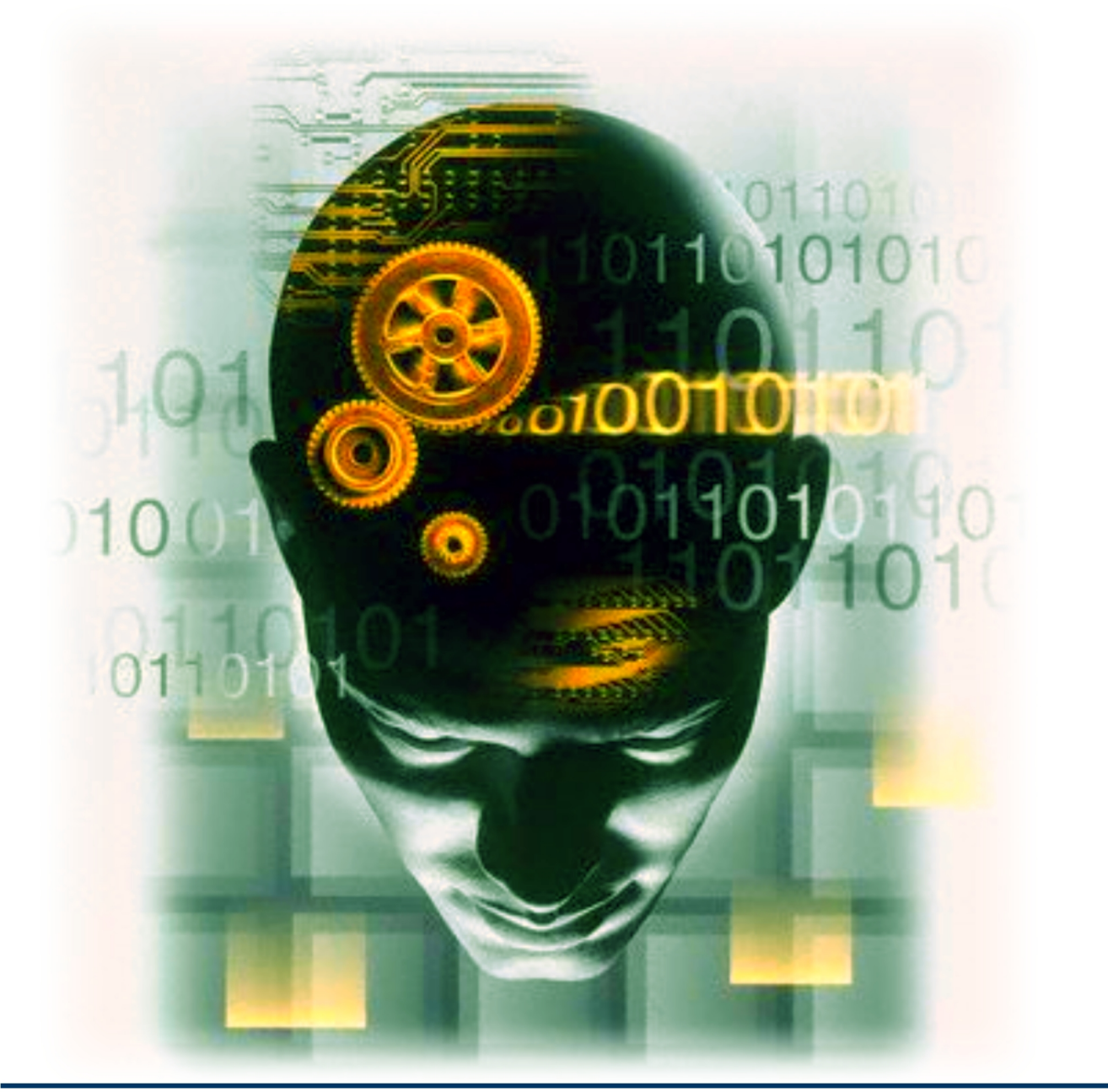


SECURITATEA INFORMAȚIONALĂ 2012

CONFERINȚĂ INTERNAȚIONALĂ,
(ediția a IX-a), 18 iunie 2012

ACADEMIA DE STUDII ECONOMICE DIN MOLDOVA
LABORATORUL DE SECURITATE INFORMAȚIONALĂ

SECURITATEA INFORMAȚIONALĂ 2012

CONFERINȚĂ INTERNAȚIONALĂ
(ediția a IX-a)

18 iunie 2012

Chişinău – 2012

CZU 004.056(082)=135.1=111=161.1
S 40

COMITETUL DE ORGANIZARE:

Grigore Belostecinic, rector al Academiei de Studii Economice din Moldova,mebru corespondent al Academiei de Ştiinţă a Moldovei, membru-corespondent AŞ RM, doctor habilitat, profesor (R. Moldova)

Tatiana Mişova, prorector al Academiei de Studii Economice din Moldova, doctor, profesor (R. Moldova)

Ilie Costaş, doctor habilitat, profesor, Academia de Studii Economice din Moldova (R. Moldova)

Veaceslav Perju, doctor habilitat, profesor, Vicepreşedinte al Consiliului Naţional pentru Acreditare şi Atestare al Republicii Moldova (R. Moldova)

Serghei Ohrimenco, doctor habilitat, profesor, Academia de Studii Economice din Moldova (R. Moldova)

Teodor Ţîrdia, doctior habilitat, profesor, Universitatea de Stat de Medicină (R. Moldova)

Tudor Leahu, doctor, Universitatea Cooperatist - Comercială (R. Moldova)

Leszek Fryderyk Korzeniowski, prof. nadzw. dr hab., preşedintele Asociaţiei Europene pentru Securitate (Polonia)

Agop Sarkisian, doctor, Academia de Economie (Svistov, Bulgaria)

Vladimir Golubev, doctor, professor, Centrul de Cercetare a Crimelor de Computator (Zaporojie, Ucraina)

Viktor Blagodstskih, doctor, profesor, Universitatea de Stat din Moscova de Economie, Statistică si Informatică (Moscova, Russia)

Veselin Dimitrov Popov, doctor, Academia Economică (Svistov, Bulgaria)

Genadii Cernei, doctor, expert, Vice-preşedinte al Băncii comerciale "Unibank" S.A. (R. Moldova)

Valerii Domarev, doctor, expert (Ucraina)

Andrzej Augustynek, doctor, AGH University of Science and Technology (Krakow, Polonia)

Vladimir Skvir, doctor, expert, Universitatea Politehnică Naţională din Lvov (Lvov, Ucraina)

Serghei Kavun, doctor, Universitatea Economică Naţională din Harkov (Harkov, Ucraina)

Constantin Sclifos, MCP, expert, Academia de Studii Economice din Moldova (R. Moldova)

Vitalie Spînachi, LL.M., expert, primar s. Cărbuna (r-nul Ialoveni, R. Moldova)

Tatiana Monasterska, dr., The President Stanisław Wojciechowski Higher Vocational State School in Kalisz (Poland)

Dimitar Georgiev Velev, dr., University of National and World Economy (Sofia, Bulgaria)

Anatoly Krapivensky, Ph.D. in Sociology, Institute of Youth Policy & Social Work (Volgograd, Rusia)

Descrierea CIP a Camerei Naţionale a Cărţii

„Securitatea informaţională 2012", conf. intern. (2012; Chişinău). Securitatea informaţională 2012: Conf. intern. (ed. a 9), 18 iun 2012 / resp. de ed.: S. Ohrimenco. – Ch.: ASEM, 2012. – 78 p. Antetit.: Acad. de Studii Econ. din Moldova, Lab. de Securitate Informaţională. – Texte: lb. rom., engl., rusă. – Bibliogr. la sfârşitul art. –100 ex.

ISBN 978-9975-75-499-6.

CD-rom:sd, col.; in container, 19 x 14 x 2 cm. Cerinte de system: Windows 98/ 2000/XP, 64 Mb hard, VOB Media Player

004.056(082)=135.1=111=161.1

Coordonatorul ediţiei - prof.univ. dr. hab. **S. Ohrimenco**

ISBN 978-9975-75-499-6

Laboratorul de Securitate Informațională al ASEM este membru al Asociației Europene pentru Securitate

PARTENER MEDIA:

PARTENER INFORMAȚIONAL

PARTENERII NOȘTRI

Cuprins:

БАЗОВЫЙ ДОКУМЕНТ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ МОЛДОВА –ОБЪЕКТИВНАЯ НЕОБХОДИМОСТЬ ИЛИ МОДНАЯ ТЕНДЕНЦИЯ?

С.Ф. ГРИЩУК-БУЧКА
Институт Истории, Государства и Права АНМ
Славянский университет Республики Молдова

The increased role of the Internet, the unique features of this network will bring «information security» to a new level, and even now regard it as a basic category of national security. This article is devoted to the legal regulation of information security and consolidate its status in the legislation of the Republic of Moldova.

Основной правозащитной функцией любого государства является обеспечение защиты прав и свобод личности, общества и своей государственности от различного рода угроз. Развитие и внедрение информационно-коммуникационных технологий (ИТК) и их повсеместное внедрение, направленное на всеобщую информатизацию общества, перед государством остро ставит новый вопрос - вопрос обеспечения информационной безопасности личности, общества и государства. Информационная сфера, длительное время рассматривающаяся в качестве составного элемента национальной безопасности, наравне с экономической безопасностью, военной безопасностью, экологической безопасностью, существенно изменила своей вектор в последнее десятилетие XX вв. Возросшая роль Интернета, уникальные возможности данной сети позволили вывести «информационную безопасность» совершенно на новый уровень, и уже в настоящее время рассматривать ее в качестве базовой категории национальной безопасности, и далее, именно посредством нее говорить об информационной безопасности в конкретной сфере - в экономике, экологии, в военной сфере и т.д. Значимость виртуального мира возросла настолько, что безопасность информационной сферы выступает серьезнейшей проблемой современности, свойственной всем государствам, вне зависимости от их политического или экономического уровня развития. Глобализация, компьютеризация, всеобщая информатизация, и, как негативный аспект данных процессов, проблема обеспечения информационной безопасности объединили все государства.

Республика Молдова является субъектом международных отношений, активно интегрируется в общеевропейские процессы и успешно внедряет различного рода научные решения и IT-технологии в сфере информатизации. В рамках данной деятельности в Республике Молдова сформирована серьезная правовая база, четко закрепляющая аспекты построения информационного общества и внедрения технических решений [5],[6]. Не смотря на то, что последние 10 лет страна

поддерживает непрерывное развитие сектора IT, по данным Министерства информационных технологий и связи Республики Молдова в разработке и использовании ИКТ мы находимся в группе стран со средним уровнем значения индекса. Если в 2002 году значение индекса развития ИКТ было 2,14, в 2007 году это значение возросло до 3,11, а в 2008 году индекс составил 3,37 [4]. В 2011 году, согласно данным Международного союза электросвязи, Республика Молдова вошла в категорию «динамичных стран», добившихся весьма существенных улучшений по индексу IDI, как в абсолютном, так и в относительном выражении [3].

Однако вопрос обеспечения информационной безопасности в Республике Молдова совершенно не регламентирован правом. Анализ состояния нормативно-правового регулирования в сфере информационной безопасности указывает на наличие многочисленных пробелов в регулировании соответствующей категории общественных отношений, противоречивости отдельных норм, несоответствия правовых актов указанной области с международными правовыми нормами, а в целом – об отсутствии комплексности и единства информационно-правового пространства. В Республике Молдова отсутствует базовый документ в сфере обеспечения информационной безопасности, будь-то доктрина, концепция или стратегия, более того сам термин «информационная безопасность» не известен правовому полю Молдовы в качестве самостоятельной правовой категории, а лишь употребляется в контексте ряда законов.

Концепция национальной безопасности Республики Молдова [1], выступая в качестве базового документа в сфере национальной безопасности, определяет цель и основные направления национальной безопасности страны, а также общие ценности и принципы, охраняемые молдавским государством и обществом. Данный нормативно-правовой акт представляет собой систему идей, отражающих приоритеты государства в области национальной безопасности, однако об информационной безопасности, к большому сожалению, в нем нет упоминаний, за исключением пункта «*1.3.6. Угрозы в сфере информационных технологий*». Однако, и в данном контексте изложения законодателем, на наш взгляд, произведена подмена понятий «защита информации» и «информационная безопасность», в частности «….прогрессивное развитие электронных информационных систем в Республике Молдова и высокий уровень их взаимодействия с международными информационными системами облегчают действие криминогенного фактора в информационной сфере и усугубляют уязвимость этих систем, в том числе в областях первостепенной важности для национальной безопасности.». Аналогичная ситуация складывается при правовом анализе Стратегии национальной безопасности Республики Молдова [2]. В частности, информационная безопасность только лишь выделена в качестве одной из главных угроз для национальной безопасности Молдовы и пункт «*4.7. Обеспечение информационной безопасности*» – по сути содержит сведения в отношении обеспечения защиты информации и информационных технологий. Лишь последний абзац данного пункта Стратегии гласит:

«информационной безопасности государства касаются и провокации медийного характера, направленные против Республики Молдова. В этом отношении следует скорректировать соответствующие правовые нормы, создать эффективные механизмы мониторинга, контроля и внедрения в целях сокращения существующих разногласий и провокаций, защиты общества от возможных попыток дезинформации и/или от манипуляционного информирования извне. В связи с этим будут проводиться консультации с гражданским обществом».

Иными словами, преуспевая в одном направлении информатизации, сформирован огромный правовой пробел в другом. Те обстоятельства, что информационная инфраструктура и ее ресурсы во все большей степени становятся ареной межгосударственной борьбы за мировое лидерство, а индивидуальное и массовое сознание все в большей степени зависят от деятельности средств массовой информации и коммуникации, по мнению А.А. Чернова [7], должны предопределить содержание национальных интересов всех государств в информационной сфере, а, соответственно, и потребностей государств в обеспечении их безопасности, включая и Республику Молдова.

Разработка, принятие и реализация государственной информационной политики, в частности Доктрины информационной безопасности или Концепции информационной безопасности, позволит заложить основы для решения таких жизненно важных задач, как формирование единого информационного пространства Молдовы, ее интеграции в мировое информационное пространство, уделяя при этом особое внимание обеспечению информационной безопасности личности, общества и государства, развитию сферы информационных услуг, совершенствованию правового поля в регулировании происходящих информационных процессов.

Литература

1. Закон Республики Молдова «Об утверждении Концепция национальной безопасности Республики Молдова» №112 от 22.05.2008. Monitorul Oficial Nr. 97-98 от 03.06.2008
2. Постановление Парламента Республики Молдова «Об утверждении Стратегии национальной безопасности Республики Молдова» №153 от 15.07.2011. Monitorul Oficial Nr. 170-175 от 14.10.2011
3. http://www.itu.int/ITU-D/ict/publications/idi/material/2011/MIS2011-ExecSum-R.pdf - Доклад Международного союза электросвязи «Измерение информационного общества» (издание за 2011 год) [Электронный ресурс] Дата обращения: 15.03.2012
4. http://www.mtic.gov.md/reports_ru/ - Отчет по глобальному индексу развития информационно коммуникационных технологий (IDI) Министерства информационных технологий и связи Республики Молдова [Электронный ресурс] Дата обращения: 14.03.2012

5. http://idsi.md/ - сайт Государственного Предприятия «Институт Развития Информационного Общества» [Электронный ресурс] Дата обращения: 12.03.2012
6. http://www.xn--e1aajfpcds8ay4h.com.ua/pages/view/330 - Грищук-Бучка С.Ф. Правовой аспект построения информационного общества в Республике Молдова [Электронный ресурс] Дата обращения: 15.03.2012
7. http://www.dzyalosh.ru/01-comm/books/stan-obshestva/3_1.html - Чернов А.А. Становление глобального информационного общества: проблемы и перспективы [Электронный ресурс] Дата обращения: 14.03.2012

ПОНЯТИЕ РИСКА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Анатолий КРАПИВЕНСКИЙ,
Институт молодежной политики и социальной работы
(Российская Федерация, г. Волгоград)

The concept of risk is the justification of one of the most important categorical indicators in the process of informational security (IS) ensuring. Author investigates the opportunities of application of this category formulations in the various directions of the above area.

В социологии понятие риска базируется, в первую очередь, на теории теории Н. Лумана, согласно которой под риском понимается "отказ от предупредительных мер" [1: 157] по пресечению угроз в рассматриваемой сфере социальной деятельности.

Рассматривая под этим углом зрения всю парадигму отношений, складывающихся в процессе обеспечения информационной безопасности, следует выделить потенциально возможные виды существующих угроз. В Доктрине информационной безопасности РФ [2] приводится подробная классификация угроз по критерию "общая направленность". Следовательно, чтобы операционализировать понятие "риск" применительно к различным направлениям сферы информационной безопасности, необходимо адаптировать его применительно к каждой из обозначенных в Доктрине видов угроз: отказ от предупредительных мер по пресечению угроз конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России; отказ от предупредительных мер по пресечению угроз информационному обеспечению государственной политики Российской Федерации; отказ от предупредительных мер по пресечению угроз развитию отечественной индустрии информации, включая

индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов; отказ от предупредительных мер по пресечению угроз безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Итак, комплексный риск в сфере обеспечения информационной безопасности можно определить как совокупность вышеуказанных рисков. Для того, чтобы минимизировать возможные риски, любые отношения в сфере информационной безопасности личности, общества или государства должны быть "помещены в контекст порядка, управления, стабильности" [3: 87].

При этом управление информационной безопасностью сводится к минимизации рисков нанесения ущерба в рассматриваемой сфере.

В этой связи уместно говорить о создании на каждом из "участков фронта" борьбы за минимизацию рассматриваемых нами рисков системы управления информационной безопасностью (СУИБ) — «той части общей системы управления ..., основанной на оценке … рисков, которая создает, реализует, эксплуатирует, осуществляет мониторинг, пересмотр, сопровождение и совершенствование информационной безопасности. Система управления включает в себя организационную структуру, политики, планирование, должностные обязанности, практики, процедуры, процессы и ресурсы. Создание и эксплуатация СУИБ требует применения такого же подхода, как и любая другая система управления» [4].

Таким образом, процесс обеспечения информационной безопасностью, по сути, представляет собой разновидность процесса управления рисками, т.е. риск-менеджмента. "Риск-менеджмент представляет собой систему управления риском и … отношениями, возникающими в процессе этого управления. Риск-менеджмент включает в себя стратегию и тактику управления… Под стратегией управления понимаются направление и способ использования средств для достижения поставленной цели… Стратегия позволяет сконцентрировать усилия на вариантах решения, не противоречащих принятой стратегии, отбросив все другие варианты. После достижения поставленной цели стратегия как направление и средство ее достижения прекращает свое существование. Новые цели ставят задачу разработки новой стратегии. Тактика - это конкретные методы и приемы для достижения поставленной цели в конкретных условиях. Задачей тактики управления является выбор оптимального решения и наиболее приемлемых в данной … ситуации методов и приемов управления. Риск-менеджмент как система управления состоит из двух подсистем: управляемой подсистемы (объекта управления) и управляющей подсистемы (субъекта управления) [5].

Разумеется, как и в любой сфере деятельности в технологичном XXI веке, риск-менеджеры в сфере обеспечения информационной безопасности должны использовать технологии разработки решений по минимизации конкретного вида риска. Под технологией разработки решений в риск-менеджменте принято понимать

"процесс преобразования имеющихся у менеджера сведений, данных, информации о возникшей перед ним проблеме или поставленной ему задаче в точно сформулированное решение... В настоящее время невозможно представить себе технологию разработки решений без информационных технологий сбора, обобщения, анализа и преобразования исходных данных о проблеме или задаче в окончательное решение руководителя" [6: 7-8].

Литература:

1. Луман Н. Понятие риска: Пер. с нем. // THESIS: теория и история экономических и социальных институтов и систем. - 1994. - № 5.
2. Доктрина информационной безопасности Российской Федерации // Российская газета. – 2000. – 28 сентября.
3. Бергер П., Лукман Т. Социальное конструирование реальности: трактат по социологии знания: Пер. с англ. – М.: Медиум, 1996.
4. Понятие системы управления информационной безопасностью / Global Trust Solution Limited - http://www.globaltrust.ru/uslugi/vnedrenie-sistem-upravleniya-informacionnoi-bezopasnostyu/ponyatie-sistemy-upravleniya-informacionnoi-bezopasnostyu
5. Риск-менеджмент (Risk Management) // http://www.risk24.ru/riskmanagment.htm
6. Балдин К.В. Риск-менеджмент: Учебное пособие. – М.: Эксмо, 2006.

ОСОБЕННОСТИ УПРАВЛЕНИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТЬЮ ВУЗА

Ольга Пугачева,
Гомельский государственный университет им. Ф Скорины

The basic stages of management by intellectual property (IP) at university are considered: at a stage of creation IP, its right protection, use of objects IP also are sewn up the rights to objects of the industrial property and the copyright.

Одним из приоритетных направлений деятельности вуза является формирование благоприятной среды для творческой деятельности, результатом которой является интеллектуальный продукт, становящийся при определенных условиях интеллектуальной собственностью (ИС). В соответствии с существующими нормами ИС представляет собой правовое положение двух основных категорий результатов интеллектуальной деятельности:

- объектов авторского права и смежных прав (литературные произведения, научные произведения, компьютерные программы и базы данных,

мультимедийные произведения, сетевые произведения, программное обеспечение и др.);

- объектов промышленной собственности (изобретения, полезные модели, промышленные образцы, товарные знаки, фирменные наименования, нераскрытая информация и др.).

Успешная реализация политики вуза в сфере ИС возможна при правильно организованном сопровождении всех этапов, связанных с созданием, правовой охраной, использованием и защитой объектов интеллектуальной собственности (ОИС). Эффективность системы управления ИС в вузе определяется в основном его организационной структурой и характером взаимоотношений между ее элементами, устанавливающих полномочия и ответственность основных участников системы ИС. Проанализируем особенности организации этой системы в вузе на основных этапах управления ИС.

1. На стадии создания объектов ИС основной задачей вуза является всемерная поддержка творческой научно-технической деятельности и формирование благоприятных условий для появления объектов ИС. К таким условиям можно отнести: наличие и подготовку высококвалифицированных исследователей, обеспечение их необходимыми ресурсами и стимулирование развития научных исследований, разработок и изобретательской деятельности по созданию объектов ИС.

В Гомельском государственном университете (ГГУ) им. Ф. Скорины используется сочетание разнообразных материальных и нематериальных стимулов, начиная от поощрений, премий, вознаграждений до награждения званием лауреата ежегодного конкурса «Скориненские научные чтения», которые стимулируют преимущественно создание объектов авторского права. Однако автор монографии обычно получает меньший гонорар, чем его месячная зарплата в вузе. Автор учебного пособия, изданного по рекомендации научно-методического совета вуза, вынужден выкупать за собственные средства часть тиража, не востребованного студентами в течение определенного времени. Для стимулирования создания объектов промышленной собственности (ОПС), к которым в университете относятся преимущественно изобретения и полезные модели, используется в основном система вознаграждения их авторов в соответствии с принятым в республике законодательством, отражающая уровень возможностей государства. Существующая система стимулирования может до некоторой степени компенсировать реализованную в конкретном продукте творческую деятельность автора, однако она не обеспечивает действительных инвестиций в будущее творчество.

2. На стадии правовой охраны ОПС управленческая деятельность включает отбор и определение правообладателя объектов ИС, выбор способа охраны (патентное право или режим коммерческой тайны), выполнение всех действий, связанных с охраной объектов ИС в зависимости от выбранного способа охраны.

Отбор объектов ИС в соответствии с выбранной вузом стратегией может осуществляться специально созданным органом, с учетом рекомендаций которого руководством принимается решение о целесообразности получения охранного

документа либо охраны объектов ИС в режиме коммерческой тайны. Патентная служба в составе научно-исследовательского сектора университета с определенной периодичностью пересматривает перечень имеющихся охранных документов на ОПС и дает заключение о целесообразности поддержания их в силе.

3. На стадии использования объектов ИС в соответствии с выбранной вузом стратегией (способом использования ОИС) проводится оценка стоимости ОИС и их учет в составе нематериальных активов. Основными способами использования ОИС в вузе могут быть: применение созданных в результате выполнения научно-исследовательских, опытно-конструкторских, технологических работ или иной деятельности ОИС для собственных нужд (в собственном производстве или для оказания услуг); приобретение у правообладателей или авторов, в том числе в обмен на другое имущество; безвозмездная передача правообладателями или авторами; продажа лицензий на право использования ОИС; внесение их в уставный фонд создаваемых субъектов хозяйствования; уступка или передача прав на объекты ИС.

4. Необходимость защиты прав на объекты ИС возникает в случае нарушения сотрудниками или третьей стороной исключительных прав учреждения образования. Вуз имеет право инициировать рассмотрение споров о нарушении его прав в судебном порядке. Перед подачей иска о нарушении прав необходимо провести экономическую и юридическую оценку возможных последствий этих действий.

Таким образом, рассмотренный вариант распределения функциональных обязанностей между имеющимися подразделениями и службами учреждения образования и соответствующий ему способ управления ИС в вузе, в основе которого лежит горизонтальное разделение управленческого труда, не требует больших затрат и реализуется в большинстве вузов. За каждым структурным подразделением приказом руководителя вуза дополнительно могут быть закреплены новые функциональные обязанности, связанные с управлением ИС или уточнены имеющиеся.

На отделы кадров при заключении трудовых договоров (контрактов) с научными и научно-педагогическими работниками возлагается обязанность составления и подписания в качестве приложения к трудовому договору соглашения о правах и обязанностях работника и нанимателя в части создания, правовой охраны и использования служебных результатов интеллектуальной деятельности.

На Региональный центр маркетинга университета возлагаются функции сбора и хранения информации о научных разработках, реализацию оперативного поиска и обмена информацией; исследования рынка научно-технических продуктов; разработки и реализация программы маркетинга по перспективным научно-техническим продуктам; разработка бизнес-планов инновационных проектов и оказание консультационных услуг в этой области.

На патентную службу возлагается обязанность ведения Реестра поданных заявок на ОПС и Реестра патентов на изобретения и полезные модели.

Планово-экономическому отделу и бухгалтерии поручается проведение оценки стоимости ОИС и учета ОИС в составе нематериальных активов, а также определение порядка использования полученных средств.

Основной недостаток существующей системы управления ИС заключается в отсутствии связующего звена между всеми стадиями от создания до использования ОИС и трудностями в выполнении отдельных видов деятельности. Ее совершенствование возможно в форме создания специализированного подразделения без права или с правом юридического лица (унитарное предприятие, общество с ограниченной ответственностью, коммерческая организация и др.) учредителем (соучредителем) которого является учреждение образования, комплексно осуществляющего управление ИС в вузе. Но использование такой организационной структуры оправдано лишь в больших по численности вузах, создающих значительное количество ОИС. В роли таких специализированных подразделений могут выступать республиканские или региональные центры трансфера технологий, имеющие в своем составе квалифицированных специалистов и оказывающие консалтинговые услуги по широкому спектру вопросов, связанных с ИС.

Анализ состояния и развития системы управления ИС в ГГУ им. Ф.Скорины в 2000-2011 гг. показывает стабильный рост основных показателей оценки результатов научно-технической и творческой деятельности, что связано с достаточно работоспособной и отлаженной системой управления научными исследованиями и разработками. Об этом свидетельствуют данные, характеризующие число поданных заявок и полученных патентов на ОПС, изданных монографий, учебников и учебных пособий, использовании результатов исследований и разработок в народном хозяйстве и в учебном процессе (таблицы 1 и 2).

Таблица 1.

Сведения о поданных заявках и полученных патентах на объекты промышленной собственности (ОПС)

Годы	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Количество поданных заявок на ОПС	4	9	7	8	11	14	10	3	9	7	11	7
Количество полученных патентов на ОПС	9	9	2	15	7	8	19	21	11	9	4	6

Таблица 2.

Использование объектов авторского права

Годы	Использование научных разработок		
	В народном хозяйстве	В учебном процессе	
		Акты внедрения	Издание монографий, учебников и учебных пособий
2000	-	12	144
2001	2	7	171
2002	12	63	176
2003	14	52	195
2004	12	51	193
2005	12	64	320
2006	6	25	197
2007	-	131	256

2008	7	96	214
2009	6	131	157
2010	15	275	153
2011	5	274	121

Однако сохраняются проблемы, связанные с продвижением наукоемких разработок в производство и использованием запатентованных результатов научных исследований.

Главной задачей управления инновационной деятельностью университета является адаптация к вызовам новой экономики в целях эффективного использования его интеллектуального потенциала.

RISK MANAGEMENT IN IMPLEMENTATION OF INFORMATION SYSTEMS IN PUBLIC ADMINISTRATION

Assistant Professor Katia Strahilova PhD,
University of National and World Economy, Sofia, Bulgaria,
department "Public administration and regional development",
katia_emilova@yahoo.com

In this paper an attempt is made to a definition of risk in the implementation of software projects in public administration. Presents are the main actors and the types of risks.

The implementation of IT projects in the public sector is complex and responsible task. In this process it is important that quality management and risk. Risk management in the implementation of software projects in the public service depends on several key stakeholder groups (figure 1):

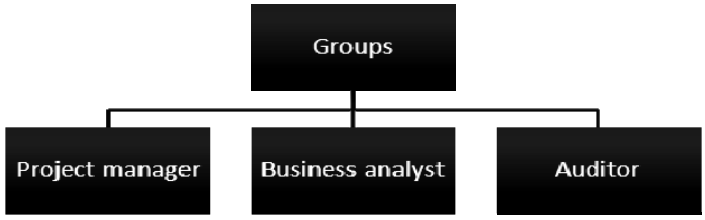


Figure 1. **Stakeholder groups**

- **Project manager** – he ran the risk of a software project. In this paper we consider that the project manager should bear the risk of the project. It is a figure that is bound to measure all risks. It is required to ensure complete customer satisfaction and all other actions necessary to ensure the project;

- **Business analyst** - responsible for developing a quality project and ensuring an effective software;
- **Auditor** – required to provide continuous review and to ensure the creation of software in accordance with all regulatory requirements.

The process of risk management through the following phases (figure 2):

Figure 2. **Risk management phases**

- **Identification**. At this stage it is necessary primarily to identify the risk points in the realization of software project;
- **Analysis.** It is necessary to identify the risk characteristics. It is to divide the main types of risk and its sources. We offer a risk analysis be performed on the following main types (table 1):

Table 1.

Types of risks

N	Type	Description
1	Team roles	Not all team roles are fully represented; roles are inappropriately combined
2	Team structure	Roles and reporting lines are not clearly identified
3	Facilities	Physical facilities are inadequate for building and delivering the product
4	Training plan	No training plan has been prepared for team members
5	Project experience	The team has limited experience of working on similar projects
6	Process experience	The team has not previously worked with the development method or tools
7	Technology experience	The team has not previously worked with the selected technology
8	Quality Attitude	Team members do not display pride in workmanship
9	Cooperation	There is a lack of team spirit; conflict resolution requires management intervention
10	Communication	Team members show poor awareness of mission or goals and/or poor communication of technical information
11	Productivity	Productivity is low; milestones missed
12	Planning	Planning is not timely, technical leads are excluded or contingency planning is omitted
13	Program Interfaces	Interfaces with the customer, other contractors, senior and/or peer managers are poor
14	Monitoring	Management metrics are undefined and development progress poorly tracked
15	Personnel Management	Project personnel are used inappropriately
16	Quality Assurance	Procedures and resources are not in place to assure product quality
17	Project objectives	Project objectives are unclear or immeasurable

18	Size and complexity	The project is large, highly complex or not decomposable
19	Dependencies	The project has dependencies on outside products or services
20	Budget size	Budget is insufficient
21	Budget security	Budget is not secured for the full project
22	Cost controls	Cost controls are inadequate
23	Defined process	No well-defined development process has been adopted
24	Informality	Inconsistencies may make the implementation difficult to understand or maintain
25	Suitability	The development process is poorly suited to the customer, contract and solution
26	Process Control	The development process is not enforced, monitored, and controlled using metrics.
27	Product Control	Mechanisms for controlling changes in the product are inadequate
28	Policies and standards	Policies and standards are un-defined, vague or unused
29	Alternatives considered	No alternative solution approaches have been considered
30	Documentation	Development documentation will not be created in parallel
31	Functionality	There are potential problems in meeting functionality requirements
32	Interfaces	Internal interfaces (hardware and software) are poorly defined or controlled
33	Performance	There are stringent response time or throughput requirements
34	Hardware Constraints	There are tight constraints on the target hardware
35	Non-Developed Software	There are problems with software used in the project but not developed by the team
36	Difficulty	Implementation of the design will be difficult to achieve
37	Complexity	The solution requires complex algorithms that may be difficult to code
38	Security	Security requirements are more stringent than the current state of the practice or team experience
39	Security testing	Security requirements cannot be successfully tested
40	Data migration	Deployment will involve significant data migration – or descriptions of existing data sources are inadequate
41	Pilot approach	Available pilot sites are reluctant to be involved
42	Parallel deployment	The solution requires a "big-bang" rather than a phased deployment
43	International deployment	Deployment requires on-site attendance in different countries
44	Human Factors	The system may be difficult to use because of poor human interface definition
45	Support personnel	Support personnel are inadequate in experience or numbers
46	Operational processes	Solution requires significant changes to existing operational processes
47	Availability / Reliability	Reliability or availability requirements are difficult to meet
48	Supplied components	Supplied components are likely to be late or do not fully meet the needs of the solution

- **Risk management plan.** This means planning for all elements of the overall risk to be addressed and referred to the measures to reduce them;
- **Mitigation.** At this point Willie is concentrating on conducting the necessary measures and establish safeguards to prevent hazardous situations;

- **Monitoring.** At all stages of the implementation of a software project is necessary organization for Monitoring and Risk Management.

Finally, it should be noted that identification of risk factors is complex. In public administration must be considered and the influence of many external factors such as legislation, macroeconomic factors and others. This will allow the deployment of effective software applications

INFORMATION SECURITY MANAGEMENT STANDARDS IN THE IMPLEMENTATION OF ERP SYSTEMS

Assistant Natalia Futekova,
Department of "Information technologies and communications",
University of National and world economy – Sofia, Bulgaria,
n.futekova@abv.bg

This report presents the essence of the information security management standard ISO 27001. It is clarified the applicability of the standard and the specifications of the individual stages of its implementation.

Standards ISO 27001:2005 "Information technology - Security techniques - Information security management systems – Requirements" put requirements for Information security management systems (ISMS). This standard is applicable to all organizations regardless of their type (private or public) and segment affiliation. Information security management system (ISMS) is a method and management tool for the information used by organization as well as information security for the decisions taken. In terms of classification, information which must be secured may be owned by the company or by the customer (Figure 1):

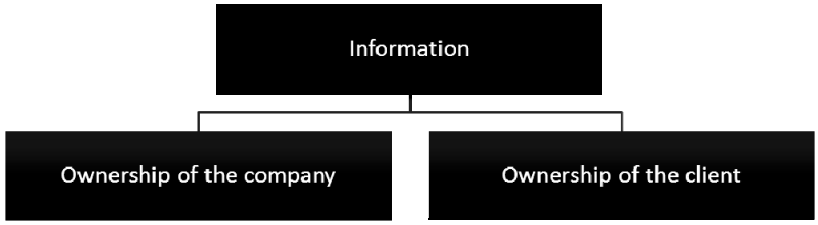


Figure 1. **Information types**

Regarding the implementation process of ERP (Enterprise resource planning) systems, ISO 27001:2005 is appropriate for use in:

- defining the security information policy that will be used or created by the ERP system;

- defining of specific security goals;
- use in Information risk management resulting from the operation of the ERP system;
- to ensure that companies and their implemented software applications meet regulatory requirements;
- in determining the existing business processes for IT security management;
- in defining new business processes for IT security management;
- establishing a consistency between the policies of the organizations and the applicable standards;
- providing a relevant information to the customers on information security

The implementation process of information security standards must be synchronized with the process of building of ERP system. That is why we offer the following milestones:

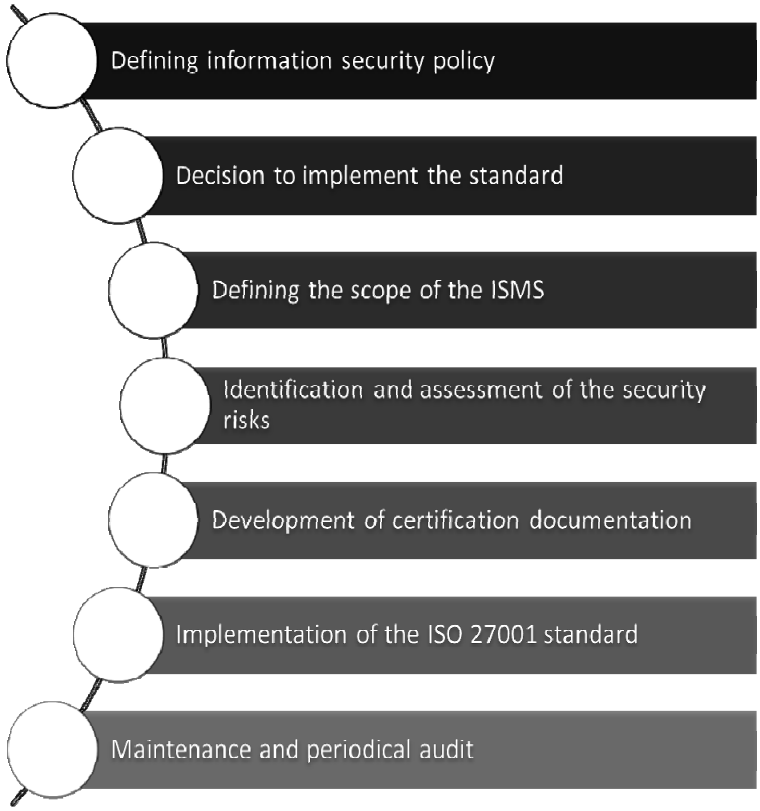


Figure 2. **Implementation process of ISO 27001**

In general, the implementation process of the standard in a company comes down to the following steps.

Firstly, the analyzed company needs to define an information security policy. This is important in terms of requirements and defining the scope of ISMS (Information security management system). At this stage it is necessary to make a decision on the ISO 27001 implementation. Once this decision is made, it is important to identify and assess the information security risks as a result of the implemented ERP system and to develop certification documentation. After the coordination with the contracting company, the implementation of the standard can be started.

ISO 27001 demands a strict observance of the relevant laws, regulations and contractual obligations regarding the information security, optimized use of available resources, as well as periodic internal audits of the system in order to its continuous improvement.

PERSONAL DATA DANGERS

Nicolae TURCAN
Lyceum of creativity and invention "Prometeu-Prim"

În această lucrare sunt reflectate problemele majore ce direct afectează securitatea datelor personale, descrierea lor, și principiile de bază care urmează a fi aplicate pentru protecția datelor menționate.

Personal data, which directly or indirectly identify an individual, especially by referring to identification number (personal code), to one or more specific details: physical, physiological, psychological, economic, cultural or social state, are divided in two groups: ordinary and special.

Special category of personal data is the information revealing racial or ethnic origin, political opinions, religion, health status or private life and the criminal convictions of an individual.

Common category is the information that reveals:

- Name and surname, sex, date of birth, citizenship, image, voice, family statute, military statute, geo-location data/pseudonym, family member's personal data, driving license data, registration certificate data, economic and financial situation, owned assets data, bank details, signature, etc.

Personal data includes plenty of subgroups, followed by their increased vulnerability because of the new threats which appear and progress at an astonishing rate. The main and the most expensive risks of personal data are:

- hackers; malwares; laptop theft; denial-of-service attacks; insiders; zombie networks; phishing; abuse of wireless networks; abuse of instant messaging; abuse of application servers; web pages attacks; DNS attacks; natural disasters.

As a result of all the menaces of personal data, organizations which possess them started to develop a policy regarding protection of personal data. This policy is prepared especially for protection from risks as disclosure, alteration, fraud, destruction, theft, and to avoid the consequences, particularly from the financial, judicial and reputation perspective.

Whole complex of measures will enable elaboration of steps according criteria for classifying information. Possession of information will be based on certain principles:

- Classification of information;
- Hierarchy of protective measures;
- Monitoring of the protection level.

Information possessor can be either an individual or a legal person. If owning secret information with a high protection level, the person becomes responsible for maintaining it. As a result, information can be classified:

- In terms of availability – accessed and used by an authorized person;
- In terms of integrity – information wasn't modified or destroyed by an unauthorized person;
- In terms of privacy – not available to unauthorized persons or for those who don't have a need to know it.

According to all above, we are able to perceive the policy concerning protection of data, the policy which is oriented to its confidentiality. It will be marked according to the security level. Classification will be periodically reviewed depending on the event. Within the organization that possesses personal information, protection will be provided through the following ways: legal protection (applying laws); protection with specific procedures (encoding, encryption); physical protection (safes).

Nonetheless, all the procedures will provide security measures, as:

Firewall.

A firewall is a device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass.

Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions.

Antivirus.

Antivirus software is used to prevent, detect, and remove malware, including but not limited to computer viruses, computer worms, Trojan horses, spyware and adware. Computer security, including protection from social engineering techniques, is commonly offered in products and services of antivirus software companies.

Protection from hackers.

All unknown files from the server should be eliminated, and also a strict control should be implemented. All the packages that have other than its own IP header (which may contribute to the information leakage) shall be removed.

Staff trainings.

Because of the constant human error, organizations should create special trainings in order to inform staff about the most frequent problems caused unwilling, and to oblige them to operate according to the rules, by checking their work or creating special departments which goal will be to analyze all the progress made by workers during a period of time.

Limited access to external networks.

Limiting or blocking the access to external networks will contribute to increasing workers efficiency, resulting in a more organized collective. Also, it can especially help in avoiding dangerous files with malwares and information loss.

Natural disasters protection.

Public responses to a major natural disaster may warrant:

a) special efforts to protect the vital interests of victims;
b) extraordinary processing of personal information to compensate for the loss of usual documentation, disrupted access to databases, communication difficulties and other challenges;
c) use of personal information held by organizations beyond their usual business purposes.

For a higher secure, the hardware which stores the most important data should be placed far from the disastrous places, and reliably protected.

Responsible organizations already include disaster recovery in their risk management planning. The resolution encourages and supports such initiatives, emphasizing the importance of protecting data and it's attribution to the lives of individuals and communities.

As a conclusion, I can state that efficiency standards for classification and protection of the personal data depend on the objectives and methodology for classification of information of all people involved. Initiatives of promoting information security policy will ensure awareness of all people holding personal data about classification and protection recommended measures.

MANAGEMENT TEMPLATE FOR SECURING BUSINESS PROCESSES USING MULTIPLE SIGNATURES TECHNIQUE

Veliko Ivanov, Valentin Kisimov
UNWE, Sofia, Bulgaria

Information security has become important for the business processes that occur in every organization and especially for the needed increasing of the security of the business processes. The contemporary business process is a collection of related, structured activities and tasks, involving computers, documents and people. By its nature, business processes are complex and changing over the time. With the new ICT corporate

technologies for Enterprise 2.0 and Enterprise 3.0 systems, the security of the business processes and their components, are becoming more and more important factor. Based on the business processes dynamics, their security also need to be managed via a dynamic mechanism and special ICT security architecture. Participation of a human in a computerised business process can be legalised via actions (message, document or process), which are digitally signed. The human involvement in the business processes, with their different corporate roles, requires implementation of separation of power, transformed into a separation of digital signatures. Implementing more than one digital signature in a business process leads to implements multiple digital signatures technique.

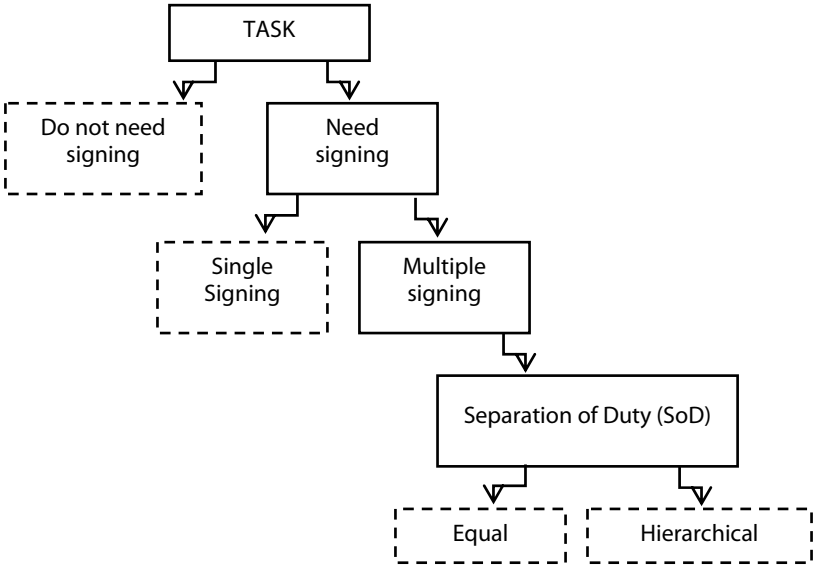
Multiple digital signatures have 3 aspect of work:

- Signing with or without verification of previous signatures;
- Multiple signing with Separation of equal duty;
- Multiple signing with Separation of different duties.

The proposed implementation of multiple digital signatures is working with previous verification, e.g. before signing, the process verify the previous signature – for availability, correctness, and validity. The Separation of equal duty corresponds to signing the message / document in non-specified sequence of the participant of the signing path (signing path is the sequence / parallelism of signatures for a given process task). The Separation of different duties requires exact sequence of signatures. For high secure business process, proposed in the paper, different signing paths can be applied – one or a few with Separation of equal duty and one or a few with Separation of different duties.

The purpose of the proposed paper is to present an Architectural Management Template for securing Business processes (AMTSBP), through which a Business process can implement multiple digital signatures techniques, increasing the security of the Business process. The Template is a software architectural component, which defines how many signing paths are valid for the Business process, what kind of separation of duties each signing path applies, what are the needed verification of signatures which have to be provided on each step of the signing path, what is the sequence of duties in signing path, and what is the workflow of supporting security processes applicable to each step of the signing path. The AMTSBP can be applied either as a micros to MS Office documents (managing the documents in the business process), or as a pure software object, plugin to the program code of the business process (managing the program code running the business process).

Every task in business process should be addressed to one of dotted line box on **figure 1** depending on whether its need of digital signing. When there is single signing task it requires simple step verification. In this case one person is responsible for the content and execution of the task. When it is about multiple signatures there are two cases of duty separation (equal and hierarchical). When it is used an equal signature multi-step verification is needed and each of the persons is equally responsible for the content and execution of the task. Hierarchical signature has specific backward verification process, which gives the advantage of precisely setting persons responsibility.



References:

1. Ivanov Veliko, Tzaneva Monika, Murdjeva Alexandra, Kisimov Valentin, Secure the core university business process, IFIP, iNetSec'2010
2. Kissel Richard, Information security, NIST, 2008
3. E-lock technologies, Business Issues in the implementation of Digital signatures
4. International Standard ISO 27000
5. Rodriguez Alfonso, A BPMN Extension for the Modeling of Security Requirements in Business Processe, 2007

ОСОБЕННОСТИ ЗАЩИТЫ ЦИФРОВЫХ ДОКУМЕНТОВ

Мастер, лектор Анатолий БРЕДИНСКИЙ
Государственный университет физической культуры и спорта

Electronic documents stored on digital media become more and more popular, which results in the appearance of new threats. To prevent the latter, businesses nowadays are recommended to develop and implement special security measures.

Активное внедрение цифровых технологий, их постоянное совершенствование, удобство в использовании и иные преимущества приводят к тому, что многие предприятия полностью или частично переходят на оборот электронных документов. А это, в свою очередь ведет к дополнительным рискам утечки информации. Если

раньше защищались сами электронные документы или информационные ресурсы, содержащие документы, то теперь изменяется основной вектор атак и соответственно изменяется объект защиты. Кроме традиционных атак на информационные ресурсы всё чаще и чаще объектом защиты становится **взаимодействие** «человек – электронный документ», «человек – информационный ресурс»[2]. Согласно данным исследования 2008 г., наиболее распространенным каналом утечки данных является сеть (кроме электронной почты) — 21,1% случаев. На втором месте — ноутбуки и мобильные компьютеры — 19,4%, на третьем и с большим отрывом — настольные ПК и серверы — 7,5%. При этом примерно в трети случаев (32,6%) путь остался не установленным. В прошлом году таких случаев было меньше в три раза — 12%. [1]

В целях защиты документов реализуется специальная система документооборота, которая включает в себя: контроль за созданием, доступом и операциями с документом, его копирование и передачу третьим лицам, а также уничтожение электронных документов. Специальный оборот документов на электронных носителях во многом аналогичен обороту бумажных документов. Вместе с тем, они обладают определенной спецификой. Так, оборот подобных документов возможен, как с помощью записи на материальный носитель (flash-drive, CD/DVD диски и иные носители) так и помощью прямой передачи документа конечному адресату, посредством сетей Internet/Intranet.

Элементы системы обеспечения специального документооборота.

Система контроля и учета должна основываться на двух важных составляющих:

1) Программно-аппаратный контроль за документами на цифровом (электронном) носителе;
2) Организационно-технический контроль за лицами, допущенными к средствам хранения и обработки информации;[3. 129 стр.]

Первая составляющую базируется на применении специализированных программных продуктов позволяющих осуществлять доступ к электронным документам, в зависимости от уровня пользователя, а так же контролировать любые манипуляции с документами.

Вторая состоит из системы предварительной проверки работников и проведения специализированного инструктажа, а также контроля персонала имеющего доступ к электронным документам с помощью технических средств (видеонаблюдение, СКУД и т.п.)

Выводы

1) В настоящий момент большинство предприятий не уделяет системе защиты электронного документооборота должного внимания, что нередко приводит к утечке конфиденциальной информации содержащейся в цифровом виде.
2) Целесообразным является разработка и внедрение системы защиты оборота цифровых документов, которая позволит предотвратить боль-

шинство случаев неавторизированного доступа к конфиденциальной информации.

3) Категорически запрещается применение работниками личных носителей информации для записи на них служебной документации. Вынос любых мобильных носителей информации за пределы предприятия без разрешения ответственных сотрудников. Соотвествующее обучение работников шифрованию документов и полному уничтожению файлов содержащих конфиденциальную информацию.

Библиография

1) Анастасия Симакина «Утечки данных поставили на поток» (ресурс интернета: http://www.cnews.ru/news/top/index.shtml?2009/03/25/341847, дата доступа 25 февраля 2012 г.)
2) Алексей Собанов «О защите электронного документооборота» ресурс интернета: http://daily.sec.ru/publication.cfm?pid=31911, дата доступа 25 февраля 2012 г.
3) Анатолий Брединский «Специальный документооборот на предприятии и защита информации на электронных носителях» Журнал "IT-Moldova" № 3-4 2009 г.

СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Филолог, психолог, доктор философских наук
Галина Колесникова,
профессор кафедры Связи с общественностью Донского государственного технического университета

In theses raises the problem of the importance of socio-psychological aspects in the implementation of information security. Is highlighting social and psychological levels of information security. One of possible decisions of the given problem Is offered.

Анализ и систематизация социально-психологических аспектов информационной безопасности представляют собой важную задачу, которая на данном этапе заключается в выявлении принципиальных положений, в соответствии с которыми и будет предложено возможное решение данной проблемы.

При этом базовыми философскими категориями в данном анализе выступают социальная система и личность, поскольку и в основе жизнедеятельности социальных систем, и в основе жизнедеятельности личности лежит один принцип - принцип обеспечения собственной безопасности.

Данный принцип, раскрывающий антиэнтропийную природу социальных систем, а личность также может рассматриваться как система, непосредственно связан не только с потребностями, но и с системой ценностей, поскольку доминирующей потребностью всегда выступает та, которая осознается в качестве главной ценности.

То есть, содержание принципа обеспечения собственной безопасности и на уровне социальной, и на уровне личностной системы всегда имеет специфическое наполнение, которое является результатом сознательной и бессознательной деятельности, направленной на снижение негативного и/или дезорганизующего влияния внешней и/или внутренней среды.

Кроме того нельзя не учитывать и такой важный феномен как борьба мотивов, которая всегда предшествует конкретизации главной ценности и определению доминирующей потребности.

Все перечисленное в совокупности указывает на главенствующую роль личности и социально-психологических аспектов ее поведения при решении проблемы защиты информации. В данном контексте личность рядового сотрудника и личность руководителя выступают как равнопорядковые величины, поскольку поведение сотрудника во многом определяется социальной средой правильно организовать которую как раз и является задачей руководителя. И именно неправильно организованная среда выступает в качестве основного фактора инициирующего формирование конфликтов, которые в последствие могут стать причиной утечки информации.

Выделяют восемь основных типов конфликтов в сфере защиты информации:[1] обусловленные требованиями режима; обусловленные ограниченностью ресурсов (вычислительных или информационных); обусловленные несоответствием целей сотрудников системы информационной безопасности и других отделов; обусловленные несоответствием ожиданий и реальности; конфликты иерархии; конфликты «человек — машина»; конфликты в личной жизни сотрудников. На наш взгляд сюда также необходимо добавить внутриличностный конфликт, который, по сути, выступает первоосновой при формировании всех остальных типов конфликтов.

Однако все приведенные конфликты являются, по нашему мнению, проявлением во вне личностного неблагополучия, которое может формироваться на разных уровнях: внешний – средний - внутренний, каждый из которых, в свою очередь, состоит из подуровней. Первый из них определяется социальными факторами, второй - социально-психологическими и третий психологическими. В таблице это будет выглядеть следующим образом.

[1] http://avoidance.ru/articles/narushiteli-informacionnoj-bezopasnosti/88.html [Электронный ресурс] Дата просмотра 18.03.2012

Структура социально-психологического неблагополучия личности				
Внешний уровень (социальный контекст ситуации)		Средний уровень (специфика реакций на происходящее, выступающая как результат взаимодействия социального контекста и психологических особенностей личности)	Внутренний уровень (психологические особенности личности)	
Социальные факторы, обусловленные объективными обстоятельствами	Социальные факторы, обусловленные субъективными обстоятельствами	Социально-психологические факторы, выступающие как равнозначные	Психологические факторы, обусловленные объективными обстоятельствами	Психологические факторы, обусловленные субъективными обстоятельствами (в данном контексте, то, что зависит от воли индивида и может быть им развито или сформировано)
Социально-экономическая ситуация в стране	Стрессовые факторы, обусловленные профессиональной деятельностью	Специфика взаимоотношений в родительской семье	Свойства темперамента, которые определяются как «трудные»: высокий или низкий уровень активности; упрямство; отвлекаемость; низкий уровень адаптивности; наличие тенденций к избеганию; страх новых ситуаций; регидность	Система ценностей и потребностей; отсутствие критического и рефлексивного мышления; низкий уровень локус-контроля, самооценка; пессимизм

По данным итальянских психологов 25 % служащих принадлежат к категории надежных людей, столько же ждут удобного случая, чтобы разгласить секретную информацию и у оставшихся 50 % поведение формируется в зависимости от обстоятельств. Кроме того, преступления в сфере информации только в 7% совершаются профессиональными программистами, остальные 93% - клерками, служащими, допущенными к работе с информационными системами, администраторами, самим управляющими.

То есть, формирование информационной культуры сотрудников на предприятии и повышение уровня ответственности за утечку информации могут значительно повысить уровень информационной защиты.

Данные параметры - информационная культура сотрудников на предприятии и повышение уровня ответственности, - выступают как взаимосвязанные категории, поскольку существует аксиома: чем выше культура личности, тем выше уровень ее ответственности и порядочности и, соответственно, наоборот. Еще древнегреческие философы справедливо полагали, что зло есть отсутствие мудрости и только мудрость открывает путь к благу. Но это уже иной аспект данной проблемы. Однако хотелось бы акцентировать внимание, что именно тренинги личностного роста для персонала (а возможно и для руководства), и тренинги, направленные на повышение уровня профессиональной компетенции и персонала и, особенно, руководителей, возможно, будут являться самым надежным способом повышения информационной безопасности.

РЕЖИМ КОНФИДЕНЦИАЛЬНОСТИ КАК МЕТОД ПРАВОВОГО РЕГУЛИРОВАНИЯ

Юлия Воробьева, Арина Куклина
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Удмуртский государственный университет»

According to the Law of Russian Federation, there are several types of confidential information (or secrets). For each type of secret a special mode is provided by Federal Law, but there are no particular rules or conditions to follow. We propose to introduce the notion "privacy information mode", which is unified for all types of secrets, and imposed conditions to execute into the Law.

XXI век – это век информационно-телекоммуникационных технологий, влияющих на формирование нового общества, которое основывается на свободном обмене информацией и знаниями.

В результате взаимодействия органов государственной власти, хозяйствующих субъектов, граждан формируется информационное поле являющиеся одним из элементов информационной инфраструктуры.

Цель работы – определить необходимый набор мер по обеспечению конфиденциальности информации, являющейся предметом обмена сторон. В результате анализа действующего законодательства вскрыты противоречия понятийного аппарата в области защиты информации. Одним из вариантов устранения противоречий предложено закрепление понятия «режим конфиденциальности» в нормативных актах РФ.

При правовом регулировании использования информации ограниченного доступа важную роль играет проблема установления определенных правил доступа к информации, которая функционирует в различных видах тайн. Основным требованием, согласно п.2 ст.9 ФЗ «Об информации, информационных технологиях и о защите информации», является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами. Федеральные законы устанавливают условия отнесения информации к категории конфиденциальной, а также обязательность соблюдения конфиденциальности, но в то же время не устанавливают правила и требования для ее обеспечения. Рассмотрим несколько примеров: в ст. 9 части 2 ФЗ от 30.12.2008 №307-ФЗ «Об аудиторской деятельности», указано, что «аудиторская организация и ее работники … обязаны соблюдать требование об обеспечении конфиденциальности информации, составляющей аудиторскую тайну». В п. 15.2 Положения об обслуживании государственных сберегательных облигаций (утв. приказом Минфина РФ от 10 января 2006 г. N 1н) указано, что «конфиденциальная информация не подлежит разглашению лицами, получившими ее при выполнении функций …». Ст. 9 части 1 ФЗ от 29.11.2007 №282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации» относит к категории информации ограниченного доступа первичные статистические данные, содержащиеся в формах федерального статистического наблюдения. Субъекты официального статистического учета обязаны обеспечить конфиденциальность информации ограниченного доступа.

Конфиденциальная информация зачастую становится не только объектом информационного обмена бизнеса и органов государственной власти, но и внутри одной организации могут функционировать сведения, составляющие коммерческую тайну, персональные данные, разновидности профессиональной тайны, в отношении которых обладатель должен обеспечить конфиденциальность.

Проблема обеспечения и соблюдения конфиденциальности информации учеными рассматривается по-разному. Одним из наиболее распространенных в науке информационного права является представление о том, что при получении конфиденциальной информации соответствующий режим тайны трансформируется из одного режима в другой.

Анализ законодательства РФ в сфере информационной безопасности показал, что для обеспечения конфиденциальности одной и той же информации приходится устанавливать различные режимы, которые могут привести к возникновению конфликтов интересов субъектов тайн. Для исключения конфликтов при осуществлении информационного обмена целесообразно закрепить в нормативных актах понятие «режима конфиденциальности информации», который позволит установить минимальный набор необходимых мер и требований по обеспечению конфиденциальности информации и учесть интересы сторон, участвующих в информационном обмене. Режим конфиденциальности информации является пред-

метом правового регулирования, которое представляет собой особый порядок, установленный государством в виде правовых норм и обеспеченный силой государственного принуждения посредством применения любых действий с информацией конфиденциального характера, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), блокирование, уничтожение.

В современных источниках фигурирует следующее определение понятия «режим». В Толковом словаре Ушакова «режим - это система правил, выполнение которых необходимо для той или иной цели». В Большом Энциклопедическом словаре, Большой советской энциклопедии и Современной энциклопедии понятие «режим» (французское regime, от латинского regimen - управление) определяется как совокупность правил, мероприятий, норм для достижения какой-либо цели. В толковом словаре русского языка Кузнецова «режим - это точно установленный порядок жизни, дел, действий». Понятие «конфиденциальность информации» закреплено в ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» и обозначает обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. Национальный стандарт РФ «Информационная технология. Практические правила управления информационной безопасностью» (ГОСТ Р ИСО/МЭК 17799-2005) определяет конфиденциальность как доступ к информации только авторизованных пользователей. Таким образом, режим конфиденциальности можно сформулировать как совокупность правил, мероприятий, норм по обеспечению выполнения требований защиты конфиденциальной информации от утечки, а также от передачи лицом, получившим доступ к такой информации, третьим лицам, без согласия ее обладателя.

Данный режим позволит:

- Установить порядок отнесения сведений к категории конфиденциальной (формирование Перечня конфиденциальной информации с учетом всех видов информации ограниченного доступа, представленных в рамках организации/предприятия)
- Разработать и внедрить документацию, определяющую порядок обработки и обеспечения конфиденциальности информации
- Сформировать разрешительную систему допуска, доступа и учет лиц, принимающих участие в процессе работы с конфиденциальной информации
- Определить обязанности лиц, допущенных к конфиденциальной информации
- Организовать конфиденциальное делопроизводство
- Контролировать исполнение режима конфиденциальности
- Установить ответственность лиц за нарушение режима конфиденциальности

- Защитить конфиденциальную информацию от неавторизованного раскрытия или модификации, а также защитить подключенные системы от неавторизованного доступа
- Определить специальные процедуры в отношении всех возможных типов инцидентов нарушения конфиденциальности
- Обеспечить физическую безопасность зданий, помещений, оборудования, людей, сетей передачи данных.

PROCEDURE FOR USER AUTHENTICATION IN THE UNIVERSITY SYSTEM FOR MANAGING SCIENTIFIC RESEARCH

PhD student Plamen Milev
University of National and World Economy – Sofia,
Department of Information Technologies and Communications

The paper examines conceptual features of the university system for managing scientific research. Emphasis is placed on the user authentication and user rights in terms of the proper functioning of the system. This paper presents such an adaptable model and highlights its potential benefits.

1. Introduction

The university system for managing scientific research automates the actions of application, evaluation, negotiation and reporting of research projects. In this sense its operation goes through several stages, illustrated in Figure 1.

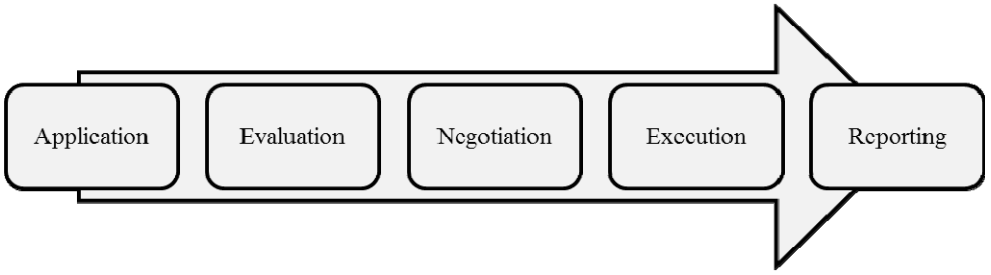


Figure 1. **Stages of operation of the university system for managing scientific research**

We are able to specify some of the security requirements of the university system for managing scientific research:

- Providing such an approach of integrating the system with other systems that do not threaten the security and integrity of data in it.

- Securing against network attacks and compromised data.
- Ensuring data integrity in multiuser mode.
- Restrict access to the functional level according to the role of the user and his access rights.
- Registration of official information for all actions of users concerning the registration, alteration and deletion of data.
- Preservation of history of changes in the data.
- Planned recovery of unforeseen circumstances, providing procedures for periodic data backup in the system and disaster recovery.

2. User roles

There are four different types of users in the university system for managing scientific research:

- Administrators – these are users, who should be able to modify all major nomenclatures and should be able to configure the system to work according to the budget allocation. These users are responsible for implementation of all documents related to the project during its life cycle. It is possible for the administrators to obtain information, monitor and inform other users about expiring terms on certain tasks where they are overdue. Administrators have rights for preparation of reports and statements.
- Project owners – users of this role have the rights to submit project proposals and for each stage of the project to introduce and edit data in the project. All the adjustments and corrections are only possible within the university regulations.
- Reviewers – these users have access to certain projects and possess the possibility to give reviews, including text reasoning, numerical estimates and conclusions on the projects.
- Members of the research board – users of this role have access to all the records in project proposals and also to the reviews of the projects. Their rights include rating and ranking of the projects, negotiation and acceptance of reports.

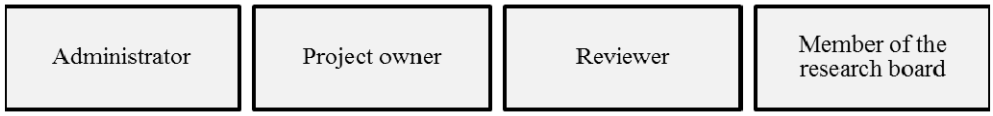


Figure 2. **User roles in the university system for managing scientific research**

3. Database schema

The data structure of the procedure for user authentication in the university system for managing scientific research is located in a database within a few tables (figure 3).

Standard user data, such as the account username, password and other connected to the user attributes, is stored within the user "data" table. When it comes to the user rights within the university system, we use another "roles" table, where all the permissions possible are described and stored in a key-value way. Given permission has its own key

and area of values, where each value uniquely identifies particular right. Structured in this way, the data organization allows restriction of the access to the functional level according to the role of the user and his access rights.

Figure 3. **Database schema for user rights within the university system**

4. Conclusion

In conclusion, the paper emphasizes the importance to address the level of security in information systems. In this sense the university system for managing scientific research contains procedures of access to the information within the system. Some of these procedures are based on user rights conception. These rights are assigned to the participants in the projects according to their roles and actions in the university system for managing scientific research. For this purpose the data is organized in an appropriate manner, so that the desired application security policies may be applied.

A SECURITY CONCEPT FOR OLAP'S N-DIMENSIONAL CUBE, DATA WAREHOUSE CONTROL AND SECURITY

PhD student Mihail Konchev
UNWE, Department "Information technologies and communications"

Much work in data warehousing has been performed on view materialization and data integration. In this paper we focus on access and security management in OLAP's N-dimensional cube and date warehouse control and security.

Keywords: OLAP, N-dimensional cube, data warehouse, database security

1. Introduction

The relevance of data warehouses and online analytical processing (OLAP) for an organization's decision support system has rapidly grown over the past ten years. At the same time a quite good sensitivity for information security and privacy has evolved. In this paper we present our security model for a data warehouse (DW) environment and On Line Analytical Process (OLAP).

2. DW and OLAP security models

Bill Inmon defined a data warehouse as a collection of subject-oriented, integrated, non-volatile, and time-variant data to support management's decisions [1]. The structure of a DW is usually represented using a star or a snowflake schema, based on a multidimensional view of data, consisting of fact tables, dimension tables, and hierarchies [2]. A fact table represents the subject orientation and the focus of analysis. It typically contains measures that are attributes representing the specific elements of analysis. A dimension contains attributes that allow to explore measures from diferent perspectives. These attributes can either form a hierarchy. DW security is concerned with ensuring the secrecy, integrity and availability of data stored in a DW. Unfortunately, most data warehouses are built with little or no consideration given to security during the development phase. We present a five-phase process concerning achieving proactive security requirements of DW:

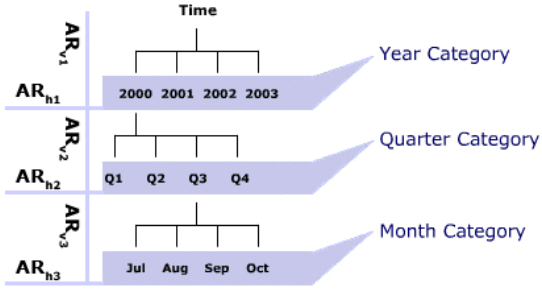
1) identifying and classifying data
2) quantifying the value of data
3) identifying data security vulnerabilities
4) identifying data protection measures
5) evaluating the effectiveness of security measures.

These phases are part of an enterprise-wide vulnerability assessment and management program. OLAP is a category of software technology that enables analysts, managers and executives to gain insight into data through fast, consistent, interactive access to a wide variety of possible views of information that has been transformed from raw data to reflect the real dimensionality of the enterprise as understood by the user [3].

Most business people already think about their business in multidimensional terms. Business data as a matter of fact is multidimensional. It is interrelated and usually hierarchical. The dimension represents descriptive categories of data such as time or location. In other words, dimensions are broad groupings of descriptive data about a major aspect of a business, such as dates, markets, or products. The value of OLAP in reporting data is having levels within the dimensions. Each dimension includes different levels of categories. Dimension levels allow you to view general things about your data and then look at the details of your data.

An important concept to OLAP is drilling. Drilling refers to the ability to drill-up or drill-down. These levels of categories (hierarchies) are what provide the ability to drill-up or drill-down on data in an OLAP cube. When we drill-down on a dimension, we increase the detail level of viewing the data. Dimensions have members or categories. A category is an item that matches a specific description or classification such as years in a time dimension. Categories can be at different levels of information within a dimension. We can group any category into a more general category. Categories have parents and children. A parent category is the next higher level of another category in a drill-up path. The measures are the actual data values that occupy the cells as defined by the dimensions selected. Measures include facts or variables typically stored as numerical fields, which provide the focal point of investigation using OLAP [4].

We propose a security model of OLAP which has only accessibility rules (AR) as the security subjects based on horizontal (AR_h) and vertical fragmentation (AR_v) of the hierarchy (shown in Figure 1).



Accessibility rules (AR)

AR_{h1} – Read, Year, 2000-2002;
AR_{h2} – Read, Quarter, Q_1-Q_4;
AR_{h3} – Read, Month, Jul-Sep;
AR_{v1} – Read, Year;
AR_{v2} – Read, Quarter;
AR_{v1} – Read, Month;

Figure 1

Table 1.

User's accessibility rules table

User	AR_h	AR_v
1	AR_{h1}, AR_{h2}, AR_{h3}	AR_{v1}, AR_{v2}, AR_{v3}
2	AR_{h1}, AR_{h2}	AR_{v1}, AR_{v2}

After security policy rules has been applied and matrix is generated (shown in user's accessibility table) which represents each rules for each user of the OLAP. For example if a user "1" wants to query yearly data (2001). The security system will generate a list of AR's that are needed to satisfy the query and this list will be compared with the list of the AR's which user "1" has access rights. If all rules needed to satisfy the query is in the list of accessibility rules table, the query will be performed. If not, the user is not authorized to retrieve some data from DW and empty result is returned.

3. Conclusion

In this article we proposed a security approach based on adapted mandatory access control for OLAP hierarchy. The advantage of this security model is its flexibility of assigning rules for access. Hence it is quite straight forward to assign a number of rules to one particular person (or group of persons) without losing consistency with respect of the security policy. The five phases of systematic vulnerability assessment and management program described in this paper are helpful in averting underprotection and overprotection (two undesirable security extremes) of the DW data.

References:

[1] W. Inmon. Building the Data Warehouse. John Wiley & Sons, 2002.
[2] R. Kimball, M. Ross, and R. Merz. The Data Warehouse Toolkit: The Complete. Guide to Dimensional Modeling. John Wiley & Sons, 2002.
[3] OLAP and OLAP server definitions. http://altaplana.com/olap/glossary.html
[4] OLAP. http://training.inet.com/OLAP/home.htm

ANOMALY DETECTION 3.0 FOR SNORT®

Maciej Szmit, Sławomir Adamus,
Sebastian Bugała, Anna Szmit,
Computer Engineering Department,
Technical University of Lodz, Poland

Snort® is an open source intrusion detection system based on signature detection. In the paper we present information about the third version of Snort AD – preprocessor designed to log and analyze network traffic information developed by us.

AD preprocessor

Snort is the most popular open source intrusion detection system based on signature detection (see e.g. [2], [14], [18], [19]). The modular construction of Snort allows one to extend its capabilities by creating own pre- or postprocessors and/or plugins. The best-known Snort tools are for instance ACID (see [15]), BASE (see [16]) or SAFE (see [17]).

In our works we develop Snort preprocessor designed to enhance Snort possibilities to monitor, analyze and detect network traffic anomalies using NBAD (Network Behavioral Anomaly Detection) approach (see e.g. [6], [7], [20]). The first version of Anomaly Detection preprocessor (see [21]) for Snort version 2.4x was published in a Master's Thesis [11] in 2006. Next the project has been developed (see e.g. [10], [12], [9], [8]) till the current version 3.0 designed for Snort 2.9.x which periodically, with a given interval, logs information about 29 parameters of the network traffic as a number of TCP/UDP packets sent/received from outside/inside the current IPv4 subnet, www download/upload speed, a number of UDP 53 (DNS) datagrams etc. Values of these parameters are the logs into a file in CSV (Comma Separated Values) format, with header line containing description of each parameter (see Figure 4).

DD-MM-YY, HH:MM:SS, Day of the Week, Time interval [s], TCP summary [number of packet], TCP outgoing [number of packet], TCP incoming [number of packet], TCP from this subnet [number of packet], UDP summary [number of packet], UDP outgoing [number of packet], UDP incoming [number of packet], UDP from this subnet [number of packet], ICMP summary [number of packet], ICMP outgoing [number of packet], ICMP incoming [number of packet], ICMP from this subnet [number of packet], TCP with SYN/ACK [number of packets], WWW outgoing - TCP outgoing to port 80 [number of packet], WWW incoming - TCP incoming from port 80 [number of packet], DNS outgoing - UDP outgoing to port 53 [number of packet], DNS incoming - UDP incoming from port 53 [number of packet], ARP-request [number of packet], ARP-reply [number of packet], Not TCP/IP stacks packet [number of packet], Total [number of packet], TCP upload speed [kBps], TCP download speed [kBps], WWW upload speed [kBps], WWW download speed [kBps], UDP upload speed [kBps], UDP download speed [kBps], DNS upload speed [kBps], DNS download speed [kBps]

```
04-10-11,16:52:16,Tue,30,0,0,0,0,16,0,0,16,60,0,0,60,0,0,0,0,0,29,0,22,127,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00

04-10-11,16:52:46,Tue,30,0,0,0,0,20,0,0,20,60,0,0,60,0,0,0,0,0,40,0,29,149,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00
```

***Figure 4.* AD log file. Source: own research.**

The next function of the preprocessor is generating alerts. Preprocessor reads a predicted pattern of the network traffic (of all parameters) from the 'profile' file and generates alert when the current value exceeds 'minimum' to 'maximum' range for the current moment (the moment is given by day of the week, hour, minute and second corresponding to the intervals from the log file) from the profile file (see Figure 5).

DD-MM-YY, HH:MM:SS, Day of the Week, Time interval [s], TCP summary MAX [number of packet], TCP summary MIN [number of packet], TCP outgoing MAX [number of packet], TCP outgoing MIN [number of packet], TCP incoming MAX [number of packet], TCP incoming MIN [number of packet], TCP from this subnet MAX [number of packet], TCP from this subnet MIN [number of packet], UDP summary MAX [number of packet], UDP summary MIN [number of packet], UDP outgoing MAX [number of packet], UDP outgoing MIN [number of packet], UDP incoming MAX[number of packet], UDP incoming MIN[number of packet], UDP from this subnet MAX [number of packet], UDP from this subnet MIN [number of packet], ICMP summary MAX [number of packet], ICMP summary MIN [number of packet], ICMP outgoing MAX [number of packet], ICMP outgoing MIN [number of packet], ICMP incoming MAX [number of packet], ICMP incoming MIN [number of packet], ICMP from this subnet MAX [number of packet], ICMP from this subnet MIN [number of packet], TCP with SYN/ACK MAX [number of packets], TCP with SYN/ACK MIN [number of packets], WWW outgoing - TCP outgoing to port 80 MAX [number of packet], WWW outgoing - TCP outgoing to port 80 MIN [number of packet], WWW incoming - TCP incoming from port 80 MAX [number of packet],], WWW incoming - TCP incoming from port 80 MIN [number of packet], DNS outgoing - UDP outgoing to port 53 MAX [number of packet], DNS outgoing - UDP outgoing to port 53 MIN [number of packet], DNS incoming - UDP incoming from port 53 MAX [number of packet], DNS incoming - UDP incoming from port 53 MIN [number of packet], ARP-request MAX [number of packet], ARP-request MIN [number of packet], ARP-reply MAX [number of packet], ARP-reply MIN [number of packet], Not TCP/IP stacks packet MAX [number of packet], Not TCP/IP stacks packet MIN [number of packet], Total MAX [number of packet], Total MIN [number of packet], TCP upload speed MAX [kBps], TCP upload speed MIN [kBps], TCP download speed MAX [kBps], TCP download speed MIN [kBps], WWW upload speed MAX [kBps], WWW upload speed MIN [kBps], WWW download speed [kBps] MAX, WWW download speed MIN [kBps], UDP upload speed MAX [kBps], UDP upload speed MIN [kBps], UDP download speed MAX [kBps], UDP download speed MIN [kBps], DNS upload speed MAX [kBps], DNS upload speed MIN [kBps], DNS download speed MAX [kBps], DNS download speed MIN [kBps]

```
04-10-11,16:52:16,Tue,
30,0,10,4,1,0,0,0,0,0,0,1,0,1,0,2,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,10.00,5.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00,0.00
```

***Figure 5.* AD profile file. Source: own research.**

The profile can be generated "manually" or by a Profile Generator using appropriate model based on historic values from the log file. The architecture affords easy implementation of different statistical models of the traffic and usage of different tools (i.e. statistical packets) for building profiles. For easy implementation of adaptive models (which have to generate profile 'incrementally' after getting current values of the traffic parameters), the values from the profile file are loaded by AD to the log file after each saving of the current traffic values.

Profile Generator

In the current version of AD the profile generator was designed based on R environment (see:[13]).

The profile generator produces four files:

- File containing predicted pattern (expected future values of parameters) of the network traffic based on the statistical model for a given future time period.
- Profile file containing minimum and maximum values of the parameters (limitations for alert generation).
- File containing calculated values of the model parameters.
- File containing traffic pattern (theoretical values of the parameters) for the past time (the same time as in the log file). This values are used to evaluate the quality of the model.

(See Figure 6), gray solid arrows means saving to and the black dotted ones – reading from the file.

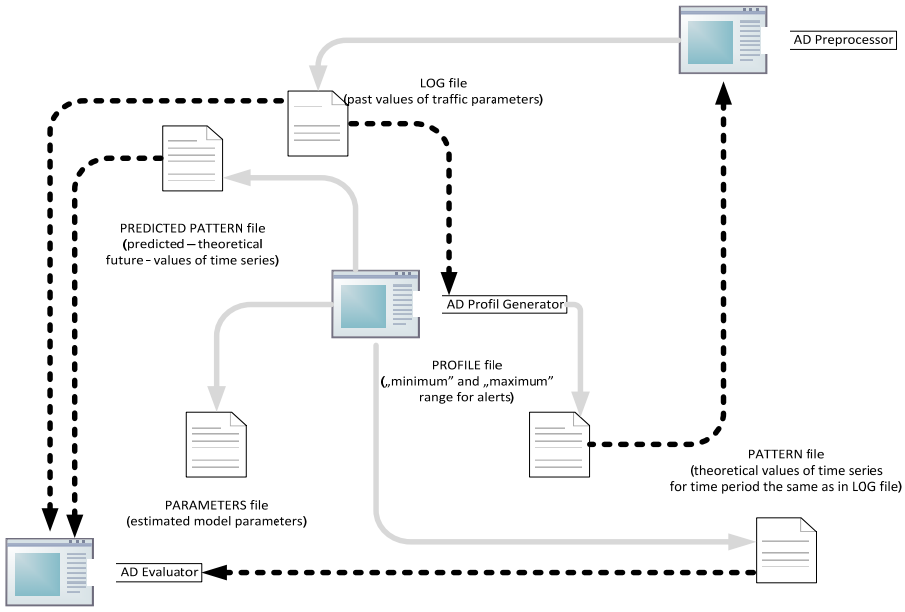


Figure 6. **AD Data flow diagram. Source: own research.Evaluator**

In the current version the Profile generator can build profiles based on four methods: Moving average, Naïve method, Autoregressive time series model and Holt-Winters model (see e.g. [4], [3], [1], [5], [8]).

The third program in the project (named Evaluator) is designed to compare simply statistic $\frac{MAE}{M}$ for two files (e.g. log file and predicted value profile).

MAE means Mean Absolute Error

$$MAE = \frac{1}{n}\sum_{t=1}^{n}|y_t - \hat{y}_t| = \frac{1}{n}\sum_{t=1}^{n}|e_t|$$

where $e_t = y_t - \hat{y}_t$ is a model residual in the moment t and M is arithmetic mean. This way the Evaluator can be used either for checking fit between the model and historical data or between the predicted and real values.

All of the programs can be downloaded for free from the AD project page http://www.anomalydetection.info

References

[1] J. D. Brutlag, 'Aberrant Behavior Detection in Time Series for Network Monitoring' *14th System Administration Conference Proceedings,* New Orleans 2000, Pp. 139-146, available at: http://www.usenix.org/events/lisa00/full_papers/brutlag/brutlag_html/

[2] A. Fadia, M. Zacharia, '*Network Intrusion Alert. An Ethical Hacking Guide to Intrusion Detection'*, Thomson Source Technology, Boston 2008

[3] P. Goodwin, 'The Holt-Winters Approach to Exponential Smoothing: 50 Years Old and Going Strong', *FORESIGHT Fall* 2010 pp. 30-34, available at: http://www.forecasters.org/pdfs/foresight/free/Issue19_goodwin.pdf

[4] R. Lawton, 'On the Stability of the Double Seasonal Holt-Winters Method', unpublished, available at: forecasters.org/submissions09/LawtonRichardISF2009.pdf

[5] E. Miller, 'Holt-Winters Forecasting Applied to Poisson Processes in Real-Time' (draft, version August 2010), unpublished, available at: http://www.scribd.com/doc/35521051/Miller-Automated-Error-Detection-in-Web-Production-Environment

[6] E. A. Patkowski 'Mechanizmy wykrywania anomalii jako element bezpieczeństwa' [*Anomaly Detection Mechanisms as Safety Component], Biuletyn Instytutu Automatyki i Robotyki* No. 26/2009, Wydawnictwo Wojskowej Akademii Technicznej, Warsaw 2009

[7] O. Siriporn, S. Benjawan, 'Anomaly Detection and Characterization to Classify Traffic Anomalies. Case Study: TOT Public Company Limited Network', *World Academy of Science, Engineering and Technology* 48/2008

[8] M. Szmit, A. Szmit, 'Use of Holt-Winters Method in the Analysis of Network Traffic. Case Study', *Springer Communications in Computer and Information Science* vol. 160, pp. 224-231

[9] M. Szmit, Využití nula-jedničkových modelů pro behaviorální analýzu síťového provozu,] Internet, competitiveness and organizational security, TBU Zlín 2011, pp. 266-299

[10] M. Szmit, R. Wężyk, M. Skowroński, A. Szmit, 'Traffic Anomaly Detection with Snort, Information Systems Architecture and Technology ISAT 2007, Information

Systems and Computer Communication Networks', Wydawnictwo Politechniki Wrocławskiej, Wrocław 2007
[11] Skowroński M., Wężyk R.: Systemy detekcji intruzów i aktywnej odpowiedzi, ['*Intruders Detection and Active Response Systems*'] Master's Thesis, Lodz 2005, available at: http://maciej.szmit.info/documents/wezyk_skowronski.zip, Łódź 2006
[12] Tynenski A.: Bezpieczeństwo sieci komputerowych. Autorska dystrybucja systemu Linux, Master's Thesis, Lodz 2008
[13] The R Project for Statistical Computing, http://www.r-project.org
[14] Rehman R. U.: Intruder Detection With Snort, Prentice HallPTR, New Jersey 2003
[15] ACID Analysis Console for Intrusion Databases – program homepage http://www.andrew.cmu.edu/user/rdanyliw/snort/snortacid.html
[16] BASE Basic Analysis and Security Engine program homepage http://base.secureideas.net
[17] SAFE Snort Analysis Front End – Virtual Machine with the software http://www.vmware.com/appliances/directory/835163
[18] Wang Y.: 'Statistical Techniques for Network Security: Modern Statistically-Based Intrusion Detection and Protection', IGI Global 2009
[19] Axelsson S.: 'Research in Intrusion-Detection System: A survey' http://www.cs.unc.edu/~jeffay/courses/nidsS05/surveys/Axelson99-ids-survey.pdf
[20] Telecommunication Standardization Sector of ITU (ITU-T) Recommendation E.507 Telephone Network and ISDN Quality of Service, Network Management and Traffic Engineering. Models for Forecasting International Traffic. ITU-T 1999,1993
[21] Skowroński M., Wężyk R., Szmit M.: Detekcja anomalii ruchu sieciowego w programie Snort, „Hakin9" Nr 3/2007, s. 64-68

КЛАССИФИКАЦИЯ ДАННЫХ КАК АСПЕКТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дмитрий Дорошев, Ольга Корнеенко

In article aspects of the information safety, concerning classifications of data are considered. Also some problems of subjects of the managing, connected with unwillingness to be engaged in this process are presented.

Практика показывает, что, разрабатывая проекты по информационной безопасности, субъекты хозяйствования часто забывают об одном немаловажном аспекте – классификации данных. В корпоративной сети информация хранится не только в папках файловых хранилищ и файлах офисных приложений. Есть еще масса программного обеспечения корпоративного уровня, ERP-, CRM- и HRM-системы, базы данных. Но и данные, хранящиеся в этих системах, могут быть классифи-

цированы. Внутри этих корпоративных систем данные уже классифицированы, упорядочены, а нередко и защищены. Однако на выходе из систем информация становится одновременно деклассифицированной и уязвимой.

Классификация, прежде всего, позволяет выявить ту информацию, которую следует защищать. Это позволяет минимизировать количество конфиденциальной информации. Очевидно, что чем ее меньше, тем легче контролировать ее использование и перемещение. Кроме того, при проведении классификации выявляются документы, потерявшие свою актуальность. Помимо этого классификация позволяет определить все места хранения информации, что может быть использовано для оптимизации бизнес-процессов в организации.

О важности классификации данных в корпоративной среде, в том числе и для целей защиты информации, известно давно. Почему же, признавая ее важность, на практике организации ею не занимаются. Причин тому несколько. Прежде всего, классификация – процесс сложный, требующий немало времени и средств, а в противном случае – не отличающийся эффективностью. Еще одна проблема – поддержание актуальности. Чтобы классификация была эффективной, действительно помогала в деле защиты информации, ее необходимо постоянно поддерживать и актуализировать. А этот процесс может оказаться даже более трудоемким, нежели первоначальная классификация «с нуля». Получается, что нужно разработать специальные механизмы, позволяющие автоматически поддерживать актуальность классификации, либо начинать очередную итерацию классификации сразу по окончании текущей. В противном случае естественный жизненный цикл данных в корпоративной среде очень скоро приведет к размытию правильных категорий. Именно поэтому многие компании даже не берутся за классификацию.

Методы, с помощью которых будет производиться проверка документов на соответствие признакам-классам, являются общими и справедливы для любого процесса классификации.

Классификация вручную – это самый надежный и точный метод. Однако пересмотреть и классифицировать сотни (тысячи, десятки тысяч...) документов, имеющихся в корпоративной среде, очень трудно. Задача титаническая, явно не осуществимая в реальные сроки в большинстве организаций. Такой поход реализуем только в случае, если организация молодая и небольшая, иначе необходима автоматизация, упрощение. Количество документов, которые требуется классифицировать, может быть уменьшено посредством отсеивания ненужных объектов. Но как бы мы процесс ни автоматизировали, сколько бы признаков не использовали, все равно финальный результат будет во многом вероятностным, неточным, требующим подтверждения со стороны человека.

Автоматизированная классификация. Один из простейших способов автоматизации – это учет некоторых формальных признаков документов (название или тип файла, автор изменений и т.д.). Очевидно, что такой метод является крайне неточным, зато он достаточно быстрый и простой для реализации. Содержимое документов, несущее основную смысловую нагрузку, вообще не учитывается.

Чуть более точной может быть классификация, учитывающая места размещения информации. В большинстве организаций имеются определенные правила, регламентирующие места хранения информации. Тем не менее, метод будет хорош, только если сотрудники действительно соблюдают правила размещения информации. Метод также никак не учитывает несоответствие задекларированного содержимого документа его реальному наполнению.

Другие типы автоматизированной классификации (морфологический анализ и анализ по цифровым отпечаткам) также являются вероятностными, однако, в отличие от описанных ранее, предполагают проверку внутреннего содержания. Определенные ограничения налагают и данные методы. Так, морфологический анализ применим только к документам с текстовым содержанием, то есть к обычным «плоским» текстовым файлам либо к файлам, из которых можно изъять текстовую составляющую (например, файлы MS Office, Adobe Acrobat и др.). Посредством лингвистических методов, основанных на поиске заданных слов, словосочетаний и их взаимного расположения в тексте, компьютерная система может определить смысловую нагрузку документа.

Наиболее точным и универсальным из всех методов признают анализ по цифровым отпечаткам. В ходе анализа по цифровым отпечаткам происходит сравнение проверяемых файлов и некоторых эталонных файлов, с которых отпечатки уже были сняты ранее. Универсальность цифровых отпечатков заключается в том, что они могут сниматься с любого типа файлов в бинарном представлении. Таким образом могут быть классифицированы и графические, и аудио-, и другие типы файлов. Из недостатков метода цифровых отпечатков следует назвать солидную предварительную работу, необходимость создания базы данных эталонных отпечатков, чувствительность к изменениям файлов.

Как уже говорилось, сама классификация – это еще полбеды. Помимо этого необходимо решить задачу по поддержанию классификации в актуальном состоянии. Тем не менее, проведя классификацию однажды, организации имеют достаточно возможностей поддерживать ее актуальность на протяжении некоторого времени. При этом могут быть использованы следующие походы:

- создание документов по шаблонам – новые документы создаются администратором, который явно указывает классы информации. Пользователи же занимаются наполнением готовых шаблонов. Таким образом, не появляется новых неклассифицированных документов, однако проблема изменения классов с изменением содержания не решается;
- изменение классов по требованию – в какой-то момент владелец документа понимает, что класс документа не соответствует заявленному, и отправляет администратору заявку на изменение класса в соответствии с новым содержанием;
- изменение классов по расписанию – ценность информации может изменяться с течением времени, и для определенных категорий можно предусмотреть изменение классов по расписанию;

- наследование классов – предусматривает разработку программных механизмов наследования классов при изменении содержимого документов. Если источники, которые используются при составлении нового документа, уже классифицированы, наследование позволит автоматически добавить класс исходной информации к конечному документу.

Чтобы провести классификацию данных на предприятии, вовсе не обязательно применять все описанные методики. Тем не менее, сочетая различные методики, можно добиться приемлемого качества классификации при разумных финансовых и временных затратах. В любом случае выбор всегда остается за человеком. Это относится как к методике, так и к результатам работы средств автоматизации. Классификация – это не просто процесс, связанный с защитой информации, а основа для построения полноценной системы безопасности.

АСПЕКТЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Кавун Сергей Витальевич, Сорбат Иван Викторович
Харьковский национальный экономический университет

This article presents an analysis of information leakage, which is based on data from the world of statistics, shows the dynamics of information leakage for a given period of time, developed by the authors is presented graph model of organizational and functional structure (FSB) of the enterprise. The conclusions and recommendations.

Актуальность. Современное развитие экономики напрямую зависит от внутренних и внешних факторов. Различные организации в ходе своей коммерческой деятельности подвержены экономическим преступлениям, халатности сотрудников, вследствие которых они несут финансовые, материальные, временные, экономические и др. виды потерь. Такая деятельность сотрудников называется инсайдерской.

Поскольку инсайдерская деятельность приносит финансовые потери, следовательно, возникает необходимость решения актуальной задачи предотвращения или выявления инсайдера или группы инсайдеров (инсайдерской деятельности).

Цель. Целью статьи является аналитический обзор инсайдерских действий как угроз экономической безопасности предприятия для разработки рекомендаций по борьбе с инсайдерами.

Результаты. Авторами статьи проведено исследование по фактам утечки информации, основанное на данных мировой статистики, которые были опубликованы в средствах массовой информации, веб-форумах, отчетов аналитических

компаний, тематических блогах и других открытых ресурсах. В табл. 1 приведены статистические данные фактов умышленных и случайных утечек информации за определенный период времени во всем мире.

Таблица 1

Данные по видам утечек информации за определенный период времени

№	Вид утечек	2010		2009		2008		2007	
		Кол-во	%	Кол-во	%	Кол-во	%	Кол-во	%
1	Умышленные	402	48,0	375	51,0	241	45,5	154	29
2	Случайные	390	46,4	320	43,5	223	42,1	376	71
3	Не установлено	47	5,6	40	5,4	66	12,5	-	-

На рис. 1 представлена динамика утечек информации за заданный период времени, построенная на основе рассчитанных данных (табл. 1). Также были рассчитаны трендовые зависимости на основе полиномиальных зависимостей и их значения достоверности (R^2), по которым возможно получение дальнейших прогнозов.

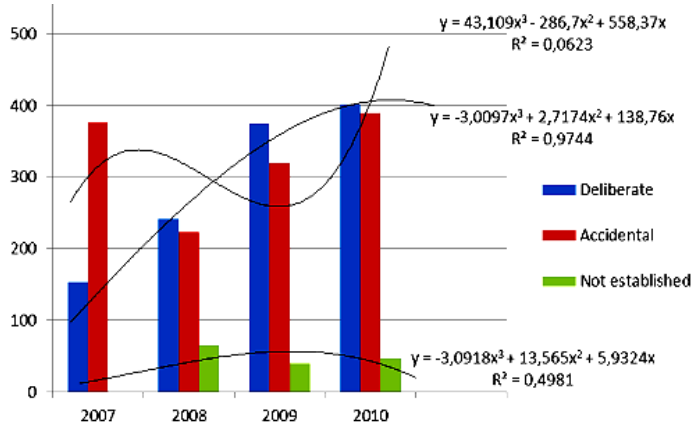


Рис. 1. **Динамика утечек информации за заданный период времени**

Снижение количества случайных утечек информации за 2010 год по сравнению с предыдущим обусловлено тем, что с каждым годом в организациях внедряются различные методы и аппаратно-программные комплексы для выявления утечек информации. В большей части эти методы и средства позволяют выявить уже совершенные действия инсайдеров, но не спрогнозировать и предотвратить их.

Для дальнейшего исследования предлагается рассмотреть метод, модель которого интерпретирована на основе использования теории графов [8].

На рис. 2. представлена разработанная авторами графовая модель организационно-функциональной структуры (ОФС) предприятия.

Выводы. Таким образом, показана возможность приведения задачи выявления инсайдеров на предприятии к задаче использования известных математических методов решения на примере теории графов.

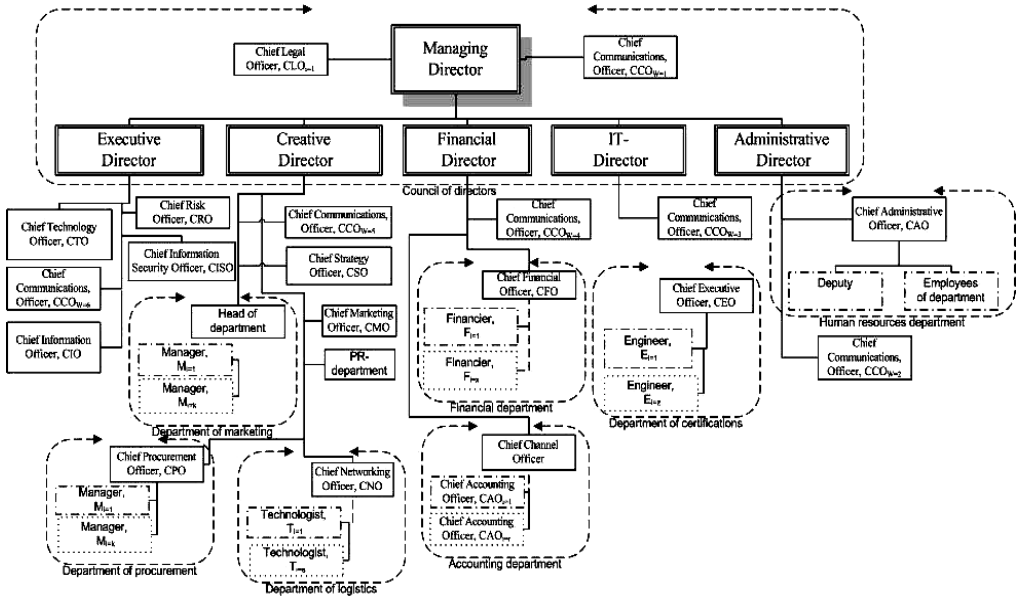


***Рис. 2.* Графовая модель ОФС предприятия**

Литература:

1. Верин В.П. Преступления в сфере экономики. - М.: Дело, 2002. – 215с.
2. Кавун С. В. Жизненный цикл системы экономической безопасности предприятия // Управління розвитком. – 2008. – № 6. – С.17-21.
3. Кавун С.В., Сорбат И.В. Инсайдер – угроза экономической безопасности // Управління розвитком. – 2008. – № 6. – С.7-11.
4. Кавун С.В. Математическая интерпретация задачи выявления инсайдеров в организации (предприятии)// Кавун С.В., Сорбат И.В. – Научный журнал "Экономика: проблемы теории и практики". Днепропетровск: Изд. Руснаука, 2009. – т. 246. – № 4. – С. 862-869.
5. Олейников Е. А. Экономическая и национальная безопасность: Учебникдля вузов. – М.: Экзамен, 2005. – 768 с.
6. Геєць В. М. Моделювання економічної безпеки: держава, регіон, підприємство: Монографія / В. М. Геєць, М. О. Кизим, Т. С. Клебанова, О. І. Черняк.– Х.: ХНЕУ, 2006. – 240 с.
7. ES INFECO International Research Portal information and economic security // http://infeco.net

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЕЕ ЗНАЧЕНИЕ В УПРАВЛЕНИИ БИЗНЕСОМ

Сайдикрамова Анна, Швеция, Eductus

Как всем известно, в последние годы ИТ-рынок динамично развивается, что позволяет нам назвать современное общество - инфомационным. На сегодняшний день руководство любой компании имеет дело с информацией, на основе которой принимаются различные бизнес-решения.

Ущерб от реализации угроз информационной безопасности в соответствии с BSI-standard 100-1 «Система управления информационной безопасности» может включать следующее:

- нарушение законов, нормативных актов и соглашений;
- нарушение конфиденциальности;
- негативное влияние на выполнение задач;
- неблагоприятные внутренние или внешние последствия;
- экономические потери.

В настоящее время для минимизации различных видов ущерба активно развивающимися направлениями являются:

- системы ограничения и контроля доступа;
- системы защиты от вредоносного программного обеспечения;
- системы аудита и мониторинга;
- системы криптозащиты.

Так, например, по данным Cryptzone (Sweden), разработчика инновационных технологий активного управления для минимизации рисков ИБ, были определены 8 ключевых областей информационной безопасности на 2012 год:

- целевые атаки – атаки, направленные на кражу информации, такой как коммерческая тайна. Так, в 2011 году были осуществлены целевые атаки хакеров на Sony, которые в результате потеряли данные до 77 миллионов пользователей. В данном случае распространенной угрозой является получение работниками зараженных писем с вредоносным кодом. Следовательно, компании должны начать думать о защите своей информации от подобных атак;
- политика для мобильных устройств – пользователи все больше хотят работать со своим собственным устройством, например, iPhone и Ipad, это повышает производительность и эффективность, но при этом накладывает ряд новых требований информационной безопасности. Компании должны предпринимать действия блокировки или уничтожения устройств, например, при краже мобильных устройств;

- безопасность производственных систем – раннее производственные системы рассматривались как область с низким риском угроз безопасности. Все больше таких систем основано на управлении операционными системами Windows, что оставляет уязвимости для атак;
- интранет iPhone – многие организации предлагают пользователям возможность интегрировать свои интрасети и другие системы, такие как Microsoft SharePoint, на частные или корпоративные IPad. Это обеспечивает большую эффективность и быстрое время отклика, не привязывая пользователей к определенному месту. Компании, в свою очередь, должны определить требования к интеграции в безопасных условиях;
- отчетность инцидентов – обеспечение защиты на 100% от всех угроз является невозможным, поэтому компании должны определять политики и процедуры для критичных инцидентов с целью уменьшения потерь;
- права доступа – их разграничение становится все более серьезной проблемой для организаций, что требует усиленного обзора и контроля прав доступа пользователей;
- безопасность данных – осуществление резервного копирования данных позволяет компаниям обратить свое внимание не на защиту аппаратных средств, а на защиту от несанкционированного доступа;
- быстрая адаптация продуктов – все чаще корпоративные клиенты обращаются к поставщикам с целью быстро адаптировать свои системы к работе, что может привести к несоблюдению требований информационной безопасности.

Управление информацией и ИТ-системами является одним из важных направлений стратегии информационного общества. По данным опроса 2011 TMT Global Security Study – Key Findings основными мерами, используемыми организациями для обеспечения информационной безопасности, являются:

- соотвествие законодательным и нормативным требованиям информационной безопасности – 30%;
- защита данных – 28%;
- подготовка персонала по вопросам информационной безопасности – 27%;
- безопасность, связанная с технологиями – 27%;
- управление идентификацией и доступом -25%.

Конфиденциальность данных, физическая безопасность, управление непрерывностью бизнеса, управление рисками были отмечены как область ответственности информационной безопасности. Исходя из этого, для обеспечения устойчивого и эффективного функционирования и высокого уровня конкурентоспособности следует применять следующие методы реализации комплексной системы управления рисками информационной безопасности:

- эффективное управление ИТ-инфраструктурой;

- управление процессами информационной безопасности;
- управление зависимостью от услуг и продуктов третьих сторон;
- управление доступом и обеспечение отчетности;
- обеспечение основных аспектов безопасности данных;
- комплексное управление инцидентами.

Функции защиты информации в любой организации определяются комплексом стоящих перед ней бизнес-задач.

В заключение можно отметить, что создание системы управления информационной безопасности не должно являться самоцелью. Информационные и коммуникационные технологии должны применяться в качестве поддержки для достижения целей организации и обеспечивать поддержку бизнес-процессов.

Литература:

1. BSI-standard 100-1 «Система управления информационной безопасности»;
2. www.cryptzone.com;
3. www.deloitte.com.

ВЗАИМОДЕЙСТВИЕ НАТО И СТРАН ПОСТСОВЕТСКОГО ПРОСТРАНСТВА В ФОРМИРОВАНИИ СРЕДЫ ЕВРОПЕЙСКОЙ БЕЗОПАСНОСТИ (ИНФОРМАЦИОННЫЕ АСПЕКТЫ)

Денис САЛТЫКОВ,
Молдавская Экономическая Академия

This article presents a security-based view on the relationship between NATO and post-soviet countries in the region of Europe. The article also points out the very special role of mass media in this relationship.

СМИ как информационная среда

После распада Советского Союза вопрос о перспективах взаимодействия стран постсоветского пространства и стран-участниц НАТО встал очень остро. Немаловажную роль в этом вопросе сыграли оставшиеся ещё со времён холодной войны стереотипы, на которых активно играли СМИ и политики, как в бывших советских республиках, так и в странах НАТО. Восприятие обеими сторон друг друга в качестве врага негативно сказывается на попытках формирования среды европейской безопасности, которые особенно интенсифицировались, начиная с начала XXI в.

В эру информации или так называемую постиндустриальную эру геополитические проблемы, становясь предметом публичного обсуждения, проникают в

головы значительной массы населения в заведомо искажённом виде. Важнейшую роль в этом процессе играют СМИ.

Для понимания того, каким именно образом формируется мнение человека на основе информационной среды, в которой он находится, следует более тщательно разобраться в «духе времени». Итак, информация в настоящее время признана главной ценностью. Доступ к большей части информации лёгок. Объём накопленных человечеством знаний никак не сравним с тем объёмом, который может вместить голова. При всей необходимости формирования новых знаний, человек не может знать абсолютно всё даже в собственной профессиональной сфере. Так можно начинать считать дилетантизм в определённом смысле не только возможным, но и необходимым свойством человека в условиях современности. Чтобы принимать решения, каждый вынужден доверять той информации, которую уже сформировали другие. Критическая оценка в таких случаях, хоть и присутствует в разной степени, всё же не может быть реализована до конца.

В современном информационном пространстве СМИ представлены чрезвычайно широко. Номинально СМИ считается таковым, если обладает лицензией, официально зарегистрировано и т. п. Но тем не менее, СМИ по духу является вся сеть Интернет, включая социальные сети и блогосферу. В этом пространстве формируются мемы и медиа-вирусы. Мем отличается тем, что он не требует в сознании человека никаких доказательств. Медиа-вирус же всё ж позволяет додумать информацию самому, но именно в таком ключе, в каком нужно создателям.

Именно в таких условиях приходится существовать попыткам НАТО и стран постсоветского пространства преодолеть наследие холодной войны и совместно участвовать в формировании среды европейской безопасности. Мнением граждан манипулировать в этом случае очень удобно. В частности, вопросы взаимодействия становятся лакомым кусочком в случае необходимости отвлечь население от внутренних проблем конкретного региона на образ внешнего врага.

Проблема европейской безопасности

Одновременно с этим важность преодоления взаимной неприязни чрезвычайно высока. Остановимся на одной из главных проблем, на которые обращает своё пристальное внимание НАТО.

Проблема европейской безопасности — не просто актуальная политическая проблема, это глубоко гуманистическая идея безопасности человека как таковой. Идеи гуманизма всегда со времён своего проявления в эпоху Ренессанса олицетворяли собой общественный прогресс.

В современном мире существует масса проблем, решение которых вовсе не является очевидным. Например, в России и странах СНГ актуальной является проблема кризиса культуры: советский тип культуры погиб, но новый ещё не родился. Этот период застоя некоторые культурологи, занимающиеся попытками решения проблемы с помощью подхода синергетики, называют хиатусом — культурной пустотой, которая затягивается на неопределённые сроки. В ЕС, к

примеру, до сих пор не решена проблема подхода мультикультурализма, который считался доминантным в области межкультурных коммуникаций. Уже было озвучено, например, Ангелой Меркель, Дэвидом Кэмероном и Николя Саркози, что политика мультикультурализма провалилась. Но, тем не менее, новый подход к решению проблем вне мультикультурализма пока что найти весьма сложно. В России те же проблемы имеют внутренний характер, выливающийся, к примеру, в напряжённых отношениях между кавказским и русским населением страны. С такой точки зрения проблема европейской безопасности значительно обостряется.

Также не следует забывать и об общих проблемах толерантности. В Европе и США, как принято считать, в этом направлении достигнуты большие успехи, тогда как постсоветское пространство слегка отстаёт. Но в данной ситуации речь идёт не просто о внешних мерах, принимаемых той или иной страной, но о ментальности населения, так что вопрос намного глубже, нежели можно подумать.

Противостояние постсоветских стран и НАТО: диалектика взаимодействия

В свете упомянутых проблем скорее можно сделать вывод о необходимости более тесного сотрудничества структур НАТО и стран постсоветского пространства. В то же время формирование среды безопасности в Европе не может успешно осуществляться без участия стран бывшего СССР.

С другой стороны каждая страна обладает собственными интересами, которыми невозможно пренебречь. Необходима защита и соблюдение интересов, как стран постсоветского пространства, так и стран-участниц НАТО самих по себе. Утверждать, что противостояние НАТО и стран бывшего СССР полностью осталось в прошлом — наивно. Проблемы остались, и противостояние сохранилось на системном уровне.

Если представить данную проблему в форме знаменитой гегелевской триады, то потребность в формировании среды европейской безопасности и потребность в соблюдении частных интересов отдельных стран можно представить как тезис и антитезис. Решением по закону диалектики должен стать синтез, который сможет слить тезис и антитезис в одно целое, чтоб каждый из них стал частным случаем нового решения.

Какое содействие могут оказать в таких условиях специалисты в области информационной безопасности? В рамках данной работы ответ дать невозможно, да и ставить подобную цель представляется бессмысленным. Тем не менее, чрезвычайно важно обозначить проблему, что и является задачей работы.

Поиск подобного направления деятельности нелёгок, но именно это в данном случае может быть названо сверхзадачей для специалистов в области информационной безопасности. Очевидно, основным объектом анализа должны стать СМИ, формирующие мнения в обществе. Тонкая и грамотная работа с источниками массовой информации несомненно призвана помочь в улучшении взаимодействия постсоветских стран и НАТО по вопросам формирования единой среды безопасности с учётом частных интересов отдельных стран.

Литература

1. Кожокин Е.М. 2011. В поисках абсолютной безопасности // Россия в глобальной политике, 15.12.2011. URL: http://globalaffairs.ru/number/V-poiskakh-absolyutnoi-bezopasnosti-15405 (дата обращения 27.03.2012).
2. Мосионжник Л.А. 2006. Человек перед лицом культуры. Ch.: Высшая Антропологическая Школа.

THE METHOD OF "INTERNET-ANALYSIS" IN GRAPH THEORY

Sorbat Ivan, Sorbat Irina
Kharkiv National Economic University (KhNEU)

The authors developed a method Intenet-analysis, this analysis can be used as a methodological basis for the preliminary study of the interests of young scientists and graduate students. This allows for some degree of objective assessment of the relevance of ongoing or planned research in virtually every sphere of interest.

Developed by authors method of Internet-analysis can be applied in any given area of activity, regardless of its properties and features. The purpose of using it is to get some assessment or collection of selected concepts (terms), which form the so-called categorical apparatus of scientific research.

Thus, the scope of the method developed Internet-analysis is multifaceted in its specificity and tolerance.

The input data for the method of Internet-analysis are:

1. Set V = $\{v_i\}$, i = 1 ÷ 6, scholars in the field of information and economic security, with their last name, first name and patronymic: Kurkin N.V., Senchagov V.K., Klebanova T.S., Geyets V.M., Oleynikov E.A., Shkarlet S.N.
2. Set T = $\{t_j\}$, j = 1 ÷ 6, categories (terms) of a set of categorical system areas: information security (IS), the economic security of the enterprise (ESE), an insider (I), the concept of ESEs (CESE), financial security (FS), the system ESEs (SESE) [1-6]. Categorical apparatus may include (and often and is) a fairly large number of terms, so as the base (to reduce the size of the sample) were selected six concepts, which represent the authors' opinion, some basis for economic security [7-10].
3. Research period: 2001-2011 – set G = $\{g_k\}$, k = 1÷10.
4. Multiple search engines, according to set of results with which the average data: Google.com, Yandex.ru, Yahoo.com, I.UA, Mail.ru, Alltheweb.com, Rambler.ru, Bing.com, Meta.ua, Nigma.ru, Metabot.ru, AltaVista.com, Wikipedia.org,

UaPORT.net, Uaportal.com, Holms.ru, Poshuk.com, Weblist.ru, List.mail.ru, Lycos.com, UP.com, Magellan.ru, Galaxy.ru, Webcrawler.com, Dmoz.org, Jayde.com, Asiannet.com, REX.ua, Euroseek.com, Search.MSN.com, Whatuseek.com, Planetsearch.com.

Then V U T = VT ≡ $\{v_i\}$ U $\{t_j\}$ = $\{vt_{ij}\}$, VT = $\{vt_{ij}\}$ – set (or matrix) averaged estimates with respect to the scientists show: a zone of activity in the chosen course of action, the relevance of their research, quantitative saturation of their publications, the relevance of their research, ranking in the world scientific community. The results are shown in table 1.

Table 1

Set VT

T = {t_j} V = {v_i}	**IS**	**ESE**	**I**	**CESE**	**FS**	**SESE**
N.V. Kurkin	659	8	1	0	8	0
V.K. Senchagov	44	21	0	0	94	2
T.S. Klebanova	109	360	0	0	116	1
V.M. Geyets	165	32	0	45	58	126
E.A. Oleynikov	1	9	0	1	13	1
S.N. Shkarlet	2	11	0	1	4	1

For further analysis, according to the set VT is possible to construct graphical dependence, which can be used to analyze the dynamics of change $\{vt_{ij}\}$ (Fig. 1-4).

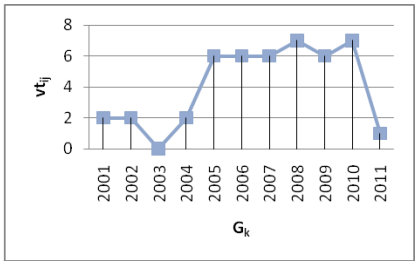


Fig. 1. $v_{i=6}$ = «S.N. Shkarlet», $t_{j=1}$ = «IS»

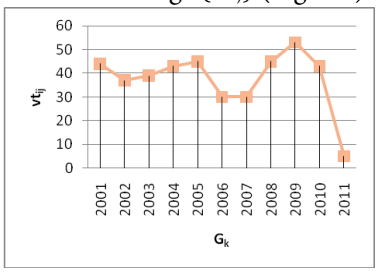


Fig. 3. $v_{i=2}$ = «V.K. Senchagov», $t_{j=1}$ = «IS»

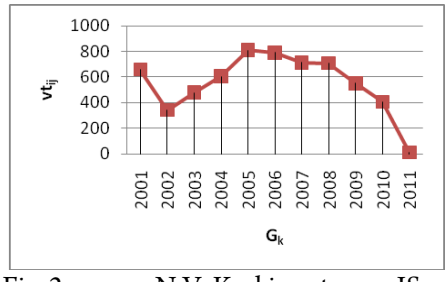


Fig. 2. $v_{i=1}$ = «N.V. Kurkin», $t_{j=1}$ = «IS»

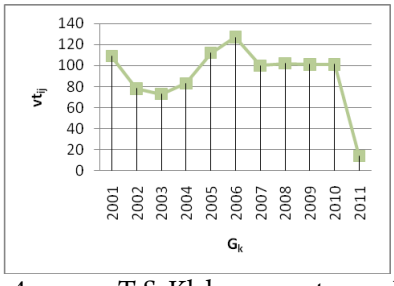


Fig. 4. $v_{i=3}$ = «T.S. Klebanova», $t_{j=1}$ = «IS»

Querying search engines in terms of graph theory would be:

{v_i} U {g_k} ≡ «Курк*н_*.В. + 2010» V «Курк*н» + «2010»,

Where V – the symbol of operations OR; * – the symbol for the search engine, which means any possible character – this is caused by specific features of spoken language and the translations of attributes of scientists (for example, Куркин (in Russian), Куркін (in Ukrainian)); _ – space character.

If we interpret the implementation of the method of online analysis, graph theory, we can construct the corresponding graph and perform the implementation in a mathematical form.

Fig. 4 is a ternary graph of the dependence of scientists attribute (set V) in a given field of study (set T) for a certain time period (set G)

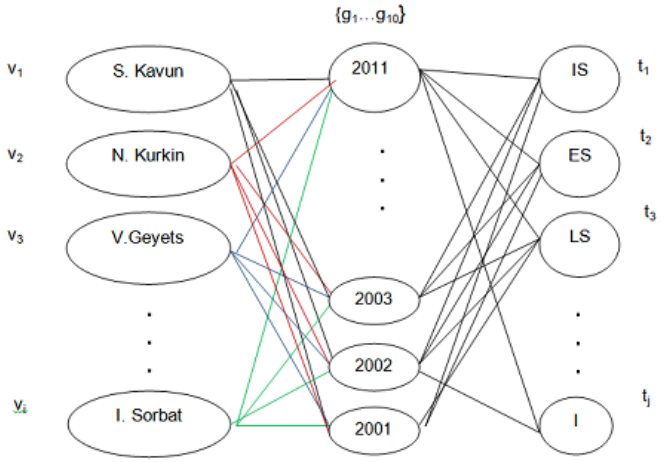


Fig. 4. Ternary dependency graph

Also, this analysis can be used as a methodological basis for a preliminary study of the interests of young scientists and graduate students. This will get to a certain extent an objective assessment of the relevance of ongoing or planned research in virtually every area of interest.

Literature:

1. ES INFECO. International Research Portal information and economic security http://infeco.net
2. Kavun S (2009) Analysis of categorical apparatus in the field of economic and information security / Kavun S, Mikhalchuk I / Economic of development: Science magazine. – Kharkiv: Pub. INZHEK – № 3 (51) 9 - 14.
3. Kavun S (2009) Insiding – the problem of economic security in conditions of reforming the Ukrainian economy / Kavun S, Sorbat I / Actual questions with problems of economics: Science magazine.– Kiev: National academy of management, – № 4 (94). – 91- 97.

ОСОБЕННОСТИ ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ СОЦИАЛЬНЫХ ПРИЛОЖЕНИЙ

***Сторож Оксана**, ASEM*

This article is about features of social software and social network testing. Here are discussed some problems of testing this king of software and proposed some types of tests which are the most applicable.

Введение

Обеспечение информационной безопасности является одним из основных аспектов ведения бизнеса. По мере развития любой организации, меняется и ее информационная система. Таким образом, вопрос обеспечения безопасности информации будет постоянно возникать, а вместе с ним всегда будет необходимость в тестировании безопасности информационной системы.

Тестирование безопасности - это стратегия тестирования, используемая для проверки безопасности системы, а также для анализа рисков, связанных с обеспечением целостного подхода к защите приложения, атак хакеров, вирусов, несанкционированного доступа к конфиденциальным данным.

В зависимости от требований заказчика тестирование безопасности может быть проведено для любой информационной системы, однако существуют такие системы, для которых этот вид тестирования не может быть проигнорирован:

- Вэб приложения
- Приложения с важной коммерческой или персональной информацией
- Платежные системы
- Приложения требующие целостности информации (БД)
- Социальные приложения
- Приложения с коммерческим лицензированием

В данной статье будут рассмотрены особенности тестирования безопасности социальных приложений

Тестирования безопасности социальных приложений

Большую популярность в последние годы приобрели социальные сети. Социальные сети и социальные приложения пользуются огромной популярностью у рекламодателей, поскольку это уникальная возможность непосредственно контактировать с потребителями. Объём рынка рекламы в социальных сетях неуклонно растет. В 2007 году, по оценкам аналитической компании eMarketer, он достиг отметки в 1,225 млрд долларов. По прогнозам, к 2013 году объём рынка рекламы в социальных сетях достигнет 10 млрд долларов. На рисунке 1 изображена диаграмма роста объема рынка рекламы (источник http://orz.com.ua/).

Исходя из вышесказанного, становится очевидным факт важности круглосуточного доступа к социальным приложениям и малейшие сбои в системе

приводят к огромным убыткам. Поэтому разработчики социальных приложений уделяют огромное внимание безопасности и соответственно тестированию безопасности этих систем.

Сбои с таких приложениях обычно возникают в результате нагрузки, поэтому особенно важно проводить нагрузочное тестирование:

- Тестирование производительности (Load Testing)
- Стрессовое тестирование (Stress Testing)
- Тестирование резких скачков (Spike Testing)
- Тестирование стабильности (Endurance or Soak Testing)
- Конфигурационное тестирование (Configuration Testing)

В рамках нагрузочных тестов, как правило проводят эмуляцию DoS и DDoS атак.

Моделирование атак ставит своей целью проверку устойчивости системы к преднамеренным дестабилизирующим воздействиям.

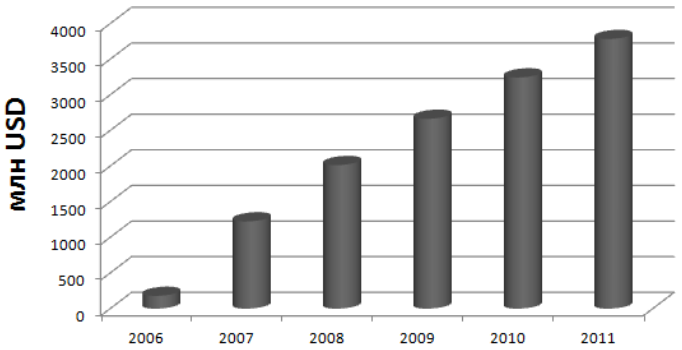


Рисунок 1. **«Рост объема рынка рекламы в млн. USD»**

DoS-атака (Denial of Service, отказ в обслуживании) — атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легитимные пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверам), либо этот доступ затруднён.

Если атака выполняется одновременно с большого числа компьютеров, говорят о DDoS-атаке (Distributed Denial of Service, распределённая атака). В некоторых случаях к DDoS-атаке приводит легитимное действие, например, размещение на популярном интернет-ресурсе ссылки на сайт, размещённый на не очень производительном сервере. Большой наплыв пользователей приводит к превышению допустимой нагрузки и отказу в обслуживании. Задача тестировщиков и разработчиков определить поведение системы в условиях нагрузки и разработать модель поведения, которая максимально уменьшит убытки.

Социальные приложения разрабатываются в виде вэб приложений. Основное преимущество заключается в том, что функции должны выполняться независимо от операционной системы данного клиента. Именно это и делает их привлекательными для клиентов и конечно для хакеров. Основная проблема тестирования социальных

вэб приложений – сложность точного определения места, где произошел сбой или возникла ошибка, и потому режим работы, или же сообщение об ошибке, которое будет получено, может быть результатом ошибок, случившихся в разных частях сетевой системы. В таком случае её исправление будет проблематичным.

Также необходимо отметить, что социальные приложения – это наиболее удобное средство распространения спама и вредоносного софта, поэтому тестирование системы аутентификации пользователей стоит в числе наиболее важных задач при обеспечении безопасности.

Выводы

Примеров уязвимостей и атак существует огромное количество. Даже проведя полный цикл тестирования безопасности, нельзя быть на 100% уверенным, что система по-настоящему безопасна. Всегда остаются факторы, влияющие на безопасность, которые нельзя заранее предугадать, например, безграмотная работа пользователей. Но можно быть уверенным в том, что процент несанкционированный проникновений, краж информации, потерь данных будет на несколько порядков ниже, чем у тех, кто не проводил тестирования безопасности. И система сможет устоять перед преднамеренными атаками, среагировав наиболее безболезненно для обладателей систем и их пользователей.

Литература:

1. http://ru.wikipedia.org/ - Социальные сети
2. “Software testing” by Brian Hambling, Peter Morgan, Angelina Soamroo, Geof Thompson and Peter Williams.

THE CASE OF DISINFORMATION ON THE EXAMPLE OF SMOLENSK CRASH OUTCOMES

Michal Jarocki,
Faculty of International and Political Studies,
University of Lodz, Poland

Disinformation is one of the most popular, yet not widely known methods of manipulation. Was this process used in the outcomes of April 2010 Smolensk crash? Certainly such a hypothesis has all the rights to be taken into consideration.

Disinformation is one of the most mysterious phenomena governing the sphere of interpersonal interaction. The mechanisms and means of actions defined as disinformation often remain in hiding. So are its initiators of main or subcontractors. Frequently also the reason of why particular persons, social groups or even whole societies are being targeted as

the main subjects of such processes. The same goes with the final goal of disinformation which is regularly a matter of conjecture and hypothesis, posed by the individual and careful observers, very often in solitude with their requests and warnings.

One of the more prominent theorists and researchers of this phenomenon was Vladimir Volkoff. This son of Russian immigrants who settled in France in the first half of the twentieth century, is a recognized author of three studies of the disinformation and numerous articles and research papers devoted to this subject. By serving as a French intelligence officer during the Algerian War, as well as his broad and reliable contacts in French Intelligence command of that time, Volkoff was able to learn about the activities measured in the deliberate manipulation of people, putting them in error, mixing facts, discrediting inconvenient persons or blackening conclusions arising from the given data. All of this is, in the understanding of Volkoof, disinformation. It is nothing but a deliberate manipulation of actors by intentional controlment of information flow, transmitted to normal people in such a way that they wouldn't be able to draw clear conclusions and make any legitimate judgments or necessary decisions.

In his theoretical considerations Volkoff has divided the process of disinformation on its individual elements, forming a characteristic pattern, which is the basis for further considerations and practical research on this phenomenon. According to the researcher, as a process of disinformation is divided into:

- **The client**, understood as the person or group of people who are beneficiaries of the whole process,
- **The agent**, defined as a person or a group of people (institutions), which are the direct masterminds and organizers of the whole process
- **Brackets**, defined as events, situations or phenomena that are the basis of disinformation, give them a start and are the background and the source of information used in the whole process
- **Transmitters**, nowadays understood as the media, immediately informing people and societies about the events and describing all publicly known facts,
- **The theme**, taken as a basis for discussion, debate and endless argues, which aim to exchange opinions among commentators of previously mentioned phenomena, as well as ordinary citizens,
- **Sound Box**, understood as means of information and its transmission, which are not directly related to or controlled by the Agents. There are all kinds of media, as well as individuals who, through spontaneous action, make an additional transfer of inaccurate and deliberately distorted information. Commonly, such people are refered to as "Useful idiots"
- **Target group**, defined as individuals, social groups and entire societies, which are the subject of the whole process. In regard to those entities, media – knowingly or not – pass false and/or distributed information to effectively disturb in making any reasonable and solid conclusions and if possible divide social opinion.

Disinformation is not a young phenomenon. Despite that fact it is hard to draw a precise time line of its beginnings and evolutions among the decades and/or centuries. It is even hard to define specific features of it, in order to determine its origins. Do you began with the press and the mass dissemination of information passed on to people? If so, disinformation would have have a few hundred years. Must not be forgotten that, as a process of influencing individuals, deception (in some form and to some extent) was also used in ancient times, when it consisted of manipulation of specific social groups, which had a decisive influence on power, such as the patricians in Ancient Rome. On the other hand, do not forget that many (including Volkoff) agree to a specific division of disinformation onto a social (political) one and the one which focus are primary military, understood as misleading enemy's commander on the battlefield. In view of this fact, we can conclude that the first mention of disinformation already appeared in the records of Sun Tzu in one of his greatest works known as "The Art of War" where he said that "war is the art of deception" and that the biggest achievement of a commander is not to win a hundred battles victories in hundred battles, but to "defeat the enemy without fighting" (eg by deliberately putting it in false interpretation of given facts).

For the purpose of this paper the Author will set an example of one of the best (to his knowledge) contemporary phenomena, which may show signs or at least circumstantial evidence of measured disinformation. For clarification, the example which Author presents is only an example of a hypothesis describing an event which happened, without any definitive implications as to the real causes of it what so ever.

When in 10th of April 2010, the Polish presidential plane crashed near Smolensk military airport, killing all the passangers inside, including the president of Poland Lech Kaczynski, everyone back in the country began to ask themselves of what really happened. Cause of the crash was unknown, the way haw it happened was undefined, so were the mistakes made during the flight as well as individual who could be blamed for them. Was the responsibility for that tragic event resting on the Russian side as the hosts and co organizers of the presidential visit or was all being an tragic result of a negligence of the Poles, who were the main organizers of that trip? Perhaps the fault laid partially on both sides? All of this was yet unknown and hard to explain.

Despite months of speculation, debates and research carried out by Polish and Russian committees responsible for investigating plane crashes, no one was able to provide the society with strait and undeniable answers and conclusions. In addition to that fat, lots of questions, rumors and myth arose, making this matter a socially dangerous and very confrontational topic. The whole thing for months (and possibly years), divided not only the Polish public opinion and society, but also the national political class.

Of course it is unclear whether such visible social divisions, and many highly emotional, debates and disagreements between different groups of Polish society which arose after the Smolensk crash were the result of deliberate actions of some undefined entity whose purpose was to polarize Polish public opinion and lead to even greater division of the political class. But, assuming, as a hypothesis, that this actually happened, one could try to compare all that with Volkoff's scheme of disinformation:

- **The customer**, a foreign state / international entity benefiting from the polarization of Polish society and political class/elite (and weakening the biggest Polis opposition party which was the political background of current President),
- **The agent**, the intelligence services of the Customer, organizing the disaster (though not necessarily), or simply using its effects,
- **Brackets**, the presidential plane crash, the death of the state elites
- **Transmitters**, global and (especially) Polish media, mass recounting and commenting on the event and its consequences,
- **The theme**, the death of the head of state, the need to investigate the cause, the search for people responsible for the crash,
- **Sound Box**, independent media, opposition, criticism of the official version of events, fans of conspiracy theories forming their own hypotheses,
- **Target group**, Polish society and political class

As one may see from the scheme, at least in theoretical terms, the assessment of the disaster in Smolensk and its aftermath, both as a reorientation of the political situation in Poland and the progressive polarization of Polish society, could be the result of intentional disinformation activities of foreign intelligence forces. Author's aim was not to prove that this fact actually took place, much less point to direct its organizer. The aim was clearly to show that, by adopting some of the most popular assumptions that describe the phenomenon of disinformation and comparing them to April 2010 events, it is clear that a hypothesis of such a scenario is not totally unrealistic and that it should be taken in the process of investigating the whole matter.

ЧЕЛОВЕЧЕСТВО НА ТРОПЕ ХОЛОДНОЙ КИБЕРВОЙНЫ

К.ф-м.н., доцент Н.Р.ЗАЙНАЛОВ
Самаркандский институт экономики и сервиса, заведующий кафедрой ЮНЕСКО «Автоматизированных информационных технологии»,

Развитые компьютерных сетей и Интернет сопровождается со многими историями по утечке информации, о выводе из строя компьютеров. Исходя из этого, попробуем проанализировать текущее положение дел в мире, а также затронуть некоторые аспекты в межгосударственных киберотношениях.

Необходимость в защите информации, компьютеров от взлома возникает не только для физических лиц, но в основном эта проблема касается крупнейших фирм и государственных организации. В этом плане достойно внимания события связанные с Wikileaks. Как известно, Wikileaks - это сайт, структура которого аналогична открытой Интернет энциклопедии Wikipedia.

С самого начало своей деятельности Wikileaks ориентировался лозунга «Информация для всех», поэтому его постоянно преследовали скандалы. Один из последних скандалов состоялся в апреле 2010 года после публикации видеозаписи, на которой миллионы людей увидели, как американские вертолеты расстреливают мирных иракских жителей. А в ноябре 2010 г после публикации 250-ти тысяч документов дипломатической переписки посольств и консульств США. И это явилось информационной бомбой для многих стран и их руководителей.

По странному обстоятельству многие международные компании начали преследовать Wikileaks, например, со стороны таких компаний как: Швейцарский банк Post Finance, международные платежные системы PayPal, Visa и MasterCard, а социальные сети Facebook и Twitter начали блокировать аккаунты сторонников Wikileaks.

Такое единодушное и целенаправленная деятельность против Wikileaks наталкывает на мысль о соответствии этих действий принципам демократии, о чем яростно пекутся западные державы. Наверное поэтому сторонники Wikileaks осуществили кибератаки на сайты выше указанных международных организации и правительства США, Франции и Австралии отчасти нарушив их деятельность. И здесь мы становимся свидетелями кибервойны.

Общеизвестно тот факт, что ученые в 2007 году продемонстрировали, как можно с помощью кибератаки организовать физическое уничтожение оборудования – генератора, подключенного к электросети общего пользования. Эксперимент поставил ребром вопросы о связи кибербезопасности с физической безопасностью и о необходимости оградить государство от атак, совершаемых в киберпространстве.

В 2010 году произошло еще одно событие: через киберпространство незамеченным распространился червь Stuxnet, способный вывести из строя промышленные системы.

Этот новый образ кибернетических угроз полностью разрушил привычные представления о том, что кибербезопасность — забота и удел исключительно компьютерного мира. Противостояние компьютерным атакам превратилось в дело государственной важности, поскольку некоторые их виды перестали быть сферой интереса исключительно правоохранительных органов и стали рассматриваться на уровне государств. До этих событий лидеры государств могли себе позволить игнорировать или терпеть большинство кибератак, без лишнего шума проводя расследования и осуществляя долгосрочные программы, направленные на повышение информированности граждан и взращивание более разумных и ответственных участников компьютерной экосистемы. Видя заголовки статей о киберугрозах, большинство граждан раньше привычно пропускало эти ставшие обыденностью сообщения. Вирусы, кража идентификационных данных, даже крупномасштабные финансовые мошенничества воспринимались в сознании общества как некая повседневность, неизбежные побочные эффекты развития Всемирной сети. Большинство понимает, что данные риски существуют и что потери могут быть очень большими, но, в конце концов, не отказываться же из-за этого от мгновенного доступа практически к любой информации.

Stuxnet донес до лидеров развитых стран идею о том, что кибератаки потребуют использования рычагов национальной власти. Например, в опубликованной «Международной стратегии по киберпространству» Белый дом четко изложил доктрину национальной безопасности по отношению к кибератакам. В этом документе прямо говорится: «В соответствии с Уставом ООН государства имеют неотъемлемое право на самооборону, которое может быть использовано в ответ на определенные агрессивные деяния в киберпространстве». При этом четко обозначены цели и задачи обороны государства: «США наряду с другими странами будут поощрять ответственное поведение и противодействовать тем, кто пытается нарушить работу сетей и систем. Правительство США будет препятствовать совершению злонамеренных деяний путем убеждения или иных мер воздействия и оставляет за собой право по мере необходимости адекватно защищать жизненно важные активы страны».

Тем самым Белый дом четко дает понять, что разрабатывается стратегия сдерживания и убедительного ответа, которая будет опираться на истолкование одних актов в качестве вопросов полицейского право применения с реальными последствиями для субъекта деяния, а других — в качестве вопросов национальной безопасности, способных повлечь за собой военный ответ. Появление понятия военного ответа на кибератаку, включающего в себя применение силы для защиты государства, — это прямое следствие тех опасностей, которые стали ощутимыми и реальными после атаки вируса Stuxnet и возникновения ему подобных угроз.

Необходимо также предотвращать попытки совершения злоумышленниками, находящимися на территории США, атак в отношении других стран, поскольку такие атаки могут вызвать обоснованный ответ со стороны этих государств. Подобные сценарии необходимо учитывать и вписывать в стратегии как сдерживания, так и обоснованного ответа.

Парадокс вот в чем: тот риск, который прежде привычно отвергался, в долгосрочной перспективе может обойтись обществу гораздо дороже, чем сами атаки, от которых теперь приходится защищаться. Денежные потери среднего или крупного предприятия от кибератаки могут быть внушительными, но гораздо более серьезная утрата — это потеря интеллектуального капитала.

Тем самым поводом начать разработку подобной стратегии кибербезопасности для многих стран послужили не только попытки проникновения хакеров в национальные информационные системы, но и попытки вывести из строя компьютерную сеть иранской ядерной программы с помощью вируса Stuxnet, о разработчиках которой, кстати, пресса умалчивает, а ведь подобную вирус программу можно создать только при координации государственных служб. Это всё наталкивает на страшный мысль: “Крупномасштабная война государств может начаться с глупой «ошибки» компьютера”. А ведь эту ошибку можно сгенерировать, поэтому не понятно, действие США, правительство которой обвинило Россию и Китай в кибершпионаже с целью заполучить секреты США. Ведь хорошие про-

граммисты есть и в Израиле, Индии, Японии… Но больше всего их в американской Силиконовой долине. Наверное поэтому с территории США хакерских атак фиксируется не меньше, чем из китайского или российского виртуального пространства.

Из всего этого можно умозаключить, что именно правительственные структуры стоят за этими масштабными кибератаками.

Таким образом, развитие киберпространства приводит посредственно и непосредственно к негативным явлениям в межгосударственных отношениях. Для предотвращения конфликтов на почве киберугроз необходимо создать прозрачную систему мониторинга киберпространства каждой страны независимой международной комиссией, членами которой могут быть любые страны. В этой организации не должно быть "старшего брата", который диктует свои правила двойных игр в корыстных целях.

РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Светлана Карпенко

Urgency of the problem. Development of the policy of information security: local policies of workstations, domain users' passwords, local groups and users of work stations

Мировые расходы на услуги по обеспечению информационной безопасности (ИБ) в текущем году вырастут примерно на 13% и достигнут $35,1 млрд. [Gartner]. В прошлом году объем рынка в денежном выражении составил $31,1 млрд. По прогнозу аналитиков, в будущем году мировые расходы на ИБ-услуги вырастут до $38,3 млрд и по итогам 2015 г. превысят $49,1 млрд. Таким образом, рост за 5 лет будет соответствовать примерно 58%. Наиболее высокие темпы роста в последующие годы, уверены в Gartner, продемонстрирует сегмент услуг по управлению безопасностью инфраструктур компаний (Managed Security Services, MSS), оказываемых сторонними провайдерами. По прогнозу аналитиков, объем этого сегмента в денежном выражении в период с 2010 по 2015 гг. вырастет более чем в 2 раза - с $6,82 млрд до $14,89 млрд.

Организация доменной структуры сети, использование сетевых экранов и издание приказа об ИБ являются предпосылками для внедрения системы ИБ на ЗАО «Гомельлифт». Дадим характеристику отдельных фрагментов ИБ организации.

Требования к локальным политикам рабочих станций приведены в таблице1. Пользователь принадлежит только к группе Пользователи.

Таблица 1

Локальные пользователи и группы

Группы	Описание
Администраторы	Имеют полные, ничем неограниченные права доступа к компьютеру или домену.
Опытные пользователи	Обладают большинством прав, но с некоторыми ограничениями. Они могут запускать любые, а не только сертифицированные приложения.
Пользователи	Не имеют прав на изменение параметров системы. Они не могут запускать многие несертифицированные приложения.
Гости	По умолчанию имеют те же права, что и пользователи, за исключением учетной записи "Гость", еще более ограниченной в правах.

Требования сложности пароля к учетной записи локального Администратора: Применение английских букв, Применение символов ! , ? @ «» № ; % : ? * ( ) -_+ / \ и д.р., Применение регистра. Требования сложности к паролям пользователей домена приведены в таблице 2.

Таблица 2

Требования сложности к паролям пользователей домена

Требования к паролю	Обязательное
Применение русских букв	Нет
Применение английских букв	Да
Применение цифр	Нет
Применение символов ! , ? @ «» № ; % : ? * ( ) -+ / \	Нет
Применение регистра	Нет

При отсутствии пользователя, за которым закреплен АРМ, за его ПК могут работать только лица, входящие в группы: Пользователи группы (например, на компьютере Начальника ОИТ могут работать пользователи группы безопасности «ОІТ»), Список пользователей (по утвержденному списку). При отсутствии пользователя на закрепленном за ним АРМе могут работать лица группы Пользователи, запрет для групп Администраторы, Опытные пользователи, Гости. Локальные группы рабочих станций приведены в таблице 3.

Таблица 3

Локальные группы рабочих станций

Группы	Описание	Применение
1	2	3
Администраторы	Администраторы имеют полные, ничем не ограниченные права доступа к компьютеру или домену	Gomellift\ Domain Admins Администратор
Гости	Гости по умолчанию имеют те же права, что и пользователи, за исключением учетной записи "Гость", еще более ограниченной в правах.	Отсутствуют
Операторы архива	Операторы архива могут перекрывать ограничения доступа только в целях копирования и восстановления файлов.	Отсутствуют
Операторы настройки сети	Члены этой группы могут иметь некоторые административные права для управления настройкой сетевых параметров	Отсутствуют

1	2	3
Опытные пользователи	Опытные пользователи обладают большинством прав, но с некоторыми ограничениями. Они могут запускать любые, а не только сертифицированные приложения.	Gomellift\ <пользователь, член домена>
Пользователи	Пользователи не имеют прав на изменение параметров системы. Они не могут запускать многие несертифицированные приложения.	Gomellift\ <пользователь, член домена, член группы>
Пользователи удаленного рабочего стола	Члены этой группы имеют право на выполнение удаленного входа	Отсутствуют
Репликатор	Поддержка репликации файлов в домене	Отсутствуют
HelpServicesGroup	Группа для центра справки и поддержки	SUPPORT_388945a0 (MICROSOFT)

Локальные пользователи рабочих станций приведены в таблице 4.

Таблица 4

Локальные пользователи рабочих станций

Пользователь	Описание	Активность
ASP.NET Machine Account	Account used for running the ASP.NET worker process (aspnet_wp.exe). Защита паролем.	Включен
HelpAssistant	Учетная запись помощника для удаленного рабочего стола	Отключен
SUPPORT_388945a0	Это учетная запись поставщика для службы справки и поддержки	Отключен
VirusBlokAda	Это учетная запись антивируса ВирусБлокАда	Включен
Администратор	Встроенная учетная запись администратора компьютера/домена	Включен
Гость	Встроенная учетная запись для доступа гостей к компьютеру/домену	Отключен

Требования к безопасности NTFS-системы. Полный доступ: SYSTEM, Администраторы (имя компьютера \ Администраторы), Опытные пользователи (Gomellift\ <пользователь, член домена>), СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ. Чтение и выполнение: Пользователи (имя компьютера \ Пользователи), Пользователи (Gomellift\ <пользователь, член домена, член группы>). Нет доступа: Все.

АНАЛИЗ МЕЖДУНАРОДНЫХ АСПЕКТОВ ГЛОБАЛЬНЫХ РИСКОВ 2012 ГОДА

Ирина БАЛИНА,
Славянский университет (Республика Молдова)

Problems of functioning of specifications IT are researched. The analysis of strategic directions of development IT – standards and modules is carried out. Global risks of 2012 are researched and formulated.

Целью работы является исследование особенностей развития рынка информационной безопасности в 2011 г. и выявление глобальных рисков IT в 2012 г**.**

Метод сбора данных - мониторинг материалов аналитических обзорных статей в СМИ, исследований маркетинговых и консалтинговых агентств отраслевых учреждений, анализ баз данных сети Internet. Рассматриваемый метод обеспечивает представление IT в виде спецификаций поведения реализаций IT-систем, которые могут наблюдаться на интерфейсах (границах) этих систем. Стандартизация спецификаций IT и управление их жизненным циклом рассматривается с точки зрения развития системы специализированных международных организаций на основе строго регламентированной деятельности. Данный процесс обеспечивает накопление базовых сертифицированных научных знаний, служит основой создания открытых технологий.

В области стратегических направлений развития IT – стандартов заслуживает внимание появление и развитие следующих модулей и стандартов:

1. Продолжается противостояние западных аналитиков и российских экспертов рынка систем электронного документооборота (ECM/СЭД) в области архивных стандартов. В ходе работы над MoReq2010® особое внимание было уделено изучению основных международных стандартов и привязке спецификации к ним. По мнению председателя руководящего совета по спецификации MoReq Мартина Уолдрон (Martin Waldron): «… выработанные требования к базовым сервисам и подключаемым модулям отвечают сформулированным в международных стандартах общим принципам управления документами, обеспечивая потребности как государственного, так и частного сектора на корпоративном, отраслевом и прикладном уровнях». [1]. Официальный выпуск первой серии модулей расширения для MoReq2010® состоялся на Трехлетней конференции DLM в Брюсселе в декабре 2011 г.

2. В декабре 2011 г. **завершились работы над окончательной редакцией проекта ГОСТ Р «Обеспечение долговременной сохранности электронных документов».** Стандарт подготовлен на основе перевода Технического отчёта ISO/TR 18492:2005 «Обеспечение долговременной сохранности электронных документов» (Long-term preservation of electronic document-based information) и

описывает возможности воспроизведения аутентичных электронных документов в тех случаях, когда срок хранения этих документов превышает расчетный срок использования технологии (оборудования и программного обеспечения), при помощи которой эти документы создаются и поддерживаются. [2].

3. На базе материалов, представленных ведущими разработчиками систем электронного документооборота, международных стандартов разработан и о**публикован проект первой версии стандарта** Гильдии Управляющих Документацией «**Понятия и термины в сфере управления электронными документами**» [2]. Стандарт учитывает сложившиеся реалии рынка Российской Федерации, а также стран Таможенного Союза. Материалы документа представляют прямой интерес для специалистов в области IT Республики Молдова в связи с продолжающимися консультациями о вступлении страны в Таможенный Союз.

Рассмотрим аналитические отчеты экспертов в области информационной безопасности по итогам 2011 г. и сформулируем **прогноз на 2012 г.** По материалам ***SecurityLab US CERT*** опубликован отчет, согласно которому в 2011 г. было обнаружено на 38% больше уязвимостей по сравнению с 2010 г. [3]. Поэтому очень важным представляется создание политики информационной безопасности IT, т.е. комплекса превентивных мер по защите конфиденциальных данных и информационных процессов. Одним из этапов которой является составление таблиц рисков. В результате разработка политики безопасности обеспечит надлежащие уровни, как отдельных рисков, так и интегрального риска. При ее разработке необходимо, однако, учитывать объективные проблемы, которые могут встать на пути реализации политики безопасности. Такими проблемами могут стать недоработки правовой базы государства и законы международного сообщества, внутренние требования корпорации, этические нормы общества.

Исследование, проведённое ***компанией Symantec***, показывает, что финансовая стоимость устранения непосредственных результатов онлайн-преступлений составляет 114 миллиардов долларов, стоимость времени, затрачиваемого на восстановление после кибератак, составляет 247 миллиардов долларов в год. В целом, суммарная стоимость борьбы с киберпреступностью в настоящее время превышает стоимость борьбы с распространением наркотиков, которая, в свою очередь, обходится мировой экономике 288 миллиардов долларов в год. [5].

По данным экспертов «***Лаборатории Касперского***» (ЛК) по итогам киберугроз за 2011 г. в рейтинге самых опасных для интернет-серфинга государств стала Россия, поднявшись на две позиции по сравнению с 2010 г. Согласно отчету, web-атакам в России подверглись более 55% Интернет-пользователей. На втором месте находится Оман (54,8%), а тройку лидеров, поднявшись с пятой позиции, замыкает США (50,1%). Все страны, попавшие в рейтинг, эксперты ЛК распределили по степени риска заражения при серфинге в Интернете. К группе повышенного риска с результатом от 41% до 60% вошли 22 страны. В группе риска оказались 118 стран с показателем 21-40%, среди которых Италия (38,9%), ОАЭ (38,2%), Франция (37%),

Швеция (32%), Голландия (37,1%) и Германия (26,6%). Среди самых безопасных при серфинге в Интернете стран находятся всего 9 государств: Эфиопия (20,5%), Гаити (20,2%), Дания (19,9%), Нигер (19,9%), Того (19,6%), Бурунди (18,6%), Зимбабве (18,6%), Бенин (18,0%), Мьянма (17,8%). [4]

На основании исследований по итогам 2011 г. составлен прогноз развития рынка безопасности IT на 2012 г. [4]. Обобщая мнение экспертов ведущих фирм – разработчиков средств безопасности и антивирусного контроля можно сформулировать следующие глобальные риски 2012 года: 1. массовые целевые атаки – в 2012 г. в зону повышенного риска попадут спектр компаний и отраслей экономики, такие как: добывающие, энергетические, транспортные, занимающиеся производством продовольствия, фармацевтики, а также крупные интернет-сервисы и компании IT безопасности, произойдет существенное территориальное расширение объектов атак: – кроме стран Западной Европы и США, составляющих сейчас основную зону атак, сюда войдут страны Восточной Европы, Ближнего Востока и Юго-Восточной Азии; 2. кибероружие – прогнозируется, что киберконфликты 2012 г. будут развиваться вокруг уже традиционных осей противостояния: США/Израиль – Иран, США/Западная Европа – Китай; 3. атаки на онлайн-банкинг - вероятнее всего, подобные атаки будут нацелены не только на пользователей персональных компьютеров, но и против мобильных пользователей, помимо стран Юго-Восточной Азии и Китая, возможны атаки на системы мобильных платежей в странах Восточной Африки; 4. хактивизм или хакерские атаки, имеющие своей целью выражение протеста против определенных событий, акции хактивистов все в большей степени будут носить политический характер – и это станет их основным отличием от атак 2011 года, однако, хактивизм может быть использован и в целях сокрытия других атак, как средство отвлечения внимания, ложный след или «безопасный» способ взлома интересующего объекта; 5. проблемы с защитой пользовательских данных, частной жизни и информации пользователей.

Таким образом, проведенные исследования позволяют сформулировать следующие **выводы:**

1. Назрела необходимость таксономии (классификационной системы) профилей IT, обеспечивающей уникальность идентификации в пространстве IT, как явное отражение взаимосвязей IT между собой при решении вопросов обеспечения безопасности.
2. Применение имеющегося методологического аппарата анализа рисков и разработка современных систем защиты информационного пространства тесно связаны с особенностями адаптации или разработки новых нормативные документов, которые будут обязательно учитывать положения международных стандартов.
3. Гиперскоростное развитие информационных технологий, создание всемирного единого информационного пространства, интеграция в это пространство Республики Молдова являются непреложными фактами. Вместе с тем, создание адекватных и надежных систем защиты информации в современных условиях не под силу отдельному государству.

4. Для плановой разработки новых концепций и технологий, их гармонизации и сертификации в качестве международных стандартов, управления жизненным циклом стандартов IT, поддержания их в согласованном состоянии, разработки методов и средств аттестации IT-систем необходимо дальнейшее развитие мощной международной системы специализированных организаций.

Цитируемая литература:

1. http://www.gdm.ru/projects/moreq/MoRoq2010.php - пресс-релиз описания базовых сервисов MoReq2010®. [Электронный ресурс]. Дата обращения: 9.03.2012.
2. http://ehointerneta.ru/sajty-i-servisy/5387-kiberprestupnost-stanovitsya-mirovym-zlom.html. [Электронный ресурс]. Дата обращения: 10.03.2012.
3. http://www.securitylab.ru/news/420293.php. Исследования рынков. [Электронный ресурс]. Дата обращения: 10.03.2012.
4. http://www.kaspersky.ru/news?id=207733691 – отчет по киберугрозам за 2011 год Kaspersky Security Bulletin 2011. [Электронный ресурс]. Дата обращения: 16.02.2012.
5. http://korrespondent.net/business/web/1258977-otchet-globalnaya-kiberprestupnost-ezhegodno-obhoditsya-v-114-mlrd - Cybercrime Report 2011. Исследования производителей ПО Norton, компании Symantec Corp [Электронный ресурс]. Дата обращения: 12.03.2012.

DISASTER RECOVERY PLANNING – THE OBVIOUS THAT WE MISS OR UNDERRATE

Asen Bozhikov,
Assistant at the Tsenov Academy of Economics – Svishtov, Bulgaria

Preparing a disaster recovery plan is a complex project which doesn't stop with its creation. Even if the organization has such a plan, it is important to regularly keep it up to date. The purpose of this paper is to outline some of the underestimated points when it comes to disaster recovery planning.

Today's business environment is quite complex and it is often characterized by rapid, unpredictable changes. This brings not only new opportunities, but also new threats to business organizations of all sizes. For sure, one of the main goals of every organization should be taking advantage of these opportunities, while mitigating the risk. When it comes to risk mitigation, every business organization needs a disaster recovery (DR) plan, which describes how to act in the event of unexpected disruption or disaster. The DR plan is about reacting to disaster after it has happened. There are

many classifications of disasters in literature, but in most cases they could be separated into two main groups:

- Natural disasters – hurricanes, tornados, earthquakes, fire, flood etc.;
- Man-made disasters – terrorism, explosion, theft, riot, power failure, software failure etc.

No matter what type of disaster has happened, the organization should be prepared to respond to the disruptive event in a timely fashion and recover mission-critical applications and data as soon as possible. Otherwise, negative effects will occur – lost revenues, lost data, loss of customer trust and even going out of business. Usually DR is more connected with the IT department and IT systems (ERP, CRM, BI, email servers etc.). The reason for this is that today's business relies more and more on new information and communication technologies. This leads to large volumes of digital data, which are the most valuable asset of every organization. The importance of having a DR plan is proven by the 2011 Forester study report which shows that almost a quarter of companies worldwide are likely to declare a disaster in a five-year time period[1]. Without a DR plan the chances of a successful recovery of business operations and data are close to zero. At the same time, many business organizations which have developed such a plan still suffer serious loss in the case of a disruptive event, or they just have inadequate plans. Taking this into consideration, we are going to outline some of the main points which are underrated or even missed during DR planning.

It's better to create a DR plan earlier rather than later - no manager would like to spend money on DR strategy when everything in the organization is working just fine at that moment and there are no signs of any kind of disasters. In fact, small-scale disasters are those that cause 80% of business downtime – problems with drive failure, application crashes, data corruption and human error[2]. So a DR plan is more than a necessity for every business organization.

Members of the DR planning team – to create a successful DR plan, the DR team should include representatives from every department in the organization and also a high-level manager, who usually is the CEO. This way, the plan will embrace all business activities in the organization and is going to be comprehensive. A common mistake is not to include members from all departments, which often results in the elimination of possibly valuable information about future DR strategy.

Defining the key assets of the organization and assessing threats and risk – on the one hand the DR team should analyze and outline which are the mission-critical business processes, applications and data, while on the other hand it should foresee as many disaster scenarios as possible. The core of this is business impact analysis, which results in the thorough analysis of the impact of not having mission-critical data, applications and processes available after a disaster has struck and how this is connected to possible

---

1 Oxton, J. Stepping Up In the Face of Crisis, Disaster Recovery Journal, Spring 2012, Volume 25, Number 2, p. 26

2 Denapoli, M. Myth-Busting the Obstacles to Disaster Recovery Planning, Disaster Recovery Journal, Spring 2012, Volume 25, Number 2, p. 53

economic loss for the organization. Business impact analysis is primarily an information-gathering process, which finishes with listing the key components for each business unit in the organization, such as[1]:

- Determine the criticality a particular system or application has to the organization;
- Learn how quickly the system or application must be recovered in order to minimize the organization's risk of exposure;
- Determine how current the data must be at the time of recovery.

A big problem at this point could be the lack of documentation for current business processes which flow through the organization. Without this information it is hard to define the key assets and what their value to the business is. Organizations that use standard frameworks, like the Information Technology Infrastructure Library (ITIL) have better chances of recoverability.

Assigning roles and responsibilities – this is an area where business organizations encounter serious difficulties. At the same time, the roles and the responsibilities of an organization's employees are vital if a disaster strikes. Everyone should know exactly what to do when a disruptive event occurs. A common mistake is to depend only on too few qualified personnel to handle the disaster, mainly from the IT department. In fact, the DR process is much more than restoring the data, it's about returning to normal business operations. To accomplish this it is necessary to include the participation of people not only from IT, but also from corporate governance, finance and the business units impacted. Another problematic area here is training. Employees' training is critical. Without proper training and clear understanding of their responsibilities, the DR plan is doomed to failure.

Testing the DR plan – testing the plan is another step which is underestimated. If the organization has developed a DR plan, this doesn't necessarily mean that it will be useful when a disruptive event occurs. Furthermore, the DR team should consider not just testing, but realistic testing, which will show real business function recovery. The closer to a real disaster the test can get, the more provable the DR plan is. Meanwhile, during the test period, missing points could be identified, inconsistencies and errors in the plan, gaps between expected and achieved results, and problems with roles and responsibilities. This is very useful and definitely would help when revisiting the DR plan and making it more provable. Nevertheless, many organizations still don't pay enough attention to this very important step when developing their DR plan. A 2011 Symantec survey of more than 1200 small and medium-sized businesses worldwide revealed that less than one-third (28%) of organizations have actually tested their disaster recovery/failover systems, leaving their companies vulnerable to massive technology and business failures in the event of a disaster[2].

---

[1] Little, D., S. Farmer. Digital Data Integrity: The Evolution from Passive Protection to Active Management, Wiley, 2007, p. 36

[2] Symantec 2011 SMB Disaster Preparedness Survey, http://www.symantec.com/content/en/us/about/media/pdfs/symc_2011_SMB_DP_Survey_Report_Global.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Jan_worldwide_dpsurvey

Regular updates to the DR plan – this is somewhat connected with the process of testing the plan. When a DR plan is successfully created and tested, it doesn't mean the organization is prepared for future disruptive events. Ongoing maintenance is equally important in order to have a reliable DR plan. The stress here is on monitoring changes in laws, standards, the organization's structure, and the impact of new technologies. If there are significant changes, they should find their place in the corresponding documentation of the DR plan, thus updating it.

Using modern IT for DR – developing a DR plan is always about searching for the balance between cost and the level of recovery. Of course, a small-sized organization can't afford a lot of money for DR compared to a big enterprise. This is going to change as some new forms of technology gain popularity as a cost-effective means in favor of DR – technologies like server virtualization and cloud computing. On the one hand, server virtualization is quite a common strategy for optimizing the organization's IT infrastructure, which leads to shorter recovery times and simpler DR plans. On the other hand, the shared resources which cloud computing offers allow on-demand recovery and great backup functionality.

In conclusion, a well-structured and comprehensive DR plan will enable organizations to recover quickly and effectively from any disruptive event, thus avoiding loss and significant interruption of business processes. Keeping in mind and paying attention to the above mentioned points would greatly increase the chances of creating and maintaining the right DR plan.

SAP SECURITY: PROTECTING YOUR DATA – AND YOUR BUSINESS

Zgardan Evghenia, Juc Stanislav
ASEM

More than 82,000 companies around the world use SAP business applications to power their enterprises. These SAP systems carry precious cargo—the mission-critical data that fuels and supports the organization.

SAP combines the technology, solutions, and services to address the three pillars of information security:

1. People – SAP offers services that can help you raise awareness of security issues among employees and establish easy-to-follow security guidelines and policies. Their broad selection of education offerings ensures that your people have the knowledge they need to protect your systems and processes.
2. Processes – SAP provides consulting and support services that focus on risk assessment and management, helping you understand security as a business issue and ensuring that all work routines and processes are secure. They also

offer a broad range of solutions to help you manage governance, risk, and compliance .

3. Technology – All SAP solutions are designed to meet the highest security standards. And with theSAP NetWeaver technology platform, you have the technology foundation you need to ensure the security of your heterogeneous infrastructure.

SAP solutions are built from the ground up to ensure the highest levels of security in the most sensitive environments. SAP follows rigorous security standards in the design and development of all its solutions, and SAP application developers receive extensive security training.

The SAP NetWeaver platform is based on a state-of-the-art security infrastructure, including network and communications security, auditing capabilities, as well as web services security capabilities. In addition, two dedicated security solutions focus on the specific challenges customers are faced with in heterogeneous IT landscapes:

- SAP NetWeaver Identity Management – The SAP NetWeaver Identity Management (SAP NetWeaver ID Management) component provides centralized tools for managing the entire user life-cycle across highly diverse system environments. It automates processes such as employee on-boarding, position changes, and access rights management for external users while ensuring compliance and auditability.
- SAP NetWeaver Single Sign-On – With the SAP NetWeaver Single Sign-On application, customers can set up secure single sign-on and single log-out scenarios tailored to their individual requirements, including all SAP GUI types, web applications, and identity federation across domain boundaries. Based on standards such as X.509 certificates, Kerberos and the security assertion markup language (SAML), SAP NetWeaver Single Sign-On is a highly flexible solution that can be configured to meet even the highest corporate security standards.

Some examples of research achievements include:

1. Secure information sharing – Privacy-preserving computing schemes use advanced cryptographic methods to allow joint computations without disclosing sensitive input data to collaboration partners or a trusted third party. We have used this technology to build secure services for benchmarking and distributed optimization tasks.
2. Automated security validation – Security flaws in business processes, services and protocols are subtle and hard to detect. With the help of the security validator, a business process or protocol designer can check his models with the push of a button and gets advice on how to fix the design in case the check fails. Results are as precise as can be, since the approach is based on sound mathematical theories.
3. Data-centric security – Cloud computing and service orientation can be most effective if data is allowed to migrate across domains of control. To maintain security upon migration, policies need to be known and enforced beyond a

single application or system context. Sticky policies are attached to the data and travel with them, keeping the data owner in control.

SAP offers key security services to protect your information assets:

SAP Security Concepts and Implementation – Helps you define and implement an enterprise-wide information security policy

SAP Security Optimization – Checks the security of your SAP solution and makes recommendations for system settings

Plus, SAP's security offerings are enhanced through our investment in security best practices.

DATA SECURITY IN DATA WAREHOUSE

Stefan PETROV
D. A. Tsenov Academy of Economics
Svishtov, Bulgaria

This article describes the most important issues of informational security in Data Warehouses, which could be summarized into four security areas. These issues should be considered before creating data security policies .

Data Warehouse is the main source of information, required for business analysis in enterprises. It collects operational data from transactional systems, transforms them into appropriate format for data analysis and stores the data for a long period of time. That is why data security policies in companies inevitably include security issues of Data Warehouses.

The security needs of Data Warehouses could be summarized into four security areas [3]:

- **Data classification and ontology**;
- **Data integrity and validation**;
- **Access policies and data restrictions**;
- **Data masking and privacy preservation**;

Palletvuori asserts that applying proper **data classification** and its understanding by all users of the system is essential for maintaining high level of informational security [3]. Data Warehouse developers should choose such shared structures and logic that could be equally interpreted by different parties. Determining the potential changes in the data security requirements through the time is possible only when the ontology of the data is well-defined and understood.

The second security area is ensuring **data integrity and validation**. Data loaded to the Data Warehouse must be valid and accurate and the Warehouse should implement techniques which manage and control the process of combining data from multiple sources.

Access policies and data restrictions could be organized into two levels [4] (Figure 1):

- Database level security
- Application level security

Both the levels allow users to be grouped into roles and each group receives some data restrictions.

Database level security contains tools and services which traditional Database Management Systems provide for informational safety maintenance, like views, SQL Grant and Revoke commands, encryption, auditing.

Palletvuori notices that a simple approach to improving the security in Data Warehouse is to inherit its access permissions from the source data and treat the Data Warehouse and source database as one distributed database [3]. However, such an approach could not be useful for ensuring data confidentiality.

Application level security refers to hiding certain menus, reports, data entry screens or application modules depending on users' roles.

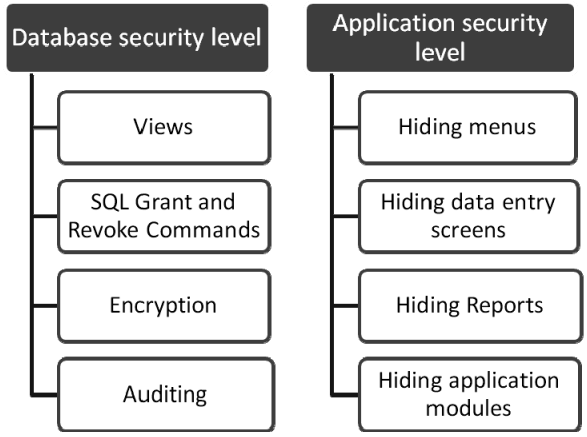


Figure 1. **Security levels of access polices in Data Warehouse**

The purpose of the security area **"Data masking and privacy preservation"** is to ensure that all privacy requirements are considered and all confidentiality needs are fulfilled. Creating data security policy requires to be given answers in advance to the following questions: [2]

- Which data should be filtered according to user permissions?
- Which data are subjected to legal restrictions?
- Which analyses may be performed on this data?
- Which data may be used only for the company's own purposes and which data may be given to third parties?

Maksimov supposes that the most appropriate technique for ensuring data confidentiality in Data Warehouse is encryption, but he marks as disadvantages of the

technique the decreasing performance of the Data Warehouse and the requirement all information systems in the company to support manipulation of encrypted data. [1]

We could conclude that improving data security in Data Warehouse would increase the benefits which analytical software products provide for users.

References:

1. **Максимов**, Р. Особенности построения хранилищ данных. IT-MANAGER, сентябрь, 09.2010.
2. **Katic**, N., **Quirchmayr**, G., **Schiefer**, J. A Prototype Model for Data Warehouse Security Based on Metadata. 9th International Workshop on Database and Expert Systems Applications. Vienna. 1998.
3. **Palletvuori**, K. Security of Datawarehousing server. TKK T-110.5290 Seminar on Network Security, 2007-10-11/12
4. http://www.ir.iit.edu/~dagr/cs761/files/DataWarehouseOverview.pdf

SECURITY IN ELECTRONIC CUSTOMER RELATIONSHIP MANAGEMENT SYSTEMS

Kremena M. MARINOVA

PhD Student, Academy of Economics "D. A. Tsenov"

(Svishtov, Bulgaria)

This report aims to describe possible security attacks in Electronic Customer Relationship Management Systems (e-CRM) and solutions to enhance security in e-CRM applications. The report outlines results of survey in Bulgarian financial sector about protection methods used in financial organizations.

Electronic Customer Relationship Managements Systems (e-CRM) use a huge variety of data about organization`s customers as: personal information (name, sex, age, ID); contact information (address and phone); education and training; social an marital status; used to date products and services. This kind of information is very sensitive and often subject to abuse. One of the major characteristic of e-CRM Systems is their convenience; however, it also opens the door for various security attacks.

The possible **security attacks** in e-CRM systems, defined by **Panko**[1], are:

1. **Denial of service.** It makes attacked system unavailable to customer. Possible attackers are angry customers, formal employees and the competitors.
2. **Intrusion of sales automation system and customer database.** Intruders can break into the systems and steal customer information.

[1] **Panko**, R. Corporate Computer and Network Security, Prentice Hall, Upper Saddle River, New York. 2004.

3. **Identity theft.** It happens when someone uses personal information without permission to commit fraud or other crimes.
4. **Malware attacks.** Malware includes viruses and worms. These attacks can cause the Denial of service, hardware damage or data loss.

Cook[1] describes some advices to enhance e-CRM security:

1. **Encription of remote data**. As a first line of defense, all confidential data on mobile devices should be encrypted. Companies have to consider using software to encrypt everything on notebooks. At the very least, business-critical information should be protected by encryption. Organizations have to use password protection on all mobile devices and to require strong passwords and frequent changes. Alternatively they can use more secure, authentication methods in place of passwords that include separate physical keys, such as USB drives, which need to be plugged into a computer to make files accessible. This is more safty if they keep the key separate from the computer.

2. **Monitoring of wireless connections.** Data is most vulnerable when it is in transit. This is especially true if organization uses wifi or other wireless connections to transmit its data to the home office. Wifi communications have to be encrypted with Wifi Protected Access (WPA) or 802.11i standards to make interception much more difficult. The older Wired Equivalent Privacy (WEP) standard is much less secure. Setting up a fake Service Set Identifiers (SSID) is one way to access a wifi session. Essentially, this involves setting up an access point on top of another wifi hot spot. In such a way that there is at least an equal chance that anyone logging in through the hot spot will connect through the phony access point — which will then read and record the entire session. Organizations can implement Virtual Private Networks (VPN) when it is available because they are more secure than a conventional connection.

3. **Role-based security**. Employees ought to have access to the data associated with their role in organization. These roles should consider what employees actually do, not their position in organization is. Each role should give them the privileges they need to do their job and no more. **Taber**[2] adds that companies have to manage carefully the customer`s access to e-CRM system too. If security infrastructure gives somebody the wrong level of access, it will irritate a fair percentage of users. Instead of trying to prevent access, organization can monitor access and create reports that alert management to abusers. The company can have HR put more specific data security guidelines into the personnel handbook, and make it clear that violations will be punished.

4. **Education of the staff**. Employees have to know up to date security best practices. The staff has to understand enough to take basic precautions to prevent system to be compromised. It is good solution to be initialized security education program which

---

[1] **Cook**, R. Checklist: 5 Principles of CRM Security. <http://www.insidecrm.com/features/checklist-crm-security-040709>, 7.04.2009.

[2] **Taber**, D. How to Get Smarter About CRM Security. <http://www.cio.com/article/682296/How_to_Get_Smarter_About_CRM_Security>, 13.05.2011.

to inform people about the dangers of sharing, writing down passwords etc. Employees should be trained not to open attachments from unknown sources and not to add unauthorized file sharing applications to their systems.

5. **Beware of phishing**. It involves sending phony email messages which aim of getting the victim to submit confidential information such as credit card numbers or account details. Organizations have to make a point of alerting their employees to the dangers. They should have a policy for dealing with suspicious emails and make sure their employees are aware of what constitutes a "suspicious" email.

Lee and etc.[1] summarize most popular protection methods. They includes: using a good passwords, installing firewalls, installing anti-virus programs and using VPN. Most common security method is to use ID and password but this is not enough. Improved methods include use of long password and its encryption. VPN is the use of a secure channel in the Internet communications. Customer awareness is important in preventing social engineering attacks.

A survey about e-CRM systems in financial sector of Republic of Bulgaria finds out which methods are effective and useful. The survey shows that most of the interviewed organizations protect data in its e-CRM system using individual passwords, codes and certificates to access the system. Common-low is system`s users to sign a privacy statement, prepared in accordance with internal rules and instructions of the particular organization. Some companies use the services of a specialized unit for security, which may be internal to the organization or service to be entrusted to a contractor (outsourcing). Some enterprises do additional data backup of the archive. Others use more sophisticated protection systems such as the Disaster Recovery Center.

In conclusion, only one of surveyed organizations said that its activities doesn`t encounter security problems using the system, which is indication that protection and data security in e-CRM systems should not be ignored and needs to be paid adequate attention. Innovative solution in this area is e-CRM system to be integrated with the Data Processing Centre, which can be placed ever-growing amounts of data and it to be stored securely and reliably.

References:

1. **Panko**, R. Corporate Computer and Network Security, Prentice Hall, Upper Saddle River, New York. 2004.
2. **Cook**, R. Checklist: 5 Principles of CRM Security.http://www.insidecrm.com/features/checklist-crm-security-040709.
3. **Taber,** D. How to Get Smarter About CRM Security. http://www.cio.com/article/682296/How_to_Get_Smarter_About_CRM_Security.
4. **Lee**, H., **Chen**, K. L., **Shing**, Ch**., Shing**, M. Security Issues in Customer Relationship Management Systems (CRM). //*37th Annual Conference Bricktown - Oklahoma City*. 2006.

[1] **Lee**, H., **Chen**, K. L., **Shing**, Ch., **Shing**, M. Security Issues in Customer Relationship Management Systems (CRM). //*37th Annual Conference Bricktown - Oklahoma City*. 2006

Materialele Conferinței "Securitatea Informațională 2012"
sunt publicate în redacția autorilor.