УДК 006.078

Рустамов Д.А., Рзаев М.Я.

ВОПРОСЫ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ В КРИЗИСНЫХ СИТУАЦИЯХ

Анотація:

У статті розглядаються питання безпеки державних інформаційних ресурсів у разі виникнення різних кризисних ситуацій. Відомо, що з точки зору безпеки електронного керівництва кризисні ситуації є основним фактором ризику. Також розглядаються міжнародні стандарти у цій сфері, вивчений досвід розвинених країн, і результати, отримані провідними науковими центрами. Мета – привернути увагу органів державної влади на важливість даного питання.

Аннотация:

В данной статье рассматриваются вопросы безопасности государственных информационных ресурсов в случае возникновения различных кризисных ситуаций. Известно, что с точки зрения безопасности электронного правительства кризисные ситуации являются основным фактором риска. Также рассматриваются международные стандарты в этой сфере, изучен опыт развитых стран, и результаты, полученные ведущими научными центрами. Цель – привлечение внимания органов государственной власти на важность данного вопроса.

Abstract:

The security problems of the state information resources in various crisis situations have been discussed in this article. It is known, that from the e-government's information security point of view, the crisis situation is one of the major risk factors. In this paper, international standards in this field, experiences of developed countries, and the results obtained by leading research centers has been reviewed. The goal of this article is to attract the attention of government agencies to the importance of this issue.

Введение

Под безопасностью государственных информационных ресурсов подразумеваются правовые, административные и программно-технические формы обеспечения конфиденциальности, целостности и доступности информации. Электронное правительство требует преобразования бумажной информации в электронную форму, в связи с чем ожидаются новые проблемы в сфере безопасности. В списке факторов риска, которые могут повлиять на безопасность электронного правительства, кризисные ситуации, с результатом около 1%, занимают последнее место [5]. Однако этот список составлен не по серьезности рисков, а лишь по частоте их появлений.

Рассмотрим сравнительную статистику:

1) Каждую неделю в аэропортах США теряются около 12 000 ноутбуков [5];

2) В результате событий 11 сентября 2011 года около 18000 компаний понесли значительный информационный ущерб [5].

В первом случае, важность утерянной информации определяется на частном уровне, в то время как во втором – на уровне компаний и государственных учреждений. Если

оценить потерю информации именно с этой точки зрения, то второй случай представляет значительно больший фактор риска.

Согласно исследованиям Техасского Университета, после событий 11 сентября 2011 года 43% потерпевших организаций не смогли восстановить свою работу, а 51% организаций были полностью восстановлены лишь в течение двух лет после инцидента.

Такие статистические данные показывают высокую вероятность полной потери важных информационных ресурсов в кризисных ситуациях, что неизбежно повлечет за собой и риск нарушения конфиденциальности.

Вероятность столкновения информаций, составляющих государственную тайну, с той же проблемой, подчеркивает серьезность и актуальность поставленной проблемы [1].

Основные факторы риска, которые влияют на информационную безопасность в случае кризиса

Кризисные ситуации для государственных информационных ресурсов, систем и их отдельных компонентов включают в себя следующие факторы риска: стихийные бедствия, террористические акты, войны, конфликты, события бытового типа (пожар, утечка газа и т.п.), потеря функциональности программного обеспечения, выход из строя сетевых инфраструктур.

Каждая из выше упомянутых кризисных ситуаций является предметом отдельного рассмотрения. Тем не менее, с точки зрения результата, любой из факторов риска считается серьезной угрозой для безопасности государственных информационных ресурсов.

Для полного восстановления предприятия после кризиса, поддержания качества услуг и тому подобных вопросов каждый субъект электронного правительства должен подготовить “IT disaster recovery plan” (ИТ план аварийного восстановления) и быть готовым к его выполнению и развитию. В соответствии с планом, необходимо периодически производить резервное копирование информации, а резервные серверы должны быть удалены на определенные расстояния от основных. Иногда высказывают мысль о целесообразности расположения “Backup” серверов на расстояниях от 50 до 100 км от основных рабочих мест. Вопрос: А, может быть 200 км...? В соответствии со стандартами, все эти мнения не являются правильными.

Международные стандарты управления в кризисных ситуациях

В 2002–2003 годах в уставах органов федеральных властей США было предложено расположение “центров восстановления после аварии” финансовых учреждений на расстояниях 200–300 миль от основных мест дислокации. Однако предложение не было одобрено и было решено, что расстояния в каждом случае должны выбираться в зависимости от различных факторов [4]. Конечно, невозможно исследовать уставы всех государственных организаций мира, но даже частичное исследование не дало никаких конкретных нормативных актов по выбору оптимальных расстояний. Во встречающихся документах указано лишь о необходимости расположения “disaster recovery center” на относительно безопасном расстоянии.

В этой области можно следовать требованиям международных стандартов. Существуют стандарты управления информационной безопасностью в кризисных ситуациях:

- ISO 22301:2012 Business continuity management systems – Requirements;
- ISO/IEC 27031:2011 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity;

- ISO/PAS 22399:2007 Guideline for incident preparedness and operational continuity management;
- IWA 5:2006 Emergency Preparedness;
- BS 25999:2007 Business Continuity Management;
- ISO/IEC 24762:2008 Guidelines for information and communications technology disaster recovery services;
- IWA 5:2006 Emergency Preparedness – British Standards Institution;
- BS 25777:2008 Information and communications technology continuity management;
- ANSI/TIA-942:2005 (Telecommunications Infrastructure Standard for Data Centers TIA I-II-III

Ответ на поставленный вопрос в выше упомянутых стандартах один и тот же: ни один из стандартов ISO 22301, BS 25999, NIST SP 800, или семейства стандартов ISO 27к не дает точного значения расстояния. Резервную копию информации с точки зрения RTO (Recovery Time Objective – целевое время восстановления) необходимо размещать как можно ближе к основным местам работы [3]. Причем, на пути, соединяющем альтернативный дата-центр с основным, не должны находиться туннели, мосты, и аналогичного рода препятствия.

В соответствии со стандартами, государственные органы должны сами принимать решение об управлении информационной безопасностью в кризисной ситуации. Однако принимаемые решения не должны опираться лишь на субъективное мнение отдельных людей, а однозначно иметь в качестве своей основы соответствующие стандарты. При принятии решений должны быть учтены следующие факторы риска:

- Землетрясения – центры обработки данных не должны быть расположены в сейсмоопасной зоне;
- Наводнения – альтернативные центры обработки данных должны быть далеко от места, где вероятны наводнения;
- Цунами – для основного и альтернативного центра обработки данных не приемлемо расположение на берегу океана;
- Другие стихийные бедствия – лесные пожары, смерчи, извержения вулканов – если основной дата центр и находится недалеко от подобных районов, то альтернативный должен быть расположен на значительном удалении от них;
- Для военно-промышленных, химических и других предприятий, один из основных или запасных дата-центров должны находиться на безопасном расстоянии от опасных зон;
- Не должно быть зависимости от одних и тех же источников электропитания;
- Если дата-центры не удовлетворяют выше приведенным требованиям, то хотя бы необходимо позаботиться о безопасности ведущих специалистов от пандемических болезней, т.к. обучение высококвалифицированного персонала требует больших временных и финансовых затрат.

Заключение

Становится ясно, что вопросы информационной безопасности в условиях кризиса являются довольно серьезной проблемой. Принимая во внимание достаточно большую вероятность столкновения информационных ресурсов, содержащих государственную тай-

ну с перечисленными выше проблемами, целесообразно уделение особого внимания к этой теме со стороны соответствующих государственных органов.

Литература:

1. Joshi J. B. D. Security and Privacy Challenges of a Digital Government / Joshi J. B. D., Ghafoor A., Aref. W. G. – Boston: Kluwer Academic Publishers, 2002. – 136 c.

2. Wold G.H. Risk analysis techniques [Electronic Resource] / Wold, G.H. Shriver R.F. // Disaster Recovery Journal. – 1997. – 7(3). – P. 24–29. – Mode of access: http://www.drj.com/new2dr/w3_030.htm;

3. Information Technology Disaster Recovery Plan. Public Version. August 31.2012. [Electronic Resource]. – College Station, USA: Texas A&M University, 2012.– 69 p. – Mode of access: http://www.tamuct.edu/departments/informationtechnology/extras/ITDisasterRecoveryPlan.pdf.

4. Kosutic D. Disaster recovery site – What is the ideal distance from primary site? [Electronic Resource] / Dejan Kosutic // Blog by on Dejan Kosutic. – Mode of access: http://blog.iso27001standard.com/2012/11/19/disaster-recovery-site-what-is-the-ideal-distance-from-primary-site.

5. 12,000 laptops lost weekly [Electronic Resource]. – Mode of access: http://www.americanownews.com/story/22046003/12000-laptops-lost-in-airports-every-week.