых защитных мер, касающихся взаимодействия пользователя с информационной системой всегда вызывает отрицательную реакцию пользователя.

Правовые рамки – это законодательные меры в сфере информационной безопасности электронного правительства, направленные на создание законодательной базы, упорядочивающей и регламентирующей поведение субъектов и объектов информационных отношений, а также определяющей ответственность за нарушение установленных норм.

Работа по созданию нормативной базы предусматривает разработку новых или корректировку существующих законов, положений, постановлений и инструкций, а также создание действенной системы контроля за их исполнением. Должны быть определённые законы и правила, чтобы решения электронного правительства были юридически обязательными к исполнению.

Конфиденциальность – необходимость предотвращения разглашения, утечки какой-либо информации. Вся личная информация используется только по своему прямому назначению. Предоставление личных данных является добровольным. Передавая данные, Вы разрешаете использовать информацию для заявленной цели. Однако непредоставление определённой информации может создать препятствия для оказания услуги, которую Вы хотели бы получить.

Культура безопасности обычно рассматривается как часть национальной культуры. На эти проблемы влияют законодательные и нормативные рамки, а также национальные институциональные культуры. Например, отсутствие участия граждан в принятии решений, традиционные ценности, консерватизм могут затруднить эффективность программ обеспечения информационной безопасности электронного правительства.

Осведомлённость. Является ли способность людей чувствовать, наблюдать и осознавать, что происходит вокруг них, и понимать смысл информации сейчас и в будущем. Это осознание определяется типом информации, будь то хорошо или плохо для конкретной работы или цели. Отсутствие осведомлённости в области безопасности и отсутствие осознания

важности информационной безопасности влияют на злоупотребление системой из-за отсутствия надлежащей программы информирования.

Доверие. Задача доверия играет важную роль в принятии услуги в электронном виде. Доверие к правительству в основном зависит от отношений между органами электронного правительства и другими правительственными учреждениями в отношении того, как работает государственная инфраструктура, провайдеры интернет-услуг (ISP) и другие правительственные учреждения. Чтобы получить высокий уровень доверия, необходимо иметь высокий уровень осведомлённости о безопасности систем. Это достигается путём привлечения государственных служащих, чтобы узнать о политике безопасности, архитектуре, компетенциях, поддержке целей безопасности и оперативных процедурах в государственных учреждениях. Доверие к правительству гарантирует, что транзакции являются наблюдаемыми и подотчётными аутентифицированному лицу.

Кроме того, создание надёжной основы для цифровой аутентификации является жизненно важным аспектом в обеспечении целостности онлайновых и мобильных финансовых транзакций.

Чтобы определить факторы успеха в обеспечении безопасности информации в электронном правительстве, важно чётко понимать, определять и внедрять как технические, так и нетехнические вопросы информационной безопасности электронного правительства. В первую очередь необходимо использовать модель в качестве контрольного перечня для определения, разработки и реализации требований безопасности электронного правительств. Затем, создаётся план требований безопасности для услуг электронного правительства, который будет коррелироваться во время выполнения проекта.

Кроме того, потребности в безопасности любой системы электронного правительства должны анализировать угрозы и атаки, которые могут возникнуть в процессе работы системы. Обычно это интегрируется в разработку защищённых приложений с использованием современной методологии анализа программного обеспечения. Это позволит государственным учреждениям подготовиться к любой уязвимости или проблеме в контексте обеспечения конфиденциальности, целостности и доступности информации.

Помимо этого, другими основными факторами успеха в обеспечении безопасности электронного правительства является создание соответствующих стратегических рамок для обеспечения безопасности ИКТ, которые определяют защиту норм и процедур в системе для обеспечения конфиденциальности, целостности и доступности информации. Государственные органы рассматривают эту проблему как фактор, который способствует успешной информационной безопасности в контексте электронного правительства. Активная поддержка руководства, информированность персонала и подготовка кадров также являются факторами, которые необходимо учитывать, поскольку, в конечном счёте, менеджер будет отвечать и за задачи инициирования и поддержки любого проекта вместе с надлежащей осведомлённостью в области

безопасности. Сотрудники государственных учреждений должны постоянно повышать квалификацию в области информационной безопасности.

Отсутствие необходимых структур безопасности, таких как инфраструктура с открытым ключом, система шифрования, является одной из тех проблем, которые влияют на качество работы информационных систем в целом.

Решающее значение имеет установление и развитие целей безопасной технической инфраструктуры для целей информационной безопасности и операционных сред. Свойства безопасности – это методы и средства, предлагающие такие средства безопасности: цифровая подпись, брандмауэры, пароли. Эти технические инфраструктуры способны обрабатывать требуемый объем и вид транзакций безопасным способом, это неизбежность в достижении целей обеспечения информации.

Информационная безопасность является одной из важных компонент предоставления государственных услуг в электронном виде. При создании единого портала государственных услуг необходимо проводить работы по анализу возможных угроз, на основе которых должны быть сформированы требования по защите информации. В системе безопасности необходимо использовать большой набор механизмов безопасности: межсетевые экраны, средства анализа содержимого, средства предотвращения вторжений, антивирусные средства защиты информации, средства мониторинга и контроля защищённости [7].

Что касается перспективы использования аппаратного и программного обеспечения, правительственные органы должны популяризировать инфраструктуру ИКТ для электронного правительства. Однако с юридической точки зрения необходимо создать законную основу для обеспечения равных возможностей всех людей перед законом. В контексте этого процесса для электронного правительства должны быть внедрены надёжные стандарты безопасности и управление знаниями. Большое значение имеет также предоставление конкретных услуг высокого качества. Защита конфиденциальности информации о гражданах имеет решающее значение для повышения уровня доверия к правительству.

Наконец, с точки зрения восприятия пользователями, государственная власть должна поощрять и поддерживать своих сотрудников для получения навыков безопасности на основе знаний. Кроме того, необходимо иметь высокую степень поддержки граждан, чтобы чётко определить полномочия и ответственность пользователей, а также улучшать навыки использования информационных технологий пользователями.

Выводы. Интернет стал и источником информации, и источником опасностей. Исследование показало, что предоставление электронных услуг для людей через Интернет создаёт существенную проблему для безопасности доверия граждан к правительствам. Это включает угрозы для систем идентификации, конфиденциальности и данных. Следовательно, защита данных и систем является основным моментом, поскольку это может повлиять

на готовность правительств и потребителей использовать предлагаемые онлайн-услуги. Широкое распространение электронных сервисов выявило ещё одну проблему. Правительственная информация требует надёжных средств защиты программного обеспечения для предотвращения (минимизации вероятности) любого несанкционированного доступа, который может раскрыть персональные данные граждан. В статье рассмотрены технические и нетехнические проблемы, которые влияют на безопасность информации в системе электронного правительства. Также были выявлены и проанализированы различные критические факторы такие как: правовая система, безопасная инфраструктура ИКТ, конфиденциальность, доверие и т.д. Из приведённых выше определений и их анализа было установлено, что проблема информационной безопасности в электронном правительстве является основным вопросом для обеспечения конфиденциальности, целостности и доступности информации.

Литература:

1. Галяутдинов Р. Р. Информационная безопасность. Виды угроз и защита информации [Электронный ресурс] / Р. Р. Галяутдинов // Сайт преподавателя экономики. – 2014. – Режим доступа: http://galyautdinov.ru/post/informacionnaya-bezopasnost.
2. Пилюгин П. Безопасность, стабильность и отказоустойчивость инфраструктуры глобального Интернета [Электронный ресурс] / П. Пилюгин // Digital.Report. – 2016. – Режим доступа: https://digital.report/infrastruktura-globalnogo-interneta/.
3. Серенок А. О. Механізми взаємодії органів влади з громадянами в системі електронного уряду: автореф. дис. канд. держ. упр : спец. 25.00.02 “Механізми державного управління” / А. О. Серенок; Нац. акад. держ. упр. при ПрезидентовіУкраїни ; Харк. регіон. ін-т держ. упр. – Х., 2011. – 21 с.
4. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions eEurope 2005 Mid-term Review COM(2004) 108 final 18.02.2004. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0108:FIN:EN:PDF.
5. Khalid M. Cloud Computing Security: A Survey / M. Khalid, A. Khreishah, M. Azeem. // Computers – Open Access Journal. – 2014. – Vol. 3, pp. 1-35.
6. Rodgers, C. 2012. Data Classification: Why is it important for Information Security? Available at: https://www.securestate.com/blog/2012/04/03/data-classification-why-is-it-important-for-information-security.
7. Serenok A.O. Information security system of electronic government / A.O. Serenok, I.V. Kobzev, O.V. Orlov // World scientific extent: Collection of scientific articles. – Agenda Publishing House, Coventry, United Kingdom, 2017. – P. 238-243.