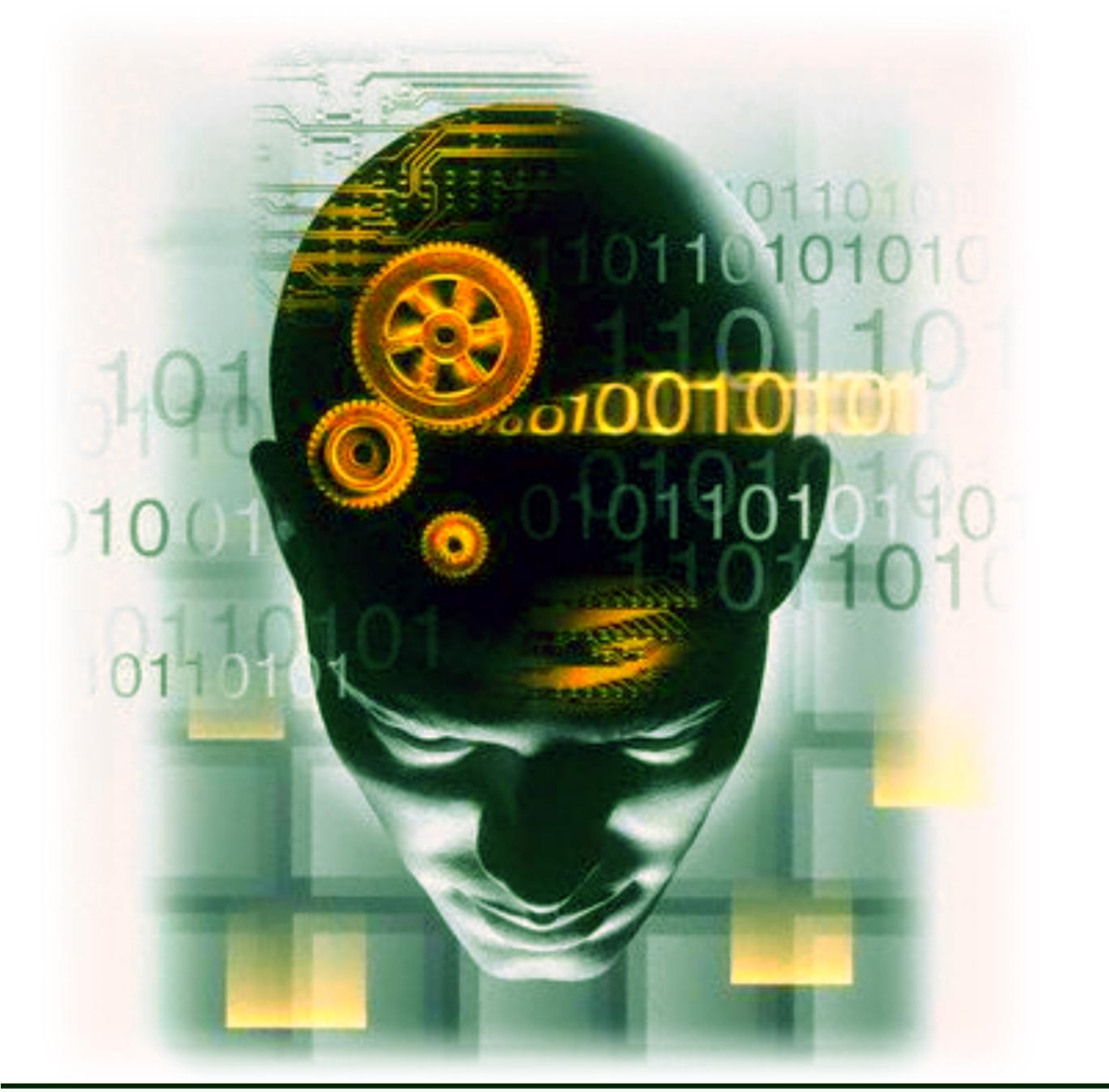


SECURITATEA INFORMAŢIONALĂ 2011

CONFERINŢĂ INTERNAŢIONALĂ,
(ediţia a VIII-a), 4 mai 2011

ACADEMIA DE STUDII ECONOMICE DIN MOLDOVA
LABORATORUL DE SECURITATE INFORMAȚIONALĂ

SECURITATEA INFORMAȚIONALĂ 2011

CONFERINȚĂ INTERNAȚIONALĂ
(ediția a VIII-a)

4 mai 2011

Chișinău – 2011

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

Tatiana Mişova, prorector al Academiei de Studii Economice din Moldova, doctor, profesor

Sergiu Tutunaru, doctor, Academia de Studii Economice din Moldova

Serghei Ohrimenco, doctor habilitat, profesor, Academia de Studii Economice din Moldova

Teodor Ţîrdia, doctior habilitat, profesor, Universitatea de Stat de Medicină

Tudor Leahu, doctor, Universitatea Cooperatist - Comercială

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

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)

Rumen Vyrbanov Stoianov, doctor, Academia de Economie (Svistov, Bulgaria)

Genadii Cernei, doctor, expert, Agenţia pentru Inovare şi Transfer Tehnologic al Academiei de Ştinţă a Moldovei

Valerii Domarev, doctor, expert (Ucraina)

Igor Juc, expert, F-Line Tehnologies

Victor Coşcodan, expert, S&T Moldova

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

Vitalie Spînachi, master în derept, expert LSI, Academia de Studii Economice din Moldova

Descrierea CIP a Camerei Naţionale a Cărţii
„Securitatea informaţională 2011", conf. intern. (2011; Chişinău). Securitatea informaţională 2011: Conf. intern. (ed. a 8-a), 4 mai 2011 / coord. ed. S. Ohrimenco. – Ch.: ASEM, 2011. – 123 p.
Antetit.: Acad. de Studii Econ. din Moldova, Lab. de Securitate Informaţională. – Texte: lb. rom., engl., rusă. – Bibliogr. la sfârşitul art. – 25 ex.
ISBN 978-9975-75-558-0.
- - 1. „Securitatea informaţională 2011" – Conferinţa internaţională (rom., engl., rusă).
004.056(082)=135.1=111=161.1

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

ISBN 978-9975-75-558-0

ORGANIZATORII CONFERINȚEI:

ACADEMIA DE STUDII ECONOMICE DIN MOLDOVA

AGENȚIA PENTRU INOVARE ȘI TRANSFER TEHNOLOGIC

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

PARTENER MEDIA:

PARTENER INFORMAȚIONAL

SPONSORI:

Cuprins:

DYNAMIC MODEL OF SECURITY

Leszek F. KORZENIOWSKI
President European Association for Security

The article presents a critical analysis of securitylogy – as a new, shaping branch. The author defines the notion of "security" as a certain objective condition based on the lack of threat, sensed subjectively by individuals or groups. Analysis leads to the dynamic model of safety which consists of four independent elements: objective situation (danger) - subjective perception - behavior (decision, activity) based on subjective perception - effects dependent on objective situation → new objective situation.

Securitology as a new approach examines **dangers to the existence, development and normal functioning of individuals and social organizations**. Safety as a subject of research has a multilateral character and is more than a sum of absence of danger. Safety is a function of numerous factors[1].

Influence of these dangers is studied by basic and applied, theoretical and practical sciences which results from the fact that numerous factors have impact on safety: objective and subjective, internal and external, abstract and concrete, constructive and destructive, static and dynamic, sociopsychological and technical, legal and natural, macro- and microeconomical, all of which are inseparably and mutually connected.

The holistic[2] approach helps to distinguish new characteristics of organized systems of codependent elements which may lead to synergic[3] effect (valued constructively or destructively).

Security means a certain objective state, which usually consists in the lack of any threat to the existence, development and normal functioning of the Man, subjectively perceived by individuals and groups[4].

It should be noticed that the word: "state" is very closely related here to the concept of situation which describes the configuration of common relations between a human and other elements of his/her environment within a certain bracket of time. About the situation we say then, when we analyze this kind of relation from the point of a human (who is one of its elements), while the "state" means here that the subject of the situation may also be non-human.

The concept of situation is very complex. As **Tadeusz Tomaszewski** notices, each situation is defined first of all by its **elements** and their **features**, by the **state** of particular

---

[1] DWORZECKI J.: KOCHAŃCZYK R.: *Współczesne zagrożenia*. Gliwice: GWSP 2010.

[2] *Holism*, the idea that the whole is more than a sum of elements, from *hólos* (gr) – whole, total.

[3] *Synergy* means that interaction of elements yields a result which in some aspects is larger than the simple sum of effects produced by each of the elements separately. SZMIT M.: *Informatyka w zarządzaniu*. Warszawa: Difin, 2003, p. 14.

[4] KORZENIOWSKI L.: *Securitology. The concept of safety*. "Comunikations" 2005, No 3, s. 20-23; KORZENIOWSKI L.F. *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*. Kraków: EAS, 2008, p. 55. www.sbc.org.pl/dlibra/doccontent?id=13871&dirids=66

elements within a certain moment of time and by the **interactions** taking part in that moment among its elements [TOMASZEWSKI 1977, s. 18][1]. The situation consists of:

1. **scheme**, in which a subject of this situation exists (a person, a group, a society),
2. **activity** of the subject, especially basic activity, by the existence of which we investigate the activity of the subject..

Taking under consideration two basic aspects of a situation – the kinds of a person's activity - two basic situations can be distinguished:

- **existential** (vital). Life means processes of the vital importance for staying alive and the satiation of needs.
- **behavioural** (functional). Activities mean actions of a subject, thanks to which he/she regulates his/her interactions with an environment, shaping by that the environment or himself/herself.

Behaviourists define situations as sets of stimuli. In reality, there exist two different levels of behaviour:

a) reactive on the elementary level,
b) purposeful on the higher level.

Dlatego też sytuacje człowieka można wprawdzie opisywać jako układ stymulacyjny bodźców, na które on **reaguje,** ale trzeba pamiętać, że jest to opis uproszczony, pomijający fakt wyższej organizacji zachowania się ludzi. Oznacza to, że sytuacja jest polem, w którym człowiek rozwija jakąś działalność, **realizuje** określone zadanie.

That is why the situations - on one hand, can be described as a set of stimuli to which he/she reacts, but it has to be remembered that this is a simplified description, not taking under the consideration any higher organization of a person's behaviour. It means that a situation is the area where a person develops any activity, realizes a certain task.

The stimulatin character of a person's situation is taking place by susceptibility and reactivity. Susceptibility means the ability of animate organisms to the reception of certain stimuli (for example: visual, auditory and tactual receptiveness, etc.). At the same time, reactivity means, characteristic for many people, relation of the power of reaction to the power of creating it stimuli. What it means is that the reaction of different people to similar stimuli varies, so the behaviour of different people in the same environment may be different.

Also, the task situation described is by the characteristics of the surroundings, the subject, as well as by the way an individual sees this relation and understands it.

The employment of an individual's consciousness in shaping his/her situation, has become the basis of three theoretical concepts:

1. **phenomenological**, where the elements of a situation are only phenomena because only these are available in recognition, felt and understood (while the essence is unrecognizable). According to Kurt Lewin, the existence of reality is always the existence to somebody and that is why the situation of a person is always as he/she sees it (senses it and understands it)[2].

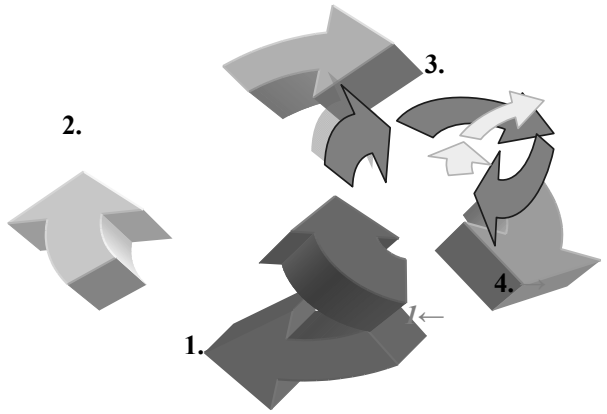
[1] TOMASZEWSKI T.: *Psychologia*. Warszawa: PWN 1977, p. 17-19.
[2] LEWIN K.: *Principles of Topological Psychology*. New York: 1936, s. 66.

2. **dual,** two contradictory situations:"objective" and "subjective". Recalled by Tadeusz Tomaszewski, Henry Murray distinguishes the objective situation existing independently from the way somebody understands it (situation Alpha), and subjective situation that exists in a certain time-frame the way somebody sees it (situation Beta)[1].
3. **hollistic**, comprehensive, encompassing the person's surrounding together with himself/herself, exactly how they are objectively and in objective relations with each other, as well as the way they are being seen by the subject and the other participants of the situation.

The objective features shape the person's behaviour depending on how he/she sees his/her situation, while the understanding of a situation by an individual depends on: a) what are the objective features of the environment, b) what are his/her own characteristics, and c) what course of action he/she takes himself/herself. Furthermore, certain elements of a situation influence a person directly, without the intervention of an individual's consciousness, for example if, estimating the situation as being safe he/she will not react then he/she will be hurt accordingly to the objective characteristics of the threat and not the imagined features of an environment.

Analysis leads to the **dynamic model of safety** which consists of four independent elements:

1. objective situation (danger)
2. subjective perception
3. behavior (decision, activity) based on subjective perception
4. effects dependent on objective situation → *1. new objective situation, etc.*



In reality, we often come across a situation, in which the individual's behaviour even if agreeable with the perception of reality, and not with its objective features, results in objective features and not the perceived or imagined ones. Modern technique of registry has shown the tragic situations being such a presented problem (26th of December, 2004 –

[1] TOMASZEWSKI T.: *Psychologia*. Warszawa: PWN 1977, p. 21.

following an earthquake in the nearby of the Indonesian Island of Sumatra, a gigantic *tsunami*-wave was created. The number of fatalities is being estimated at over 300000, wounded at a few million. It was perceived that the environment was friendly, safe.

References:

1. DWORZECKI J.: KOCHAŃCZYK R.: *Współczesne zagrożenia*. Gliwice: GWSP 2010.
2. KORZENIOWSKI L.F. *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*. Kraków: EAS 2008. http://www.sbc.org.pl/dlibra/doccontent?id=13871&dirids=66
3. LEWIN K.: *Principles of Topological Psychology*. New York: 1936.
4. SZMIT M.: *Informatyka w zarządzaniu*. Warszawa: Difin, 2003.
5. TOMASZEWSKI T.: *Psychologia*. Warszawa: PWN 1977.

ВОЗМОЖНОСТЬ ПРИМЕНЕНИЯ СТАНДАРТА ISO 27001 В СФЕРЕ PUBLIC RELATIONS (PR)

Анатолий КРАПИВЕНСКИЙ,
ГОУ ДПО «Волгоградский институт молодежной политики и социальной работы» (Российская Федерация)

The process of informational security ensuring in the XXI century is actual practically for all the fields of human activity, especially for such a basic field of social stability as Public Relations (PR). Author investigates an opportunity of application of standard ISO 27001 in the above area.

Процесс связей с общественностью, или Public Relations (PR), вне зависимости от того, на каком уровне он осуществляется (государство-общественность, организация-общественность, политик-общественность и т.д.), по сути представляет собой частный вариант достижения общественного консенсуса, в котором заинтересованы все задействованные в данном процессе социальные акторы – как коллективные, так и индивидуальные.

PR-деятельность представляет собой, с одной стороны, разновидность процесса управления (в данном случае – управления общественным мнением по какому-либо значимому для базисного субъекта вопросу), а с другой стороны – разновидность процесса коммуникации (информационного обмена, инициированного базисным субъектом).

С функциональной точки зрения управление есть "целенаправленное воздействие на сознание и поведение людей, осуществляемое с целью направить их действия на достижение желаемых целей" [1: 4], а в самом общем, схематичном виде - "воздействие субъекта управления на его объект" [2: 33]. В свою очередь,

коммуникация заключается в "информационном воздействии субъекта коммуникации на объект, преследующем цели, заданные субъектом" [3: 40].

По определению Э.А. Сидельник, "в современной литературе сложилось два подхода, определяющие сущность PR: социальный и технологический. Первый подразумевает достижение социального согласия, обеспечение социального взаимодействия… Второй подход обращается к технологиям управления, методам воздействия на людей" [4: 5].

Очевидно, что именно второй подход (технологический) и позволяет говорить о возможности управления уровнем информационной безопасности в данном процессе.

В этой связи вызывает интерес возможность использования стандарта ISO 27001 Международной организации по стандартизации (International Organization of Standardization) применительно к сфере Public Relations.

Указанный стандарт "предназначен для разработки системы управления информационной безопасностью организации вне зависимости от ее сферы деятельности" [5]. Более того, система управления информационной безопасностью (СУИБ) — это «та часть общей системы управления организации, основанной на оценке бизнес 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» [6].

Российский аналог этого стандарта – ГОСТ Р ИСО/МЭК 27001-2006 указывает, что при разработке системы менеджмента информационной безопасности (СМИБ) необходимо: " a) определить область и границы действия СМИБ с учетом характеристик … организации, в том числе детали и обоснование любых исключений из области ее действия; b) определить политику СМИБ на основе характеристик бизнеса, организации, …которая: 1) содержит концепцию, включающую в себя цели, основные направления и принципы действий в сфере информационной безопасности (ИБ); 2) принимает во внимание требования бизнеса, нормативно-правовые требования, а также договорные обязательства по обеспечению безопасности; 3) согласуется со стратегическим содержанием менеджмента рисков организации, в рамках которого будет разрабатываться и поддерживаться СМИБ; 4) устанавливает критерии оценки рисков; 5) утверждается руководством организации; c) определить подход к оценке риска в организации, для чего необходимо: 1) определить методологию оценки риска, подходящую для СМИБ, которая должна соответствовать требованиям обеспечения деятельности организации и нормативно-правовым требованиям информационной безопасности; 2) разработать критерии принятия риска и определить приемлемые уровни риска. Выбранная методология оценки риска должна обеспечивать сравнимые и воспроизводимые результаты" [7: 3-4].

Следовательно, стандарт ISO 27001 по своим принципиальным положениям, касающимся построения эффективной системы управления информационной безопасностью, вполне может быть применим и к сфере Public Relations.

Здесь хотелось бы уточнить три момента:

1) под риском в PR следует понимать "отказ от предупредительных мер" [8: 157] по пресечению угроз общества в данной сфере деятельности;
2) несмотря на то, что декларируемой целью PR-деятельности в первую очередь является удовлетворение интересов именно ее организатора, что, как уже указывалось выше, происходит при любой коммуникативной интеракции, тем не менее, в рамках PR, безусловно, некорректно рассматривать общественность как жертву базисного субъекта (организатора) PR-акций. Говорить о наличии жертвы в данном случае неуместно, так как цель PR-акции по определению не должна нарушать законодательно закрепленные права общественности, а при отсутствии нарушения прав объекта информационного воздействия, его невозможно рассматривать в качестве жертвы;
3) определять законодательно закрепленные правила ведения коммуникативной деятельности в сфере PR и обеспечивать соблюдение действующего законодательства, является прерогативой государства. В Российской Федерации эта деятельность регулируется, в частности, Доктриной информационной безопасности Российской Федерации (утверждена Президентом РФ 9 сентября 2000 г., № Пр-1895), Законом РФ «О средствах массовой информации» от 27.12. 1991 г. № 2124-1, Федеральным законом «О противодействии экстремистской деятельности» от 25.07.2002 г. №114-ФЗ, Федеральным законом «О рекламе» от 13.03.2006 г. № 38-ФЗ и рядом других нормативно-правовых актов.

Литература:

1. Гулиев М.А., Епифанцев С.Н., Самыгин С.И. Социология и психология управления. – Ростов н/Д: Феникс, 2006.
2. Шепелева Ю.Е. Муниципальное управление: организационно-правовой аспект. М.: АНО РЖ «Социально-гуманитарные знания», 2006.
3. Науменко Т.В. Социология массовых коммуникаций в структуре социологического знания // Социологические исследования. – 2003. - № 10.
4. Сидельник Э.А. PR в современном обществе: сущность и социальное значение. – Таганрог: Изд-во ГОУ ВПО «ТГПИ», 2005.
5. Digital Security: Сертификация по ISO 27001. - http://dsec.ru/consult/cert
6. Понятие системы управления информационной безопасностью / Global Trust Solution Limited - http://www.globaltrust.ru/uslugi/vnedrenie-sistem-upravleniya-informacionnoi-bezopasnostyu/ponyatie-sistemy-upravleniya-informacionnoi-bezopasnostyu

7. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования / ФГУП «Стандартинформ» . – М.: «Московский печатник», 2008.
8. Луман Н. Понятие риска: Пер. с нем. // THESIS: теория и история экономических и социальных институтов и систем. — 1994. — № 5.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ

***Владимир ШКВИР**, Львовская Политехника, (Украина),*
***Анджей АУГУСТЫНЕК**, Научно-технологический Университет, Краков, (Польша)*

В процессе подготовки специалистов по экономическим специальностям (бухгалтерский учет, менеджмент, маркетинг и другие), необходимо должное внимание уделять основам информационной безопасности. Это обусловлено рядом объективных причин, основными из которых являются следующие:

- деятельность экономистов, напрямую связана с формированием информационных ресурсов предприятия, часть которых попадает под действие Закона «О коммерческой тайне»;
- технологические процессы сбора, обработки и хранения информации, выполняемые пользователями, должны быть надежно защищены от несанкционированного доступа и утечки.

Предлагаемые структура и состав средств обеспечения информационной безопасности, используемые пользователями, включает следующие компоненты:

- правовые методы защиты. Пользователи должны обладать глубокими знаниями законодательного обеспечения, которое регулирует отношения в области информационных отношений. В первую очередь, это относится к Закону «О коммерческой тайне», «О персональных данных», «О бухгалтерском учете» и др.;
- организационные средства защиты;
- технические и программные средства.

Пользователи должны понимать и знать основные принципы системы информационной безопасности. Основными из них являются::

- принцип законности – заключается в соответствии принимаемых мер законодательству о защите информации, а при отсутствии соответствующих законов – другими нормативными документами по ее защите;
- принцип комплексности – с позиций предотвращения разноплановых угроз и используемых методов. Имеется в виду полнота защиты по

соответствующему методу и по перечню угроз, а также взаимовлияние методов и средств защиты;

- принцип минимальной достаточности состоит в использовании набора средств, обеспечивающих выполнение комплекса установленных требований по защите информации при заданной степени риска ее нарушения. При этом необходима увязка функционирования различных средств защиты по месту и времени, хранения и преобразования информации;
- принцип обоснованности. Под названным принципом подразумевается наличие достаточных доказательств актуальности выдвинутых требования или оценка риска нарушения защиты информации;
- принцип тактической организации защиты – предусматривает необходимость упреждающих действий в виде методов предотвращения, а не ограничения последствий. Данный принцип объединяет
- саморегулируемость сложности защиты (структурированность, позволяющая использовать более простые методы для оперативного контроля и наращивания ресурсов при возникновении угрозы для ее максимального отражения);
- автотестируемость (выполнение контроля правильности функционирования системы защиты, возможность самообучения с адаптацией и моделируемостью ситуаций);
- принцип непрерывности состояний во времени и пространстве, предполагающий невозможность функционирования объекта при исключении защиты;
- принцип восстановления нормальной работы системы.

В рамках отдельной темы необходимо рассматривать состав и структуру информационных угроз по отношению к производственно-хозяйственной деятельности фирмы (предприятия). Немаловажным является ознакомление с методиками определения экономической эффективности мероприятий по обеспечению информационной безопасности, расчетом инвестиционной привлекательности системы информационной безопасности.

У пользователей информационных и коммуникационных технологий должно сформироваться устойчивое представление о необходимости соблюдения:

- конфиденциальности, т.е. защищенности информации от ее раскрытия без разрешения владельца. Одновременно конфиденциальность – это статус, предоставляемый данным и определяющий степень их защиты;
- целостность, т.е. защищенность точности и полноты информации и информационных ресурсов. Целостность означает также гарантированность того, что данные не были изменены, подменены или уничтожены в результате случайных или преднамеренных действий;
- доступность, т.е. возможность получения доступа к информации или информационным ресурсам за приемлемое время с возможностью выполнения операций копирования, модификации или уничтожения.

Конечной целью подготовки студентов является получение комплекса теоретических знаний и практических навыков использования информационных ресурсов. Основными задачами являются следующие:

1. Обеспечение безопасности информации должно проводиться системно и комплексно на всех этапах проектирования, внедрения и эксплуатации информационных систем.
2. Система обеспечения безопасности информационных ресурсов функционально должна перекрывать все существующие угрозы безопасности информации.
3. Система обеспечения безопасности должна быть ориентирована на тактическое опережение возможных угроз.
4. В системе безопасности должны быть разработаны механизмы восстановления нормальной работы информационной системы в случае реализации угроз.

Литература

1. Девятин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. – М.: Радио и связь, 2006.
2. Джеймс Л. Фишинг. Техника компьютерных преступлений. -М: НТ Пресс, 2008.
3. Краткий аналитический вопросник по бот-сетям в РФ 2009 год. www.securitylab.ru/analytics/370022.php
4. Информационная безопасность открытых систем: В 2 т. Том 1 – Угрозы, уязвимости, атаки и подходы к защите. – М.: Горячая линия-Телеком, 2006.
5. Информационная безопасность систем организационного управления. Теоретические основы: В 2 т. – М.: Наука, 2006.

ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С. В. КАРПЕНКО
Белорусский торгово-экономический университет потребительской кооперации (Гомель, Республика Беларусь)

Развитие информационных технологий (ИТ) создает качественно новые угрозы, способные приводить к катастрофическим по своим масштабам последствиям. Организационно-правовое обеспечение информационной безопасности (ИБ) представляет собой совокупность решений, законов, нормативов, регламентирующих общую организацию работ по обеспечению информационной безопасности, создание и функционирование систем защиты информации на конкретных

объектах. Поэтому организационно-правовая база должна обеспечивать следующие основные функции:

1) разработка основных принципов отнесения сведений, имеющих конфиденциальный характер, к защищаемой информации;
2) определение системы органов и должностных лиц, ответственных за обеспечение информационной безопасности в стране и порядка регулирования деятельности предприятий и организаций в этой области;
3) создание полного комплекса нормативно-правовых руководящих и методических материалов (документов), регламентирующих вопросы обеспечения информационной безопасности как в стране в целом, так и на конкретном объекте;
4) определение мер ответственности за нарушение правил защиты;
5) определение порядка разрешения спорных и конфликтных ситуаций по вопросам защиты информации.

Разработка законодательной базы ИБ любого государства является необходимой мерой, удовлетворяющей первейшую потребность в защите информации при развитии социально-экономических, политических, военных направлений развития каждого государства.

В составе республиканской нормативной базы выделены следующие группы документов: законы, концепции, стандарты, положения. Значительный блок документов представляют нормативно-правовые документы Национального банка Республики Беларусь.

В докладе выполнен анализ содержания нормативно-правовых документов Республики Беларусь по вопросам информационной безопасности. Значительное внимание уделено правовому полю стандартизации.

В состав общей нормативной базы входят 4 закона: Об информации, информатизации и защите информации, Об электронном документе, О цифровой подписи, Об органах государственной безопасности Республики Беларусь, и 2 концепции: Концепция государственной политики в области информатизации, Концепция Национальной безопасности Республики Беларусь. Необходимо отметить разработку новой редакции Концепции национальной безопасности Республики Беларусь. В концепции отмечается, что важной сферой в системе обеспечения национальной безопасности является информационная. Более четко в новой редакции прописан раздел "Совершенствование основных направлений государственной политики в области обеспечения информационной безопасности. Разработка и реализация государственных научно-технических программ".

На смену гос программе «Электронная Беларусь», реализованной в период прошедшего десятилетия, пришла «Стратегия развития информационного общества».

В Стратегии развития информационного общества в Республике Беларусь на период до 2015 года (Постановление Совета Министров Республики Беларусь от 09.08.2010 N 1174 "О Стратегии развития информационного общества в Республике Беларусь на период до 2015 года и плане первоочередных мер по реализации

Стратегии развития информационного общества в Республике Беларусь на 2010 год") отмечено, что успешное развитие информационного общества сдерживается рядом факторов. Для их устранения необходимо:

- совершенствовать государственную систему управления процессом информатизации и развитием рынка телекоммуникационных услуг;
- обеспечить более четкое взаимодействие государства и бизнеса в сфере информатизации;
- совершенствовать нормативную правовую базу в области защиты авторских прав на цифровой контент и программное обеспечение;
- ускорить создание инфраструктуры и нормативной правовой базы для предоставления государственными органами электронных услуг, в том числе с использованием средств электронной цифровой подписи;
- расширить представительство государства, бизнеса, общественных организаций в сети Интернет;
- принять меры по повышению уровня компьютерной грамотности государственных служащих и населения в целом.

Стандартизация - инструмент обеспечения качества ИБ. Стандарты направлены на реализацию единой политики в сфере использования ИТ. Это стандарты в сфере использования ИТ, интеграции информационных систем на основе общих стандартов и требований в рамках общего информационного пространства, обеспечение эффективного и защищенного информационного обмена.

Стандарты регулируют процессы управления объектами. Все положения стандартов являются рекомендациями по созданию, включению в систему и управлению объектами, а также обеспечению соответствия объектов установленным характеристикам.

Стандарты в области ИБ регламентируют вопросы терминологии, применения антивирусных средств, безопасности автоматизированных систем, вопросы жизненного цикла программных средств, управления ИБ. Выделены группы стандартов: Криптографические методы и средства, Общие критерии, Оборудование.

В республике ведется разработка регламентов и стандартов по ИБ. В настоящее время в Республике Беларусь действуют стандарты в области информационной безопасности, разработанные на базе международных стандартов ISO. Имеются разработки по комплексной системе управления информационной безопасностью на основе национальных и международных стандартов. Такой комплекс позволяет достигнуть необходимого уровня защищенности системы и значительно снизить риск реализации угроз информационной безопасности. Система управления информационной безопасностью является каркасом, который связывает различные компоненты средств информационной безопасности и позволяет надежно и прозрачно управлять системой обеспечения информационной безопасности компании.

Проанализированы регламенты и стандарты по ИБ Республики Беларусь, что позволяет сформировать представление о данном информационном пространстве.

Самостоятельный раздел представляют Положения. Это Положение о порядке разработки, производства, реализации и использования средств криптографической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, Положение о коммерческой тайне, Положение о порядке хранения сведений, составляющих налоговую тайну, доступа к ним и их разглашения, Положение о Государственном центре безопасности информации при Президенте Республики Беларусь.

Документы Национального банка Республики Беларусь - пример правового обеспечения передовой корпоративной информационной системы, влияют на регламент нормативно-правовой деятельности всех предприятий республики и включают концепции, руководящие документы, методики испытаний. Концепции представлены двумя документами: Концепция ИБ Национального банка РБ, Концепция ИБ платёжной системы.

ЦИФРОВАЯ ПОДПИСЬ НА БУМАЖНОМ ДОКУМЕНТЕ

Юрий ПУШНЯК, Владимир ШКИЛЁВ, Аркадий АДАМЧУК
Государственное предприятие ЦГИР "REGISTRU"

The new technology of cryptographic protection of paper documents from a fake is offered. The technology bases on the general approach to protection of the material objects, formulated earlier. The technology borrows the effective mechanism of the digital signature used up for protection of electronic documents only.

Предложена новая технология криптографической защиты бумажных документов от подделки. Технология опирается на общий подход к защите материальных объектов, сформулированный ранее. Технология заимствует эффективный механизм цифровой подписи, применявшийся до этого для защиты только электронных документов.

Многовековая проблема защиты от подделки разнообразных бумажных документов – официальных текстовых документов, финансовых документов строгой отчётности, паспортов и удостоверений личности, дипломов, аттестатов, сертификатов, ценных бумаг, денежных банкнот, бюллетеней для голосования, виз, акцизных марок, этикеток для упаковки товара и др. – остаётся весьма актуальной и в наши дни.

Особенность нынешней ситуации заключается в том, что теперь в обращении наряду с бумажными документами участвуют и электронные документы, причём последние защищены гораздо надёжнее. Этому способствовало интенсивное развитие современной криптографии, предложившей эффективные альтернативы для традиционной печати и подписи.

Очевидно, что в будущем доля бумажных документов в общем обороте будет постепенно снижаться, но они ещё достаточно долго будут оставаться востребованными.

Этими обстоятельствами продиктован интерес к новым технологиям, которые обеспечивали бы безопасное и эффективное **совместное** обращение как электронных, так и бумажных документов в составе единой автоматизированной системы документооборота.

Использовавшиеся ранее технологии полиграфической защиты бумажных документов, основанные на применении специальной бумаги, особой краски, "водяных знаков", рельефных рисунков, специальных вкраплений, микротекста и т.п., в сочетании с традиционной печатью и подписью, никак не соответствуют этому требованию.

Технологии нового поколения - голограмма, RFID – представляются перспективными, но пока достаточно затратными. Поэтому интенсивный поиск новых подходов и технологий продолжается.

Авторами доклада предлагается новая технология криптографической защиты бумажных документов от подделки. Технология опирается на ранее предложенный авторами общий подход к защите материальных объектов произвольной природы, а также заимствует общеизвестный механизм цифровой подписи, который до этого применялся только по отношению к электронным документам.

Общий подход заключается в следующем. В состав объекта искусственно вводится специальная физическая метка, по своей природе адекватная защищаемому объекту, но не нарушающая его потребительских свойств и других важных качеств.

Применительно к бумажному документу это может быть совокупность отверстий произвольной конфигурации, полученная на бумажном носителе документа с помощью неуправляемого электрического разряда [1].

Метка наносится на бумажный носитель документа с помощью специальной электроразрядной установки на этапе подготовки документа к выпуску в обращение.

В докладе показано, что полученная в результате стохастического физического процесса метка обладает следующими интересными качествами:

(a) Она физически неотделима от защищаемого объекта (бумажного документа).
(b) Она уникальна, неповторима.
(c) Она характеризуется набором случайных параметров.
(d) Она невоспроизводима.

Указанные качества делают метку ценнейшим элементом механизма криптографической защиты бумажного документа на основе традиционной цифровой подписи [2].

Процедура подписания документа выглядит так. Сначала на бумажный документ наносится физическая метка. Затем метка сканируется. Полученное цифровое изображение метки подписывается цифровой подписью (закрытый ключ) авторитетного лица. Далее подписанное изображение преобразуется в штриховой код, который печатается на бумажном документе рядом с меткой.

Поскольку метка физически неотделима от документа, то, "подписав" изображение метки, авторитетное лицо фактически подписывает соответствующий бумажный документ, т.е. удостоверяет его подлинность.

Процедура проверки подлинности документа выглядит так. Любой проверяющий читает штриховой код, напечатанный на документе, раскрывает цифровую подпись с помощью открытого ключа авторитетного лица и узнаёт "правильное" изображение метки. Затем он сканирует реальную физическую метку, нанесенную на документ, и сравнивает оба изображения. Если они совпадают, то документ признаётся подлинным.

В докладе показано, что предложенная технология надежно защищает бумажный документ от любых потенциальных атак злоумышленника. Запускать в обращение подделку собственного изготовления или нелегальную копию (дубликат) уже имеющегося подлинника бессмысленно – первая же проверка выявит факт подделки.

Литература:

1. Шкилёв В., Недиогло В., Адамчук А. Электроразрядная защита от подделки бумажных документов. – Securitatea informațională 2010: Conf. intern. (ed. a 7-a) – Ch.: ASEM, 2010. – p. 24-26.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – Издательство "Триумф", 2002 г. – 816 стр.

НАДЕЖНОСТЬ АНАЛИТИЧЕСКОЙ ИНФОРМАЦИИ ПРИ УПРАВЛЕНИИ ПРЕДПРИЯТИЕМ

Росица Н. ИВАНОВА
Университет национального
и мирового хозяйства (София, Болгария)

The Financial-Economic (business) analysis is an information system. In the process of generation of result-oriented analytical information regarding the company management should be provided and secured objective conditions for its protection against the multiple and various threats and risks. Therefore, an information security system for analytical information should be developed and should effectively operate by observing the security principles. This is an objective prerequisite for the formation of competitive advantages for the company.

Финансово-хозяйственный (бизнес) анализ представляет собой специализированную функцию управления предприятием. Он обеспечивает информацию всем уровням управления. Административное управление отвечает за достижение ключевых целей предприятия, а оперативное – за достижение специфических целей отдельных структурных звеньев. Таким образом достигается объективная синхронизация целей предприятия с целями по функциональным центрам ответственности.

Финансово-хозяйственный (бизнес) анализ представляет собой информационную систему. Информация определяется как совокупность определенных

данных. Она философское понятие, в содержании которого отражается познание в любой области объективной действительности, выраженное посредством соответствующих характерных знаков. Анализ как информационная система обладает общими и специфическими характеристиками. Общие характеристики присущи любой информационной системе, а специфические – только анализу. Для осуществления полноценного, качественного и эффективного анализа целостной деятельности предприятия (маркетинговой, иновационной, инвестиционной, производственной, торговой и финансовой) необходима входящая информация, которая подлежит обработке при помощи присущих и специфических элементов его научного метода, методологии и методики, в результате чего получается качественно новая информация, необходимая для принятия правильных управленческих решений. Информационная система финансово-хозяйственного (бизнес) анализа является генератором новой информации. Параллельно с этим осуществляется передача результатной аналитической информации соответствующим потребителям.

Специфическими характеристиками аналитической информационной системы являются ее элементы, между которыми объективно существуют взаимные связи и зависимости. Эти элементы следующие: 1) человеческие рессурсы; 2) информация; 3) носители информации (входящей и результативной); 4) хардвер; 5) софтвер; 6) методологический инструментариум.

В процессе генерирования результатной аналитической информации об управлении предприятием необходимо создать и обеспечить объективные условия относительно: 1) наличности информации к уполномоченным менеджмента предприятия лицам; 2) обеспечения доступа к информации только лицам, имеющим право на это (конфиденциальность); 3) сохранения точности и целости информации и методов ее обработки; 4) принятия риска при обработки и сохранения информации; 5) перманентного идентифицирования источников риска; 6) анализа, оценки и контролирования риска; 7) выбора и выполнения конкретных действий для минимизирования эффекта риска; 8) создания и поддержки системы управления информационной надежностью.

Современные информационные технологии имеют значительное применение и значение во всех областях бизнеса – от управления отдельных бизнес процессов, до управления предприятия в целом. Использование информационных ресурсов и технологий в практике финансово-хозяйственного (бизнес) анализа требует обеспечения их защиты и минимизирования возможностей злоупотребления ими. Надежность информационных продуктов и систем является индикатором для достижения целей предприятия в связи с поверительностью, отчетностью, целостью, доступностью и уверенностью. Тем более, что для него информация является специфического вида нематериальным активом, для которого оно должно обеспечить определенной степени надежность. Это приводит к потребности создания и поддержки системы правил и процедур для управления информационной надежности на предприятии, в т.ч. и в отношении аналитической информации. С ее помощью определяются основные угрозы безопасности при осуществлении внутренних бизнес процессов,

оценивается риск и принимаются решения об эффективном управлении информационной системой и бизнесом в критических ситуациях.

Система управления информационной надежности на предприятии представляет собой множество политик, бизнес процессов и процедур, направленных на обеспечение защиты информации от многочисленных и разных угроз и рисков.

Управление надежностью информации на предприятии в целом, в т.ч. и результатной аналитической информацией, требует правильного определения угроз к информации. Эти угрозы могут быть внешними и внутренними. Внешние угрозы следующие: 1) захват и извлечение информации; 2) умышленная замена части информации; 3) подделка; 4) блокирование информации и невозможность ее получения потребителем. Внутренние угрозы информации следующие: 1) умышленная замена информации сотрудниками предприятия; 2) извлечение и использование информации против предприятия при помощи неразрешенного доступа; 3) неумышленная замена информации (человеческие ошибки); 4) неясные решения, приводившие к составлению и получению ошибочной информации.

Система управления информационной надежностью на предприятии, в т.ч. и аналитической информацией, основывается на системе определенных принципов надежности. Они следующие: 1) осознание потребности в надежности информационных систем и сетей для создания надежной бизнес среды; 2) ответственность за ненадежность информационных систем и сетей; 3) оценка риска; 4) проектирование и внедрение систем надежности в информационные системы и сети; 5) управление информационной надежностью; 6) своевременное вмешательство и сотрудничество для предотвращения, обнаружения и конкретных действий при инцидентах по информационной надежности; 7) периодическая оценка системы и ее адаптирование к современным реальностям и тенденциям развития при помощи интегрирования подходящих практик, мер и процедур.

Для достижения надежности информации, предоставляемой финансово-хозяйственным (бизнес) анализом об управлении предприятием можно выполнить действия в следующих направлениях: 1) Персональная надежность. Требования ко всем администраторам, техническим сотрудникам, руководителям и пользователям о покрытии критериев работы с информацией соответствующего уровня. 2) Документальная надежность. Требования в отношении ведения отчета, сохранения и пользования результатной аналитической информации. 3) Физическая надежность. Требования в отношении контроля доступа к информационным носителям. 4) Криптографская надежность. 5) Организационная надежность. 6) Надежность при управлении коммуникациями. 7) Надежность при управлении непрерываемости бизнеса.

Преимущества использования системы управления информационной надежностью в области финансово-хозяйственного (бизнес) анализа можно систематизировать в следующих направлениях: 1) Она является важным элементом управления и представляет собой фактор для выполнения миссии предприятия. 2) Надежность информации является конкурентным преимуществом для предприятия. 3) Возрастает доверие клиентов, персонала, менеджмента и собственников, так как

информация надежно защищена и система управления этой защиты работающая и адекватная современным условиям глобализации, рыночной конкуренции, мощному развитию информационных технологий, действию финансового и экономического кризиса. 4) Предприятие понимает и объективно применяет законодательство страны в области управления информационной надежностью, стандартов обеспечения непрерываемости бизнеса при возникновении чрезвычайных ситуаций и кризисов и для управления риском. 5) Гарантируется конфиденциальность и интегритет информационных активов при помощи управления доступа к ним с применением необходимых и достаточных ресурсов для их защиты. 6) Повышается международное признание и авторитет предприятия как на внутреннем, так и на международных рынках.

ИНВЕНТАРИЗАЦИЯ РЕСУРСОВ В УПРАВЛЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Анна МИЛОВАНОВА,
Швеция, Стокгольм, Lärcentrum

На сегодняшний день как крупные, так и небольшие организации характеризуются отсутствием четко определенной структуры имеющихся ресурсов, особенно с точки зрения критериев информационной безопасности.

В соответствии с национальным законодательством в автоматизированных системах защищается только информация ограниченного доступа и состояние информационной безопасности определяется критериями конфиденциальности, целостности и доступности ресурсов. Инвентаризация ресурсов в свою очередь позволяет решить ряд важных задач для построения эффективной системы обеспечения информационной безопасности, что доказывает необходимость ее проведения. Также она является одним из главных аспектов в управлении рисками внутренней информационной безопасности.

Важно отметить, что основной целью проведения инвентаризации ресурсов является обеспечение их соответствующей защитой. Проведение инвентаризации ресурсов обеспечивает достижение и следующих целей:

- ведение учета ресурсов и обеспечение уверенности в их защищенности;
- идентификация владельцев и собственников ресурсов, и определение их ответственности;
- идентификация относительной ценности ресурсов для управления рисками организации.

Приступая к инвентаризации ресурсов, необходимо внести определенность и четкость в используемые понятия, то есть обеспечить однозначность представления

используемых понятий руководством организации и различными структурными единицами. Так, ресурс подразумевает совокупность материальных благ принадлежащих одной организации (например, информационные, технические, программные и другие ресурсы, входящие в состав информационных систем).

При проведении инвентаризации необходимо определить критерии выделения категорий ресурсов, подготовить основу для постоянного ведения реестра ресурсов и создать нормативную базу разграничения доступа к ним. Согласно международным стандартам и практикам, среди которых ISO 17799 «Информационная технология. Методики безопасности. Практическое руководство для информационного управления безопасности», выделяют следующие категории ресурсов:

- информационные ресурсы (базы и файлы данных, контракты и соглашения, системная документация, исследовательская документация, руководства пользователей, обучающий материал, рабочие процедуры, планы обеспечения непрерывности бизнеса и т.д);
- программные ресурсы (прикладное, системное, инструментальное программное обеспечение и утилиты);
- физические ресурсы (компьютерное оборудование, оборудование связи, сменные носители и другое оборудование);
- сервисы (вычислительные службы и службы связи, службы общего назначения).

Классификация ресурсов не должна быть слишком сложной во избежание обременительности и неэкономичности, но при этом необходимо учесть все бизнес требования и внутренние требования организации.

Действия, выполняемые в ходе инвентаризации ресурсов, включают следующее:

- определение области проведения инвентаризации, то есть какие будут рассмотрены осуществляемые бизнес-процессы и выполняемые задачи;
- определение и классификация ресурсов (для информационных ресурсов также определение видов информации, таких как входящая, исходящая, хранимая, обрабатываемая информация);
- определение владельцев и собственников ресурсов;
- категорирование ресурсов по критериям информационной безопасности (например, общая информация, информация ограниченного пользования, государственная или коммерческая тайна и тд). Это позволяет выделить наиболее критичные ресурсы, нарушение информационной безопасности которых может привести к ущербу;
- определение субъектов ресурсов, то есть пользователей, которым предоставляется доступ к защищаемой информации (разграничение доступа и полномочий);
- регламентирование способов хранения и защиты критичных ресурсов, а также безопасной работы с ними в случае чрезвычайных ситуаций;
- документирование процесса инвентаризации ресурсов, включая инвентаризационные описи.

Необходимо отметить, что для обеспечения должного управления ресурсами следует руководствоваться следующим:

- ресурсы четко идентифицируются с учетом их относительной ценности и важности, а также с точки зрения критериев информационной безопасности;
- любой ресурс рассматривается с точки зрения технологии создания, обработки, хранения, отправки или приема информации;
- любой ресурс рассматривается с точки зрения разделения его на составные части;
- ресурсы учитываются и закрепляются за ответственными владельцами и/или собственниками;
- определяется ответственность за поддержание соответствующих мероприятий по управлению информационной безопасности, в случае делегирования обязанностей ответственность остается за назначенным владельцем ресурса;
- указывается фактическое местоположение ресурса, так как это является важным моментом при восстановлении ресурсов в случае их потери или повреждения.

Основываясь на полученной информации в результате инвентаризации ресурсов, организация может определить, какая информация должна быть обработана и защищена, то есть обеспечить заданные уровни защиты используемых информационных ресурсов. Это обусловлено тем, что некоторые виды информационных ресурсов могут потребовать дополнительной защиты или специального обращения.

Полученные результаты инвентаризации ресурсов в обязательном порядке должны быть оформлены в инвентаризационных описях по каждой категории ресурсов. После оформления инвентаризационных описей по каждой категории ресурсов составляется единый акт о проведении инвентаризации.

Так например, в инвентаризационных описях для информационных ресурсов рекомендуется отражать следующие параметры:

- вид ресурса (например, база данных, папка или файл);
- наименование ресурса;
- краткое содержание ресурса;
- принадлежность к функциональным подсистемам и прикладным сервисам;
- характер и вид информации;
- место размещения (например, имя компьютера, сервера, диска);
- список пользователей, имеющих доступ к ресурсу;
- размер ресурса;
- необходимый уровень защиты;
- необходимость резервного копирования.

Информационные ресурсы являются базовыми составляющими в части обеспечения управления и информационно-аналитической поддержки функционирования

организации вне зависимости от сферы деятельности. Исходя из этого, общие положения по инвентаризации ресурсов, порядок ведения учета ресурсов, правила формирования реестра информационных ресурсов, порядок сбора, анализа, пересмотра и контроля учетной информации об информационных ресурсах должны определяться внутренней организационно-распорядительной документацией организации.

Таким образом, инвентаризация ресурсов определяет важные сведения, необходимые для обеспечения информационной безопасности автоматизированных информационных систем. А как известно, построение эффективной системы информационной безопасности является одним из наиболее важных условий успешного функционирования любой ИТ-инфраструктуры, что в свою очередь становится критическим фактором успешного ведения бизнеса.

Литература:

1. ISO/IEC 17799:2005 «Информационная технология. Методики безопасности. Практическое руководство для информационного управления безопасности»;
2. www.iso27000.ru;
3. www.itsec.ru.

ОСОБЕННОСТИ ТРАНСФЕРА РЕЗУЛЬТАТОВ НАУЧНО-ТЕХНИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ВУЗА, СОДЕРЖАЩИХ ОБЪЕКТЫ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

О. ПУГАЧЕВА,
Гомельский госуниверситет им. Ф. Скорины (Республика Беларусь)

In article features of a transfer of results of scientific and technical activity of the high school, containing objects of intellectual property are considered, and also the general algorithm of protection of not opened information is resulted

Вузовский сектор Республики Беларусь, обладающий значительным научно-техническим и инновационным потенциалом, играет важную роль в создании экономики инновационного типа. Практика показывает, что новая модель университета как учебно-научно-инновационного комплекса, сочетающего академическую науку с развитой сетью высокотехнологичных инновационных структур и малых предприятий, является одним из наиболее эффективных базовых элементов национальной инновационной системы.

Развитию инновационной деятельности в регионе способствует создание в Гомельском госуниверситете им. Ф.Скорины опытно-промышленных производств абразивного инструмента и полирующих суспензий для полировки пластин полупроводниковых и других материалов, договора на производство и поставку которых

заключены с предприятиями города, Республики Беларусь и России. Созданные в 20 научно-исследовательских лабораториях наукоемкие и конкурентоспособные разработки неизменно вызывают интерес на различных выставках, становятся основой для последующих контактов и переговоров (таблица 1).

Таблица 1

Участие университета в выставках

Годы	Количество выставок, в которых участвовали учреждение и подразделения				Количество экспонатов, демонстрировавшихся на выставке							Количество и стоимость совершенных сделок (контракты, договора, соглашения)			
	всего	в том числе			всего	из них			в том числе			всего	в том числе		
		РБ	РФ	Дальнее зарубежье		Натур. образцы	планшеты	Компьют. техн. и прог. средства	РБ	РФ	Дальнее зарубежье		РБ	РФ	Дальнее зарубежье
2005	16	6	2	8	35	3	2	30	35	24	26	-	-	-	-
2006	17	5	5	11	37	1	2	34	37	30	25	5	1	2	2
2007	17	5	4	8	31	9	3	19	31	25	16	2	-	-	2
2008	17	5	5	4	27	12	3	12	27	23	16	2	-	-	2
2009	16	3	5	8	27	12	3	12	27	23	16	2	-	-	2
2010	14	5	3	6	30	10	4	16	30	23	16	7	1	3	3

В университете функционирует Центр коллективного пользования по экологическому мониторингу и исследованию состава и свойств вещества, способствующий продвижению в реальный сектор экономики разработок, выполненных на основе научных исследований в области технологий микро - и наноразмерных систем, физики и химии полимеров, спектрометрического анализа и исследования экосистем. Университет внедряет результаты научно-технической деятельности в производство и в учебный процесс (таблица 2).

Таблица 2

Использование научных разработок университета

Годы	Использование научных разработок		
	в народном хозяйстве	в учебном процессе	
		акты внедрения	издание монографий, учебников и учебных пособий
2005	12	64	320
2006	6	25	197
2007	-	131	256
2008	7	96	214
2009	6	131	157
2010	15	275	153

Анализ состояния и развития системы управления инновационной деятельностью в университете в 2005-2010 годах показывает стабильный рост основных показателей оценки результатов научно-технической и творческой деятельности, что связано с достаточно работоспособной системой управления инновационными процессами в вузе. Об этом также свидетельствуют данные, характеризующие число поданных заявок и полученных патентах на объекты промышленной собственности (таблица 3).

Таблица 3

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

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

Трансфер технологий накладывает на его участников определенные обязательства, связанные со знанием норм и правил общения с объектами интеллектуальной собственности (объектами авторского права и ОПС), а также с практическими навыками их применения в конкретных ситуациях. Важным элементом успешного осуществления научно-технической деятельности вуза является охрана нераскрытой (конфиденциальной информации) или коммерческой тайны.

Основными каналами утечки сведений, содержащих коммерческую тайну, являются: любые формы сотрудничества; партнеры по совместным работам; экспонирование на отечественных и зарубежных выставках и иные формы рекламы; передача документации и образцов устройств, веществ, компьютерных программ, ноу-хау, результатов НИОКР партнерам; публикации в отечественных и зарубежных изданиях; договоры о выполнении НИОКР, договоры подряда; участие в конференциях и семинарах в стране и за рубежом; участие в конкурсах на получение грантов от иностранных и отечественных фондов; деятельность сотрудников вузов или иных научных организаций в качестве сотрудников или консультантов иностранных или отечественных исследовательских центров и предприятий; пребывание в лабораториях вуза специалистов зарубежных фирм, в том числе командированных, стажеров, аспирантов и студентов; предоставление сведений о лучших разработках вузов по запросам различных министерств, ведомств, ассоциаций, фирм, предприятий, фондов; плохая организация учета, хранения и прохождения документов, образцов, других носителей информации; обиженные сотрудники и др.

Общий алгоритм защиты нераскрытой информации может быть сведен к следующему: определение объекта защиты; выявление угроз и оценка их вероятности; оценка возможного ущерба; анализ эффективности применяемых мер защиты (физическая безопасность документации, надежность персонала, безопасность используемых для передачи информации каналов связи); определение

необходимых мер защиты (организационных, финансовых, юридических); внедрение дополнительно принятых мер защиты с учетом установленных приоритетов, доведение до персонала организации реализуемых мер, осуществление контроля; мониторинг и корректировка внедренных мер целью анализа работоспособности созданной системы безопасности информации.

МЕТОД ВЫЯВЛЕНИЯ ИНСАЙДЕРСКОЙ ДЕЯТЕЛЬНОСТИ

С. КАВУН, И. СОРБАТ,
Харьковский национальный экономический университет (Украина)

Актуальность. Предприятия и организации, банковские и финансовые учреждения, IT-компании разных стран Европы, США, России и Украины несут огромные финансовые потери вследствие экономической преступности и халатности сотрудников организаций, так называемой инсайдерской деятельности. Следовательно, возникает необходимость решения актуальной задачи выявления инсайдера или группы инсайдеров (инсайдерской деятельности), ответственных за утечку определенных категорий конфиденциальных данных в организации (на предприятии).

Над проблемами в данной сфере работают многие известные специалисты и ученые: Верин В.П., Гуров М.П., Олейников Е. А., Кизим М.О., Куркин Н.В., Шкарлет С.Н., Кавун С.В. и др. [1-8] В их работах были исследованы вопросы систематического подхода для устранения угроз информационной и экономической безопасности, но в большей части эти исследования касаются внешних угроз. Не до конца решенным остается вопрос внутренних угроз, и, как следствие, вопрос выявления (обнаружения) инсайдеров.

Целью статьи является представление нового метода, который позволит решить задачу выявления инсайдеров (инсайдерской деятельности) в организации (на предприятии).

Основной материал. По результатам анализа отчетов аналитических компаний – предлагается разделить предприятия и организации, в которых произошли обнародованные утечки на три категории: государственные учреждения, коммерческие предприятия, а так же учебные заведения и общественные не коммерческие структуры, для которых рассчитаны распределения источников утечек по видам организаций (табл. 1).

Для определения наиболее важных данных, подвергшихся утечке, выделено три основные категории конфиденциальной информации: персональные данные, государственная и коммерческая тайны. Подавляющее число инцидентов (90-98%) за весь период наблюдений охватывают персональные данные, что затрудняет выделение тенденций. Также получены распределения утечек по типам конфиденциальных данных (табл. 2).

Таблица 1

Распределения источников утечек по видам организаций

№	Вид организаций	1 полугодие 2009		1 полугодие 2010	
		Кол-во	%	Кол-во	%
1	Коммерческие	265	64,2	296	73,8
2	Государственные	88	21,3	61	16,0
3	Образовательные и не коммерческие	43	10,4	127	8,1
4	Не установлено	17	4,1	8	2,1

Таблица 2

Распределения утечек по типам конфиденциальных данных

№	Тип конфиденциальных данных	1 полугодие 2009		1 полугодие 2010	
		Кол-во	%	Кол-во	%
1	Персональные данные	360	87,2	374	97,9
2	Коммерческая тайна, ноу-хау	12	2,9	2	0,5
3	Государственная и военная тайна	9	2,2	2	0,5
4	Другая конфиденциальная информация	28	6,8	4	1,0
5	Не установлено	4	1,0	0	0

Полученные результаты анализа позволяют предложить новый метод выявления инсайдерской деятельности, который основывается на использовании некоторой совокупности критериев (признаков) – $\{p_i\}$, по которым можно выявить инсайдеров причастных к утечке данных в организациях. Для этого необходимо построить матрицу критериев (признаков) $P = \{p_i\}$.

Выводы. Общее число утечек продолжает оставаться на уровне примерно 2 инцидента / сутки. При этом имеются основания полагать, что количество скрытых утечек столь же велико, как и количество обнародованных, а, возможно, и существенно превосходит их. В государственных и негосударственных, коммерческих и некоммерческих организациях должны использоваться одинаковые методы выявления мошенничества и защиты от утечек данных.

Для дальнейшего исследования предлагается построить новый критериальный метод выявления инсайдеров применив разработанный авторами статьи специальный подход системы фильтрации, а так же его формализация в математическом виде.

Литература:

1. Верин В.П., Преступления в сфере экономики. - М., Дело.2002.
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 "Эконо-

мика: 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. Гуров М.П., Кудрявцев Ю.А. Теневая экономика и экономическая преступность в вопросах и ответах: Учебное пособие. - СПб.: Санкт-Петербургский университет МВД России, 2002. - 237 с.

ФОРМИРОВАНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТОРГОВОЙ КОМПАНИИ

С. В. КАРПЕНКО, Е.В. ПРОКОФЬЕВА
Белорусский торгово-экономический университет потребительской кооперации (Гомель, Республика Беларусь)

В сфере информационных технологий растет объем предложений по обеспечению безопасности информационных систем. Действия служб, направленные на повышение уровня информационной безопасности, не приносят доходов, но с их помощью можно уменьшить потери от возможных инцидентов.

Потребности организации в некотором уровне защищенности автоматизированной системы можно определить, воспользовавшись руководящими стандартами СТБ 34.101.1 - 2001(ИСО/МЭК 15408-1-99), ("Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий").

Требования к автоматизированным системам защиты обобщены в таблице 1, где выполнен анализ системы защиты информации, условно состоящей из следующих четырех подсистем: подсистема управления доступом; подсистема регистрации и учета; криптографическая подсистема; подсистема обеспечения целостности.

Таблица 1

Требования к автоматизированным системам защиты

Подсистемы и требования	Класс 3	Класс 2	Класс 1

Анализ данных таблицы и сопоставление ее характеристик с реальными характеристиками технологий и программных продуктов предприятия позволяет говорить о принадлежности корпоративной информационной системы компании к 1 классу и отметить достаточно высокий уровень соответствия.

При этом отмечен ряд недостатков системы. Они определяют направления совершенствования системы защиты организации. Даны рекомендации для развития 4-х перечисленных подсистем.

Для совершенствования информационной системы «Алеси» на основе разделения доступа к информационных ресурсам выполнено категорирование информации**. Использованы два подхода:**

1. Категорирование безопасности информации и информационных систем на основе оценки ущерба
2. Категорирование безопасности информации и информационных систем с точки зрения критичности.

Представлены результаты, внедренные в практику работы Алеси.

Проведенное категорирование информации для информационной системы «Алеси» позволило выполнить разделение прав доступа к информационным ресурсам корпоративной системы.

Формирование прав доступа для пользователей и групп пользователей ОАО НТК «Алеся» находится в состоянии разработки. Рассмотрены направления их совершенствования, а также вопросы администрирования программного комплекса «SBC - предприятие» в данном аспекте.

Распределение доступа к основным группам электронных документов. В ОАО НТК «Алеся» авторизованными субъектами являются все работники предприятия, которые имеют в своем распоряжении ПК. Механизмы управления доступом субъектов к объектам информации выполняют основную роль в обеспечении внутренней безопасности компьютерных систем. Их работа строится на концепции единого диспетчера доступа. Сущность этой концепции состоит в том, что диспетчер доступа (монитор ссылок) - выступает посредником-контролером при всех обращениях субъектов к объектам. Схема работы механизма разграничения доступа к информационным ресурсам включает: правила разграничения доступа, диспетчер доступа, субъекты доступа (работники предприятия), объекты доступа (папки с документами, электронные документы).

Диспетчер доступа обязан выполнять следующие основные функции:

- проверяет права доступа каждого субъекта к конкретному объекту на основании информации, содержащейся в базе данных разграничения доступа хранящейся на главном офисном сервере ОАО НТК «Алеся»;
- разрешает (производит авторизацию) или запрещает (блокирует) доступ субъекта к каталогу, документу;
- при необходимости регистрирует факт доступа и его параметры в системном журнале (в том числе попытки несанкционированного доступа с превышением полномочий).

Основными требованиями к реализации диспетчера доступа являются:

- полнота контролируемых операций (проверке должны подвергаться все операции всех субъектов над всеми объектами системы, - обход диспетчера предполагается невозможным);

- изолированность диспетчера, то есть защищенность самого диспетчера от возможных изменений субъектами доступа с целью влияния на процесс его функционирования;

Форма представления базы данных защиты может быть различной.

Основу базы данных средств разграничения доступа в общем случае составляет абстрактная матрица доступа или ее реальные представления. Каждая строка этой матрицы соответствует субъекту, а столбец - объекту АИС.

Разработана матрица распределения доступа к основным группам электронных документов для сотрудников ОАО НТК «Алеся», представленная в виде таблицы. По вертикали 13 субъектов, по горизонтали 9 объектов. На пересечении – варианты доступа: полный доступ, чтение, нет доступа, создание.

Представлены права для следующих категорий пользователей: 1) администратор баз данных или администратор системы (инженер программист), 2) пользователи 1-го уровня доступа (бухгалтер, экономист, сотрудники коммерческого отдела; товароведы; работник строительной группы; сотрудник инженерной службы финансист; специалисты отдела кадров; ревизионной службы и т.д.), 3) пользователи 2-го уровня доступа (начальники всех отделов; кассиры торговой сети; заведующие магазинами; генеральный директор; операторы терминалов).

Предложены возможные сценарии работы по разграничению прав доступа группам пользователей к информационным ресурсам АИС «SBC - предприятие».

Администратор баз данных может создавать, копировать, читать, и удалять электронные документы. Факт удаления электронного документа должен быть отражен в регистрационном журнале.

Систему санкционирования доступа целесообразно строить на основе структурно-функционального (задачного) подхода к разделению всего множества защищаемых ресурсов АИС. Отдельная задача должна описывать все используемые при ее решении ресурсы (файлы, каталоги, таблицы БД и т.п.), все категории пользователей (роли в задаче) и права доступа для каждой такой категории к ресурсам задачи. Описания задач в виде формуляров должны формироваться с участием специалистов по сопровождению данных задач и системных администраторов (администраторов баз данных) и могут храниться в архиве эталонных дистрибутивов программ.

Полномочия руководителей отделов давать разрешения на допуск к решению тех или иных задач должны быть закреплены решениями (приказами) высшего руководства организации. Как правило, задачи закрепляются за конкретными подразделениями, а права допуска сотрудников этих подразделений к ресурсам этих задач предоставляются руководителям подразделений.

Важно, чтобы затраты на создание и поддержание безопасности информационных систем и её уровень были соизмеримы.

SECURITY MODULES IN BI SYSTEMS FOR BULGARIAN MUNICIPALITIES

Rosen KIRILOV, Katia STRAHILOVA,
University of National and World Economy (Sofia, Bulgaria)

Bulgaria is a parliamentary republic with local government. The main administrative territorial unit in which local self-government is the municipality. The territory of Bulgaria is divided into 28 districts and 264 municipalities. To improve its activities municipalities must collect, interpret and use data to maximum benefit, and in ensuring maximum security. It is well municipalities to invest in developing business intelligence systems.

In designing the concept of building a business inteligeltni systems for municipal revenue administration, and security modules to them, it is necessary to embed the highest degree of analytical complexity. Such a system would have the following logical architecture (fig. 1):

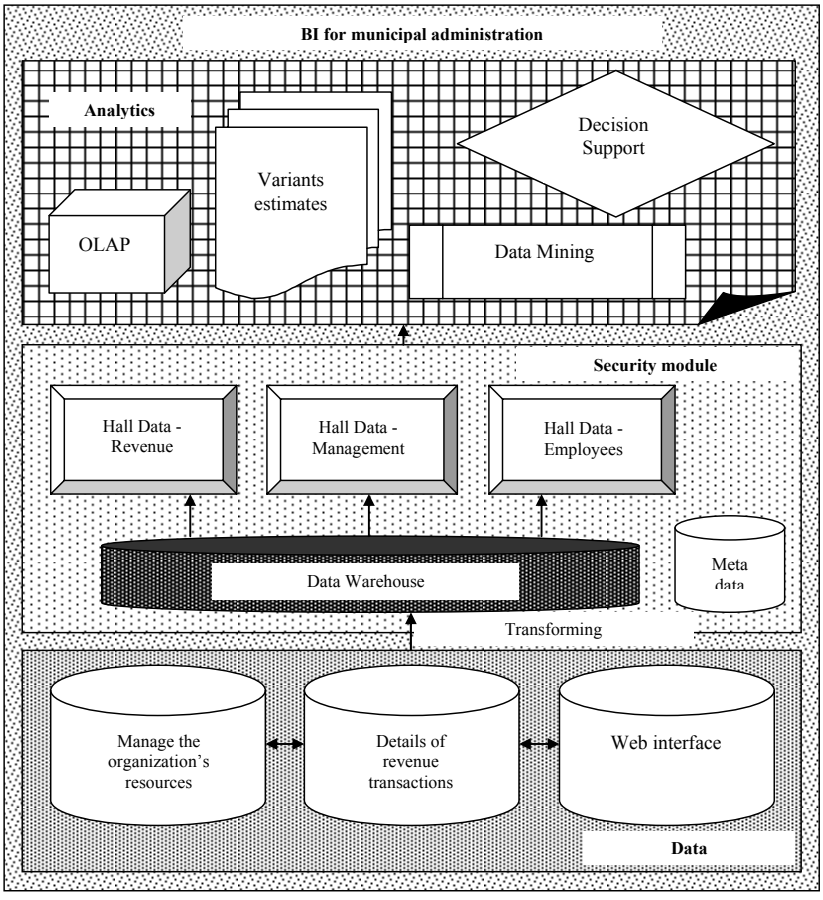


Fig. 1. **BI architecture for municipal administration with security module**

- ***Data Warehouse.*** It is a specialized database or repository of data written to provide job applications to support processes for decision making, ranging from those for regular accounts and inquiries to complex optimization. Data warehouse is constructed with methods, mainly metadata extraction, transformation and loading data;
- The halls are data repositories of information on a specific topic or a specific department (eg property tax);
- ***Business Analytics.*** It provides a large number of software tools that allow users (employees of Revenue Administration) to prepare reports and queries on demand and to analyze the data. They are known as online analytical processing (OLAP). Through these means can be analyzed different dimensions of multidimensional data, time series analysis of trends, ie can quickly and easily identify trends, using a staggered analysis of information and graphics capabilities of products, ensuring the complex data analysis and with integrated capabilities of calculated fields;
- ***Data Mining***. Mining data from a class analysis of information in databases that look for hidden patterns in data group, but can also be used to predict future behavior. It may be developed variants of local budgets. Sometimes the term is misused by connecting only with the possibility of presenting data in new ways, but the real software to extract regularities from the data not only changes the presentation, but really unknown until discovered relationships between data. Subsequently, this knowledge is used in making decisions and achieving certain goals. These instruments are used to reinforce human activity by scanning the large stores of data to detect meaningful new correlations, patterns and trends, using technology to recognize patterns and contemporary statistics;

In this material we define seven principles to consider when developing a strategy for reducing risks to critical information infrastructure:

1. Municipalities should have emergency warning networks regarding cyber vulnerabilities, threats, and incidents.
2. Municipalities should raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures, and the role each must play in protecting them.
3. Municipalities should examine their infrastructures and identify interdependencies among them, thereby enhancing protection of such infrastructures.
4. Municipalities should promote partnerships among stakeholders, both public and private, to share and analyze critical infrastructure information in order to prevent, investigate, and respond to damage to or attacks on such infrastructures.
5. Municipalities should create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.
6. Municipalities should ensure that data availability policies take into account the need to protect critical information infrastructures.
7. Municipalities should facilitate tracing attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other municipalities.

The results of the experimental part of this study allow to conclude that municipalities in Bulgaria to comply with laws regarding the budget process and its stages. In this sense, the proposal to build a business intelligence system in a municipal administration would allow much easier budget planning based on operational data. It will also enable the creation of optimistic and pessimistic versions of local budgets, and assist in decision making.

ABOUT CERTAIN VULNERABILITIES OF PSEUDO-M-ROUTERS

Maciej SZMIT
Computer Engineering Department of
Technical University of Lodz (Poland)

This article provides the results of the tests carried out on two models of inexpensive network devices (called „routers", though their functions go beyond the range of the meaning of this term), which are designed for the use in home networks and shows potential dangers which can result from non-standard behaviour of these machines.

Introduction

When the issues regarding network computers are discussed, it is sometimes mentioned about certain incoherency, which takes place between reference model ISO/OSI assumptions and the particular network protocols, and between the network protocols and their specific hardware or software implementations. However, the subject does not attract much attention, especially in the publications on network traffic engineering, which in many cases satisfy themselves with providing information on simplified models[1] and conducting, on their base, computer simulations. Meanwhile, although the ISO/OSI reference model is thirty years old[2], and the basic of the TCP/IP stack protocols came into being more or less at the same time[3], the implementation of the rules and algorithms they provide leave a lot to be desired, causing unforeseen behaviours of their software or hardware. In practical solutions such unforeseen or non-typical behaviour of a specific device can usually lead to its

---

[1] Model means „simplified reflection of a phenomenon, system, process etc., (. . .), schematic presentation of a fragment of reality, where the insignificant parts are omitted to allow a better explanation of the operation, form or structure of the fragment" [Błaszczuk 2006] s.21. "Model is a depiction of a theory or causal situation, which is assumed to generate the data being observed" [Kendall, Buckland 1986] page 102. "Model (…) is a formal mathematical notation of regularities (…) occurring in the reality" [Witkowska 2005] page 28.

[2] The origin date for the model is considered to be the year 1977, while its present standard was formed in [ISO 7498-1:1994] standard.

[3] [RFC 791] and [RFC 793] are dated 1981

replacement (usually produced by a different vendor); only single cases of such strange behaviours happen to be investigated and characterized in professional publications[1]. Yet reliability, which means the capability of the functional unit to perform a required function in the defined environment and in the defined period of time[2], is one of the safety attributes of computer systems[3]and the information.

Multicast frames and packets

In the article [Szmit, Tomaszewski 2007] we presented non-standard behaviours of the router-switch devices from D-Link and Lucent with respect to frames addressed with Ethernet multicast. In the case of receiving frames with Ethernet multicast as designation MAC-address, - apart from sending multicast frames to their ports – they made a peculiar routing by sending additionally a packet in the frame with unicast designation address, whereas the receiver's frame MAC address was the MAC address of the computer, of which IP was contained in the packet that was carried by the frame. Interestingly, router-switch was sending both of the frames to all of its ports including the one, from which received the multicast frame (Figure 1), therefore its operation is something between operation of a classical switch (which should send the multicast frame to all ports like a hub and an m-router) or a switch with IGMP-snooping handling technique, which should send it to appropriate address, that is to the multicast group members). In the case of using in the packet IP broadcast address, unicast frames with broadcast destination address packet were forwarded by the devices to the particular computers in the network.

In this article, within the scope of this research, two behaviours of today's (in sale in 2011) devices of cable and wireless routers Edimax BR-6314K and Belkin F5D7234-4-H V5 has been tested. Both devices are equipped with four RJ-45 ports dedicated to a LAN and one port dedicated to a WAN, besides the Belkin router has also got WLAN 802.11. Both contain a series of functions, among others 2nd ISO/OSI layer switch, router with Network Address Translation and firewall in the architecture of screening router with statefull packet inspection and webpages URL filtering.

---

1 It is worth mentioning two articles here: [Mogul 2003] in which the Author analysed the dangers connected with the use of the technique of TCP Offloading Engine; among other things, in workstations, in which the driver is delivered by the manufacturer of the equipment supporting TOE, it does not have to properly work with some other – for example those changed in the installation process of patches – versions of the systems libraries serving TCP/IP protocol stack and [UoBC 2004], where two case studies are described connected with problems caused by non-standard service of the multicast by switches. One of them concerned Norton Ghost program using one of the agents applying IGMP ver. 2, which hung up in the presence of the switches applying IGMP-snooping for IGMP ver.3, the second – over-intelligent switch applying PIM (of what wasn't aware his administrator), which won the process of choosing of the designated router PIM, that caused the redirection of the multicast traffic to improper network and in consequence blocking all of the services in the corporate m-internetwork operating with the basis of multicasts

2 PN-ISO/IEC 2382-14:2001 – 14.01.03

3 Compare against [Korzeniowski 2008] p. 133, [Jašek, Dolejšová, Rosman 2007] p. 21.

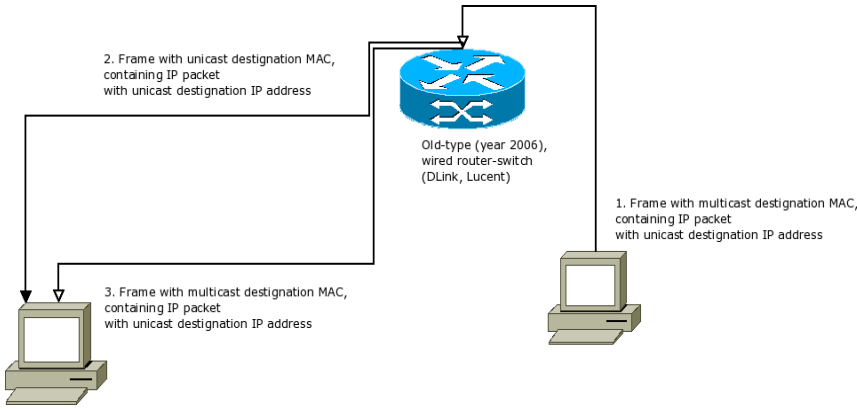


Figure 1. **Handling of Ethernet multicast by pseudo-m-router-switches. By [Szmit, Tomaszewski 2007].**

Results

Both routers behave in a different way than previously tested devices, however still not quite properly. Handling of the packets with broadcast destination addresses has been improved: multicast frames containing broadcast destination addresses are simply passed on to other ports without any changes.

In the case of Belkin router the change of multicast to unicast MAC address take place only on the WAN interface. The LAN interfaces do not handle multicasting at all. (i.e. do not forward any frames or packets contained in them). So possible problems concern two situations: the trial of using the router as a m-router (what will not succeed) and the possible malicious attempts of the user, who has access to the WAN interface. In the last case still one more oddity needs to be taken into consideration regarding this router: if the multicast frame carries a packet with a random source IP address, even out of either inner or outer network, it will also be passed forward (i.e. as a unicast frame with the proper destination address it will get to the WAN). Moreover, sending such a frame from the multicast MAC address source will cause change of address into the MAC of the router interface (see Figure 2). This is then an alternative of the Source Network Address Translation.

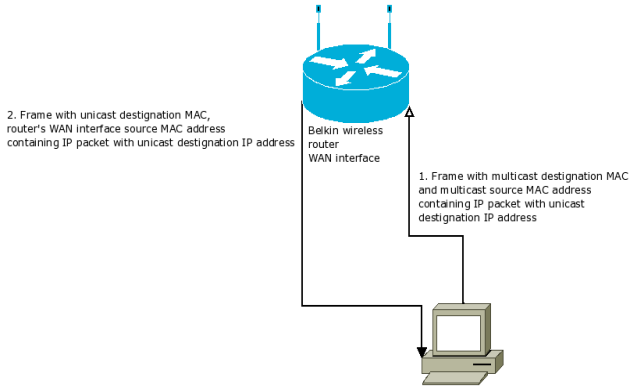


Figure 2. **Handling of Belkin router. Source: own study.**

This kind of behaviour could be risky, since it enables in certain cases fairly effectively committing of an attack being something between a Smurf attack and a Distributed Denial of Service with Reflection (DRDoS). In particular in amateur networks, in which individual home networks are connected to the Internet Service Provider with this type of access devices (see Chart 3).

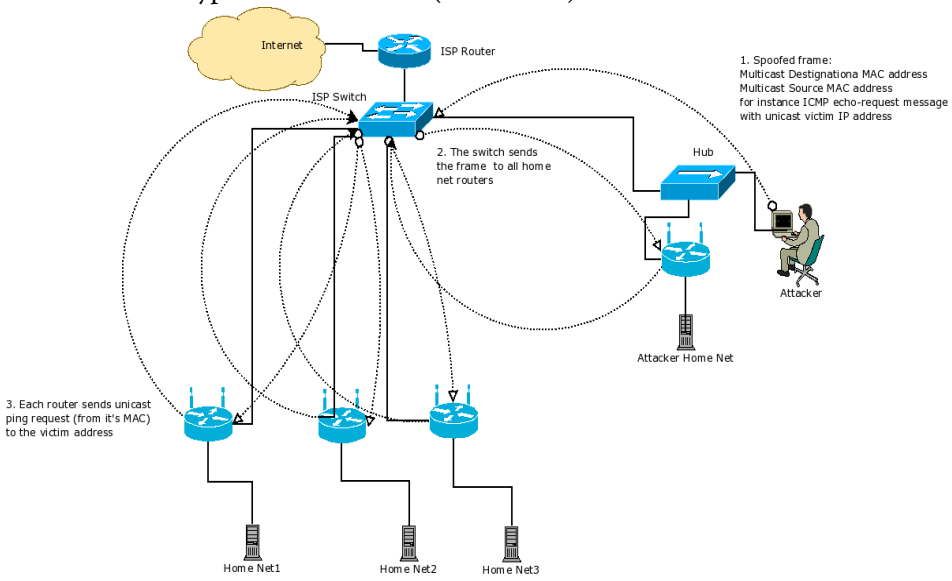


***Figure* 3. Scheme of attack. Source: own study.**

The attack scenario proceeds as follow:

1. The attacker places in the network the multicast frame (with the multicast MAC addresses of a sender as well as a receiver), containing the packet (with one of the routers or the computers from one of the others from the home networks), launching an attack, (in the figure it is one of the ICMP echo request, but it might as well, for instance, be the TCP SYN, if the attacker intends to carry the SYN-flood type of attack).
2. The frame is sent via the switch to all the users of the provider's connected networks.
3. Each of the routers „corrects" the frame giving it its own source MAC address, destination MAC of the Internet Access Gateway installed by the provider and leaving the IP address of the routers or computers from one of the home networks (what allows to avoid their possible filtering by the firewall of the Internet provider). In this way it will be multiplied.
4. Even in the case of possible traffic logging on the provider's side there will only be information, that few routers sent a packet from beyond its own network. Without a 3rd layer switch, i.e. the device, that analyses and filters incoming packets (according to the IP address) and frames (according to MAC address) on each of its ports, there will be no chance to reveal the perpetrator of the

attack. Routers of the home network will then serve the role of something halfway between the reflector of the DRDoS attack and an amplifier of the Smurf attack (efficiently hiding the source of the carried attack).

The EDIMax router, similarly to the Belkin router has an improved handling of the broadcast packets contained in the multicast frames, while in the case of the multicast frames carrying the unicast packets it comes up their duplication: apart from the original frame, – created by the router – the frame with the unicast receiver address is transferred. This is even, when the router is connected to the switch, where such a frame appears (the router „ping-pongs back" two frames to the switch). Theoretically it could happen – similarly like in the previous examples – serve to boost the Smurf type attack. In practice this could also be used for detection of the presence of such a device in the network.

References:

1. [Błaszczuk 2006] Błaszczuk D.: Wstęp do prognozowania i symulacji, PWN, Warszawa 2006
2. [ISO 7498-1:1994] ISO 7498-1:1994 Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model
3. [Jašek, Dolejšová, Rosman 2007] Jašek R,, Dolejšová M., Rosman P.: Informační technologie ve veřejné správě, UTB, Zlín 2007
4. [Kendal, Buckland 1986] Kendal M. G., Buckland W. R.: Słowik terminów statystycznych, PWE, Warszawa 1986
5. [Korzeniowski 2008] Korzeniowski L. F.: Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych, EAS, Kraków 2008.
6. [Mogul 2003] Mogul J. C.: TCP offload is a dumb idea whose time has come, Proceedings of the 9th conference on Hot Topics in Operating Systems - Volume 9, http://www.usenix.org/events/hotos03/tech/talks/mogul_talk.pdf
7. [RFC 791] Postel J. (ed.): Internet Protocol, Defense Advanced Research Projects Agency, Information Processing Techniques Office, 1981, http://www.rfc-editor.org/rfc/rfc791.txt
8. [RFC 793] Postel J. (ed.): Transmission Control Protocol, Defense Advanced Research Projects Agency, Information Processing Techniques Office, 1981, http://www.rfc-editor.org/rfc/rfc793.txt
9. [Szmit, Tomaszewski 2007] Szmit M., Tomaszewski M: Huby w pajęczynach i złośliwe m-routery [in:] „Hakin9" Nr 1/2007, s. 36-41
10. [UoBC 2004] Multicast on the LAN, Multicast Workshop. University of British Columbia. Vancouver, BC. May, 2004, http://andrew.triumf.ca/AG/multicast/internet2-multicast-workshop-may-2004-2-LAN- SSM.pdf
11. [Witkowska 2005] Witkowska D.: Podstawy ekonometrii i teorii prognozowania, Oficyna ekonomiczna, Kraków 2005

SECURITATEA REȚELELOR DE INFORMARE

Mădălina MATEI (NIȚOIU)
Academia de Studii Economice din București (România)

Social innovation requires research regarding the profit potential of human interaction, in various settings and information environments. Throughout networking processes, the added value of information, together with organizational skills and methods brought into the system helps render a more efficient governance control of the national security systems. Previous studies showed the influence of social networks on political and business systems as well as the need to create intelligent social structures, in order to foster innovation and competitive advantage. This paper examines the intelligence network concept and methodological issues contained in the structure design processes.

***Keywords**: Intelligence networks, network theory, methodology, innovation.*

Introducere

Teoria rețelelor de informare a apărut în ştiințele sociale, împreună cu creşterea gradului de conştientizare cu privire la rolul de cunoştinţe în sustenabilitatea sistemelor. În acest articol este prezentat conceptul de rețele de informații, în scopul de a explica şi a avansa un nou cadru pentru abordarea proceselor de luare a deciziilor pentru securitatea națională.

Obiectivele principale sunt următoarele:

1) pentru a stabili rolul de abordare informații în mediul de securitate contemporan. Prin urmare, în prima parte a acestei lucrări voi sintetiza cercetări în teorie, inteligență şi voi justifica efectul de pârghie a acestei abordări în ceea ce priveşte politica de securitate națională;
2) de a introduce factorii de decizie cu elementele şi metodologiile proceselor de informații. Partea a doua a lucrării va descrie cicluri vechi şi noi de inteligență, şi va contura, de asemenea, avantajul de a dezvolta procese de informații privind structurile de rețea,
3) şi, în final, pentru a duce mai departe această teorie am introdus o nouă metodă care să îmbunătățească procesele de informații. Astfel, în ultima parte a lucrării, voi da un exemplu de luare a deciziilor de informații şi fluxul de lucru, prin intermediul structurilor matematice numit metagrafuri.

Cercetătorii în general au recunoscut faptul că unitățile în sistemul global contemporan se comportă ca structuri de prelucrare a informațiilor. Mai mult, conexiunile între societățile interioare sunt deservite prin fluxuri informaționale şi structuri menite să avertizeze împotriva schimbărilor de mediu. Astfel, apariția analizei de rețea în luare deciziilor rămâne extrem de legată de necesitatea evaluării riscurilor şi minimizării incertitudinii. Valoarea predictibilității unui sistem îşi are izvorul în unitățile specializate prin capacitatea de a colecta, de a înțelege, şi de a gestiona informațiile.

Lucrarea de față este susținută de studiile anterioare în teoria inteligenței şi preocuparea cercetătorilor contemporani cu privire la nevoia de a reforma gândirea inteligenței şi organizațională. De asemenea, datorită evoluțiilor recente în teoria grafurilor, suntem în posibilitatea de a aborda aspectele metodologice.

Cercetări în teoria inteligenței

Teoria inteligenței s-a născut la începutul erei Războiului Rece, când sporirea sectorului energetic național a fost principalul obiectiv al Guvernului SUA. Toate cele trei valori combinate au produs un sistem de informații care a oferit baza pentru cursurile de acțiune care trebuie luate pentru a asigura securitatea națională şi puterea. Abordările contemporane sunt aduse de Berkowitz şi Goodman (2000), Herman Michael (2001), Gregory Treverton F. (2001), Johnson Loch (2003) şi alții, toate acestea pentru a crea metodologii adecvate, şi pentru a umple golul în teoria inteligenței.

Deşi, mediul conflictual, cerințele pentru comunitate şi calitatea tehnologiilor au evoluat, cea mai importantă reformă trebuie să abordeze procesul de inteligență. Autori încep prin a susține că vechiul ciclul de inteligență nu mai poate răspunde la provocările care provin de la agenții de rețea, fie pentru că fluxul de lucru în cadrul comunității de informații este ineficient, fie pentru că bugetul nu acoperă cheltuielile. După cum au arătat studiile recente, opinia publică americană îşi exprimă nemulțumirea față de cheltuielile bugetare pentru securitatea națională. Prin urmare, se poate anticipa că alocările bugetare viitor, ar putea fi atât de redusă, astfel încât actuala conducere nu va fi în măsură să susțină acest proces.

În ultimii ani, sistemele de informații au apărut în afara cadrului guvernamental şi în afaceri şi în domeniul social. Unitățile de informații similare cu comunitățile de informații din interiorul aparatului guvernamental au preluat sucursalele prin gestionarea companiilor şi organizatiilor. Un accent deosebit se pune pe sistemul Open Source Intelligence (OSINT). Robert David Steele – fondator al Open Source Solutions Inc - explică de ce sursele deschise sunt cele mai adecvate instrumente în viitorul inteligenței. Potrivit argumentației sale, "OSINT este unic şi cel mai potrivit pentru sprijinul operațiunilor de securitate națională, deoarece OSINT se bazează exclusiv pe informațiile şi expertizele obținute prin mijloace legale şi etice".

Un alt aspect larg discutat este identificarea actorilor relevanți pentru a forma o rețea eficientă. Teoreticienii sunt de acord că agențiile de informații din interiorul aparatului guvernamental trebuie să colaboreze cu oamenii de afaceri, cu organizațiile non-guvernamentale şi cu cetățenii, în scopul asigurării nevoilor de resurse informaționale. Două motive stau la baza acestui argument: primul se referă la accesibilitatea la informațiile obținute din surse deschise şi la calitate analitică a produselor; al doilea se referă la prețul de informațiilor obținute din surse deschise, care generează servicii de informații avantajoase din punct de vedere financiar.

Cu toate acestea, acest salt evolutiv trebuie să fie susținut cu reforme educaționale şi politici publice care promovează strategii de învățare şi capacități adecvate la nivel de cunoaştere a societății. Rețelele de informare au potențialul de a conecta actorii publici, actorii privați şi cetățenii într-o relație de cooperare, pe baza identităților comune şi a intereselor comune.

Sisteme inteligente

În zilele noastre, dezbaterea privind inteligența s-a deplasat în arenele ştiințelor sociale şi politice. Deşi există o anumită detaşare de la gândirea matematică, cercetătorii sunt încă obligați să recurgă la modele matematice, în scopul de a defini şi a organiza aceste procese.

Oricât de eficient şi revoluționar pot fi tehnologiile de comunicare în masă, utilizarea lor a modificat proprietățile sistemului social global. Flexibilitatea în transmiterea de informații, facilitățile în transportul persoanelor sau a bunurilor, accesul la tot felul de produse, au creat un mediu incert pentru persoane fizice şi subsisteme, sau ceea ce se numeşte, în general, societatea de risc. În această etapă, cercetătorii au apelat la algebra liniară pentru a găsi modele adecvate în explicarea câtorva din tendințele din societatea contemporană.

Una dintre ele este crearea de rețele sociale. Utilitatea de a studia crearea şi compoziția de rețele sociale constă în anticiparea relațiilor, intereselor şi fluxurilor informaționale (Basu şi Blanning).

În comunitățile de informații, rețelele explicative şi anticiparea impacturilor modelor cu privire la politicile de gestionare a informațiilor pentru securitate națională. Rețelele sunt importante pentru specialişti, pentru că ele constituie morfologia care stă la baza organizațiilor teroriste, a lanțurilor de crimă organizată, a războiului din spațiul cibernetic şi a altor amenințări de securitate.

Transformările profunde din mediul de informații prevăd stimulente serioase pentru factorii de decizie politică pentru a susține reforma inteligentă a organizației. Potrivit Berkowitz şi Goodman, organizațiile trebuie să devină mai flexibile şi să permită configurarea unor echipe de lucru. Mai mult, autorii să enunțe avantajele acestui nou model, după cum urmează: spre deosebire de modelul tradițional, o echipă descentralizată include trei tipuri de analişti - analiştii, care sunt legați de utilizatori şi plătiți de ei, "analiştii super" responsabili pentru alocarea resurselor şi de comunicare cu consumatorii, şi analiştii de specialitate din sectorul privat. Mai mult decât atât, având în vedere morfologia noii rețele, structura organizatorică este mai fluidă. Analiza produselor este diseminată direct către utilizatorii finali, fără a trece prin procesul de control al calității.

Noua echipă este întotdeauna pregătită să furnizeze în timp util produsele analitice, în cazul unor sarcini neaşteptate care apar. În cele din urmă, managerii recrutează contractori part-time, în scopul de a se integra într-o echipă ori de câte ori apare o cerință. (Berkowitz şi Goodman).

Interacțiunea permanentă între factorii de decizie şi personalul de informații, de-a lungul intregului proces de inteligență, este recomandat de către teoreticieni.

În primul rând, relațiile dintre şi în interiorul echipelor nu sunt direcționate, aducând lipsa de informații cu privire la funcțiile îndeplinite de fiecare element din sistem. În al doilea rând, echipa virtuală nu poate fi folosită pentru a identifica relațiile critice şi pentru a evalua eficiența acestuia.

În ultima parte a lucrării, folosim o nouă metodologie pentru procesul de inteligență avansat, prin introducerea metagrafurilor ca structuri matematice capabile de a capta modelele atributelor conectivității sistemelor de inteligență.

Metodologia modelului de bază

Cerințele metodologice pentru sistemul de informații au venit din două direcții. Din perspectiva internă, inteligența de process a avut loc în interiorul organizațiilor de informații cerut de restructurare, întrucât problemele schimbat atât de radicale şi designul traditional birocratic nu mai era eficient. Problemele de comunicare între şi în inte-

riorul agențiilor, între consumatorul de inteligență şi analişti, între analişti şi colectorii de informații, a indus ideea că este nevoie de un model de planificare mai complex. De asemenea, aspectele metodologice de rețea oferă o a doua perspectivă de structura şi funcțiile sistemelor de pericol din mediul global. Flexibilitatea reței ar putea fi rezolvată printr-o bine-cunoscută problemă de cursuri asimetrice de acțiune în situații de conflict.

Modelele de construcție de rețea, precum şi procesele de destabilizare a rețelei sunt problem foarte dezbătute, cu consecințe în diverse domenii de luare a deciziilor. Astfel, utilitatea metodologiei de creare a rețelelor poate fi observateă în ceea ce priveşte modelul de gestionare, procedurile de organizare a fluxului de lucru, şi de datele şi sarcinile de gestionare a statului (Basu şi Blanning, 2007). Pe de altă parte, destabilizarea rețelelor de discuții îşi găseşte înțelesul său în problemele de securitate apărute în ultimele decenii.

Din punct de vedere al inteligenței, aceste două perspective oferă stimulente pentru tratarea problemelor legate de securitate națională, bazate pe modele de rețea şi de analiză. Selectarea unui tip de grafic pentru a fi utilizat în rețelele este direct legată de scopul grafic şi de complexitatea problemei. În această lucrare vom folosi metagrafurile, în scopul construirii unui model de proces de management şi a unui flux de sistem de inteligență de lucru.

Graficele sunt definite ca diagrame constând dintr-un set de puncte, numite noduri şi un set de perechi ordonate sau neordonate de noduri, numite margini (Basu şi Blanning, 2007). Deoarece graficele simple si regizate pot ilustra doar relațiile dintre elementele individuale, cercetătorii au introdus conceptul hipergraf care arată conectivitatea între seturile de elemente. În plus, metagrafurile au apărut ca o necesitate pentru a ilustra mapările regizate set-set.

Modelele deciozionale fac parte din sistemele de prelucrare a informațiilor. Când sunt reprezentate ca metagrafuri, modele de decizie ilustrează o cartografiere de intrare-ieşire a unui model, care corespunde mapărilor setului stabilit într-o margine a metagrafului. Marginile într-un model metagraf sunt decizii numite colectiv "modelului de bază" (Basu şi Blanning, 2007). În această situație, analiza pune accentul pe relația dintre modelele şi poziția lor în interiorul procesului.

Există patru modele care compun modelul de bază: model de colectare, modelul de analiză, modelul de ipoteze şi modelul de recomandare. Model de colectare spune că politica are nevoie de element de intrare şi de ieşire de date şi informații şi date operative. Modelul de analiză are ca date de intrare şi de ieşire informațiile secrete. Modelul de ipoteze are ca date de intrare şi informațiile şi datele operative şi ca ieşire analiza raportului. Modelul recomandări are ca date de intrare informațiile şi datele operative şi ca ieşire are politicile necesare. Acest metagraf descrie un model ciclic de bază.

Concluzii

Conceptul de inteligența rețelelor reprezintă un avantaj pentru comunitățile de informații şi factorii de decizie, deoarece ajută la crearea unei imagini mai clare cu privire la sistemele şi mediile lor corespunzătoare. De asemenea, rețele oferă anticiparea configurației viitoare a sistemului pentru care sunt create, minimizează asimetria în situații de conflict, şi asigură un mediu mai bun de organizare pentru activitatea de informații. Structura lor şi forma furnizează informații de intrare despre acțiunile care ar putea fi

întreprinse pentru a le destabiliza. Teoria Grafurilor a asigurat suficient material, în scopul de a construi rețele care sunt durabile şi eficiente.

Această lucrare a examinat, într-un mod scurt, teoria inteligenței, impactul său asupra elaborărilor de politici, precum şi motivele pentru a răspunde provocărilor la activitatea de informații prin intermediul teoriei de rețea.

Studiile de viitor vor abordare rețelele de informare şi metodologiile dintr-o perspectivă mai complexe, inclusiv atributele specifice metagrafurilor, conectivitate şi aplicații, care necesită abstracție matematică.

Bibliografie:

1. Bandura, A., *Social Cognitive Theory: An Agentic Perspective*, "Annual Review of Psychology", 2001.
2. Basu, A., Blanning, R. W., *Metagraphs and Their Applications*, New York, Springer Verlag, 2007.
3. Behman, R., Carley, K. M., *Social Network Influences on Strategic Choices*, "CASOS Working Paper Series", 2004.
4. Berkowitz, B. D., Goodman, A. E., *BEST TRUTH: Intelligence in the Information Age*, New Haven and London, Yale University Press, 2000.
5. Carley, K. M., Lee, Ju-Sung, Krackhardt, D., *Destabilizing Networks,* "Connections", vol. 24(3), INSNA, 2002.
6. Castells, M., *The Information Age: Economy, Society, and Culture*, vol. 1: *The Rise of the Network Society*, Blackwell Publishers, 1998.
7. Clark, T., *International Marketing and National Character: A Review and Proposal for an Integrative Theory*, "Journal of Marketing", vol. 54(4), 1990.
8. Dandeker, C., *National Security and Democracy: The United Kingdom experience*, "Armed Forces and Society", vol. 20(3), 1994.
9. Dunning, J. H., Kim, C., *The Cultural Roots of Guanxi: An Exploratory Study*, "The World Economy", vol. 30(2), 2007.
10. Harary, F., *Graph Theory*, Addison Wesley Publishing Company, Reading, Massachusetts, Menlo Park, California, London, Don Mills, Ontario, 1969.
11. Herman, M., *Intelligence Services in the Information Age: Theory and Practice*, Frank Cass, London, Portland, OR, 2001.
12. Hulnick, A. S., „What is Wrong with the Intelligence Cycle?", in Johnson, L. K. (editor), *Strategic Intelligence*, vol. 2, Praeger Security International, Westport, Connecticut, London, 2007.
13. Johnson, L. K. (editor), *Strategic Intelligence*, Vol. 1–5, Praeger Security International, 2007.
14. Van Loon, J., *Network*, "Theory, Culture and Society", vol. 23(2–3), 2006.
15. Steele, R. D., "Creating a Smart Nation", in Mark TOVEY (editor), *Collective Intelligence: Creating a Prosperous World at Peace*, Earth Intelligence Network, Oakton, Virginia, 2008

КОНФИДЕНЦИАЛЬНОСТЬ В СОВРЕМЕННОМ ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

Иван БАБЕНКО,
выпускник CSIE, ASEM

This article describes the characteristics of privacy in modern society and the evolution of the privacy perception. The reasons for increasing the risks are described, related to the drain of confidential information, and types of information subject to risk are listed.

Конфиденциальность, как понятие, впервые было озвучено ещё в 1890 году. С тех пор, в его толковании мало что изменилось, но эволюция общества внесла свои коррективы в отношение общества к конфиденциальности.

По принадлежности конфиденциальную информацию можно разделить на 3 группы

- личностная (приватность) – это способность конкретного индивидуума свободно распоряжаться и контролировать персональную информацию;
- коммерческая – регламентируется обязательством о неразглашении информации принадлежащей компании, организации либо группе компаний;
- государственная/международная (секретность) – ограничение государством или международными политическими формированиями распространения данных, которые могут нанести ущерб безопасности государства.

Конфиденциальность регламентируется международными соглашениями, государственными законами, внутренними соглашениями в компаниях и сообществах, а также морально-этическими нормами общества.

Информационные технологии оказали огромное влияние на восприятие конфиденциальности обществом. Сегодня большое количество конфиденциальной информации располагается на цифровых носителях в зашифрованном, либо открытом виде, но при этом у заинтересованных лиц намного больше возможности получить к ней физический доступ, незаметно скопировать или скомпрометировать, а у обладателя секретов всегда есть риск случайно потерять устройство с конфиденциальными данными. Наши тайны транспортируются при помощи сетей передачи данных, а получить доступ к трафику сети теоретически может не только обладатель или получатель этой информации, но и третьи лица, используя методики перехвата данных.

Наибольшую угрозу конфиденциальности представляют: социальные/коллективные сети и сообщества, блоги, почтовые сервисы, cloud-computing сервисы, мобильные и планшетные устройства с выходом в Internet, онлайн-мессенжеры, новостные и медийные ресурсы и т.п.

Эти ресурсы содержат огромные объёмы конфиденциальной информации, осознано или бессознательно доверенной пользователями. Риски, связанные со взломом или утечкой информации от этих сервисов, достаточно велики. Приватностью

пользователя нередко пренебрегают и может произойти, что данные, которые сейчас видите только Вы – завтра станут доступны всем.

По персональным страничкам в социальных сетях, именам, логинам, никам, адресам электронной почты, чаще всего можно составить полный портрет о каждом человеке, использующем Internet если правильно построить механизм агрегации этих данных. Приватности в сети Internet становится всё меньше.

Если просто говорить о том, какую персональную информацию мы передаём на хранение Internet-сервисам и компаниям, то можно перечислить очень много: логины, пароли, даты рождения, идентификационные номера наших документов, календари и расписания, реквизиты банковских счетов, номера телефонов, список родственных и дружественных связей, информация о предпочтениях и увлечениях, биографические данные, истории поиска, фотографии, список посещённых ресурсов, данные о местонахождении, беседы и корреспонденция со знакомыми друзьями, близкими и партнёрами, пробы голоса, данные о биометрических характеристиках, места работы и досуга, комментарии и статьи по поводу основных событий в мире, блогах, людях, компаниях и государствах, политические и религиозные предпочтения, мнения других людей о них и многое другое. Такую информацию можно найти в сети Internet (в большем или меньшем количестве) о каждом человеке не зависимо от того является ли он пользователем глобальной сети.

Субъекты конфиденциальности часто ошибочно считают, что всю эту информацию невозможно собрать объединить и использовать. Существуют мифы о том, что личность в любой момент может быть отчищена от нежелательных конфиденциальных фактов, чаще всего – это заблуждение. Люди склонны доверять сервисам, которыми пользуются, при этом лишь единицы бегло просматривают соглашения о конфиденциальности с которыми соглашаются. Те же пользователи часто считают, что они могут обратиться к «хакерам» и взломать любой аккаунт, пробить любую защиту другого пользователя, причём на том же сервисе, где присутствуют сами.

Сеть Internet даёт каждому заинтересованному инструментарий «для работы с конфиденциальной информацией»: публикации, «вирусного» распространения, искажения, компрометации, поиска, автоматического сбора и многое другое.

Конечно есть и положительные аспекты этого феномена. Нередко человек оставляет в сети следы своей преступной деятельности, заказывая преступления, совершая нарушения авторских прав, высказывая преступные по своей сути мысли, получая несанкционированный доступ к защищённому контенту и т.д. На основе данных сети Internet и других информационных систем, которые имеются в доступе у исследователя, конфиденциальная информация даёт возможность:

- расследовать и раскрывать преступления;
- создавать морально-этический образ этого человека и анализировать его устойчивость или компетентность в той или иной сфере;
- делать мониторинг конкуренции на рынке;
- получать информацию об общественном мнении и социальных трендах;
- быстро создавать информационный повод и распространять информацию.

На сегодняшний день этим уже пользуются спецслужбы и органы охраны правопорядка, посольства таможенные структуры, крупные компании (делая рыночные исследования, участвуя в информационной войне с конкурентами и оценивая кандидатуры работников при приёме на работу) и обычные граждане желающие узнать больше о других и использовать эту информацию либо в своих целях. Информация, которую можно получить таким способом, бывает порой более содержательной и полезной чем данные, содержащиеся в государственных базах данных.

Проблема конфиденциальности продолжает существовать, так как с эволюцией средств хранения и передачи данных, носителей масс-медиа, с зарождением сети Интернет правоприменительная практика в области конфиденциальности информации отступает перед стремительным ростом технологий. Правоохранительные органы на сегодняшний день не располагают достаточной подготовкой кадров, для расследования компьютерных преступлений в области нарушения конфиденциальности, а население делает всё меньше различий между конфиденциальной и общедоступной информацией, что делает эти преступления невидимыми. Необходимо повышать квалификацию для правоприменения существующих законов и соглашений, и информировать население об опасности разглашения конфиденциальной информации.

КЛАССИФИКАЦИЯ СПОСОБОВ НАНЕСЕНИЯ АТАК ДЛЯ ВЫБОРА СИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Лидия СИВКО, Александр ДОРОХОВ
Харьковский Национальный Экономический Университет (Украина)

Currently there are many methods of application attacks at the systems technical data protection in modern society. This led to the need for research to the classification of these methods. The obtained results of the work listed below.

Развитие и внедрения в Украине европейских и международных стандартов информационной безопасности, актуализация проблем противодействия компьютерной преступности создали благоприятные условия для стремительного развития средств зхащиты от угроз нарушения режима безопасности.

Выбор средств защиты зависит от того, какими возможными способами злоумышленник будет пытаться совершить информационную атаку. Атака на информацию – это преднамеренное нарушение набора правил, установленных собственниками информационного объекта или уполномоченного им лица при хранении, поддержке или предоставлении доступа к данному информационному объекту.

Целью исследования является анализ вероятных способов совершения атак (ВССА) системы технической защиты информации (СТЗИ) на основе рассмотрения уже существующих неоднозначных классификаций. Важность определения более четкой классификации данных способов обусловлена необходимостью учета данных способов при осуществлении технической защиты в учреждении, использующем в своей деятельности государственную тайну.

Для СТЗИ, не составляющей государственной тайны, ВССА непосредственно влияют на объем средств, выделяемых на создание и обеспечение функционирования такой системы, что также немаловажно в условиях современной рыночной экономики.

Класиификация способов совершения атак на информацию представляет собой разностороннюю проблему и, в значительной, степени зависит от формы хранения, обработки и передачи информации, а также от тех целей, которые преследует вероятный нарушитель.

Обобщенные пути несанкционированного воздействия на информацию перечислены в государственном стандарте ГСТУ 3396.0-96 (Техническая защита информации Основные положения). Согласно этому документу атаки могут осуществляться [2] техническими каналами (оптические, радио и т.п.), каналами специального воздействия (через формирование полей и сигналов с целью нарушения целостности информации), несанкционированным доступом (маскировка под зарегистрированного пользователя, внедрение компьютерных вирусов).

Однако опыт использования стандарта ГСТУ 3396.0-96 в практической деятельности позволяет сделать выводы относительно неоптимальности вышеупомянутых положений.

Существуют и другие научно обоснованные классификации. Большинство специалистов в области ТЗИ признают существование технических каналов утечки информации (ТКУИ), как одного из основных источников несанкционированной утечки информации.

Однако следует отметить, что однозначное и общепринятое определение термина ТКУИ на сегодня отсутствует. В данном исследовании используется собственное формализованное определение, сочетающее в себе оба подхода: технический канал утечки информации – это совокупность носителя информации, среды распространения информационного сигнала, помех и шумов, мешающих передаче сигнала и средства технической разведки.

Существует еще один довольно распространенный подход, сторонники которого считают, что ТЗИ является одним из способов несанкционированного доступа к информации [1]. Особого внимания заслуживает предположение о том, что каждый вид потенциальной угрозы осуществляется по определенной совокупности потенциальных каналов несанкционированного доступа (по мнению западных специалистов, такие угрозы занимают приоритетное место), или потенциальных каналов несанкционированного воздействия в отношении защищаемой информации [1].

Следует отметить [1], что в некоторых случаях злоумышленник, которому не удается получить информацию по техническим каналам, может прибегнуть к ее уничтожению.

Все изложенное выше позволяет с полным основанием выделить два вида возможных способов совершения атак на информацию: атаки, которые реализуются путем несанкционированного доступа (подвидом таковых являются атаки, которые реализуются путем использования технических каналов утечки информации) и атаки, которые реализуются путем несанкционированного воздействия (подвидом таких являются атаки реализующиеся путем использования технических каналов несанкционированного воздействия на информацию).

Ниже приведен перечень ВССА на информацию в электронном виде, которые реализуются путем использования каналов несанкционированного доступа:

- похищение данных всей автоматизированной системы (АС) или ее компонентов;
- похищение магнитных, оптических и электронных носителей информации;
- подмена отдельных компонентов АС на аналогичные;
- атаки, которые реализуются путем использования технических каналов утечки информации (получения и извлечения информации за счет использования побочных электромагнитных излучений и наводок, с использованием компьютерной сети – так называемые "дистанционные атаки", с экрана монитора путем подсматривания, с использованием закладных устройств, получение информационных сигналов из сети электропитания, с цепей заземления и т.д.).

Перечень же ВССА на информацию в электронном виде, которые реализуются путем использования каналов несанкционированного воздействия слежующий:

- физическое уничтожение АС, или ее составляющих (например, организация пожара или другогочрезвычайного события в помещении, где находится такая АС);
- уничтожение магнитных, оптических и электронных носителей;
- уничтожение источников питания АС;
- умышленное силовое воздействие сетями питания;
- уничтожение проводных коммуникаций и коммуникационного оборудования компьютерных сетей;
- атаки, которые реализуются путем использования технических каналов несанкционированного воздействия на информацию (вирусное воздействие, влияние путем использования деструктивных программных средств).

В результате проведения исследования нами предлагается использовать вышеописанную классификацию, которая может стать системообразующей в процессе исследования всей совокупности вероятных способов совершения атак на информацию, и следовательно, может быть использована в процессе построения систем ТЗИ, предназначенных для защиты открытой информации и информации с

ограниченным доступом на общегосударственном уровне и на уровне отдельных учреждений, предприятий, организаций, при формирования концепции противодействия компьютерной преступности.

Литература

1. В. Хорошко, А.Чекатов. Методы и средства защиты информации. – М.: ЮНИОР, 2010. – 501 с.
2. ДСТУ 3396.0-96. Технічний захист інформації. Основні положення. – К.: Держстандарт України, 1996. – 20 с.

ЭКЗИСТЕНЦИАЛЬНЫЙ АСПЕКТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Денис САЛТЫКОВ,
Молдавская Экономическая Академия

This article presents an existential view of information security problem. Also, here will be specified a great goal of information technologies and very special level of responsibility of security experts.

Новые условия человеческого существования

Стремительное развитие информационных технологий поставило общество на совершенно новый уровень. Само существование человека отныне приобретает принципиально иной характер, так как становится всё более обусловленным процессами информатизации. Стоит отметить тот факт, что тенденция проникновения информационных технологий во все области человеческой жизни – от быта до наивысших уровней управления – ставит специалистов перед высокой ответственностью.

Процесс информатизации явился главным этапом становления так называемого постиндустриального или информационного общества, когда информация становится главной ценностью, вытесняя материальные товары и средства их производства. В процессе развития информационных технологий сократилось множество рабочих мест в силу их неактуальности, но процесс породил и немалое количество совершенно новых специфических задач, которые в свою очередь породили новый спрос на рынке рабочей силы. Двумя основными секторами, обеспечившими этот спрос, явились наука и бизнес-сектор. Специалисты в области информационных технологий стали занимать в указанных областях ключевые посты, а также были сформированы многочисленные соответствующие отделы, которые стали играть одну из главных ролей в деятельности научных и коммерческих учреждений.

Таким образом, можно суммировать вышесказанное, отметив факт, что человек поставлен в качественно новые условия существования, что явилось закономерным следствием развития науки. Тема конечной цели процессов информатизации и ответственности учёных специалистов в области информационных технологий является главной в данной работе.

Проблема отчуждения

Немаловажны процессы, происходящие с человеческой сущностью в условиях современной культуры. Ещё Карл Маркс указывал в своих работах, что человек, играя роль рабочей силы, сталкивается со значительными экзистенциальными проблемами.

Будучи поставлен в условия рыночной экономики и свободной конкуренции, человек вынужден большую часть своей жизни представлять себя как рабочую силу. Таким образом, большое количество времени он представляет собой некую роль, функцию, которая вовлечена в активно развивающиеся процессы производства тех или иных ценностей. Олицетворяя собой эту роль, человек идентифицирует себя с тем типом работника, который требуется на соответствующем рабочем месте. Существование требований к работникам предприятий, к персоналу различных уровней управления формирует целый ряд чётких характеристик, которым должен соответствовать человек на своей должности. Свободная конкуренция побуждает каждого максимально соответствовать определённой системе требований для успешного существования в обществе.

Корпоративная и рабочая этика, формируя в человеке своеобразные черты, сталкивает его с серьёзными противоречиями между внутренним Я и искусственно созданной и воспитанной в себе личностью, исполняющей конкретные социальные функции. Социальная роль, занимая большую часть жизни современной личности, создаёт проблему отчуждения. Человек осознанно или неосознанно сталкивается с проблемой потери собственной идентичности. В условиях современности закономерно возникает вопрос, где же личность выражена наиболее полным образом, где же именно настоящий человек, а не социальная роль. Немаловажным фактом является, что потеря самоидентичности порождает отчуждение, многочисленные психологические проблемы, связанные с несогласованностью условий человеческого существования с его внутренними устремлениями.

Современная культура, делая труд на рабочем месте в рамках социума необходимым условием человеческого существования, порождает глубокие экзистенциальные проблемы, разрешение которых представляется сложнейшей задачей.

Цель информатизации

В связи со всем вышесказанным, необходимо прояснить цели информатизации как глобального культурного процесса.

Самыми очевидными ответами на вопрос о целях информатизации являются качественное улучшение производственных процессов и максимизация конечной

прибыли. Но данные решения представляются неполными в силу собственной ограниченности и логической незавершённости. Если последовательно задавать вопросы, то возникает необходимость уточнить, что именно подразумевается под улучшением производственных процессов и под максимизацией прибыли. При ближайшем рассмотрении можно увидеть, что и сами производственные процессы, как и прибыль, не могут быть самоцелью. Это непременно должны быть средства для чего-то большего. Так, и информатизация не может представляться средством, имеющим цель, которая посредственна сама по себе.

В связи с экзистенциальной проблемой отчуждения процессы информатизации могут получить совершенно определённое рассмотрение в ключе экзистенциальных проблем существования человека. В таком случае высшей, конечной целью информатизации можно обозначить максимальное освобождение человека от необходимости нетворческой работы. Такая высокая цель, будучи особенно гуманной, может послужить лучшей апологией информатизации как таковой.

Разумеется, ни в коем случае нельзя упускать из внимания тот факт, что, будучи предельно сложным явлением, сама по себе информатизация порождает уникальные и специфические проблемы, появление которых ставит всё новые задачи. Разрешение этих вопросов в связи с их новизной является сложным процессом, требующим значительных усилий и постоянных инноваций. Пожалуй, самым важной проблемой информатизации является проблема информационной безопасности.

Информационная безопасность как путь к освобождению человека

В силу того, что информация в современных условиях является наивысшей ценностью, все аспекты информатизации подчинены главной проблеме – проблеме информационной безопасности.

С точки зрения предложенного экзистенциального взгляда на вопрос, ответственность специалистов в области информационной безопасности приобретает истинно огромные масштабы. При вышеуказанном взгляде на проблему обнаруживается, что информационная безопасность является ключевым аспектом оптимизации процессов нетворческого труда, а, следовательно, и освобождения человека от рутины и от главной обозначенной выше проблемы – отчуждения. Так, безопасность является необходимым условием и катализатором движения информатизации к конечной цели.

Таким образом, проблема информационной безопасности, будучи рассмотрена в экзистенциальном ключе, приобретает крайне высокую гуманистическую цель, играя главную роль в процессе освобождения собственного Я человека от искусственных условий существования. Разумеется, при таком аспекте хорошо видно, сколь велика ответственность учёных, специализирующихся в этой области.

НЕЧЕТКО-МНОЖЕСТВЕННЫЙ ПОДХОД К ФОРМИРОВАНИЮ ИНФОРМАЦИОННЫХ СОСТАВЛЯЮЩИХ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ

Людмила МАЛЯРЕЦ, Михаил ДОРОХОВ
Харьковский Национальный Экономический Университет, (Украина)

The general structure of economic's safety systems for the enterprises has been considered. The main criterias and characteristics of information safety are allocated. The application of SWOT-analysis in fuzzy conditions for models of an estimation of information safety has been offered.

В условиях конкуренции стабильное функционирование любого коммерческого и производственного предприятия в значительной степени обеспечивается надежностью его экономической безопасности. Практика показывает, что для этого требуется создание и поддержание интегрированной, многоуровневой и комплексной системы экономической безопасности, обеспечивающей обнаружение, анализ и оценку возникающих, существующих и потенциальных угроз по каждой функциональной составляющей экономической безопасности, а затем – разработка и осуществление соответствующих противодействующих им превентивных мероприятий. В общем случае экономическая безопасность предприятия может рассматриваться с внепроизводственной и внутреннепроизводственной стороны. Первая включает рыночную и интерфейсную безопасность. Вторая, в свою очередь, содержит такие составляющие безопасности, как финансовая, интеллектуальная, кадровая, технологическая, правовая, экологическая, силовая, информационная.

Необходимо подчеркнуть, что хотя в узком смысле информационная безопасность выделяется, как отдельная составляющая, реально (в широком понимании) она всегда присутствует и в значительной степени определяет обеспечение всех остальных компонент. Прежде всего информационная безопасность состоит в осуществлении эффективного, оперативного и достоверного информационно-аналитического обеспечения бизнес-процессов.

К информационным составляющим системы безопасности предприятия относятся:

- сбор всех видов информации, касающихся как функционирования собственно самого предприятия, так и состояния рыночной окружающей среды, клиентов-заказчиков, контрагентов, партнеров, поставщиков, конкурентов;
- накопление, систематизация и анализ полученной и имеющейся информации;
- прогнозирование тенденций развития рынка, научно-технологических, экономических, социальных процессов на нем и в обществе в целом (касающихся деятельности данного предприятия);

- оценка и мониторинг состояния экономической безопасности предприятия в целом и по отдельным компонентам, разработка рекомендаций и мер по ее обеспечению и усилению;
- другие виды деятельности и меры по обеспечению информационной безопасности (организационные, финансовые, технологические, кадровые и так далее).

При этом, рассматривая потоки внешние (входящие)информации, следует разделять ее по источникам формирования на открытую (официальную, общедоступную, из средств массовой информации, интернета и т.п.) и вероятностную несекретную информацию (полученную через неформальные контакты и каналы с носителями такой информации).

Практическая реализация и организация мероприятий по охране информационной составляющей экономической безопасности обеспечивается последовательным выполнением комплекса действий – сбором различных видов необходимой информации, ее обработкой и систематизацией, анализом с привлечением компетентных экспертом и использованием специальных математических методов, практическими действиями по информационной защите всей составляющих жизнедеятельности охраняемого обьекта. Обычно такая защита направлена на противодействие промышленному и экономическому шпионажу со стороны конкурентов или иных заинтересованных юридических и физических лиц; техническую безопасность средств связи, хранения информации, корреспондении, переговоров и исключение несанкционированного доступа (как извне, так и изнутри) к закрытой, конфиденциальной, служебной информации; сбор информации из внешних источников о потенциальных инициаторах промышленного шпионажа, ожидаемых попытках нарушения информационной безопасности и принятие предупредительных мер с целью их пресечения и недопущения.

Уровень информационной безопасности тесно взаимосвязан со степенью использования неполной, неточной и противоречивой информации в процессе принятия управленческих решений на предприятии. Поэтому при принятии решений основными факторами становятся:

- полнота информации (характеризующая соотношение имеющейся в распоряжении лица,принимающего решение информации к общему обьему имеющейся, необходимой информации по данному вопросу);
- точность информации (отношене обьема релевантой – достоверной информации к общему обьему имеющейся информации);
- противоречивость информации (количество суждений за предлагаемое решение к общему количеству мнений в суммарном обьеме доступной релевантной информации).

Очевидно, что в процессе организации системы информационной безопасности, как части общего комплекса мероприятий по экономической безопасности предприятия, необходимо учитывать ряд труднопрогнозируемых и слабо-

формализованных факторов [1]. Среди них – сложность самой среды существования обьекта информационной защиты (предприятия в рыночном конкурентном окружении) среды принятия решений, информационные ограничения, временные факторы, поведенческие ограничения, возможные побочные негативные последствия, личностные оценки и предпочтения руководителей и лиц принимающих решения, взаимосвязь решений, факторы неоднозначности и неопределенности.

Наличие факторов слабой структурированности задач обеспечения информационной безопасности, экспертных оценок и предпочтений, позволяет утверждать, что в данном случае необходимо совместно обрабатывать как данные, так и знания, при этом для обоих компонент должны быть учтены факторы неопределенности. Представляется, что одним из адекватных инструментов для решения таких задач является аппарат теории нечетких множеств.

Нами предлагается использовать для решения таких многокритериальных задач комплексного оценивания уровня информационной безопасности предприятия (компонент его жизнедеятельности и функционирования) методологию SWOT-анализа в нечетко-множественной постановке [2]. Такой подход позволяет учесть различного вида и точности исходные данные и оценки – экспертные (индивидуальные и коллективные), числовые и лингвистические, представленные в различных и несогласованных шкалах измерений, с различной степенью недостоверности (неточности). При этом не требуется (в отличие от статистический методов) обеспечение определенных характеристик выборок, количества и состава опрошенных экспертов (или данных) и тому подобного.

Развитие программного обеспечения и практическая доступность компьютерных средств нечеткого моделирования (Matlab Fuzzy logic toolbox, Fuzzytech, Fuzicalc, Cubicalc) позволяют создавать соответствующие компьютерные модели, доступные для практического использования непосредственно на предприятиях руководителями, отвечающими за информационную и, в более широком смысле, общую экономическую безопасность предприятий.

Литература

1. S.Kavun, R.Brumnik, O.Dorokhov, I.Zolotaryova. The uncertainly-plural model for the estimation of enterprises economic safety level. Social control in contemporary society – practice and research: policing in Central and Eastern Europe: conference proceedings / the 7th biennial International Criminal Justice Conference, Ljubljana, September 2008. – Ljubljana: Faculty of Criminal Justice and Security, 2008. – PP.53-54.
2. А.Дорохов, В.Чернов. Целесообразность и возможность использования нечеткого моделирования для оценки рисков в информационных системах. Securitatea informațională 2010 : Conf. intern., 15-16 apr. 2010. - Ch.: ASEM, 2010. - P.18-21

СБАЛАНСИРОВАННАЯ СИСТЕМА ПОКАЗАТЕЛЕЙ АНАЛИЗА ЭФФЕКТИВНОСТИ ПРЕДПРИЯТИЯ И IT - ЗАЩИТА ВНУТРИФИРМЕННОЙ БИЗНЕС ИНФОРМАЦИИ

Марко ТИМЧЕВ,
Университет национального и мирового хозяйства,
(София, Болгария)

ССП анализа эффективности предприятия "Balanced Scorecard Method of Analysis"(BSc) базирована на четыре основные перспективы: „Финансы", „Маркетинг", „Внутренные бизнес процессы", „Обучение и развитие". Каждое из четырех направлений (перспектив) включает факторы, которые формируют экономическую добавочную стоимость предприятия (Economic Value Added - EVA).

Направление "Финансы" включает показатели финансового состояния, стабильности и стоимости предприятия.

Бизнес метрика факторов стоимости предприятия представляет система показателей.Управление факторов - „EVA- Economic Value Added", осуществляется при помощи анализа показателей основной (оперативной) деятельности предприятия, которые, в свою очередь, определют экономеческую добавленную стоимость.

Каждое из четырех направлений BSc включает факторы стоимости (Economic Value Added). EVA определяется как разница между чистой операционной прибылью после налогообложения и затратами на капитал за тот же период:

$$EVA = EBIT * (1-T) – Kw * C,$$

где: EBIT – величина доходов до уплаты налогов и процентов;
T – ставка налога на прибыль (в долях единицы);
Kw – средневзвешенная цена капитала (WACC);
C – стоимостная оценка капитала.

Если EVA больше 0, то предприятие приносит прибыль, превышающую затраты на капитал. Это является основным фактором создания стоимости. Если EVA>0, то предприятие создает стоимость, если EVA<0 – то оно теряет ранее созданную стоимость.

В рамках направления „Маркетинг"(„Клиенты") маркетологи определяют ключевые области (сегменты) рынка, в которые предприятие сосредоточивает свои усилия. Дефинируются генераторы эффективности (performance drivers) и показатели анализа. Направление „Маркетинг"(„Клиенты") учитывает влияние человеческого капитала, способом формализации некоторых категорий как лояльность клиентов и ценность офертного предложения. Направление „Внутренные бизнес - процессы" показывает структурную часть человеческого капитала посредством идентификации внутренних бизнес-процессов, подлежащих совершенствованию с

целью укрепления конкурентных преимуществ. Для каждого бизнес процесса должен быть определен соответствующий двигатель (driver), характеризующий эго эффективность. Направление „Внутренные бизнес процессы" включает бизнес-метрику анализа и оценки эффективности применения производственных активов и организационно-технического уровня.

Направление „Обучение и развитие" определяет инфраструктуру, которую предприятие должно создать для того, чтобы обеспечить развитие человеческого капитала в долгосрочной перспективе. Это связано с ростом качества интеллектуального капитала. В этом направлении основными драйверами эффективности могут быть удовлетворение персонала, задержание сотрудников, их умения и квалификация, возможность мгновенно получать информацию, необходимую для принятия управленческих решений, генерация инициатив, эффективность работы информационной системы и т.д.

ССП анализа эффективности надо интегрировать с "EVA Method of Analysis", "Z-Score and ZETA Methods of Analysis" (анализ риска несостоятельности) и "SWOT and Pest Analysis" (анализ специфики и рыночного позиционирования предприятия). Информация "Bsc", "EVA","Z-Score Analysis" и „SWOT Method of Analysis" в высшей степени конфиденциальная. Проблему защиты информации нужно решать надежно прецизной IT защитой.

Все виды информационных угроз можно разделить на две большие группы:

1. Отказы и нарушения работоспособности программных и технических средств;
2. Преднамеренные угрозы, заранее планированные злоумышленниками с целью нанесения вреда.

Защита информации от исследования и копирования предполагает криптирование данных. Задачей криптографии является обратимое преобразование исходного текста (открытого текста) в случайную последовательность знаков, часто называемых шифротекстом, или криптограммой.

Одной из основных угроз хищения информации является угроза доступа к остаточным данным в оперативной и внешней памяти компьютера. Под остаточной информацией понимают данные, оставшиеся в освободившихся участках оперативной и внешней памяти после удаления файлов пользователя, удаления временных файлов без ведома пользователя, находящиеся в неиспользуемых хвостовых частях последних кластеров, занимаемых файлами, а также в кластерах, освобожденных после уменьшения размеров файлов и после форматирования дисков.

Основным способом защиты от доступа к конфиденциальным остаточным данным является своевременное уничтожение данных в рабочих областях оперативной и внешней памяти компютера, выделенных пользователю, после окончания им сеанса работы, как и в местах расположения файлов после выдачи запросов на их удаление.

Системы защиты информации семейства Secret Disk позволяют защищать информацию путем организации для конкретных пользователей ПЭВМ защищенных

носителей информации – виртуальных логических дисков. Вся информация, записываемая на такие носители, подвергается «прозрачному» (на лету) преобразованию с использованием одного из следующих алгоритмов: встроенный алгоритм преобразования данных с длиной ключа 128 бит; входящая в Windows реализация RC-4 (с длиной ключа 40 бит); алгоритм шифрования по длиной ключа 256 бит (при использовании эмулятора платы «Криптон», имеющего сертификат, так напр. ФАПСИ).Семейство средств защиты информации «Secret Disk» включает в себя модификации для защиты информации на автономных ПЭВМ и комплексы защиты информации, хранимой и обрабатываемой на выделенных серверах ЛВС.

Широкое внедрение в повседневную практику компьютерных сетей, их открытость, масштабность делают проблему защиты информации исключительно сложной. Выделяют две базовые подзадачи: 1.Обеспечение безопасности обработки и хранения информации в каждом из компьютеров, входящих в сеть; 2.Защита информации, передаваемой между компьютерами сети.

Международное признание для защиты передаваемых сообщений получила программная система PGP (Pretty Good Privacy - очень высокая секретность), разработанная в США и объединяющая асимметричные и симметричные шифры. Являясь самой популярной программной криптосистемой в мире, PGP реализована для множества операционных сред -MS DOS, Windows , Windows NT, OS/2, UNIX, Linux, Mac OS, Amiga, Atari и др.

Бизнес информация экономического анализа имеет строго конфиденциальным характером. Современный финансовый бизнес анализ невозможен без применений IT системы. Проблемма конфиденциальноти и защитый IT информации результатов анализа сложная но она имеет ключевое значение.

ВИРУСЫ СЕМЕЙСТВА МОБИЛЬНЫХ УСТРОЙСТВ И ИХ МОДИФИКАЦИИ

Михаил БАЛЫЧЕВ, Владимир ФЕДОРЧЕНКО
Харьковский Национальный Экономический Университет, (Украина)

Viruses are a family of mobile devices is appearing more frequently, as well as new operating systems for these devices. Developers virus software codes, each time finding more and more sophisticated method of distribution, using all communication devices.

Вирусы семейства мобильных и их модификации на сегодняшний день появляются с такой же завидной регулярностью, с какой выходят на рынок новые устройства под управлением все новых операционных систем (ОС) [1, 2]. Чаще

всего у ничего не подозревающего пользователя смартфона с встроенным Bluetooth сначала без видимых причин происходит перезагрузка, а потом и вовсе устройство выходит из строя.

История развития вирусов для мобильных устройств не продолжительна. Она началась 14-го июня 2004 года, когда появился очередной проект команды 29A (http://www.29a.net, известная специалистам группа разработчиков специфического программного обеспечения, сейчас часть ее участников осуждена, а другая прекратила поддержку проекта 29A).

Имя, которое они дали первому вирусу – Caribe – надолго осталось в истории и трудах исследователей вирусов. Данный вирус для телефонов под управлением Symbian OS (телефонов Series 60 от Nokia) умел только инсталлировался, ОС при этом просила подтверждения прав доступа, после чего программа рассылала инсталяторы, используя интерфейс Bluetooth. Целью атаки было любое устройство, имеющее этот стандарт. Caribe не фильтровал устройства, посылая вирус на них, хотя работал только на телефонах от Nokia.

Вирус, действительно начинающий историю вирусов под мобильные платформы, появился в марте 2005 года под именем Commwarrior. Он уже мог распространяться не только через Bluetooth, а еще использовал принципиально новый способ распространения - через MMS, что значительно ускорило его распространение, вирус был написан российским программистом «e10d0r», позже появился похожий иностранный вирус – Mabir.

Ситуация с карманными компьютерами и мобильными устройствами под управлением WinCE или Windows Mobile более стабильна: существует несколько вирусов и ряд их модификаций. Один из них - Duts - вирус в классическом понимании этого слова, он заражает exe-файлы, дописывая собственный код в зараженный файл,. Другой – Brador - троян, открывающий порт 2989 и предоставляющий право отправлять и получать файлы, отображать сообщения и исполнять некоторые команды операционной системы. По одной из версий оба вируса принадлежат группе 29A, причем исходный код Duts еще можно найти в Сети. Однако этот вирус написан на ассемблере, что подразумевает знания в этой области, а также в работе ОС Windows Mobile для того чтоб разобраться в принципе работы вирусов.

Способов распространения вирусов под мобильные телефоны немного. Так, это технология Bluetooth (радио с ограниченным около десяти метров радиусом действия). Беспроводные технологии в современном мире обретают все большую популярность, программисты не могли пропустить возможность таким способом распространять свои вирусы. Поэтому любое устройство, находящееся в режиме обнаружения, может подвергнуться атаке, при этом посылается сообщение в виде установочного SIS-файла (для Nokia стандарт первоначально служил для распространения игр), при получении файла пользователь вправе выбрать, принимать сообщение или нет. После принятия сообщения пользователь снова получит право выбирать, устанавливать ли приложение, и только после того, как

будет получено согласие, вирус получит доступ к устройству. Следовательно, возможно исключение заражения вирусом на любом этапе, что сказывается на его распространяемости. Классическими примерами вирусов, использующих Bluetooth для распространения, являются Caribe, CommWarrior, Mabir, MGDropper.

Существует стандарт MMS, он позволяет присоединять всяческие файлы к сообщению, и вирусы таким образом получают дополнительный способ размножения. При открытии присоединенного к сообщению файла, его установке, открывется дорога вирусу. Так распространяются такие вирусы, как Commwarrior и Mabir.

Также переносчиком вируса может выступить O-DAY soft. Используя желание пользователей получить и установить последнюю версию игры или популярной программы с каким либо дополнением, вирус встраивает и внедряет в установочные файлы версию себя - в придачу к общему пакету. Так размножается Dampig, Mos, который пользуется игрой Mosquitos, Doomboot, прикрывающийся игрой Doom.

Остановимся на последствуях заражения телефона вирусами. Как пример, рассмотрим смартфон Nokia или другой фирмы с Symbian OS. Эта ОС широко распространена, развита с точки зрения функциональности, имеет открытое детальное описание, которое может быть использовано как разработчиком так и создателем вируса. В результате с телефоном можно сделать практически все: отключить Bluetooth, встроенный файловый менеджер, телефонную книгу (вирус Dampig), повредить системные файлы ОС (Doomboot и Hobbes). Также может произойти рассылка SMS-сообщений (Mos), а вирус Onehop, который перезагружает телефон как только пользователь попытается воспользоваться системными приложениями.

Механизмы самозащиты у самих вирусов не слишком разнообразны. Так, вирус под названием Drever после инсталляции начинает затирать все антивирусные программы, обнаруженные им на карте памяти мобильного телефона. Вирус Doomboot просто не показывает своего присутствия в телефоне, он устанавливается вместе с игрой (похожий механизм у Dampig). CommWarrior прикрывается в MMS фантастическими программами или обновлениями от www.symbian.com ("Dr.Web! New Dr.Web antivirus for Symbian OS. Try it!", "MS-DOS emulator for SymbvianOS. Nokia series 60 only. Try it!", "SymbianOS update" и т.д.).

Изначально вирус должен где-то распространяться, поэтому ему нужна как основа ОС с множеством функций. Она должна быть популярна, хорошо документирована, так как вирус нуждается в информации для анализа уязвимостей ОС. И как только новая ОС становится популярной, тут же появляются и вирусы под нее.

Однако опасность возникнет лишь когда разработчики вирусов являются профессионалами и нацелены на финансовые результаты от действия вируса. Это возможно при широком распространения какой-либо одной ОС, то есть в случае монополизации рынка, или в результате глобального развития кросс-платформенных языков типа Java, которые позволят полноценно управлять телефоном.

Поэтому для исключения заражения не следует открывать и устанавливать программы, приходящие по Bluetooth, MMS с незнакомых номеров. Даже если

программа пришла от знакомого, следует это перепроверить. Разумеется, следует опасаться программ, скачанных из ненадежных (непроверенных) источников, например p2p-сетей. Также необходимо использовать шифрование особо важных данных: номеров кредитных карт, паролей и т.д. И наконец, рекомендуется использовать соответствующие антивирусные программы.

Очевидно, что с развитием технологий и программных средств под мобильные устройства вирусы для них станут такими же развитыми, как их PC-варианты. Ожидается появление полиморфных вирусов, новых методов их маскировки и противодействия антивирусам.

Таким образом складывается новое научно-техническое направление – безопасность мобильных устройств, требующее как исследования непосредственно самих вирусов, так и развития аппаратных и программных средств антивирусной защиты.

Литература

1. М.Букин. Секреты сотовых телефонов. М., «Питер», 2005, 206 с.
2. P.Wang, M.González, C.Hidalgo. Understanding the Spreading Patterns of Mobile Phone Viruses. // Science, 2009, Vol. 324 No. 5930 pp. 1071-1076.

МОЛДОВА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

А. К. РУСНАК,
Молдавская Экономическая Академия,
Кишинев, Республика Молдова

Статься рассматривает некоторые проблемы информационной безопасности в Республике и предлагает пути их решения.

Ключевые слова: *информация, информационная безопасность.*

Под информационной безопасностью понимается состояние защищённости информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера.

Цель информационной безопасности – обезопасить главные ценности информационной системы, защитить и гарантировать доступность и целостность информации, не допустить утечку информации, свести к минимуму ущерб от событий несущих угрозу информационной безопасности.

Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый целостный механизм.

Существующая в настоящий момент в мелком, среднем и даже крупном бизнесе и государственном секторе практика обработки важной (в том числе секретной) информации на компьютерах, подключенных к сети Интернет, а так же исполь-

зование для деловой переписки и передачи конфиденциальной информации бесплатных почтовых сервисов представляет реальную угрозу ее утечки или несанкционированного уничтожения.

Также в большинстве случаев предприятия, компании и органы публичной власти при построении собственных информационных систем практически не уделяют внимания вопросам информационной безопасности, не обращают внимания на существующие угрозы информационной безопасности, а также не проводят анализ рисков.

В настоящее время в Республики Молдова существуют следующие проблемы обеспечения информационной безопасности:

1. Несовершенство действующей нормативно-правовой базы в области обеспечения информационной безопасности.
2. Отсутствие во многих средних и крупных компаниях и органах публичного управления единой комплексной системы защиты информации.
3. Нехватка квалифицированного персонала в области информационной безопасности.
4. Недостаточное внимание к проблеме обеспечения безопасности информационных систем, отсутствие таких регламентирующих документов как политика безопасности, инструкции и планы по обеспечению информационной безопасности и бесперебойной работе информационных систем. При этом большинство пользователей информационных систем зачастую не владеют элементарными понятиями и навыками в области информационной безопасности.
5. Недостаточное финансирование сектора информационной безопасности.

Кроме того существуют реальные угрозы информационной безопасности:

- Поражение отдельных компьютеров или всей информационной системы компьютерными вирусами, что может привести как к уничтожению информации, так и к утечке.
- Несанкционированный доступ заинтересованных лиц (в том числе и пользователей информационных систем) к информационным ресурсам, что может привести к незаконной модификации обрабатываемой информации, ее уничтожению или хищению.
- Блокирование работы информационных систем, что может привести к серьезным сбоям в функционировании.
- Передача конфиденциальной информации с помощью электронной почты, что может привести к утечке информации.
- Нецелевое использование компьютерных систем, Интернета, государственных и корпоративных баз данных.

Заключение. Исходя из сложившейся ситуации, можно предложить следующие для обеспечения защиты информационных систем и ресурсов:

1. Дальнейшее совершенствование нормативно-правовой базы в области обеспечения информационной безопасности и специальных телекоммуникационных систем Республики Молдова.

2. Создание и внедрение комплексной системы защиты информации и информационных ресурсов, включающую в себя криптографическую и антивирусную защиту, систему межсетевого экранирования, подсистему аутентификации и идентификации при доступе, подсистему управления, доступом, подсистему защиты информационных систем при их интеграции между собой, а так же при подключении к внешним телекоммуникационным системам.
3. Создание системы аттестации объектов информатизации на предмет соответствия требованиям информационной безопасности.
4. Распределение полномочий между компетентными ведомствами в области организации и обеспечения информационной безопасности и создание реальных механизмов для реализации концепций и политик.

THE LEGAL BASIS OF INFORMATIONAL SECURITY IN FACE OF MODERN WORLD REALITY OR ONLY A MYTH

Michał MAZUR,
Institute of Political Studies and International Relations
(Cracow, Poland)

The article examines contemporary issues combined with the problem of legal basis of informational security. In this brief text author tries to underline some of the most important questions which arise from many attempts to create the sufficient legal model of information protection. The task seems obviously to be very hard but in the end it's not impossible.

1. Introduction

In modern world almost all critical aspects of people activity are supported by legal regulations. This matter has fundamental meaning for their stability and continuity. Generally when something is obvious it is much easier to obey, to comply with regulations.

Informational security, both real and legal, seems to be the first rate factor for the functioning of individuals, institutions and, in the first place, for political organisms which are independent states. For centuries one can point many examples where the effective information handling was essential for the final result of each scuffle.

Real informational security, mentioned above, must have, in every case, foundation. This foundation is legal regulation which is able to sanction effective security of identified data. Symptomatic, in this field, is statement that to keep a secret, silent is not sufficient [1].

2. Contemporary patterns and issues

Most of contemporary states rest their legislation, as regards informational security, on regulations focused around information defined as classified or secret. The other area, which is thought to be crucial, are the issues of state security, fundamental for every political authority. These are usually gathered by legislator in constitution or in the legal acts of the highest rank. Exceptions in certain states are capital planning practices within the government or agency-specific policies [2].

For example we can take Republic of Poland, where the foundation is act that specifies the protection of classified information or data. It determines the procedures and organization of this partly restricted state area [3]. One can enumerate some of act's aspects such as: classification of information in order of it's importance, access to specified types of data, the course of examine proceedings which let particular units to have opportunity to familiarize with classified information, the bureaucratic system which carries secret documents, and finally the physical protective means combined with IT services able to process information.

As one can see it is very specific field of legislation. The creators of this type system must know not only the unique character of informational security, but also must be familiar with nowadays IT threats which seem to be uncontrollable. Nevertheless it's almost impossible to compose such perfect network, able to stop criminal elements. Elements that attack with growing aggression due to the rising price of information in modern world.

The state informational security and its legal basis is not everything. It doesn't cover the whole scope of problems combined with this issue. On the other hand we have private sector, present and highly important in every country, which is also exposed to the same type of threats.

Access to stored information on computer databases has increased greatly. More and more companies store business and individual information on computer hard disks than ever before. Much of the information stored is highly confidential and not for public viewing. Its value is often higher than some fixed assets of particular company.

Many businesses are solely based on information. Personal staff details, client lists, salaries, bank account details, marketing strategies and sales information may all be stored on a database. Without this information, it would often be very hard for a business to operate. Information security systems need to be implemented to protect this information. But not only this. It is crucial to ensure that in case of emergency, in case of committed crime, the information will be properly secured and that each state will make sufficient efforts to protect valuable information with proper legal regulations. It is all because nowadays typical guarantees can be simply useless [4].

In highly networked IT society, IT trouble caused by one often even not significant company may possibly cause damages to the entire society. Therefore, ensuring information security in companies should be done not only to obey the law and to minimize its damage, but also to instill everyone the responsibility as a member of the society. Thus, the task of the government is also to value companies efforts to improve their information security. It can't be done without proper legal basis.

The same refers to online identity theft, in which confidential information is illicitly obtained through a computer network and used for profit. It is undoubtedly a rapidly growing enterprise. Credible estimates of the direct financial losses exceed much more than a billion dollars per year. Indirect losses are much higher, including customer service expenses, account replacement costs, and higher expenses due to decreased use of online services in the face of widespread fear about the security of online financial transactions. Increasingly, online identity theft is perpetrated using malicious software. It can be used to obtain many kinds of confidential information, including user names and passwords, social security numbers, credit card numbers, bank account numbers, and

personal information such as birthdates and mothers' maiden names. In this field the number of legal acts is growing but there is still much to improve.

3. Summary

To summarise, there is none legal environment which fully protects information, which can assure the owner of particular data that it is safe and absolutely nobody can get access to check it. In case of information security is never ending process that requires constant monitoring, updates, research, investment and implementation of new technologies. But before everything the secret lies within the law system which is able to control all abuses. The perfect model simply can not be done. The role of each legislator is to try to gain such a level that will increase, as much as possible, probability of safety.

On the other side the punishment must be also quite severe. But here emerges another problem. To punish with pecuniary penalty or with insulating penalties. Consciousness of concrete society is crucial in this case.

Nevertheless, does every modern country has that kind of muscle to enforce the implementation of its own legal regulations, basis, in relation to informational security. For many reasons, some of them were mentioned above, it raises concerns.

Information security is becoming more demanding, as the skills involved become more complex and managerial. Experts who create protection models or systems must be aware of the enormity of obstacles which have to be surmount. Obviously it is not easy but also can't be left unsolved.

Bibliography

1. Claudel, *Journal 1904-1955*, PAX, Warsaw 1977
2. Abeles, Bartol, Batdorff, Hash, Rollins, Robinson, *Integrating IT Security into the Capital Planning and Investment Control Process*, NIST, Gaithersburg 2005
3. Namieśnik, Wesołowski, *Security and protection of data*, Gdańsk 2007
4. Kifner, *Security policy and the protection of information*, Helion Publishers, Warsaw 1999

О ТЕХНОЛОГИЧЕСКИХ АСПЕКТАХ ЕДИНОГО ГОСУДАРСТВЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Андрей САУЛЯК,
ЦГИР "REGISTRU" Министерства информационных технологий и связи Республики Молдова

Aspects of security at creation uniform system of paper and electronic state document circulation. Protection methods of electronic documents. Electrodigit Technology of Protection of the paper documents.

Построение единого государственного документооборота (ЕГД) кажется задачей невыполнимой или требующей несоизмеримых усилий. Но даже если она будет жестко-вертикально внедрена не факт, что она сможет существовать и поддержи-

ваться пользователями (государственными служащими) и/или ее не парализуют внутренние противоречия и коллизии.

Функциональные (типовые) требования – необходимое базовое условие существования АСЭД, а не-функциональные (специальные) требования – условие *эффективной* работы системы государственного документооборота. Как видится авторам, специальные требования к АСЭД могут быть сформированы Единым электронным административным регламентом государства (ЕЭАРГ).

Со способами обмена электронными документами и методами обеспечения их долговременного хранения тесно связаны проблемы обеспечения их *аутентичности и безопасности*.

С появлением и развитием технологии "цифровой подписи" проблема аутентичности и целостности электронных документов была успешно решена. Более того, "электронные" документы теперь защищены гораздо надёжнее "бумажных", а широкий арсенал вариантов реализации "цифровой подписи" [8] – классическая подпись, коллективная подпись, слепая подпись, подпись с забыванием и др. – позволяет в любых конкретных ситуациях получать гибкие и эффективные решения с недостижимыми ранее возможностями.

"Бумажные" документы защищены хуже. Полиграфические методы защиты "не вписываются" в рамки концепции современного автоматизированного документооборота. Поэтому если некая система документооборота предполагает работу как с "электронными", так и с "бумажными" документами, то возникают определённые сложности. В частности, возникает потребность в универсальных автоматизированных методах и средствах, которые позволяли бы одинаковым образом обрабатывать документы обоих видов при их идентификации и проверке подлинности. Очевидно, что при этом уровень автоматизации и уровень надёжности защиты должны соответствовать более высоким критериям, присущим обороту именно "электронных", а не "бумажных" документов.

Автором статьи предлагается новый метод идентификации и защиты "бумажных" документов, который полностью совместим с аналогичными процедурами для "электронных" документов, что позволяет организовать единый документооборот для документов обоих видов.

Основу метода [5] составляет специальная физическая метка, которая наносится на защищаемый документ с помощью неуправляемого стохастического электрического разряда (пробоя). В результате пробоя на бумажном носителе создаётся множество отверстий, общее количество которых, а также размеры и взаимное расположение имеют случайный характер.

Теперь задача идентификации может быть решена следующим образом. На начальном этапе жизненного цикла документа – перед выпуском документа в оборот – на "чистый" бланк документа наносится уникальная метка, затем на бланке печатаются порядковый номер документа, информация о его происхождении и собственно содержание (текст) документа.

Метка проставляется в специально отведенной для этого зоне, удобной для автоматизированного нанесения (записи) и считывания. С помощью специального

мобильного сканера производится считывание изображения метки и его преобразование в компактный двоичный код – т.н. цифровой образ метки.

Далее возможны варианты. Например, в простейшем случае, который приводится здесь только для иллюстрации общих положений, пара "порядковый номер документа – цифровой образ метки" помещается в базу данных системы документооборота и используется в дальнейшем для идентификации и проверки подлинности документа, находящегося в обороте.

Более реалистическим представляется другой подход, который не предполагает постоянных обращений к удаленной базе данных. На этапе подготовки документа цифровой образ метки, полученный при сканировании, а также другие данные о документе – порядковый номер и информация о происхождении – "подписываются" цифровой подписью (закрытым ключом) официального лица, выпускающего документ. Подписанная информация печатается на документе в виде штрихового кода. После этого информация о документе регистрируется в базе данных, а сам документ выпускается в оборот. Обращение к базе данных происходит в исключительных случаях.

Объединив технологию ЭЦП и электроразрядных меток можно получить достаточно защищенную систему государственного документооборота, в котором бумажный и электронный документ будут иметь соизмеримую юридическую силу. Один и тот же документ в бумажной и виртуальной форме может быть однозначно идентифицирован и защищен, и может быть осуществлен переход из электронной версии документа в бумажную и обратно с сохранением юридической силы такого изменения.

Литература

1. Тихонов В.И., к.и.н., директор Центрального архива документов на электронных носителях Москвы (ЦАДЭНМ) Архивное хранение электронных документов: проблемы и решения. Журнал «Делопроизводство и документооборот на предприятии». М., (№2)2006.
3. Г. Ретер. Электронные лавины и пробой в газах. Перевод с английского под редакцией В.С. Комелькова, Издательство «Мир». Москва, 1968, -390 с.
4. Шкилев В.Д., Адамчук А.Н., Недиогло В.Г. Электроразрядная технология защиты документов особой важности (строгой отчетности) Электронная обработка материалов, №2, 2008, с. 4-10.
5. Шкилев В.Д., Мартынюк Н.П. Патент Российской Федерации .RU 2 399 496 C2 «Электроразрядный способ изготовления бумажных документов строгой отчетности и бумажных денежных знаков».
6. Шкилев В.Д., Патент Российской Федерации .RU 2 397 845 C2 «Электроразрядный способ изготовления бумажных документов строгой отчетности и бумажных денежных знаков».
7. W. Diffie, M. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, 22(6): 644-654, November 1976.
8. B. Mao. Современная криптография. Теория и практика. – М.: Изд-во "Вильямс", 2005 г., 768 с.

BALANCED SCORECARD AS A STRATEGIC MANAGEMENT ACCOUNTING TOLL – A CASE STUDY

Joanna TURLEJ,
University of Science and Technology (Cracow, Poland)

Article presents the issue of Balanced Scorecard. BSC is one instrument that is more and more often used in strategic management of the organizational units. This tool includes the most important goals and efficiently indicators of the company visualized in four dimensions (perspectives): financial, customers, internal processes and learning perspective. BSC is a peculiar lint between the predefined strategic goal of the company and the holistic system of the operational type controlling solutions.

1. Introduction

In a company there is high demand for information useful in the process of controlling their accomplishment, which became a reason for a new field of accounting to develop – the management accounting. The created information is addressed mainly to the internal users – the organization's managers. The gained information plays a significant role in the decision making process. It allows the realization of the strategic goal the transactor through the formalised system of measurement, gathering, analysing and transforming both financial and next-financial data, which are passed on the decision-mating people of teams responsible for taking optimal actions in short, medium and long period [3]. This information can be expressed valuably (e.g. the cost of manufacturing the finished product), quantitatively (e.g. the number of contractors, number of commissions) al well as in the form of indices (profitability nation, ROE). Owing to the modern Technologies of information in the field of data processing using new management accounting techniques and method the company has the opportunity to optimize the decisions concerning the strategy realisation, create the expenses budgets, receipts, profits and form the financial plan for the future periods.

2. Management accounting tools – Balanced Scorecard (BSC)

The range of tools in management accounting is very wide, which is described in the professional literature [2]. There has been a growing interest in the strategic management accounting instruments recently, especially the Balanced Scorecard, which is a only tool integrating both organizational and strategic goals of an economic unit.

The administration of companies noticed the usefulness of this tool to deliver the strategic guidelines and to determine the aims and activities for the lower level managers in their organizational structure. BSC is a strategic management tool, which translates the mission and strategy into goals and indicators grouped in four different perspectives: financial, customers, internal processes and learning perspective [1].

Owing to those perspectives, the strategic and operational goals of the company are balanced and the evaluation of the diver pens between the executed company's strategy and the operational activities is possible. The financial perspective shows whether the introductions and realization of the companies economic growth. The customer perspective singles out the type of

dients and the company's objective market and presents the most important issues related to this market. The internal processes perspective determines the company's factors and activities that are necessary to meet the customers' requirements. The learning perspective defines the state of the company's basic recourses and the necessity of the organisational infrastructure.

3. A case study

The company of the IT branch – company XYZ exemplifies the usefulness of the Balanced Scorecard. The XYZ mission is to provide the safety of the offered systems, the constant development of it's own products, the acquisition and use of the modern techniques and technologies and the provide the service standards which will satisfy the customer.

The XYZ strategy is based on the priority generation of the increase of the process efficiency.

The next stage is the elaboration of BSC is the preparation of the strategy map for the organizational unit. The identification of the key success factors is very helpful, therefore the client's perspective is the most important one in BSC. The main thesis of the strategic map is the improvement of the operational effectiveness. The rate of sale growth, the raising of the customers satisfaction, the reduction of the orders realization time and the improvement of the complaints service can be marked out as the main strategic aims. The basic indicator is the ROE growth.

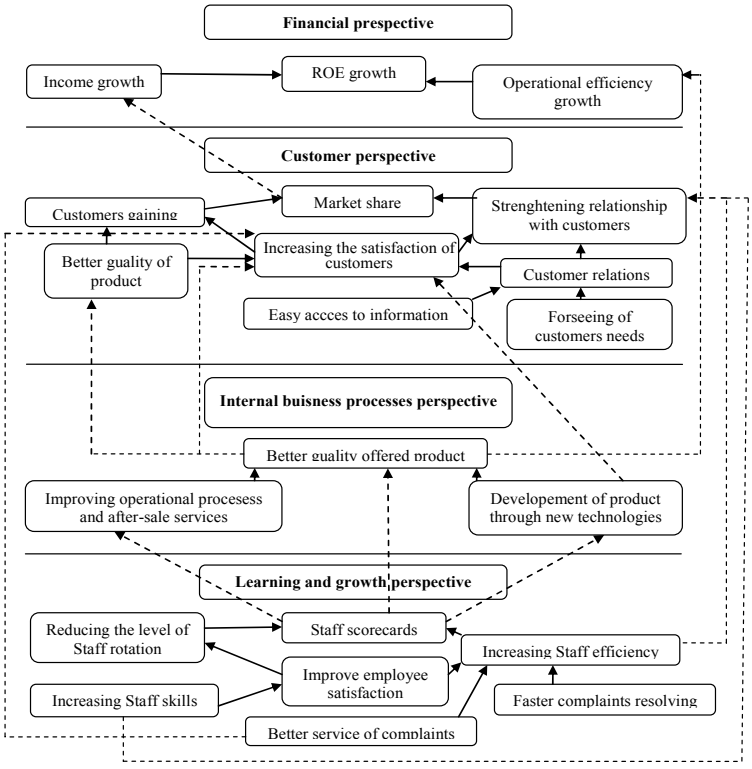


Figura 1. **The strategy map – an expression of the four perspective for the company XYZ**

Source: Own work based on data obtained from the company XYZ.

4. Summary

Article presents the issue of Balanced Scorecard. BSC is one instrument that is more and more often used in strategic management of the organizational units. This tool includes the most important goals and efficiently indicators of the company visualized in four dimensions (perspectives): financial, customers, internal processes and learning perspective.

BSC become very popular and gained the approval of the managers , because it allows to fully monitor the realization of the chosen strategy. BSC is the method which completes the project on the controlling introduction. It originates in a systematic way incorporating other tools. BSC is a peculiar lint between the predefined strategic goal of the company and the holistic system of the operational type controlling solutions.

Bibliography

1. Kaplan, Norton, *The Balanced Scorecard,* Polish Scientific Publishers PWN, Warsaw 2001
2. Piosik, *Theoretical Accounting Papers volume 32(88),* Warsaw 2006
3. Sobańska, *Costing and Management Accounting*, C.H.Beck, Warsaw 2003

ОБЩАЯ ХАРАКТЕРИСТИКА НЕЧЕТКИХ МОДЕЛЕЙ ОЦЕНКИ РИСКОВ ПРОЕКТА ВНЕДРЕНИЯ КИС

Екатерина АВДЕЕВА, Владимир ЧЕРНОВ
Владимирский государственный университет
(Российская Федерация)

In this article fuzzy models of risk evaluation during the introduction of enterprise information systems are described. Fuzzy model of SWOT-analysis of riskiness estimation of introduction project is considered. Fuzzy model of alternative choice of enterprise information systems is offered.

Анализ существующих методов оценки рисков: вероятностный анализ, экспертный анализ, метод аналогов, анализ чувствительности, анализ сценариев развития проекта, метод построения дерева решений проекта и имитационное моделирование с помощью метода Монте-Карло позволяет сделать вывод, что данные методы оценки трудно применимы к рискам внедрения КИС. Это объясняется тем, что для реализации этих методов необходимы статистические данные, которые отсутствуют, поскольку при внедрении КИС на предприятиях используется информация, актуальная на момент внедрения. Кроме того такие методы оценки рисков предполагают использование вероятностных характеристик или числовых экспертных оценок, применение которых к рискам внедрения КИС затруднительно. Поэтому существующие методы не отражают в полной мере специфику процессов внедрения КИС, что требует создания новых методов и моделей оценки рисков.

Рассматриваемые в работе подходы к оценке рисков внедрения КИС основаны на нечетких множествах, которые позволяют обрабатывать качественные экспертные оценки рисков проекта внедрения КИС.

Одной из простейших практических экспертных методик анализа рисков является SWOT-анализ – это качественный подход, базирующийся на сравнении или «взвешивании» противоположных качеств проекта. Классический вариант SWOT-анализа проекта внедрения КИС заключается в следующем. Сначала экспертным путем оцениваются сильные и слабые стороны проекта, его возможности и угрозы. Если сильные стороны больше слабых сторон и возможности больше угроз проекта, то такой проект можно реализовывать, поскольку его можно считать удовлетворительным с точки зрения риска. В противном случае такой проект является рискованным и его реализация нежелательна.

Классическая процедура проведения SWOT-анализа, несмотря на простоту реализации и наглядность результатов, имеет значительный недостаток: использование балльных оценок. Во-первых, при использовании баллов трудно доказать, почему применяются именно такие баллы (необходим метод назначения числовых оценок, который позволяет проверить их корректность). И, во-вторых, часто возникают ситуации, когда экспертам удобнее оценивать характеристики проекта не числами (или баллами), а качественными оценками. Примерами таких характеристик проекта внедрения КИС могут быть следующие:

1) квалификация команды внедрения (например, низкая, средняя, высокая);
2) цели и задачи внедрения (например, не сформулированы, плохо сформулированы, четко сформулированы);
3) участие и заинтересованность руководства (например, слабое, среднее, высокое);
4) опыт ведения аналогичных проектов (например, низкий, средний, большой) и другие.

Кроме того, традиционный SWOT-анализ не учитывает значимость и возможность реализации сторон проекта, а также отношение лица, принимающего решение (ЛПР), к возможности их реализации.

Новая методика проведения SWOT-анализа проекта внедрения КИС заключается в следующем. На основе оптимистической позиций (свертка нечетких множеств выполняется через операцию объединения) или пессимистической позиции ЛПР (свертка нечетких множеств выполняется через операцию пересечения) сначала выполняется свертка отдельно сильных сторон, слабых сторон, возможностей и угроз проекта. Затем выполняется свертка положительных характеристик проекта (сильные стороны и возможности) и отрицательных характеристик проекта (слабые стороны и угрозы). Если мощность нечеткого множества положительных характеристик проекта больше мощности нечеткого множества отрицательных характеристик проекта, то такой проект можно реализовывать. И наоборот, если мощность нечеткого множества отрицательных характеристик проекта больше мощности нечеткого множества положительных характеристик проекта, то такой проект рискованный и нежелателен для реализации.

Нечеткая модель SWOT-анализа проекта внедрения КИС не только основана на использовании нечетких множеств для обработки качественных экспертных оценок, но и рассматривает разное отношение ЛПР к реализации сторон проекта. Комбинации позиций ЛПР позволяет смоделировать различные варианты развития проекта внедрения КИС и сделать оценку рискованности проекта до начала его реализации.

В процессе управления рисками проекта важно не только оценивать риски до внедрения проекта, но и в процессе его реализации. Одним из главных этапов проекта внедрения КИС является выбор системы для внедрения, который влияет на риск неудачного выполнения самого проекта внедрения.

При выборе КИС для внедрения наличие неопределенности в выборе критериев или требований может привести к тому, что при реализации одной альтернативы (системы) возникает избыточность требований и, следовательно, излишние затраты. Или наоборот, заниженные требования могут привести к выбору неудачной альтернативы. Поэтому задачу выбора системы для внедрения целесообразно решать на основе необходимого и возможного уровня соответствия альтернатив заданным требованиям.

В общем виде модель альтернативного выбора КИС заключается в следующем. Экспертным путем определяются требования к системе, и оценивается важность рассматриваемых критериев. Также оценивается набор альтернатив на основе заданных требований. Для каждой альтернативы находятся мера различия оценок важности критериев и оценок соответствия альтернативы заданным требованиям; уровень идентичности альтернативы каждому критерию; необходимый и возможный уровень соответствия альтернативы каждому критерию и субъективная уверенность. Далее вычисляются результирующие оценки по каждому показателю с помощью аддитивной свертки (среднее арифметическое) и мультипликативной свертки (среднее геометрическое).

Наилучшей системой для внедрения может считаться та альтернатива, у которой мера различия оценок важности критериев и оценок соответствия альтернативы заданным требованиям минимальная; уровень идентичности альтернативы каждому критерию максимальная; необходимый и возможный уровень соответствия альтернативы каждому критерию максимальные и субъективная уверенность максимальная.

Рассмотренная методика альтернативного выбора КИС для внедрения может быть реализована, когда оценки важности критериев и оценки соответствия альтернатив заданным требованиям представлены в виде качественных оценок. На основе нечетких множеств вычисляется уровень соответствия и несоответствия каждой альтернативы заданным требованиям, а также мера неопределенности. Наилучшей системой для внедрения может считаться такая альтернатива, у которой максимальный уровень соответствия, минимальный уровень несоответствия и минимальная мера неопределенности.

Нечеткая модель SWOT-анализа проекта внедрения КИС удобна своей простотой и не требует особых навыков и больших затрат. Но аналитику данная модель для оценки рискованности проекта может показаться слишком простой.

Поэтому необходима более сложная модель, требующая детального анализа. В таком случае аналитик может воспользоваться моделью альтернативного выбора КИС, которая позволит не только выбрать наилучшую систему, но и снизить риск неудачной реализации проекта.

ОРГАНИЗАЦИЯ СИСТЕМЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

И. СОРБАТ, И. МИХАЛЬЧУК,
Харьковский национальный экономический университет (Украина)

Актуальность. Проблемы экономической безопасности предприятия приходится решать не только в период кризиса, но и при работе в стабильной экономической среде. Экономическая безопасность предприятия (ЭБП) – один из основных элементов современного менеджмента предприятия. Под экономической безопасностью понимают совокупность мероприятий (организационных, правовых, режимных, технических, информационных), направленных на достижение достаточного уровня безопасности от воздействия различных угроз внутренней и внешней среды. [1] На сегодняшний день к причинам нарушения стабильной деятельности предприятия отнесли внутренние угрозы, такие как мошенничество, недобросовестная конкуренция, умышленные утечки информации о коммерческой тайне и интеллектуальной собственности (инсайдерская деятельность), а стихийные бедствия, пожары отступили на задний план. В следствии возникает актуальность решения задачи организации системы экономической безопасности предприятия. Над проблемами в данной сфере работают известные специалисты и ученые: Верин В.П., Гуров М.П., Олейников Е. А., Кизим М.О., Клебанова Т.С., Шкарлет С.Н., Кавун С.В. и др. [2-7] Не до конца решенным остается вопрос внутренних угроз, и, как следствие, вопрос выявления (обнаружения) инсайдеров для предотвращения их деятельности.

Целью статьи является формализация положения о службе организации системы экономической безопасности предприятия для прогнозирования и предотвращения внутренних угроз ЭБП на примере инсайдерской деятельности.

Основной материал. Проанализировав основные открытые источники известных отечественных и зарубежных авторов в сфере ЭБ, предложим основные группы средств и методов обеспечения ЭБП: организационно-правовые; инженерно-технические; информационно-технологические; морально-психологические; специальные. Возникает задача – кем должна быть организованна служба ЭБП. Предлагается два решения, одним из которых является создание внутренней службы ЭБП и второе решение это передача функций обеспечения ЭБП в аутсорсинг. В данной статье предлагается первый вариант решения поставленной задачи это создание внутренней службы ЭБП. Рекомендуются

следующее положение о службе ЭБП, состоящей из четырех основных разделов: 1. Общие положения; 2. Задачи и функции службы; 3. Функции службы безопасности. 4. Организация работы службы ЭБП. Рассмотрим самые основные задачи предложенных разделов положения о службе ЭБП.

1. Служба ЭБП является самостоятельным подразделением предприятия. В своей деятельности подразделение руководствуется положениями конституции, требованиями законов государства, уставом службы безопасности, положением о коммерческой тайне, другими соответствующими актами государства. Структура и штаты службы ЭБП утверждаются председателем правления.

2. Основными задачами службы являются: 1) разработка и осуществление профилактических мероприятий; 2) сбор, обработка, хранение и анализ официальной и конфиденциальной информации; 3) организация и проведение мероприятий по обеспечению безопасности персонала предприятия, основных фондов и финансовых активов; 4) проведение работ по обеспечению защиты информации; 5) внедрение нормативных актов по организации охраны помещений; 6) проведение единой технической политики в вопросах охраны; 7) контроль, выполнение требований службы ЭБП; 8) проведение инструктажа и обучения работников предприятия правилам работы с конфиденциальной информацией.

3. В вопросах ЭБ: 1) организация и осуществление совместно с отделами предприятия мероприятий по защите конфиденциальной информации; 2) проверка сведений, а также данных о попытках шантажа, провокаций и иных неблаговидных акций в отношении персонала; 3) взаимодействие с правоохранительными органами; 4) организация сбора, накопления, анализа и автоматизированного учета информации; 5) проведение проверок в подразделениях предприятия и оказание им практической помощи; 6) взаимодействие с другими подразделениями при осуществлении ими деятельности, связанной с иностранными специалистами; 7) внедрение положения о коммерческой тайне; 8) обучение работников банка практическим навыкам по обеспечению экономической, информационной и физической безопасности; 9) оказание содействия отделу кадров по работе с персоналом; 10) сбор, обработка, хранение, анализ информации о клиентах предприятия; 11) выполнение поручений руководства службы.

4. Службу ЭБП возглавляет руководитель, назначаемый и освобождаемый от должности приказом председателя правления предприятия. Служба имеет право: 1) получать от подразделений информацию, необходимую для выполнения возложенных на нее основных задач; 2) давать разъяснения по правильному применению ведомственных актов по вопросам компетенции службы; 3) проверять соблюдение экономической безопасности в подразделениях; 4) требовать от сотрудников представления письменных объяснений по фактам нарушения ЭБ.

Вывод. Для дальнейшего исследования предлагается на основе стандарта IDEF0 построить и описать бизнес процесс создания положения о службе ЭБП, с целью эффективной организации работы внутренних подразделений службы ЭБП для предотвращения инсайдерской деятельности.

Литература

1. Экономический словарь//http://abc.informbureau.com/html/einaeaad.html
2. Верин В.П., Преступления в сфере экономики. - М., Дело.2002.
3. Кавун С. В. Жизненный цикл системы экономической безопасности предприятия // Управління розвитком. – 2008. – № 6. – С.17-21.
4. Кавун С.В., Сорбат И.В. Инсайдер – угроза экономической безопасности // Управління розвитком. – 2008. – № 6. – С.7-11.
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. Гуров М.П., Кудрявцев Ю.А. Теневая экономика и экономическая преступность в вопросах и ответах: Учебное пособие. - СПб.: Санкт-Петербургский университет МВД России, 2002. - 237 с.

ВНЕДРЕНИЕ СТАНДАРТА ISO 27001 В ОРГАНИЗАЦИИ

А. ХВОСТОВЕЦ,
FLT (Молдова)

This piece of information covers some major aspects regarding the ISO/IEC 27001 Standard, including its' brief description and implementation within organization.

Информация зачастую является ключевым активом компании, а ее защита - приоритетной задачей. Получение сертификации по стандарту ISO 27001 позволит сохранить и защитить Ваши информационные активы.

ISO 27001 является единственным пригодным для сертификации международным стандартом, определяющим требования к Системе Управления Информационной Безопасностью (СУИБ). Этот стандарт предназначен для обеспечения выбора адекватных и соразмерных средств защиты (контролей).

СУИБ помогает защитить Ваши информационные активы и придать уверенность любым заинтересованным сторонам, особенно Вашим клиентам. Стандарт определяет требования к созданию, внедрению, эксплуатации, контролю, обслуживанию и постоянной оптимизации СУИБ.

ISO 27001 – международный стандарт по информационной безопасности. Стандарт разработан Международной Организацией по Стандартизации (ISO) и Международной Электротехнической Комиссией (IEC). Данный стандарт содержит требования в области информационной безопасности для создания, развития и поддержания Системы Управления Информационной Безопасностью (СУИБ).

ISO 27001 подходит для любой организации, крупной или малой, относящейся к любой отрасли и расположенной в любой части мира. Этот стандарт осо-

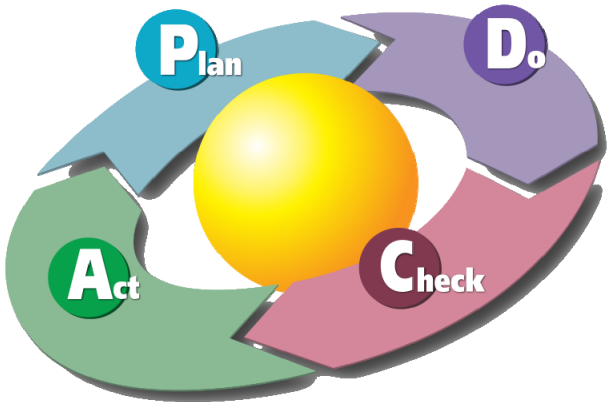
бенно полезен там, где защита информации приобретает очень важное значение, например в таких отраслях, как финансы, здравоохранение, госучреждения и IT.

ISO 27001 также эффективно используется в организациях, управляющих информацией по поручению другой стороны, например в компаниях, занимающихся аутсорсингом IT-ресурсов. Он может служить клиентам гарантией того, что их информация надежно защищена.

Ключевой характер в стандарте ISO 27001 носят **анализ рисков** и **оценка рисков**. Под анализом рисков *понимается систематическое использование информации для выявления источников и для оценки степени риска*. Под оценкой рисков - *целостный процесс анализа риска и оценки значительности риска.*

Организация может быть сертифицирована аккредитованными агентствами в соответствии с данным стандартом. Процесс сертификации состоит из трех стадий:

- **Стадия 1** - изучение аудитором ключевых документов Системы Менеджмента Информационной Безопасности — Положения о применимости (SoA), Плана Обработки Рисков (RTP), и др. Может выполняться как на территории организации, так и путём высылки этих документов внешнему аудитору.
- **Стадия 2** - детальный, глубокий аудит, включая тестирование внедренных мер и оценку их эффективности. Включает полное изучение документов, которые предусматривает стандарт.
- **Стадия 3** - выполнение инспекционного аудита для подтверждения, что сертифицированная организация соответствует заявленным требованиям. Выполняется на периодической основе.



Система управления информационной безопасностью (СУИБ) — часть общей системы менеджмента, основанная на подходе анализа бизнес-рисков и направленная на создание, внедрении, функционировании, мониторинге, анализе, поддержке и улучшении информационной безопасности (ISO 27001:2005).

В случае построения в соответствии с требованиями стандарта ISO 27001: 2005 основывается на модели Plan-Do-Check-Act:

- **Plan (Планирование)** – фаза создания СУИБ, создание перечня активов, оценки рисков и выбора мер;
- **Do (Действие)** – этап реализации и внедрения соответствующих мер;
- **Check (Проверка)** – фаза оценки эффективности и производительности СМИБ. Обычно выполняется внутренними аудиторами.
- **Act (Улучшения)** – выполнение превентивных и корректирующих действий.

Литература

1. Стандарт ISO2700:2005
2. Материалы сайта BSI (http://www.bsi.ru)
3. Материалы сайта ISO (http://www.iso.org)

СОТОВЫЕ СЕТИ ГСМ И ИХ БЕЗОПАСНОСТЬ

Михал СЭРВА,
Политехнический институт (Вроцлав, Польша)

В Польше первые системы сотовых сетей стали доступными в 1991 году (фирма Центртел). Это была самая простая аналоговая сотовая сеть первого поколения 1Г (*first-generation*), работающая на частоте 450MHz. Она покрывала свыше 90% территории страны. Системы сотовых сетей подвергнуты угрозам безопасности в такой же степени, как и проводные сети. Кроме того, в отношении радиотрансфера информации появляются дополнительные опасности.

Аналоговые системы (первого поколения) не были защищены, прежде всего, от радиоперехвата и использования для создания клона телефона. Такой обман был довольно распространенным в данном типе сотовых сетей и стал причиной больших финансовых потерь операторов. Эти системы была также неустойчивы к перебоям. У них не было международного роуминга, а также передача данных происходила очень медленно. Это вызвало появление цифровой системы второго поколения 2Г (2G), называемой системой ГСМ. Теоретическая скорость данных в такой системе достигала 9,6 кб/с, а трансмиссия речи с кодированием колебалась в пределе 13 кб/с. Были добавлены также узкополосные услуги такие как: данные, SMS, VMS, Fax. Система ГСМ900 была в Польше внедрена в 1996 году фирмами: Польская Телефония Цифровая (PTC ERA GSM) и Полкомтел (PLUS GSM). Следующей системой была система 2,5Г (2,5G), к которой добавлена трансмиссия данных GPRS. Система 2,5Г стала переходной к технологии третьего поколения в которой добавлена трансмиссия EDGE. Это сделало возможным трансмиссию с теоретической пропускной

способностью 384 кб/с через инфраструктуру ГСМ, UMTS (imt-2000), а также стали развиваться интернетовские и мультимедийные функции. В 2011 году оператор П4 (PLAY) планирует внедрить новый стандарт 4Г. Система 4Г это только маркетинговое название, а не сеть четвёртого поколения, такая как в США, а только расширение уже существующей технологии UMTS. Ещё долгое время системы UMTS будут существовать вместе с технологией ГСМ.

Требования, предъявляемые к операторам сотовых сетей и касающихся безопасности, вызываны следующими обстоятельствами:

- всеобщий рост доступности телеинформационных услуг,
- открытость операционных систем,
- введение трансфера данных,
- соединение с сетями IP,
- рост преступной деятельности (вирусы, обманы, перехваты).

Источники опасности системы ГСМ (*Global System for Mobile Communications*).

Самыми распространенными источниками опасности являются такие, как мошенничество в сети путем перехвата секретных данных (также данных персональных абонентов), а также «перехват», то есть перехват разговора в реальном времени. Это было нетрудно сделать. Существует также возможность «подделаться» под абонента и выманивать системные услуги за счёт абонента.

Существуют три типа действий, которые должны обеспечить телеинформационную безопасность:

- аутентификация пользователя с идентификацией места, с которого происходит передача информации,
- проверка тождества потребителя с помощью цифровой подписи,
- конфиденциальность и доступность информации должна быть гарантирована только санкционированным потребителям.

В сегодняшних сотовых (цифровых) системах сфера безопасности дополняется криптографическими технологиями, например:

- цифровой подписью,
- кодированием данных,
- сообщениями трассировки.

Главной основой безопасности является полное отделение оборудования потребителя (например мобильный телефон, смартфон) от данных этого потребителя. Это стало возможно с помощью SIM-карты (*Subscriber Identity Module*). Самые важные данные, определяющие возможности доступа к услугам, записаны именно на SIM-карте. Такая SIM-карта идентифицирет абонента в сети ГСМ при помощи уникального номера (*IMSI - International Mobile Subsciber Identity*), который приписан только одному абоненту.

Угрозы безопасности сотовым сетям можно разделить на следующие группы:

- несанкционированный доступ,

- блокирование через процесс идентификации, используя электронную подпись,
- блокирование несанкционированного доступа через шифрование данных с помощью зашифрованного ключа,
- использование максимальной частности абонента через добавление TSMI (*Temporary Mobile Subscriber Identity*), то есть временный номер мобильного абонента, который делает возможным идентификацию настоящего абонента.

Исключение также использования несанкционированного (украденного) терминала, например мобильника, блокируя его IMEI (*International Mobile Equipment Identity*) у операторов сети.

Литература:

[1] Kabaciński W., Żal M.: *Sieci telekomunikacyjne,* WKŁ, Warszawa 12/2008.
[2] Simon A., Walczyk M.: *Sieci komórkowe GSM/GPRS. Usługi i bezpieczeństwo*, Xylab, Kraków 2002.

ОРГАНИЗАЦИЯ СИСТЕМЫ ВНУТРЕННЕГО КОНТРОЛЯ

Лилия ПАВЛОВА,
IT&IS Management SRL (Республика Молдова)

Внутренний контроль затрагивает все сферы деятельности компании от целей бизнеса, включая эффективность и прибыльность, до сохранности ее ресурсов и защиты от мошенничества. Это контроль обоснованности принятия управленческих решений, которые могут оказать влияние на бизнес, а также принятие мер, предотвращающих мошенничество со стороны персонала.

Наиболее удачным и актуальным определением внутреннего контроля является определение в соответствии с моделью COSO (Committee of Sponsoring Organizations).

Внутренний контроль – это процесс, осуществляемый советом директоров, руководством и другим персоналом компании, который направлен на обеспечение разумной уверенности в том, что будут достигнуты цели организации в следующих аспектах:

- эффективность и результативность деятельности;
- достоверность финансовой отчетности;
- соответствие деятельности действующему законодательству.

При организации системы внутреннего контроля (СВК) необходимо руководствоваться следующими документами:

- стандарт COBIT (the Information Systems Audit and Control Foundation's Control Objectives for Information and related Technology) - обеспечивает решение задач о соответствии применяемых информационных технологий существующим бизнес-процессам и является основой для создания механизма контроля за эффективностью использования информационных технологий;
- документ COSO (the Committee of Sponsoring Organizations of the Treadway Commission's Internal control - Integrated Framework) – включает основные принципы организации системы внутреннего контроля и является руководством для ее создания и совершенствования;
- документ SAC - (the Institute of Internal Auditors Research Foundation's Systems Auditability and Control) – включает определение системы внутреннего контроля и описывается ее состав;
- Sarbanes-Oxley Act (SOX) – определяет требования к системе внутреннего контроля и прозрачности финансовой отчетности компаний.

Вероятность утечки активов компании в результате умышленного мошенничества и неумышленной некомпетентности персонала довольно высока, именно поэтому основным инициатором организации СВК является собственник бизнеса. СВК направлена противодействовать нарушению установленных в компании процедур управления, препятствовать несанкционированному распространению конфиденциальных сведений, своевременно оповещать топ-менеджмент и собственников о допущенных нарушениях. В прозрачности бизнеса заинтересованы и внешние инвесторы, которые серьезно относятся к сохранности своих средств и требуют того же от владельцев бизнеса.

Построение СВК должно основываться на следующих принципах:

- принцип ответственности - каждый сотрудник компании за ненадлежащее исполнение своих функций несет ответственность (экономическую, административную и дисциплинарную), которая закрепляется в его должностной инструкции;
- принцип разделения критических полномочий - распределение обязанностей с учетом конфликта интересов;
- регламентирующий принцип - любая операция осуществляется в строгом соответствии с регламентом, процедурой ее осуществления;
- принцип непрерывности - постоянное функционирование СВК и своевременное предупреждение о нарушениях и отклонениях в деятельности компании;
- принцип комплексности - все объекты должны быть охвачены внутренним контролем, адекватным характеру и масштабам деятельности этого объекта;
- принцип заинтересованности - обязательное наличие заинтересованности органов управления компании в эффективном функционировании СВК;

- принцип информационной достаточности - ограничение доступа к информации, не относящейся к выполнению конкретной функции и/или превышающей функциональную необходимость в рамках должностных обязанностей персонала;
- принцип соответствия - СВК должна быть адекватной масштабам деятельности компании, сложности его организационной структуры, характеру совершаемых операций, разнообразию объектов и направлений контроля;
- принцип приоритетности - при реализации контрольных функций каждым субъектом внутреннего контроля отдается приоритет направлениям деятельности компании, подверженным наиболее существенным рискам;
- принцип интеграции - наличие взаимодействия и координации между всеми элементами СВК;
- принцип сбалансированности - , который предполагает, что при определении полномочий, функций и обязанностей каждого субъекта внутреннего контроля ему предписывается соответствующий объем средств их выполнения (прав и возможностей), и наоборот, не допускается наличие средств, не связанных той или иной функцией; затраты и издержки на контрольные действия не должны превышать результаты и выгоды от их выполнения;
- принцип независимости и беспристрастности - лица, осуществляющие контроль процессов, не должны участвовать в реализации этих процессов и/или быть ответственными за них;
- принцип единоличной ответственности - закрепление каждой отдельной контрольной функции за одним субъектом контроля, допускается закрепление за одним субъектом внутреннего контроля нескольких контрольных функций.

Эффект от внедрения процедур внутреннего контроля не всегда может быть получен мгновенно и поддается количественной оценке. Система внутреннего контроля будет неполноценной, если не охватывает деятельность всех сотрудников компании независимо от выполняемых ими работ. Это позволяет управлять максимальным количеством рисков, которым подвержена деятельность компании.

Организация СВК должна включать следующие этапы:

- анализ требований регулирующих актов – на данном этапе необходимо определить применимые для компании регулирующие требования законов, определить критичные области в бизнес-процессах и информационной инфраструктуре;
- описание бизнес процессов – детально описать существующие процессы с четким описанием действий каждого участника процесса, а также входящей и исходящей информацией;
- определение рисков – идентифицировать риски на основании анализа детального описания процессов; сформировать перечень рисков, привязанных к соответствующим процессам и операциям;

- оценка рисков – осуществлять оценку рисков для последующей выработки эффективной стратегии их минимизации и предотвращения. Определить критичность рисков, стратегию управления рисками (принимать, страховать, избегать, предотвращать) и мероприятия по их устранению;
- разработка контрольных процедур – осуществлять исключение или минимизацию найденных рисков путем создания контрольных процедур. Наиболее эффективными являются превентивные контрольные процедуры, которые минимизируют саму вероятность появления риска, для повышения надежности процесса, превентивные процедуры применяют в комплексе с периодическими проверочными;
- тестирование контрольных процедур – осуществлять периодическую проверку выполнения контрольных процедур посредством набора тестов. Тестирование контрольных процедур включает проверку наличия базового документа (политики, процедуры, регламента), в котором определяется порядок и правила выполнения данного процесса. В рамках данного этапа формируется и выполняется система тестов, задача которых проверить правильность выполнения контрольных процедур в компании. Результаты данного этапа являются входной информацией для совершенствования контрольных процедур и системы внутреннего контроля в целом. Периодичность проведения тестирования устанавливается в зависимости от критичности процесса;
- управление внутренним контролем, осуществляемое владельцем процесса внутреннего контроля, который назначает собственников контролей, разрабатывает график тестирования, оповещает тестеров и собственников контроля о сроках проведения очередного тестирования, собирает и архивирует результаты тестирования.

Эффективность создаваемых процедур контроля зависит от следующих факторов: определение и понимание ответственности должностных лиц за выполнение контрольных процедур; разграничение доступа к информации или процессу; наличие документально оформленного описания процедур контроля; распределения задач контроля, исполнения и принятия решений между сотрудниками.

В заключение хочется отметить, что внутренний контроль должен быть регулярным процессом. Данный процесс требует правильного планирования, выполнения, проведения и совершенствования.

Список нормативной и научной литературы

1) COBIT (Control Objectives for Information and related Technology);
2) COSO (the Committee of Sponsoring Organizations of the Treadway);
3) Sarbanes-Oxley Act;
4) Постановление № 368 об утверждении Регламента о системах внутреннего контроля в банках.

ДИРИЖЕР СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Олег СОЛОНЕНКО,
Экономическая Академия Молдовы

In the paper analyzed requirements for building the information security system

Введение

По мнению экспертов в области информационной безопасности и в аналитических отчетах крупных брендов говориться о том, что самым слабым звеном в любой системе безопасности является человеческий фактор. Это значит, что построение системы управления информационной безопасности (СУИБ) необходимо начинать с человека, причем с человека, который будет эту систему строить и заботиться о ее каждодневной работе.

Профиль компетентности Офицера информационной безопасности

Найти офицера информационной безопасности является самой настоящей проблемой по причине несформированности профиля компетенции и отсутствия подготовленных специалистов. Главная его задача - это оценка и управление технологическими, производственными и иными рисками компании в срезе информационной безопасности. Предполагается, что данный специалист должен быть способен идентифицировать риски и управлять ими в соответствии с целями и задачами компании и уровнем ее развития. По-видимому, он будет входить в верхний эшелон управления компанией, чтобы иметь возможность сбалансировать потребности бизнеса и требования безопасности с учетом усложняющихся технологий, возросшего числа действий злоумышленников, требований законодательства и ожиданий партнеров. В дополнение к солидному образованию и опыту в области защиты информации он, несомненно, должен обладать стратегическим складом ума, познаниями в управлении предприятием и лояльностью к компании.

Есть несколько путей замещения вакантной позиции. Один заключается в заполнении этой позиции аудиторами или аналитиками в области безопасности. Проблема в том, что хороший аналитик и хороший управленец - не одно и то же. Это люди с принципиально разным складом ума, структурой мотивации и компетентностью, для совмещения в этом случае нужно учить и укреплять его по менеджерской составляющей. Второй путь - привлечение готового или почти готового специалиста из числа своих же сотрудников. В этом случае профессиональная компетенция будет усилена еще и знанием конкретного производства. [1]

С одной стороны, для офицера информационной безопасности необходимы знания таких понятий, как ACL, DES,VPN, с другой стороны ROI, SLA, бизнесс процессы. Не плохо бы иметь высшые образования в области: электротехники, информатики, экономики, психологии.

Построение системы информационной безопасности

Построение информационной безопасности в организации не стоит в списке задач под номером один. Существуют отдельные технические и программные средства – иначе организация больше простаивает, чем работает, но все это приобретенный опыт предыдущих лет [2]. И тут возникает серьезный инцидент или внешнее воздействие в виде закона (либо требования) – и тогда возникает потребность в построении системы способной реагировать на такие воздействия.

Самый простой способ возложить все на плечи ИТ. Если строить информационную безопасность снизу то при особом умении, каждый пользователь системы будет отвечать за состояние информации, не имея необходимых для этого инструментов. Может дойти до абсурда, когда собственнику информации необходимо доказывать право на доступ к ней. Организация при этом делиться на "Админов" (доступ ко всей информации) и "юзеров" (доступ к той ее части, к которой доступ получен в результате долгих хождений, многих подписей и изматыванием нужных админов) - и при этом топ-менеджмент в группе юзеров. Информация живущая за пределами ИТ систем – на бумаге или в вербальном виде живет своей отдельной жизнью.

Другая сторона медали – построение информационной безопасности сверху. Политика, процедуры, инструкции – все есть. Мы получаем красивую глянцевую обложку, можно даже с аудитом и с необходимыми сертификатами по безопасности. Кто-то видел в аудиторском заключении Ernst&Young, KPMG, PWC, строку о том, что в ИТ инфраструктуре организации найден сервер с игрой "Counter-Strike" где отдел маркетинга сражается с системными администраторами (и те и другие люди креативные), а на серверах организации собрана самая большая (после хостинговых и торентовых серверов) коллекция музыки от классики до хауса и последние фильмы (даже не вышедшие в прокат)? Программисты занимаются взломом чужих программ и изучением алгоритмов игр, в оболочке игры от первого лица - для "повышения своего профессионального уровня".

Понятно, что тот, кто платит, тот и заказывает музыку. А ответ лежит в области вычисления интеграла с пределами от 0 до беконечности. Думаю, что нужно сузить область. Нужно строить живой организм похожий на нейронные сети, которые отличаются от компьютера тем, что в них нет процессора, и они не хранят информацию в централизованной памяти. Знания и память сети распределены по ее соединениям. А офицер информационной безопасности не центральный процессор, а скорее маршрутизатор подбирающий путь с наименьшей стоимостью.

Люди – это главное, что определяет успех

Сейчас почти никого не нужно убеждать в том, что люди мотивированные, обученные, обладающие необходимыми для данной работы и данной организации компетенциями, в очень большой степени определяют успех бизнеса. Почти не осталось монопольных рынков, любое "ноу-хау" быстро подхватывают конкуренты, поэтому чаще всего теперь побеждает тот, у кого лучше команда. Известно, что характер человека включает в себя много качеств, таких как жизненный опыт, уровень интеллекта, социальный слой и среда, образование, пол, состояние здоровья, в том числе и психи-

ческого, темперамент, генотип и многое другое. Существует множество подходов к подбору и оценке персонала – необходимо рассматривать и применять те методики, которые выдержали испытание практикой и показали свою эффективность, что позволит использовать их для создания оптимальной систему оценки и мотивации персонала.

Выводы

Информационной безопасности – это синергия таких областей как математика, информатика, экономика, кибернетика, психология. "Один в поле не воин" – поэтому задача офицера информационной безопасности построить систему, в которую вовлечены все участники информационного пространства. Не стоит забывать о том, что со временем офицер информационной безопасности будет владеть объемом информации большим, чем кто-либо другой в организации [3].

Литература

1. Марк Розин – "Советы консультанта: Аутсорсинг до абсурда" [Электронный ресурс] - http://www.vedomosti.ru/newspaper/article/254596/autsorsing_do_absurda
2. А. Голов, В.Кузнецов - "Практический подход к построению системы управления ИБ" [Электронный ресурс] - http://www.topsbi.ru/default.asp?artID=903
3. Брюс Шнайер - "Психология безопасности" [Электронный ресурс] - http://www.securitylab.ru/analytics/350910.php
4. Статья "Хакер в столовой" - Электронный журнал "Хакер" [Электронный ресурс] - http://www.xakep.ru/post/35784/default.asp

ОЦЕНКА РИСКОВ, ВОЗНИКАЮЩИХ ПРИ ВНЕДРЕНИИ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Наталья ГРИГОРЬЕВА,
Антон ШУТОВ,
Денис ГРАДУСОВ,
Владимирский государственный университет (Российская Федерация)

The article addresses issues related to the assessment of risks arising from the implementation of corporate information systems. It is proposed risk assessment using fuzzy sets theory.

Декларируемые разработчиками корпоративного программного обеспечения выгоды и преимущества, получаемые в результате приобретения конкретной корпоративной информационной системы, проявятся только в случае ее успешного внедрения. Проект внедрения является сложным, многоэтапным процессом, связанным со значительными изменениями на предприятии и часто сопровождающимся различными трудностями и рисками. Поэтому при внедрении корпоративных информационных систем важно управлять рисками, которые необходимо заранее определять и оценивать. Своевременное определение рисков и связанных с ними факторов, позволит устранить недостатки проекта, тем самым повысив его эффективность.

Важным этапом при управлении рисками является их измерение или количественная оценка рисков. В работе предложен новый подход к оценке рисков внедрения КИС на основе метода экспертных оценок и теории нечетких множеств Л.Заде [1].

При проведении экспертного оценивания в целях максимальной автоматизации обработки экспертной информации при организации опроса экспертов чаще всего используется анкетирование. В предлагаемой эксперту анкете каждому фактору ставится в соответствие множество вариантов оценки, представляющих собой качественные суждения, характеризующие вероятность возникновения этого фактора. Опрашивается *K* экспертов и анкета содержит *P* факторов. Тогда каждому фактору можно поставить в соответствие лингвистическую переменную L_i ($i = \overline{1,P}$), значениями которой являются варианты оценки L_{ij} ($j = \overline{1,J^i}$), где J^i – количество вариантов оценки *i*-го показателя. Применительно к приведенному выше фактору:

L_i *(вероятность возникновения фактора)* = {*«очень низкая»* (L_{i1}), *«низкая»* (L_{i2}), *«средняя»* (L_{i3}), *«высокая»* (L_{i4}), *«очень высокая»* (L_{i5})}.

Эксперт должен сопоставить каждую оценку из этого множества с количественным показателем степени уверенности в том, что именно она будет иметь место. В теории нечетких множеств этот показатель называется значением функции принадлежности, обозначается $\mu_{L_{ij}^k}(u_{is})$ $(i = \overline{1,P}, j = \overline{1,J^i}, k = \overline{1,K}, s = \overline{1,S^i})$ и характеризует степень уверенности *k*-го эксперта, выбравшего в качестве оценки *i*-го показателя *j*-е значение лингвистической переменной, в том, что количественная оценка этой переменной может принять значение u_{is}. Функция принадлежности $\mu_{L_{ij}^k}(u_i), u_i \in U_i$, элементов базового множестваU_i нечеткому множеству L_{ij}, по мнениюk-го эксперта, в этом случае будет задаваться строкой:

$$\mu_{L_{ij}^k}(u_i) = \left[\mu_{L_{ij}^k}(u_{i1}); \mu_{L_{ij}^k}(u_{i2}); \ldots; \mu_{L_{ij}^k}(u_{iS^i})\right].$$

Каждое значение лингвистической переменной является нечетким и поэтому для его описания используется нечеткое множество. Это множество задается на базовом (четком) множестве $U_i = \{u_{is}, s = \overline{1,S^i}\}$ действительных чисел, охватывающем, по мнению организаторов опроса, весь возможный диапазон количественных оценок лингвистической переменной L_i.

Если уровень компетентности всех экспертов одинаков, то обобщенная нечеткая оценка может быть получена как пересечение нечетких множеств, соответствующих индивидуальным оценкам экспертов.

Функция принадлежности, количественно характеризующая эту оценку в соответствии с правилом выполнения операции пересечения нечетких множеств, определяется по формуле:

$$\mu_{B_i}(u_i) = \min_k\{\mu_k(u_i)\} == \left[\min_k(\mu_k(u_{i1})); \min_k(\mu_k(u_{i2})); \ldots; \min_k\left(\mu_k(u_{iS^i})\right)\right],$$
$$k == \overline{1,K}, \quad i = \overline{1,P}$$

Однако сформировать группу экспертов одинаковой компетентности практически невозможно. В связи с этим возникает необходимость определения степени компетентности экспертов и ее учета при получении обобщенной оценки. Влияние уровня компетентности эксперта на нечеткую количественную меру $\mu_k(u_i)$ предла-

гается реализовать путем выполнения операции «размывания». Математическое «размывание» нечеткой количественной меры $\mu_k(u_i)$ реализуется путем возведения ее в степень, соответствующую коэффициенту компетентности эксперта $\eta_k \leq 1$:

$$\tilde{\mu}_k(u_t) = \mu_k(u_t)^{\eta}, t = \overline{1,P}.$$

В результате опроса множества всех экспертов $(\Im = \{э_k, k = \overline{1,K}\})$ для каждого *i*-го $(t = \overline{1,P})$ фактора имеем *K* нечетких количественных мер $\tilde{\mu}_k(u_t)$, учитывающих степени компетентности опрашиваемых экспертов. Тогда нечеткое множество, характеризующее обобщенное мнение группы опрашиваемых экспертов при оценке *i*-го фактора, можно определить как пересечение нечетких мнений экспертов, имеющее функцию принадлежности:

$$\tilde{\mu}_{\Im_t}(u_t) = \min_k\{\tilde{\mu}_k(u_t)\}, \quad k = \overline{1,K}, \quad t = \overline{1,P}.$$

Полученные в ходе экспертного оценивания факторы могут оказать различное влияние на цель проекта. Таким образом, большое значение здесь имеет значимость факторов. Она также определяется экспертной оценкой. Наиболее подходящим здесь является метод парных сравнений [2], в котором экспертам предлагается произвести сравнение факторов попарно с тем, чтобы установить в каждой паре наиболее значимый.

Для количественного выражения каждого из *N* рисков, величина которых оценивается с помощью *N* факторов, необходимо воспользоваться аддитивной моделью:

$$f_t = \sum_{j=1}^{N} f_t^j a_j, \quad t = \overline{1,N},$$

где f_t^j – значение *j*-го фактора для оценки величины *i*-го фактора;

a_j – опасность *j*-го фактора.

Так как все значения факторов представлены в нечеткой форме, то аддитивная модель преобразуется следующим образом:

$$\tilde{\mu}_{\Im_t}(f_t) = \sum_{j=1}^{N} \tilde{\mu}_{\Im_t}(f_t^j)a_j = \tilde{\mu}_{\Im_t}\left(\sum_{j=1}^{N} f_t^j a_j\right), \quad t = \overline{1,N}.$$

Для получения однозначного количественного значения риска обычно выбирают тот элемент f_t^*, который имеет максимальную степень принадлежности к полученному обобщенному нечеткому множеству мнений экспертной группы:

$$f_t^* = \arg\max_{f_t} \tilde{\mu}_{\Im_t}(f_t).$$

Предложенный в работе подход на основе нечетких множеств позволяет устранить субъективность суждений отдельных экспертов и тем самым позволит существенно повысить качество оценки рисков проектов внедрения КИС.

Литература

1. Zadeh L. A. Fuzzy sets. Information and Control. – 1965. Vol. 8. – P. 338–353.
2. Дэвид Г. Метод парных сравнений. М.: Статистика, 1978.
3. Галкин Г. Методы определения экономического эффекта от ИТ-проекта // Intelligent enterprise. – 2005. №22. – с. 12-20

ВОПРОС ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ МИРОВОЙ ЭКОНОМИКИ

О. А. САХНО,
Харьковский Национальный Экономический Университет, (Украина)

Актуальность. Одним из ключевых процессов развития мировой экономики XXI века является прогрессирующая глобализация, т.е. качественно новый этап в развитии интернационализации хозяйственной жизни [1].

Несомненно, последствия глобализации могут носить как позитивный, так и негативный характер, однако альтернативы ей нет, в связи с чем основное внимание сейчас уделяется исследованию вопросов обеспечения экономической безопасности (ЭБ), а именно оценке уровня ЭБ при существовании потенциальных опасностей (угроз), которые несут процессы глобализации [1] .

Кроме того, усложняется решение вопросов экономической безопасности предприятий (ЭБП), в частности [2]. Об этом свидетельствует статистика, представленная на рис. 1.

Согласно исследованию PricewaterhouseCoopers, Украина занимает шестое место по уровню экономической преступности. Выше из стран СНГ - только Россия. 45% всех отечественных предприятий, которые принимали участие в опросе, сообщили, что хотя бы раз за последние 12 месяцев сталкивались с экономическими злоупотреблениями.

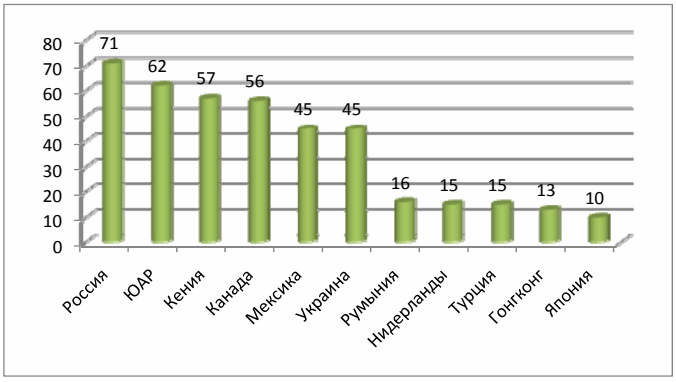


Рис. 1. **Распределение показателя экономической преступности по странам мира**

Цель статьи. Анализ вопросов экономической безопасности предприятий в условиях глобализации мировой экономики.

Основной материал. Такой анализ по отношению к Украине был проведен впервые, в котором Украина попала в лидеры черного списка. В отчете представлено 45% всех отечественных предприятий, которые принимали участие в опросе,

сообщили, что хотя бы раз за последние 12 месяцев сталкивались с экономическими злоупотреблениями (выявляли их в процессе своей деятельности или становились жертвами). По этому показателю Украину обогнали Россия (71%), Южно-Африканская Республика (62%), Кения (57%), Канада (56%) и Мексика (51%) [3].

Предприятие, работая в изменчивой среде, вынуждено оперативно реагировать на любые изменения, чтобы быть эффективным и конкурентоспособным на рынке. Актуальность решения вопросов ЭБП обусловлена наличием таких угроз, как нестабильность экономических процессов, устаревающее оборудование, морально устаревающие технологии, конкуренция, невыполнение договорных обязательств, промышленный шпионаж и т.п.

Самые распространенные типы экономических преступлений, согласно [3] представлены на рис.2.

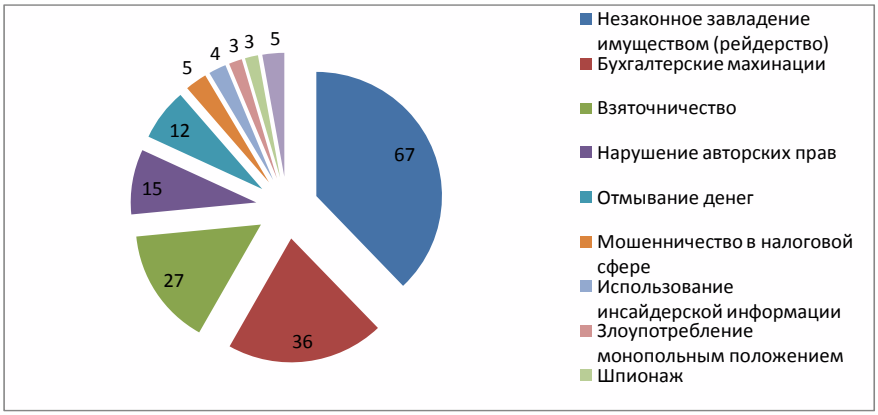


Рис. 2. **Распределение типов экономических преступлений**

Отечественное предпринимательство, получив прямой выход на мировые рынки [4], во многих случаях сталкивается не просто с отдельными конкурентными компаниями, а с государственно-монополистическими структурами, противостоять которым в одиночку они оказываются неспособными.

Вывод. Таким образом, предотвращение, своевременное выявление угроз – это задачи диагностики (оценки) уровня экономической безопасности предприятия. Системы экономической безопасности, существующие на предприятиях, в основном ориентированы на защиту коммерческой тайны, предупреждение промышленного шпионажа, информационной безопасности, наблюдение за сохранностью имущества предприятий, в то время как экономической и финансовой составляющим системы экономической безопасности на предприятиях практически не уделяется внимание, и этот вопрос требует дальнейшего исследования.

Литература:

1. Глобализация мировой экономики: проблемы и последствия. – [Электронный ресурс]. – Режим доступа: http://www.cfin.ru/press/management/2001-3/10.shtml

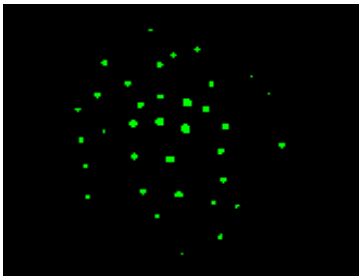
2. Кавун С.В. Аналіз стану інформаційної безпеки в системах дистанційного навчання. / С.В. Кавун, О.А. Сахно // Збірник наукових праць «Фінансово-кредитна діяльність: проблеми теорії та практики». – Харків: Вид. ХІБС УБС НБУ.– 2010. – № 1(8). – Частина ІІ. – С. 222-234.
3. Украина - на шестом месте по уровню экономической преступности. – [Электронный ресурс]. – Режим доступа: http://www.prostobiz.ua/biznes/upravlenie_biznesom/stati/ukraina_na_shestom_meste_po_urovnyu_ekonomicheskoy_prestupnosti
4. Выход украинских предприятий на мировой рынок капитала с помощью IPO. – [Электронный ресурс]. – Режим доступа: http://www.rusnauka.com/35_PWMN_2008/ Economics/38471.doc.htm

ВЫЧИСЛЕНИЕ ВЕРОЯТНОСТИ ПОВТОРА, МЕТОДЫ РАСПОЗНАВАНИЯ И СРАВНЕНИЯ ЭЛЕКТРОРАЗРЯДНОЙ МЕТКИ БУМАЖНЫХ ДОКУМЕНТОВ

Игорь ОГЛИНДЭ,
Министерство информационных технологий и телекоммуникаций (Республика Молдова)

The technology of protection of paper carriers by means of Electrodigit Technology, mathematical features of the given labels is investigated, proved them no reproducibility and singularity, the likelihood analysis of possibility of repetition of an Electrodigit Technology is carried out, possible algorithms of definition of authenticity of labels are resulted at comparison.

На прошлой конференции Securitatea Informationala господином *Шкилёв Владимир, Недиогло Виктор и Адамчук Аркадий* был представлен патент об электроразрядной защите бумажных документов. Схема проведения эксперимента чрезвычайно проста: на бумаге электроразрядным способом пробиваются небольшие отверстия; затем полученные образцы сканируются на просвет на обычном сканере и сохраняются в базе данных или подписываются цифровым кодом, в котором содержится информация о метке.



Целью исследований было выявление вероятности повтора метки и как следствие подделки документа. При проведении ряда экспериментов было обнаружено, что полученные отверстия имеют разные величины от 1-го до 30 пикселей и разные формы полимино. Теоретически, если даже одно отверстие сформировано из 15 пикселей, то оно может принимать до 27.394.666 различных форм, что дает нам уже возможность с уверенностью сказать, что практически невозможно пробить повторно такое же отверстие. Можно сказать, что каждое отверстие уникально в своем роде.

При ряде математических расчетов используя комбинаторный метод, было выявлено, что вероятность появления отверстий в том же месте, размером в один пиксель, нанесенных на метку очень мала:

$$C_n^r = \frac{n!}{r!(n-r)!}$$

80 отверстий – $0.2334*10^{-253}$, **100 отверстий** – $0.1119*10^{-307}$, **120 отверстий** – $0.9665*10^{-358}$

А если учесть и вероятность повтора формы отверстий, то вероятность уменьшается далеко за 10^{-450}. Так что с позиции уровня защиты эта величина равна бесконечности. Технологический аспект проблемы показывает, что бесконечность и 10^{-450} – слабо отличимые понятия. Данные расчеты доказывают, что электроразрядная технология защиты документов эффективна и безопасна – даже производитель этой метки не в состоянии создать две одинаковые метки.

Для распознавания меток было предложено несколько методов. Один из них состоит в следующем: метка сканируется, после чего осуществляется бинаризация изображения. Таким образом, можно получить различные математические характеристики метки, такие как число отверстий, величина и интенсивность расположений отверстий, площадь распределения, координаты и многие другие. Эти характеристики можно также использовать, как генератор случайных чисел, характерных для каждой метки в отдельности. Данный метод дает возможность составить единый цифровой код для каждой метки. Также из этих характеристик можно составить базу данных. Эту базу данных в дальнейшем можно использовать для сравнения и выявления подлинности меток. То есть при повторном сканировании и бинаризации метки, можно сравнивать характеристики и сказать с какой-то долей вероятности о подлинности метки. Такой метод хорош, если повторное сканирование происходит в тех же идеальных условиях что и первое, что на практике невозможно из-за изменений характеристик метки при сканировании под разными углами поворота.

Для решения этой проблемы было предложено несколько математических методов. На метку наносятся реперные точки для удобства определения координат и других характеристик отверстий, в дальнейшем используя различные алгоритмы, можно определить подлинность метки. Другой возможный метод без реперных точек состоит в вычислении после бинаризации центра тяжести каждого отверстия и площади, определяются два самых отдаленных отверстия и центры тяжести этих

отверстий можно использовать как реперы. Эти алгоритмы дают нам возможность при повторном сканировании не зависимо от угла расположения метки на сканере определить подлинность метки.

После определения характеристик точек для дальнейшей обработки меток можно использовать различные алгоритмы: теория графов и геометрические алгоритмы дают нам много возможностей. Например, **Алгоритм Краскала** для построения минимального остовного дерева, триангуляция **Делоне** и многие другие.

По итогам серии опытов и создания программ, где будут использоваться различные алгоритмы, можно будет сделать вывод о том какой алгоритм и какие методы будут наиболее эффективны и применимы на практике и наименее затратные и ресурсоемкие. Итоги данных работ в дальнейшем будут опубликованы и представлены на будущих конференциях.

Литература:

1) Шкилев В.Д., Адамчук А.Н., Недиогло В.Г. Электроразрядная технология защиты документов особой важности *(строгой отчетности)* Электронная обработка материалов, №2, 2008, с. 4-10.
2) Томас Кормен, Чарьлз Лейзерсон,Рональд Риверст, Клифорд Штайн. Алгоритмы построение и анализ.
3) Шкилев В.Д. и др. Патент Республики Молдова № 3389 «Способ идентификации объектов». MD-BOPI №8, 2007, с. 51.

ТЕНЕВАЯ ИНФОРМАЦИОННАЯ ЭКОНОМИКА

Григорий БОРТЭ,
Экономическая Академиа Республики Молдова

С развитием информационных технологий, проблема правонарушения в данной области становится всё более и более актуальной. Криминальные сообщества находятся в постоянном поиске путей получения дохода из любых возможных источников, и бизнес, основанный на вредоносном программном обеспечении, в наше время не является исключением в наши дни. Они ищут новые возможности для отмывания денег, и Internet стал для этого очень удобным средством. Ущерб, нанесенный данным криминальным сектором пользователям, компаниям и даже государствам не может быть переоценен. В этом отношении, Республика Молдова – не исключение. Молдавской экономике нужна защита от компьютерного криминала и теневой информационной экономики.

В соответствии с данными, предоставляемыми всемирным банком, теневая экономика составляет порядка 35,2% от мировой экономики. Конечно, эта оценка очень приблизительна, относительна и усреднена, ведь, например, в США теневой

сектор составляет 8,9%, в то время как в Нигерии он достигает 76%, при этом, учитывая, что в США ВВП больше, чем в любой другой стране, то и 8,9% составляют 700 миллионов долларов, что также превышает уровень теневой экономики в любой другой стране мира. Также, по данным всемирного банка, ВВП проявляет тенденцию к росту на протяжении последних 50ти лет[1]. Это относится как к уровню теневой экономики в отдельно взятых странах, так и к общемировому уровню. Дойче Банк (Deutsche Bank)[2] отмечает, что рост теневого сектора экономики может нести как нежелательные, так и положительные последствия. Очевидно, что во время недавнего экономического кризиса, некоторые страны противостояли ему лучше, чем другие. По данным Дойче Банка[2], страны с относительно высоким (например, Греция) и относительно низким (например, Австрия) уровнем теневой экономики лучше справляются с кризисом, чем страны со средним её уровнем (например, Германия). Подъем может быть вызван появлением новых инструментов нелегальной деятельности. Помимо прочих, в данной категории не последнюю роль играют инструменты, относящиеся к теневому сектору информационной экономики, например, сюда относятся[5] все виды вредоносного программного обеспечения, такие как троянские программы, вирусы и так далее. Абсолютно всё вредоносное программное обеспечение производится, продаётся и используется нелегально, все денежные потоки связанные с данной категорией программ может рассматриваться, как часть теневой экономики. В Молдове уровень теневой экономике оценивается на уровне 50ти-70ти процентов[6][7], что, безусловно, является очень тревожным знаком.

Но если подъем в теневом секторе экономики может и благоприятно сказываться на том, как страна справляется с кризисом, то возникает вопрос о том, надо ли вообще с ним бороться. Может, напротив, стоит его стимулировать? Но ответ прост. Согласно исследованию, проведенному Добаеввм И.А., теневая экономика составляет значительную долю в финансовых источниках терроризма, которые в последнее время показывают тенденцию к диверсификации[3]. Кроме того, теневая экономика нарушает законы, принципы государственности, а также подрывает благосостояние и процветание страны, уменьшая бюджет и ВВП, а также значительно ухудшает инвестиционный климат[4].

Существует множество соглашений, законов, договоров о противостоянии теневой информационной экономике, как государственных, региональных, так и международных. Однако, постоянство возникновения новых эпидемий компьютерных вирусов, количество существующих ботнетов, а также количество ущерба, нанесённого пользователям, компаниям и даже государствам показывает, что данные меры несколько неэффективны. Поэтому, данный сектор нуждается не просто в некоторых улучшениях, а, возможно, в новом, комплексном подходе к данной проблеме.

Библиография:

1. World Bank, *Underground Economy: Causes and Size.* No-Wook Park, Korea Institute of Public Finance.
http://siteresources.worldbank.org/PSGLP/Resources/UndergroundEconomyPark.pdf

2. Deutsche Bank, http://www.dbresearch.com/servlet/reweb2.ReWEB?addmenu=false&document=PROD0000000000252019&rdLeftMargin=10&rdShowArchivedDocus=true&rwnode=DBR_INTERNET_EN-PROD$NAVIGATION&rwobj=ReDisplay.Start.class&rwsite=DBR_INTERNET_EN-PROD.
3. Добаев И.А., *Источники, формы и методы финансирования современных террористических организаций в глобализирующемся мире.* Ростов-на-Дону, Издательство СКНЦ ВШ ЮФУ, 2008, ISBN 978-58-7872-371-8.
4. Ермаков С.М., *Теневая экономика: анализ и моделирование.* Москва, Финансы и статистика, 2005, ISBN 5-279-02996-3.
5. Охрименко С.А., Саркисян А.С., *Подпольная Информационная Индустрия*. За матеріалами ІІІ- ї міжнародної науково-практичної конференції Інформаційна та Економічна Безпека (INFECO-2010), Свиштов, Болгария, 2010.
6. Олару Б., *Молдова – это рыба, которая испортилась с головы*. 2005, http://mdn.md/ru/index.php?day=956
7. Павук О., *Фридрих Шнайдер извинился за ошибки в расчетах теневой экономики в Латвии*. 2010, http://www.baltic-course.com/rus/es_baltija/?doc=32259

АНАЛИЗ НОВЫХ ПОДХОДОВ К РЕГУЛИРОВАНИЮ МЕЖДУНАРОДНОЙ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ И УПРАВЛЕНИЮ РИСКАМИ НА ОСНОВАНИИ РЕКОМЕНДАЦИЙ BASEL III

Ирина БАЛИНА,
Славянский университет (Республика Молдова)

The problems of efficiency of usage of requirements of Basel Committee Basel II and preparations for passage on Basel III are researched. On the basis of the analysis of recommendations in the field of banking regulation lacks Basel II, singularities and advantages Basel III are formulated.

Планируемая в настоящее время глобальная реформа по выработке новых стандартизованных директив банковского сектора, получившая название «Basel III», станет крупнейшей за последнее десятилетие. Аналитики отмечают, что работа над новыми международными стандартами велась давно, концепция переписывалась, менялась несколько раз. Первоначально «Basel III» выглядел как серьезное улучшение уже существующего закона «Basel II», однако, пересмотр законопроекта, который состоялся летом 2010 г., привел к исключению большинства серьезных изменений. Окончательный вариант новых правил регулирования банковской

деятельности, получивших название «Basel III», представители органов банковского надзора и центральных банков 27 стран мира, входящих в Базельский комитет по банковскому надзору при Банке международных расчетов (Bank for International Settlements, BIS) утвердили 12 сентября 2010 г. Решения Базельского комитета одобрены в ноябре 2010 года на саммите «группы двадцати», а затем введены в действие на уровне отдельных стран. [1, 4-5].

Появление новых стандартов (Basel III) - это реакция на глобальный финансовый кризис. Первыми в ходе недавнего кризиса пострадали те национальные финансовые посредники, которые проводили активные трансграничные операции с трансрыночными продуктами на международных рынках денег и капиталов. Например, банкротство английского банка Northern Rock (сентябрь 2007 г.), американских банков Merrill Lynch (август 2008 г.) и Lehman Brothers (сентябрь 2008 г.). До начала глобального финансового кризиса это были крупные, известные структуры.

Суть новых директив состоит в существенном ужесточении требований к банковским резервам на покрытие возможных потерь от активных операций. А конкретнее – к банковским ликвидным резервам и их качеству. Главное положение реформы предполагает постепенное увеличение к 2019 году уровня ликвидных резервов собственного капитала банковского учреждения с 4% до 6%. За неисполнение требований к буферному капиталу предусматриваются санкции в виде ограничений на выплату бонусов сотрудникам и дивидендов акционерам [2].

Новые директивы начнут действовать с 1 января 2013 года. Таким образом, у банков есть 2 года на то, чтобы привести свои резервы в соответствие с новыми нормативами. Авторы реформы рассчитывают, что при повторении кризиса у банков не будет необходимости прибегать к помощи государства для спасения от банкротства. [3].

Принятый 12 сентября 2010 г. новый пакет международных банковских нормативов «Basel III», предусматривает последовательное ужесточение минимальных требований к достаточности капитала банков. Так, коэффициент достаточности основного капитала первого уровня (common equity, или обыкновенные акции банка плюс нераспределенная прибыль, в отношении к совокупным активам, взвешенным по уровню риска) будет повышен до 4,5% с текущих 2%. Кроме того, банки обязаны сформировать специальный буферный резервный капитал в размере 2,5% от активов (сверх капитала I уровня). С учетом этой «подушки безопасности» минимальные требования к базовому капиталу первого уровня (common equity) возрастают до 7% - то есть более чем в 3 раза с текущих 2%. Если банки не смогут сформировать необходимый буферный капитал, они столкнутся с регулятивными ограничениями на выплату дивидендов и бонусов сотрудникам. Стандарт «Basel III» также предусматривает повышение минимальных требований к капиталу I уровня (Tier 1), состоящему из базового компонента и дополнительных инструментов, поглощающих убытки в ходе текущей деятельности банка, до 6%, вместо нынешних 4%. [5-8].

Анализ рекомендаций Basel III позволяет выявить ряд его **особенностей:**

I. Новая опубликованная редакция Basel III только на первый взгляд содержит более мягкие требования по регулированию, чем зафиксированные в версии декабря 2009 г., сократив количество исключений и

установив достаточную продолжительность переходного периода. Эти требования, очевидно, играют на руку банкам Австралии и Японии, обеспечивая им рост в краткосрочной перспективе. Однако, существуют вопросы, которые не так явно освещены в документе, но при этом представляют значительный интерес.

II. Установленный восьмилетний период действия лицензий выбран не случайно и связан с массовым процессом латания прорех в балансах, который сейчас наблюдается в ряде крупнейших банков. При этом новые правила регулирования не намного строже, чем те, что были зафиксированы в Basel II, их ужесточение явно свидетельствует о наличии опасений со стороны центральных банков в отношении экономики в целом и состояния финансовой системы в частности.

III. Несмотря на очевидные достоинства новых правил регулирования, в частности, на улучшение показателей доходов в отчетности финансовых институтов за счет меньшего отвлечения капиталов на резервирование, смягчение требований регуляторов и длительный переходный период вызывают опасения и возможные проблемы в долгосрочной перспективе для участников финансового рынка, особенно в Европе и США.

IV. Не определена длительность переходного периода для нового норматива достаточности капитала. С этим связаны опасения недостаточной кредитоспособности финансового сектора, которая наблюдается сегодня и, судя по всему, продлится еще несколько лет, несмотря на положительные результаты недавно опубликованного стресс-теста. Если эти опасения верны, дальнейшее замедление темпов восстановления мировой экономики способно оказать жесткое давление на финансовый сектор США и Европы.

Решение о необходимости ежемесячно с марта 2010 г. подвергать коммерческие банки стресс - тестам принято и НБМ, основная цель которых - контроль ликвидности и валютной деятельности банков. По данным агентства «ИНФОТАГ», такой контроль со стороны регулятора рынка предусмотрен в Меморандуме с Международным валютным фондом, рассчитанным на 2010-2012 гг. В документе говорится, что по результатам стресс тестов и проводимого независимого диагностического исследования портфелей банков будет определяться потребность банков во вливании капитала с тем, чтобы коэффициент его достаточности оставался на безопасном уровне, превышающем 12% [9].

Аналитики банковского рынка считают данный пункт Меморандума формально правильным, но не имеющим практической ценности. Так эксперты финансовой компании Credit-Profit отмечают, что по состоянию на конец 2009 г. коэффициент достаточности капитала составлял 32,28%, что выше норматива в 2,7 раза. По их мнению, не имеет смысла писать о задаче поддержания достаточности капитала в Меморандуме, т.к. НБМ, как регулятор призван следить за основными банковскими показателями и не допускать их выхода за допустимые нормы. К примеру, за стабильностью лея и недопущению резких скачков его курса. Однако, указанная задача в документе не оговаривается, хотя в заглавии пункта упомянут пристальный контроль

за валютной деятельностью. Вместе с тем, в данном документе НБМ следовало подчеркнуть свое наблюдение за структурой кредитного портфеля, акцентировать внимание на необходимости снижения процентных ставок по кредитам и недопущении перекоса кредитного портфеля, тем более что положительные примеры в указанной сфере у НБМ имеются. Так, в 2008 – 2009 гг. НБМ удалось спасти банковскую систему РМ от кризиса ликвидности и всех вытекающих отсюда негативных последствий: в 2008 г. НБМ регулируя объемы потребительского кредитования банков, собрал приготовленные для этого ресурсы в фонд обязательных резервов и выпустил их во время последовавшего весной 2009 г. оттока депозитов. [10]

Среди **достоинств Basel III** можно отметить:

1. Список обязательных исключений из показателя капитала первого уровня, опубликованный в декабре 2009 г. после обсуждений летом - осенью 2010 г., был сокращен на два элемента. Базельский комитет банковского надзора отреагировал на пожелания Франции и Германии на включение в новую редакцию Basel III более мягких регулирующих требований.
2. Одновременно в расчет показателя капитала первого уровня были снова включены ранее удаленные элементы: отложенные налоговые активы и разрешенные инвестиции в общий капитал финансовых институтов. Однако для обоих элементов установлен максимальный порог на уровне 100 % от общего капитала банков. Установлен минимальный норматив доли заемных средств (капитал первого уровня / активы) на уровне 3%.
3. Смягчен норматив покрытия ликвидности.
4. Также предусмотрены меры реагирования на риски, связанные с государственными долгами, беспокоящими участников рынка в последнее время. В частности, по некоторым видам государственных облигаций установлен 15 % фактор риска.
5. Новые правила в отношении нормативов доли заемных средств и покрытия ликвидности вступят в действие в январе 2018 года. В отношении нового норматива достаточности капитала сроки вступления в действие не были четко определены, но ожидается, что переходный период все же будет достаточным по продолжительности.

Несмотря на то, что предполагаемый ввод новых правил начнется с 2013 года, а вступление в силу в январе 2019 года и позднее, во многих странах, в том числе и в Республике Молдова сейчас в самом разгаре находится внедрение предыдущих изменений в банковское регулирование, утвержденных Базельским комитетом «Basel II».

Таким образом, нормативы Базельского комитета банковского надзора «Basel III» имеют принципиальное значение для развития РМ, всего мирового финансового рынка, IT – структур, аутсорсинга банковского риск – менеджмента.

Библиография:

1. Показатели финансовой устойчивости. Руководство по составлению – Вашингтон, округ Колумбия, США: Международный валютный фонд, 2007 год, стр. 31, 66, 162, 186 - 187. ISBN 1-58906-401-0

2. Greg N. Gregoriou. Operational Risk Toward Basel III: Best Practices and Issues in Modeling, Management, and Regulation. The Wiley Finance Series, 2010, 498 p.
3. International Convergence of Capital Measurement and Capital Standarts Basle Committee on Banking Supervision. Basel: Guli, 1988.
4. Powel. Basel II and developing countries: Sailing through the sea of standards, рабочий документ по стратегическим исследованиям Всемирного банка №3387, 2004, стр. 27
5. Basel Capital Accord, Базель I Соглашение о достаточности капитала, Базельский комитет по банковскому надзору, Basel: Guli, 1988.
6. International Convergence of Capital Measurement and Capital Standarts Basle Committee on Banking Supervision. Basel: Guli, 2006.
7. http://www.bis.org/publ/bcbs118.htm - Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework November 2005.
8. www.bis.org/publ/bcbs107.pdf - The International Convergence of Capital Measurement and Capital Standards: a Revised Framework, Basel II Framework, 2004.
9. http://www.vedomosti.md/news/Natsionalnyi_Bank_Moldovy_Budet_Podvergat_Kommercheskie_Banki_Ezhemesyachnomu_Stresstestu - Национальный банк Молдовы будет подвергать коммерческие банки ежемесячному стресс-тесту. Молдавские ведомости, №2 (1348) от 13 января 2011 г.
10. http://www.nbm.md – сайт НБМ

РАЗРАБОТКА АЛГОРИТМА КОДА АУТЕНТИФИКАЦИИ СООБЩЕНИЙ

Татьяна БИЛЫК,
Московский государственный институт электроники и математики (технический университет) (Российская Федерация)

This article describes the Message authentication code algorithm, which was developed by the author. This algorithm ensures the authenticity of the message between two or more parties to the transaction. The algorithm may use variable key and tag lengths.

1. Введение

Код аутентификации сообщений представляет собой функцию, получающую на вход два аргумента (сообщение произвольной длины и известный отправителю и получателю секретный ключ), на выходе выдается результат, называемый имитовставкой. Обычно имитовставка передается или хранится вместе с самими защищаемыми данными. При получении данных, пользователь вычисляет значение имитовставки и сравнивает ее с имеющимся контрольным значением. Несовпадение

говорит о том, что данные были изменены либо подделаны. Таким образом, код аутентификации сообщений обеспечивает целостность и подлинность информации.

2. Стойкость кода аутентификации сообщений

Исследования показали, что сложность атаки на код аутентификации сообщений с длиной секретного ключа t бит и длиной имитовставки n бит оценивается как $O(2^{\min(t, n/2)})$, а число операций для её реализации $\min(t, n/2)$. Увеличивая параметры t и n, мы можем увеличить защищенность алгоритма, однако выбор слишком больших значений приведет к удорожанию его эксплуатации. В настоящее время минимально «безопасными» параметрами можно считать 128 битную длину ключа и 256 битную длину имитовставки, однако в связи с ростом вычислительных возможностей предвидится увеличение этих значений. Оптимальным является выбор t и n, удовлетворяющих соотношению $\begin{cases} t = n/2 \\ t \geq 128 \\ n \geq 256 \end{cases}$ (1)

3. Постановка задачи

В связи с неоднозначностью определения верхней границы параметров t, n, необходимо разработать универсальный алгоритм кода аутентификации сообщений, позволяющий выбирать любые t, n, удовлетворяющие соотношению (1).

4. Существующие подходы построения кода аутентификации сообщений

В настоящее время существуют следующие подходы построения кода аутентификации сообщений: на основе хэш-функции, на основе блочного шифра, на основе «универсального» хэширующего преобразования. Исследования показали, что для построения кода аутентификации сообщений, удовлетворяющего приведенным требованиям, оптимальным является второй подход. Далее приводится описание алгоритма кода аутентификации сообщений, разработанного на основе алгоритма CMAC.

5. Алгоритм кода аутентификации сообщений

Второй подход в простейшем виде заключается в использовании блочного шифра в режиме сцепления блоков шифртекста. Имитовставкой при этом является последний выходной блок шифрующего преобразования, т.е. длина имитовставки равна длине выхода этого преобразования. Для решения поставленной задачи был разработан алгоритм блочного преобразования, выдающий на выходе блоки любой длины кратной 64 битам. Обозначим b – длину имитовставки в битах, b кратно 64.

5.1 Получение ключевой информации

Алгоритм для инициализации требует один секретный ключ K` длины b/2 бит, на основе которого вычисляется ключ K длины кратной 256 бит и ключи K1, K2 длины b/2 бит каждый:

1) Вычисляем $L = E_K(0^b, K')$, где E – блочное преобразование, описанное в п. 5.3;
2) Вычисляем $K1 = L \cdot u$, где выражение $L \cdot u$ - произведение L и u в поле $GF(2^b)$;
3) Вычисляем $K2 = L \cdot u^2$;
4) Если $b/2 = 32s : 256$, то K=K` и конец, иначе переходим к следующему шагу;

5) Разбиваем K' на блоки длины 256 бит, последний блок будет неполным: $K'[1],...,K'[\lfloor s/8 \rfloor], K'[\lfloor s/8 \rfloor + 1]$.

6) Вычисляем $K'[i] = K[i]$ для $\forall i = \overline{1, \lfloor s/8 \rfloor}$ и $K'[\lfloor s/8 \rfloor + 1] = Hash(K[\lfloor s/8 \rfloor + 1])$, где Hash – вычисление хэш-функции по алгоритму ГОСТ Р 34.11-94.

5.2 Основной алгоритм кода аутентификации сообщений

Входное сообщение дополняется с конца 32 битами, содержащими длину сообщения. Результат M разбивается на блоки длины b бит. Имитовставка вычисляется применением к входному сообщению шифрующего преобразования E в режиме сцепления блоков шифртекста. При этом если последний блок входного сообщения полный, то к нему предварительно операцией XOR прибавляется ключ K1, иначе блок дополняется слева нулями и операцией XOR складывается с K2. Последний выходной блок преобразования E является имитовставкой.

5.3 Преобразование E

Преобразование E основывается на двукратном применении алгоритма шифрования ГОСТ 28147–89 в режиме простой замены и одной операции перестановки. Для введения зависимости от порядка следования 64–битных блоков в сообщении к каждым 64 битам прибавлять операцией XOR их порядковый номер (нумерация сквозная для всего защищаемого сообщения).

На вход E получает b–битный вектор M[i], $i = \overline{1, n}$, который разбивается на 64–битные блоки R[j], $j = \overline{1, s}$, где s = b/64, а также очередной порядковый номер 64-битного блока l и ключ K длины $256 \bullet \lceil s/8 \rceil$ бит.

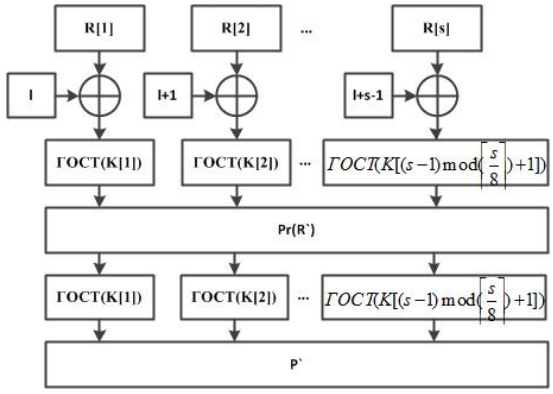


***Рис. 1.* Преобразование E**

Преобразование E представлено на рисунке 1 и состоит из следующих вычислений:

1. $R[j] = R[j] \oplus (l + j - 1)$ для $\forall j = \overline{1, s}$.
2. $R`[j] = ГОСТ(R[j], K[(j-1) \bmod(\lceil s/8 \rceil) + 1])$ для $\forall j = \overline{1, s}$, где ГОСТ – шифрование по алгоритму ГОСТ 28147-89 в режиме простой замены.
3. $P = \Pr(R`)$, где $R` = R`[1] \| ... \| R`[s]$, Pr – перестановка, описанная в п. 5.4.
4. $P`[j] = ГОСТ(P[j], K[(j-1) \bmod(\lceil s/8 \rceil) + 1])$ для $\forall j = \overline{1, s}$, где $P = P[1] \| ... \| P[s]$.

5.4 Перестановка Pr

На вход Pr поступает вектор R длины b бит, каждые 64 бита которого разбиваются на s фрагментов. Если $64 \vdots s$, то длина каждого фрагмента равна 64/s, иначе каждый 64 битный блок разбивается на s-1 фрагментов длины $\lfloor 64/s \rfloor$ бит и один неполный фрагмент длины $64-(s-1)\bullet\lfloor 64/s \rfloor$ бит. Далее к полученной последовательности $r_{1,1}, r_{1,2}, ..., r_{1,s}, r_{2,1}, r_{2,2}, ..., r_{2,s}, ..., r_{s,1}, r_{s,2}, ..., r_{s,s}$ применяется перестановка, как показано на рис. 2, по соотношению: $r'_{i,j} = r_{(i+j-2) \bmod s+1, j}$ для $\forall i, j = \overline{1,s}$. В результате получаем последовательность 64-битных блоков, каждый из которых зависит от каждого 64-битного блока, полученного на вход Pr.

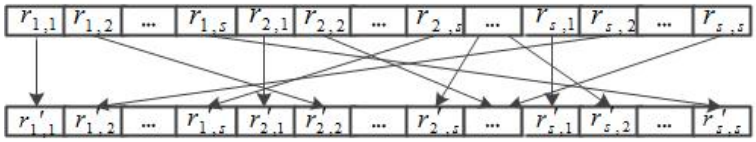


Рис. 2. **Перестановка Pr**

ОБЕСПЕЧЕНИЕ СТАНДАРТИЗАЦИИ БИЗНЕС ПРОЦЕССОВ ОБРАБОТКИ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И ВНЕДРЕНИЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Михаил НИЩИЙ,
Эксперт (Республика Молдова)

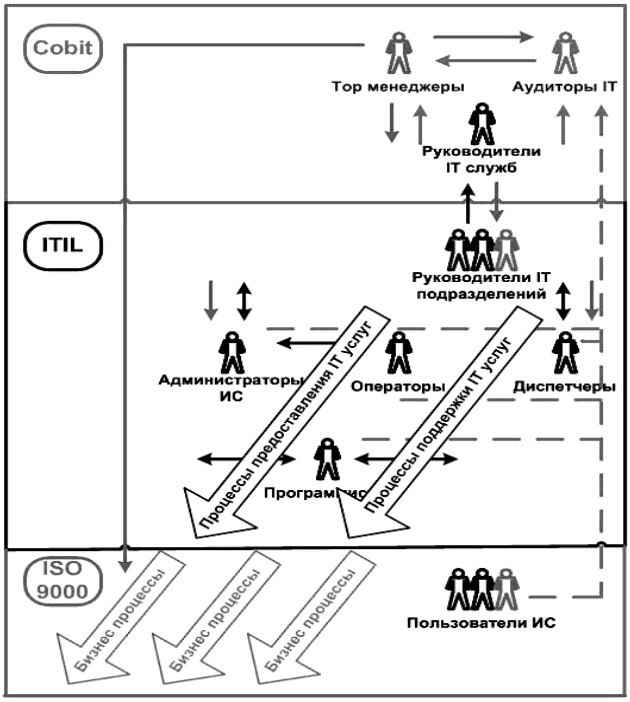
The purpose of this article is to discuss practical aspects of possible directions for standardization of data processing and business processes based on international standards ISO 27001, ISO 9001 and ITIL library in terms of improving information security systems.

Целью настоящей статьи является обсуждение практических аспектов разработки и внедрения системы управления информационной безопасностью в организации, предоставляющей социальные услуги населению.

Внедрение политики ИБ предполагает разработку совокупности документированных правил, регламентов, процедур, инструкций или руководящих принципов в области информационной безопасности, которыми должны руководствоваться сотрудники организации в своей повседневной деятельности. При этом, как правило, основное внимание уделяется требованиям и рекомендациям соответствующей международной и внутригосударственной нормативно-методической базы в области защиты информации. Особое значение этот факт имеет , когда организация внедряет

несколько стандартов, как в нашем случае стандарт управления качеством ИСО 9001:2008 и проводит работы по внедрению требований стандарта управления информационной безопасностью ИСО 27001:2005

В работе [1.2] мы определили место системы управления информационной безопасностью ISO 27001 в общей архитектуре менеджмента организации, в условиях внедрения стандарта ISO 9001 управления качеством, а также использования библиотеки ITIL (рис.1). В таблице 1 приведено сопоставление требований регуляторов управления качеством стандарта ИСО 9001 с соответствующими показателями (регуляторами) с стандарта управления информационной безопасностью – ISO 27001 (см. табл.1).



Одним из основных условий эффективного функционирования системы управления ИБ является вовлеченность руководства организации в процесс разработки и внедрения системы управления ИБ.

При этом важно отметить необходимость понимания всеми сотрудниками организации следующих основных моментов:

1) вся деятельность по обеспечению ИБ инициирована руководством организации и обязательна для выполнения всеми сотрудниками компании, 2) руководство компании лично контролирует разработку и функционирование системы управления ИБ, 3) само руководство выполняет те же правила по обеспечению ИБ и требует того же от сотрудников организации.

Разработка политики безопасности собственными силами – длительный и трудоемкий процесс, требующего высокого профессионализма, отличного знания

нормативной базы в области информационной безопасности. В соответствии с принятой практикой руководством организации было принято решение выбрать внешнюю специализированную компанию для проведения аудита информационной безопасности (ИБ) автоматизированных информационных ресурсов организации и разработки концепции и политики ИБ.

В докладе обсуждаются некоторые практические вопросы выполненного аудита системы управления ИБ организации, полученные результаты и рекомендации, представленные компанией аудитором.

Анализ информационных рисков – составная часть процесса управления рисками. При выполнении работ по анализу информационных рисков были оценены уязвимости информационной инфраструктуры организации к угрозам информационной безопасности, их критичность и вероятность ущерба, выработаны контрмеры по уменьшению рисков до приемлемого уровня и предложены методы контроля для защиты информационной инфраструктуры.

Оценивая информационные риски, ИТ-специалисты не ограничились только лишь одними информационными системами, программным, аппаратным и коммуникационным обеспечением, а также были рассмотрены вопросы физической безопасности и учтены и вопросы, связанные с человеческим фактором.

Сегодня высшее руководство любой компании по существу имеет дело только с информацией – и на ее основе принимает решения. Понятно, что эту самую информацию готовят множество нижестоящих слоев достаточно сложной организационной системы, которая называется современным предприятием. И нижние слои этой системы вообще могут не иметь понятия о том, что они производят не только какую-то продукцию или услугу, но и информацию для руководства. Глубинный смысл автоматизации бизнес-процессов заключается как раз в том, чтобы ускорить и упорядочить информационные потоки между функциональными уровнями и слоями этой системы и представить руководству компании лишь самую необходимую, достоверную и структурированную в удобной для принятия решения форме информацию. Критичная для производства и бизнеса информация должна быть ***доступной, целостной и конфиденциальной.*** Отсюда нетрудно сделать вывод, что ключевой бизнес-задачей корпоративной системы ИБ является обеспечение гарантий достоверности информации, или, говоря другими словами, гарантий доверительности информационного сервиса. В соответствии с рекомендациями стандарта по управлению информационной безопасностью ISO 27001:2005, в организации были определены требования к функционированию системы документов информационной безопасности, в том числе, и связи этих документов с документами системы управления качество, которая внедряется в соответствии с требованиями стандарта ИСО 9001:2008.

В процессе внедрения стандартов ИСО 9001 и ИСО 27001 были определены взаимосвязи с документами, которые разрабатываются на предприятии в рамках внедрения стандарта ISO 9001.

Система управления ИБ фактически охватывает три основные области, где действуют следующие стандарты:

а) стандарт ISO 9001 (регламентация и описание бизнес процессов предприятия),
в) описание процессов предоставления ИТ услуг и поддержки ИТ услуг (регламентация и описание осуществляются на основании требований библиотеки ITIL),
с) описание процедур и правил информационной безопасности, основанные на методологии оценки информационных рисков (регламентация и описание на основании требований и рекомендаций международных стандартов типа ISO/IEC 17799:2005 , ISO/IEC 27005, а также стандартов в области управления информационными рисками Cobit).

Одной из важнейших составляющих эффективной системы управления информационной безопасностью является набор работающих политик, регламентов, процедур и инструкций. Указанные документы необходимы, чтобы у всех работников предприятия было одинаковое понимание о том, что, когда, как и кто должен делать для защиты информации.

В докладе приводится таблица возможной классификации документов в области ИБ в соответствии со стандартом ИСО 27001 и связи этих документов со стандартом ИСО 9001.

Выводы:

1. Сравнительный анализ показывает, что в обоих стандартах ИСО 9001 и ИСО 27001 прослеживается концептуальное единство регуляторов управления качеством и информационной безопасностью производства и это даёт предпосылки для выстраивания сквозной процедуры аттестации (сертификации) организации одновременно как по показателям качества, так и гарантии обеспечения непрерывности основных бизнес-процессов на основе доверительности информационного сервиса.

2. Внедрение политики ИБ требует регламентации практически всех процессов обработки, хранения, передачи и обмена информации, разработки документированных процедур и инструкций. В этой связи целесообразно использовать имеющиеся стандартные методологии для повышения качества подготавливаемых документов (например, библиотека ITIL, методология Microsoft MOF и т.д.).

3. Как показывает практика, организационные меры играют очень важную роль во внедрении мероприятий политики ИБ в организации, поэтому необходимо организовать непрерывное повышение осведомленности, повышения квалификации и обучения сотрудников организации в области ИБ.

Список литературы:

1. Т.Мишова, М.Нищий. Информационный менеджмент и моделирование развития системы социального страхования. Информационно осигурование на бизнеса. Юбилена международна научна конференция. Академично издательство «Цинев», 7-8 юни, 2006, стр.28-39.
2. М.Нищий. Практические аспекты разработки и внедрения политики информационной безопасности. Securitatea informațională 2010. Conferință ineternațională (ediția a VII-a), 15-16 aprilie 2010. pag.108-110.

4. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
5. ISO/IEC 27005:2008 Информационная технология – Методы Безопасности – Управление рисками информационной безопасности.

EFICIENTIZAREA SERVICIILOR PUBLICE PRIN GUVERNARE ELECTRONICĂ ÎN REPUBLICA MOLDOVA

Vitalie SPÎNACHI,
Academia de Studii Economice din Moldova

Dificultățile şi barierele în obținerea serviciilor publice

Fiind o țară în curs de dezvoltare, R. Moldova este sortită, într-o măsură mai mare, să aibă un decalaj accentuat între nivelul de servire a clienților, în instituțiile publice, față de serviciile oferite de sfera privată. Nivelul necompetitiv de servire a clienților în sfera publică constituie o parte din moștenirea transmisă societății la destrămarea URSS. Conform unui sondaj de opinie (organizat de Magenta Consulting, la inițiativa Institutului de Politici Publice, în iulie 2010), de cele mai dese ori, în obținerea serviciilor publice cetățenii se confruntă cu durata mare de așteptare, indiferență din partea personalului, dezorganizare, corupție, calitate proastă a deservirii, incompetența personalului ș.a.

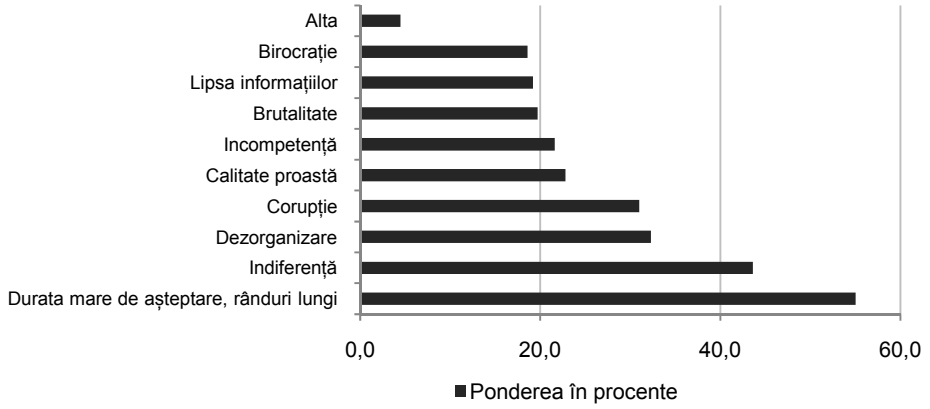


Figura 1. **Dificultățile şi barierele cu care se confruntă cetățenii în obținerea serviciilor publice**

Una din soluțiile referitoare la îmbunătățirea calității serviciilor publice, care se implementează, mai mult sau mai puțin cu succes, constă în guvernarea electronică. Această sarcină este înscrisă în agenda Departamentului Tehnologiilor Informaționale, încă din anul 2005, când a fost adoptată Strategia Națională de edificare a societății

informaționale "Moldova Electronică", aprobată prin Hotărârea Guvernului nr.255 din 9 martie 2005, prin care a fost lansată implementarea guvernării electronice. În scopul asigurării bazei conceptuale a acestui proces, la data de 28 iunie 2006, Guvernul Republicii Moldova a aprobat Concepția Guvernării Electronice.

În domeniul eficientizării serviciilor publice, se așteaptă ca programul de guvernare electronică să se soldeze cu următoarele efecte:

- îmbunătățirea cunoaşterii sistemului de guvernare şi sporirea gradului de participare a cetățenilor în procesul de guvernare, sporirea transparenței în activitatea Guvernului şi a instituțiilor publice, consolidarea democrației electronice;
- crearea informațiilor disponibile /livrabile, prin punerea la dispoziția cetățenilor a bazelor de date, a paginilor web şi a site-urilor guvernamentale şi municipale, actualizarea informației;
- reducerea birocrației şi corupției în activitatea autorităților administrației publice;
- facilitarea feedbackului, mai ales, prin intermediul telefoniei sau al poștei electronice;
- eficientizarea activității administrației publice prin optimizarea utilizării resurselor materiale şi umane, precum şi a timpului prestării serviciilor;
- acces extins la serviciile statului;
- crearea şi implementarea sistemelor şi aplicațiilor informatice, menite să susțină procesele de reformă şi dezvoltare politică, socială şi economică din țară, a mecanismelor performante de gestiune economică;

Principalele realizări în acest domeniu au fost următoarele:

- Pagina oficială a Republicii Moldova (www.moldova.md);
- Pagina oficială a Guvernului – www.gov.md;
- Regulamentul cu privire la modul de publicare a informației pe paginile oficiale ale autorităților publice în rețeaua Internet (H.G. nr. 668 din 19 iunie 2006);
- Strategia Națională de edificare a societății informaționale – "Moldova Electronică";
- Planul de acțiuni pentru realizarea strategie menționate ce este divizat în următoarele compartimente: Infrastructura societății informaționale, Guvernarea şi democrația electronică, Economia electronică, Educația electronică, Ştiința electronică, Cultura electronică, Sănătatea electronică. Respectiv, pentru fiecare acțiune este stabilit termenul de realizare şi autoritățile responsabile;
- Crearea centrului de guvernare electronică - www.egov.md;
- Crearea portalului de servicii electronice - www.e-services.md.

Domeniile prioritare de dezvoltare a serviciilor electronice: Educația, Sănătatea, Protecția socială şi Agricultura. E-serviciile publice vor fi oferite la câteva niveluri de complexitate: nivelul I – Informare, nivelul II – Interacțiune, nivelul III – Tranzacții , nivelul IV – Transformare.

Totodată, Uniunea Europeană recomandă statelor-membre prestarea, în format electronic, a 20 de servicii publice on-line pentru cetățeni şi mediul de afaceri. Domeniul

serviciilor publice electronice vizează trei direcții: „Guvern-cetățean", „Guvern-business" şi „Guvern-Guvern".

Serviciile publice electronice de bază pentru cetățeni sunt următoarele:

- Plata taxelor şi impozitelor;
- Căutarea unui loc de muncă prin intermediul bursei muncii;
- Contribuții pentru protecția socială;
- Documente personale (buletin de identitate, paşaport, permis de conducere);
- Înmatricularea vehiculelor;
- Eliberarea autorizațiilor de construcție;
- Declarații la poliție;
- Asigurarea accesului la bibliotecile publice (cataloage on-line, motoare de căutare, cărți electronice);
- Solicitarea şi eliberarea certificatelor (de naştere, de căsătorie);
- Admiterea în învățământul superior;
- Anunțul schimbării domiciliului;
- Servicii de sănătate.

Serviciile publice electronice de bază pentru mediul de afaceri includ:

- Achizițiile publice;
- Contribuțiile sociale pentru angajați;
- Înregistrarea unei noi societăți comerciale;
- Autorizațiile de mediu, inclusiv dările de seamă;
- Domeniul fiscal (TVA: declarația, anunțul);
- Domeniul vamal (declarația vamală, notificarea);
- Taxele corporative (declarația, anunțul);
- Publicarea de date statistice.

Servicii electronice disponibile pentru cetățenii Republicii Moldova

ÎS „CRIS „Registru" prestează doar o parte din aceste servicii: comanda actelor personale, un complex de servicii ce țin de înregistrarea transportului auto, eliberarea certificatelor şi serviciul de înştiințare privind schimbarea domiciliului. Serviciul Stării Civile prestează servicii ce permit solicitarea, în regim on-line, a duplicatelor adeverințelor şi a extraselor de pe actele de stare civilă, iar Camera Înregistrării de Stat prestează servicii on-line de înregistrare a întreprinzătorilor individuali.

Nivelul de solicitare a serviciilor publice

Instituțiile şi organele administrației publice, la care au apelat cei mai mulți respondenți, sunt policlinicile şi centrele medicilor de familie – 39%, urmate de primării – 24%, spitalele publice – 18% şi oficiile de documentare a populației – 16%. Nivelul de solicitare a fiecărui serviciu public a fost măsurat prin ponderea persoanelor, care, în decursul ultimelor 12 luni, s-au adresat, cel puțin o singură dată, la instituția publică ce prestează serviciul respectiv.

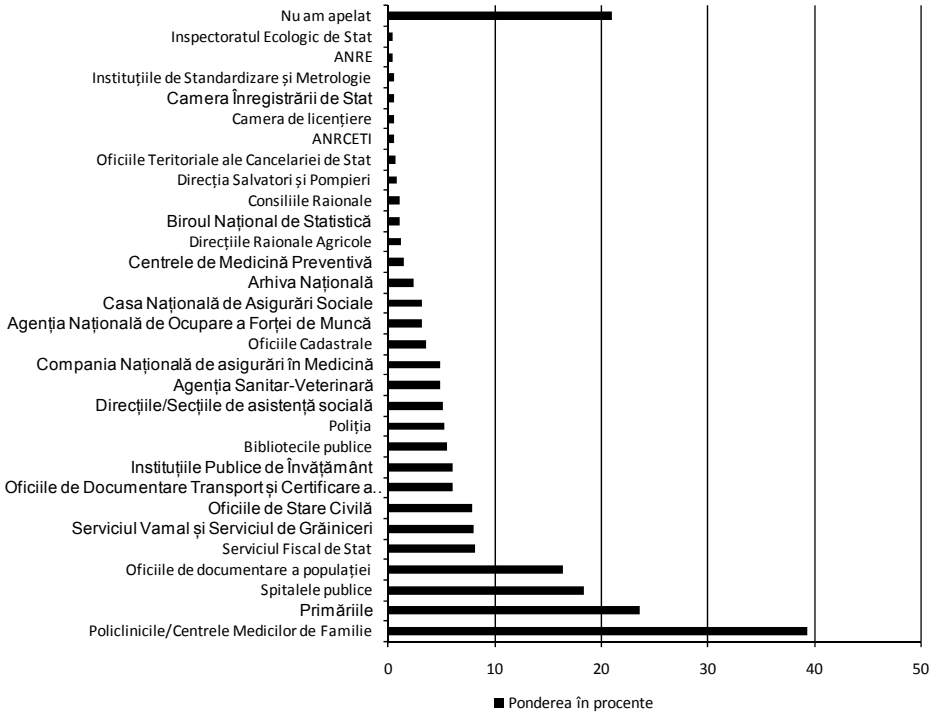


Figura 2. **Nivelul de solicitare a serviciilor publice**

Serviciile publice pe care cetățenii ar prefera să le primească prin Internet sau telefonia mobilă

Conform rezultatelor sondajului de opinie menționat mai sus, serviciile publice, de care ei ar prefera să beneficieze prin intermediul Internetului sau al telefoniei mobile, sunt următoarele: serviciile de sănătate (60%), de căutare a unui loc de muncă (60%), de perfectare a documentelor personale (49%), de înscriere în instituțiile de învățământ (40%).

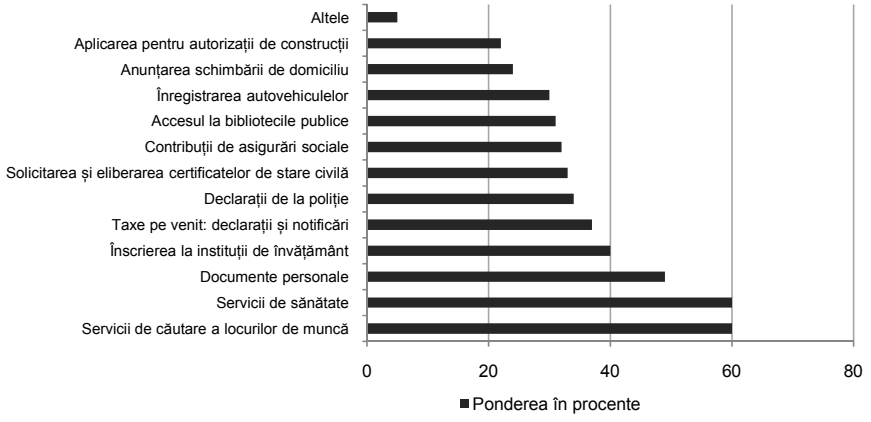


Figura 3. **Serviciile publice de care cetățenii ar prefera să beneficieze prin Internet sau telefonia mobilă**

Benchmarking și recomandări

Analiza comparativă între domeniile recomandate de UE, pentru a fi prestate în regim electronic, cu domeniile serviciilor cel mai des solicitate de populația Republicii Moldova și domeniile care sunt disponibile, la moment, în regim on-line, relevă următoarele:

- Cel mai des populația apelează la serviciile policlinicilor, primăriilor, spitalelor, oficiilor de documentare a populației, Serviciului Fiscal de Stat.
- Cetățenii ar dori să apeleze on-line serviciile de căutare a locurilor de muncă, serviciile de sănătate, oficiile de documentare a populației, instituțiile de învățământ, Serviciul Fiscal de Stat.
- Serviciile, care, momentan sunt disponibile să fie prestate în regim electronic, sunt următoarele: comanda actelor personale, un complex de servicii ce țin de înregistrarea transportului auto, eliberarea certificatelor şi serviciul de înştiinţare privind schimbarea domiciliului, solicitare în regim on-line, a duplicatelor adeverinţelor şi extraselor de pe actele de stare civilă, înregistrarea on-line a întreprinzătorilor individuali.

Astfel, se atestă un decalaj între domeniile în care se așteaptă digitalizarea și domeniile care prestează servicii online. Se recomandă implementarea, în continuare, a guvernării electronice în domeniile documentării populației, concomitent cu implementarea guvernării electronic în asemenea servicii publice, ca învățământul, administrația publică locală, serviciile de sănătate și serviciile Inspectoratului Fiscal de Stat. Argumentele, care susțin această teză, constă în faptul că aceste domenii sunt mai des solicitate de către cetățeni și cu acestea se interacționează pe o perioadă mai îndelungată. Orientarea către serviciile vitale pentru societate ar avea un impact de amplificare a satisfacției cetățenilor prin deservire unei ponderi mari de populație. Respectiv, susțin ideea că unele îmbunătățiri minore ale deservirii, în domeniul serviciilor foarte des solicitate, ar putea să aibă un impact mai mare decât digitalizarea completă a unui serviciu foarte rar apelat.

Conceptul de implementare a guvernării electronice, în domeniile menționate, nu se referă numai la prestarea de servicii online, care implică o transformare integrală a modului de organizare a deservirii, ci se referă și la îmbunătățirea calității deservirii prin următoarele detalii:

- Asigurarea accesului la informații prin e-servicii de nivelul I – Informare (elaborarea de pagini electronice ale instituțiilor, ale localităților). Actualizarea permanentă a informațiilor disponibile.
- Îmbunătățirea accesului prin telefon la instituțiile date (facilitarea înregistrărilor on-line, instituirea personalului care oferă consultații la telefon despre procedurile necesare de parcurs)
- Instruirea personalului în domeniul deservirii clienților, inclusiv deservirea prin telefon și prin Internet.
- Îmbunătățirea circulației informației în cadrul instituțiilor de stat, reducerea cazurilor de dublare a informațiilor mai ales pe parcursul trecerii la documentele electronice

- Schimbarea managementului informațional odată cu dotarea tehnică și instruirea personalului. Eliminarea cazurilor în care medicii sau profesorii care dispun de calculatoare, dar le utilizează doar pentru lucru intern, fără a se integra în fluxuri externe de informații, fără a se implica în schimb activ de informații cu pacienții/studenții.
- Repartizarea unor curatori din partea instituției care ar fi disponibili pentru colaborări on-line.

Bibliografie:

1. Bogdan Ghilic-Micu, *Guvernarea electronică*, Revista Informatică Economică, nr. 1 (21)/2002.
2. Daniela Gărăiman, *Repere privind eficientizarea administrației publice prin informatizare*, Revista de Ştiinţe Juridice.
3. Hotărârea Guvernului Republicii Moldova privind Strategia Națională de edificare a societății informaționale – Moldova electronică
4. http://www.ipp.md
5. http://egov.md
6. http://e-services.md
7. http://www.seap.usv.ro

ПРАВОВОЙ АНАЛИЗ ПОТЕНЦИАЛЬНЫХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА И ГОСУДАРСТВА

С. ГРИЩУК-БУЧКА
Институт истории, Государства и Права АНР (Республика Молдова)

The threats in information security are extremely dangerous, as by means of a criminal encroachment information can be exposed to certain influences. This article presents the legal analysis by given problematics.

Информационная безопасность – состояние защищенности информационной среды общества от внутренних и внешних угроз, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций и государств [1]. Исходя из данного определения, объектом угроз информационной безопасности выступают сведения о составе, состоянии и деятельности объекта защиты (персонала, финансовых ценностей, информационных ресурсов и т.д.), угрозы же выражаются в нарушении целостности и достоверности информации. Угроза выступает в качестве потенциально возможного или реального действия злоумышленников,

способного нанести моральный и материальный ущерб, и даже подорвать государственность, в частности, аспект «информационных войн».

Если ранее злоумышленники и киберпреступники, концентрировали свое внимание преимущественно на «сведениях и данных» физических лиц, то в последнее время все чаще объектом преступного посягательства выступают данные коммерческих компаний и правительственных учреждений. В частности:

- за весь 2010 год китайские правительственные сайты в общей сложности становились жертвами атак более 4 600 раз[2];
- 1 марта 2011 американский банк Morgan Stanley подвергся атаке хакеров, в результате которой в руках злоумышленников оказались закрытые данные, касающиеся деятельности банка и интересов его клиентов [3];
- 5 марта 2011 массированной кибератаке со стороны неизвестных хакеров подверглись Интернет-сайты аппарата президента Ли Мен Бака и 40 государственных учреждений Южной Кореи [4];

Подобные примеры шокируют. Весьма ужасающе в данном контексте звучат данные государственного Управления по киберпреступности Великобритании и компания Detica, - «киберпреступность ежегодно обходится британской экономике в 27 млрд фунтов стерлингов» [5].

Угрозы в сфере информационной безопасности чрезвычайно опасны, поскольку посредством преступного посягательства, «информация» может подвергаться определенным воздействиям:

- *ознакомлению*, противоправному деянию, не приводящему к изменению или разрушению информации, однако существенно снижающему ее ценность, в частности, ознакомление с конфиденциальной информацией
- *искажению*, случайным или преднамеренным преступным действиям, приводящим к частичному изменению содержания, определенной модификации сущности самой информации
- *разрушению,* противоправным действиям, приводящим к значительному или полному уничтожению информации и информационных ресурсов.

В конечном итоге, как отмечает В.И. Ярочкин, противоправные действия с информацией приводят к нарушению ее конфиденциальности, полноты, достоверности и доступности [6,20].

Базовая классификация потенциальных угроз информационной безопасности строится на положении «местонахождение источника потенциальной угрозы» и соответственно подразделяется на *внутренние*, (источник угрозы находится непосредственно внутри организации или государства) и *внешние* угрозы (источник угрозы расположен за пределами самого объекта преступного посягательства.). К внутренним угрозам следует отнести: неквалифицированную внутреннюю политику субъекта по организации информационных технологий и управлению безопасностью; преднамеренные и непреднамеренные действия персонала по нарушению правил безопасности; отсутствие соответствующей квалификации персонала по обеспечению деятельности и управлению объектами защиты [7]; предательство

персонала посредством разглашения или утечки информации, несанкционированного доступа; техногенные аварии и разрушения, пожары Источниками внутренних угроз могут быть: администрация организации или государства, персонал или чиновники, технические средства обеспечения производственной и трудовой деятельности.

Источниками внешних угроз чаще всего выступают: преступные группировки и формирования, недобросовестные конкуренты, отдельные лица и организации административно-управленческого аппарата. Среди внешних угроз выделяют: негативные воздействия недобросовестных конкурентов и государственных структур; несанкционированное проникновение на объект защиты [7]; несанкционированный доступ к носителям информации и каналам связи с целью хищения, искажения, уничтожения, блокирования информации без соответствующего вовлечения в преступные действия сотрудников или представителей потенциального субъекта-жертвы; преднамеренные и непреднамеренные действия поставщиков услуг по обеспечению безопасности и поставщиков технических и программных продуктов, стихийные бедствия и другие форс-мажорные обстоятельства.

На условном уровне соотношение внешних и внутренних угроз можно охарактеризовать, как отмечает В.И. Ярочкин, следующими показателями [6,22-23]:

- 82% угроз совершается собственными сотрудниками организации при их прямом или опосредованном участии;
- 17 % угроз совершается из вне – внешние угрозы;
- 1% угроз совершается случайными лицами.

Потенциальные угрозы в сфере информационной безопасности представляется возможным классифицировать и по иным основаниям:

- по объектам преступного посягательства: персонал, материальные или финансовые ценности, информация, стабильность общества, государственность.
- по ущербу: материальный или моральный,
- по характеру воздействия: активные и пассивные угрозы,
- по причинам появления – стихийные и преднамеренные,
- по вероятности возникновения – весьма вероятные, вероятные, маловероятные.

Представленный анализ позволяет сделать вывод о том, что потенциальные угрозы в информационной сфере в большинстве случаев носят преднамеренный и целенаправленный характер, выражающийся чаще всего в активном воздействии внутренних источников потенциальных угроз на объект преступного посягательства.

Литература

1. Организациооно-правовое обеспечение информационной безопасности: учеб. пособие для студ.высш.уч.зав./ А.А.Стрельцов. – М.: Издательский центр «Академия», 2008. – с.36
2. Китайские эксперты сообщили об увеличении числа хакерских атак на государственные сайты http://www.securitylab.ru/news/405062.php

3. Morgan Stanley стал жертвой серьезной утечки данных http://www.securitylab.ru/news/404944.php
4. Хакеры атаковали сайты 40 министерств Южной Кореи http://www.securitylab.ru/news/404990.php
5. Киберпреступники наносят Великобритании ежегодный ущерб 27 млрд фунтов http://www.securitylab.ru/news/404871.php
6. Ярочкин В.И.Информационная безопасность: учебник для вузов.-5-е издание. – М.: Академический проспект, 2008. – 544с.
7. Угрозы информационной безопасности http://itsecblog.ru/ugrozy-informacionnoj-bezopasnosti/

ПОЛИТИКА БЕЗОПАСНОСТИ И ЕЁ АНАЛИЗ В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Денис ГАЛЕЦКУЛ,
Приднестровский Государственный Университет имени Т.Г.Шевченко

Локальная вычислительная сеть - компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт). Также существуют локальные сети, узлы которых разнесены географически на расстояния более 12 500 км (космические станции и орбитальные центры). Несмотря на такие расстояния, подобные сети всё равно относят к локальным.

Должны быть поставлены следующие цели при разработке эффективной защиты ЛВС:

- обеспечить конфиденциальность данных в ходе их хранения, обработки или при передаче по ЛВС;
- обеспечить целостность данных в ходе их хранения, обработки или при передаче по ЛВС;
- обеспечить доступность данных, хранимых в ЛВС, а также возможность их своевременной обработки и передачи
- гарантировать идентификацию отправителя и получателя сообщений.

Адекватная защита ЛВС требует соответствующей комбинации политики безопасности, организационных мер защиты, технических средств защиты, обучения и инструктажей пользователей и плана обеспечения непрерывной работы.

Многие организации используют средства ЛВС для обеспечения нужд обработки и передачи данных. ЛВС логически и физически рассредоточена по всей организации.

Службы безопасности, защищающие данные, а также средства по их обработке и передаче, также должны быть распределены по всей ЛВС. Пользователи должны быть уверены в том, что их данные и ЛВС адекватно защищены. Защита ЛВС должна быть интегрирована во всю ЛВС и должна быть важной для всех пользователей.

Распределенное хранение данных обеспечивает пользователей прозрачным доступом к части дисковой памяти удаленного сервера. Распределенное хранение данных предоставляет такие возможности, как удаленную работу с данными и удаленную печать. Удаленная работа с данными позволяет пользователям получать доступ, читать и сохранять данные. В общем случае, удаленная работа с данными обеспечивается путем предоставления пользователям возможности подключения к части удаленного устройства дисковой памяти (файлового сервера, сервера баз данных и других серверов приложений) так, как будто это устройство подключено напрямую. Удаленная печать позволяет пользователю печатать на любом принтере, подключенном к любому компоненту ЛВС.

Проблемы безопасности ЛВС

1. Распределенное хранение данных - проблемы

Файловые серверы могут контролировать доступ пользователей к различным частям файловой системы. Этого обычно осуществляется разрешением пользователю присоединить некоторую файловую систему (или каталог) к рабочей станции пользователя для дальнейшего использования как локальный диск. Это представляет две потенциальные проблемы. Во-первых, сервер может обеспечить защиту доступа только на уровне каталога, поэтому если пользователю разрешен доступ к каталогу, то он получает доступ ко всем файлам, содержащимся в этом каталоге. Чтобы минимизировать риск в этой ситуации, важно соответствующим образом структурировать и управлять файловой системой ЛВС. Следующая проблема заключается в неадекватных механизмах защиты локальной рабочей станции.

2. Удаленные вычисления - проблемы

Удаленные вычисления должны контролироваться таким образом, чтобы только авторизованные пользователи могли получать доступ к удаленным компонентам и приложениям. Серверы должны обладать способностью аутентифицировать удаленных пользователей, запрашивающих услуги или приложения. Эти запросы могут также выдаваться локальными и удаленными серверами для взаимной аутентификации. Невозможность аутентификации может привести к тому, что и неавторизованные пользователи будут иметь доступ к удаленным серверам и приложениям. Должны существовать некоторые гарантии в отношении целостности приложений, используемых многими пользователями через ЛВС.

3. Топологии и протоколы - проблемы

Топологии и протоколы, используемые сегодня, требуют, чтобы сообщения были доступны большому числу узлов при передаче к желаемому назначению. Это гораздо дешевле и легче, чем иметь прямой физический путь между каждой парой машин. (В больших ЛВС прямые связи неосуществимы). Вытеакющие из этого возможные угрозы включают как активный, так и пассивный перехват сообщений, передаваемых в линии. Пассивный перехват включает не только чтение информации, но и анализ трафика (использование адресов, других данных заголовка, длины сообщений, и частоту сообщений). Активный перехват включает изменение потока сообщений (включая модификацию, задержку, дублирование, удаление или неправомочное использование реквизитов).

Прочие проблемы безопасности ЛВС включают:

1) неадекватную политику управления и безопасности ЛВС,
2) отсутствие обучения особенностям использования ЛВС и защиты,
3) неадекватные механизмы защиты для рабочих станций,
4) неадекватную защиту в ходе передачи информации.

Слабая политика безопасности также увеличивает риск, связанный с ЛВС. Должна иметься формальная политика безопасности, которая определяла правила использования ЛВС, для демонстрации позиции управления организацией по отношению к важности защиты имеющихся в ней ценностей. Политика безопасности является сжатой формулировкой позиции высшего руководства по вопросам информационных ценностей, ответственности по их защите и организационным обязательствам. Должна иметься сильная политика безопасности ЛВС для обеспечения руководства и поддержки со стороны верхнего звена управления организацией. Политика должна определять роль, которую имеет каждый служащий при обеспечении того, что ЛВС и передаваемая в ней информация адекватно защищены.

Использование ПК в среде ЛВС также приносит риск в ЛВС. В общем, в ПК практически отсутствует меры защиты в отношении аутентификации пользователей, управления доступом, контроля деятельности пользователей и т.д.

Отсутствие осведомленности пользователей в отношении безопасности ЛВС также увеличивает риск. Пользователи, не знакомые с механизмами защиты, мерами защиты и т.п. могут использовать их неправильно и, возможно, менее безопасно. Ответственность за внедрение механизмов и мер защиты, а также за следование правилам использования ПК в среде ЛВС обычно ложится на пользователей ПК. Пользователям должны быть даны соответствующие инструкции и рекомендации, необходимые, чтобы поддерживать приемлемый уровень защиты в среде ЛВС.

БУДУЩЕЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ирина РОТАРЬ,
Школа им. М. Коцюбинского (Кишинев, Республика Молдова)

Для того чтобы полностью раскрыть тему, давайте разберёмся в терминологии.

Безопасность – это такое состояние сложной системы, когда действие внешних и внутренних факторов не приводит к ухудшению системы или к невозможности её функционирования и развития (Заплатинский В. М. «Терминология науки о безопасности».)

Информация - (от лат. *informatio* — осведомление, разъяснение, изложение, от лат. *informare* — придавать форму) — в широком смысле абстрактное понятие, имеющее множество значений, в зависимости от контекста. В узком смысле этого

слова — сведения (сообщения, данные) независимо от формы их представления. Сведения об объектах живой или неживой природы, их свойств и взаимном влиянии друг на друга.В настоящее время не существует единого определения термина *информация*. С точки зрения различных областей знания, данное понятие описывается своим специфическим набором признаков.

Соединив два термина понятно, что **безопасность информации** (данных) - состояние защищенности информации (данных), при котором обеспечены её (их) конфиденциальность, доступность и целостность.

Информационная безопасность же это - защита конфиденциальности, целостности и доступности информации.

Информационная безопасность может быть как и организации, так и всего государства, где в организации это- состояние защищённости информационной среды организации, обеспечивающее её формирование, использование и развитие, а в государстве - состояние сохранности информационных ресурсов государства и защищенности законных прав личности и общества в информационной сфере.

То есть - это своего рода программа, защищающая какой либо объект как независимую территорию от каких либо захватов, через угрозу раскрытия и использования информации, а так же людей, как граждан, которые по закону имеют право на личную жизнь.

Система информационной безопасности включает в себя несколько составляющих.

1. Законодательная, нормативно-правовая и научная база.
2. Структура и задачи органов (подразделений), обеспечивающих безопасность ИТ.
3. Организационно-технические и режимные меры и методы (Политика информационной безопасности).
4. Программно-технические способы и средства обеспечения информационной безопасности.

Где следует учитывать уязвимость информации:

- хищение носителя информации или отображенной в нем информации (кража);
- потеря носителя информации (утеря);
- несанкционированное уничтожение носителя информации или отображенной в нём информации (разрушение);
- искажение информации (несанкционированное изменение, несанкционированная модификация, подделка, фальсификация);
- блокирование информации;
- разглашение информации (несанкционированное распространение, раскрытие)

На мой взгляд будущего у информационной безопасности нет… Как утверждает прочитанная мною литература виной этому является интернет, а точнее вирусы распространяемые в интернете которые способны разрушить все.

Но по видимому высшие органы власти ни одной из стран это особо не волнует, хотя может кто- то и беспокоится по этому поводу, но судя по всему не очень сильно по тому, что как мне удалось выяснить эта проблема появилась еще в 70-х годах XX века. Мало того, что она не решена в принципе, так еще и различные технологии прогрессируют, а информации все сложнее находиться в безопасности… Ярким примером этого является публикация более 400 тысяч секретных документов по Ираку. Ну и усилят сейчас меры безопасности, ну и что это даст? Предположим, что какое-то время все будет хорошо, но ведь прогресс не стоит на месте, взломают снова… почему? Потому, что постоянно программы перерабатывать, переделывать и усовершенствовать никто не будет потому, что стоит это больших затрат, а властям все равно, они не вечны, через определенный промежуток времени они меняются и каждый думает, что это проблема следующего.

Есть еще один вариант экономии бюджета на сохранении целостности данных, примером этого является Россия. Я вполне допускаю мысль о том, что я ошибаюсь и даже возможно ошибаюсь сильно, но все же не исключаю вероятности того, что всеобщий допуск к секретным советским архивам был открыт именно по этой причине, под предлогом того, что современная Российская Федерация, как суверенное, демократическое, правовое государство, не может быть преемником политики коммунистического режима. Ведь все- таки, наверное, проще самому раскрыть государственные тайны и убедить народ, что это правильно, чем получить сюрприз от WikiLeaks, который грозится в ближайшем будущем разоблачением России и Китая. Это же на самом деле проще, чем создать достойную охрану информации и плевать, что большая часть общества просто не готова к таким откровениям, плевать, что многие живут еще по тем правилам и идеалам… зато бюджет сэкономили…

Как я уже упоминала ранее, я нашла довольно много статей о том, какую серьезную угрозу информационной безопасности представляют компьютерные вирусы, которые попросту уничтожают все данные. А в наш компьютеризированный век это одна из самых страшных проблем, ведь вся информация храниться именно в компьютерах, будь то попросту семейные фотографии или секретные государственные документы. И как я уже тоже упоминала эта проблема, наверное, не закончится, как бы это пессимистично не звучало, но государственные власти никогда не договорятся со своими гражданами. Причем тут власти и граждане? Объясняю, власти экономят бюджет, а для граждан - это не плохой заработок, причем как для тех, кто создает вирусы, так и для антивирусных компаний.

Вывод из этого всего у меня получился не утешительный даже для самой себя, так как осознавать, что в государстве, в котором я живу, могут произойти серьезные проблемы или, что любой кому не лень может считать мою личную информацию с моего же компьютера, не доставляет мне радости. Но серьезней всего над этим стоит задуматься именно властям, ведь от информационной безопасности зависит, наверное, и будущее государства. Хотя может это и слишком сильно, и громко сказано… но в любом случае, думать об этом необходимо уже сейчас пока не стало слишком поздно!

ТЕХНОЛОГИЯ ЗАЩИТЫ ФОТОГРАФИЧЕСКИХ ДОКУМЕНТОВ: ГОЛОГРАФИЧЕСКИЙ ПОДХОД PHOTOWATERMARK

Евгений КАЧУРОВ,
Всероссийская государственная налоговая академия,
(Российская Федерация)

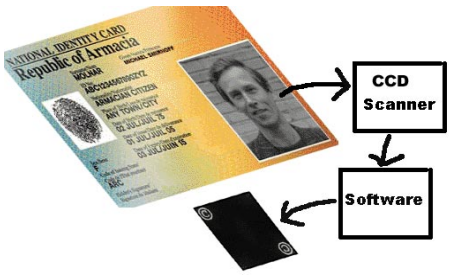
Противодействие методам подделки и фальсификации бумажных, а в последнее время и пластиковых документов является традиционной и актуальной задачей защиты носителей информации. Одним из ключевых элементов для многих документов является фотография. Можно не говорить какой экономический и правовой вред наносит фальсификация и подделка фотографий на таких документах как паспорт, водительское удостоверение, кредитная или идентификационная карта, медицинский полис и другие.

В настоящее время интенсивно разрабатываются новые средства защиты, основанные на последних достижениях физики, химии, микроэлектроники. Наиболее привлекательным решением выглядит встраивание микрочипов. Цифровое представление данных, обеспечивает удобный ввод и редактирование данных, высокую помехоустойчивость записи, простоту считывания данных. Однако подобная простота привлекательна и для взломщиков. Эксперименты с взломом микрочипов, встроенных в паспорт, продемонстрировали весьма низкую безопасность этой технологии - все данные, хранящиеся в электронном виде, стали доступны "злоумышленникам", включая отпечатки пальцев, фотографию и весь шифрованный и открытый текст.

Основной недостаток существующих средств защиты документов с фотографиями состоит в отсутствии условной зависимости между событием подмены объекта идентификации (фотографии владельца документа) и состоянием элемента защиты (например: оптической голограммы или встроенного микрочипа). В этом случае, подмена фотографии на карте при сохранении защитного элемента не приводит к выводу о подделке документа.

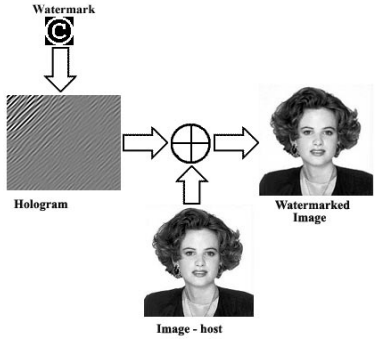
В этом контексте проиллюстрируем технологию PhotoWaterMark для защиты фотографических документов на бумажной или пластиковой основе.

Технология PhotoWaterMark представляет собой сочетание стеганографического подхода сокрытия и криптографического подхода шифрования данных, что обеспечивает практическую невозможность взлома. Причем, основное неудобство для взлома заключается в аналоговом представлении скрываемых данных. Сущность стеганографическго подхода состоит в сокрытии самого факта передачи или внедрения информации в носитель. Один из таких методов встраивания скрытых водяных знаков в фотографии положен в основу настоящей технологии.

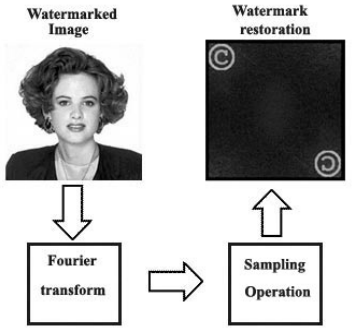


Рассмотрим процедуру контроля документов. Схематично процесс идентификации, например владельца ID карты, можно представить как совокупность программных и технических средств, работающих в режиме реального времени, когда фотоизображение считывается сканером на ПЗС матрице, подвергается некоторым преобразованиям с целью выделения сокрытого водяного знака, а затем скрытая информация визуализируется на экране монитора. На схеме, скрытые данные представлены в виде графического изображения знака копирайта ©.

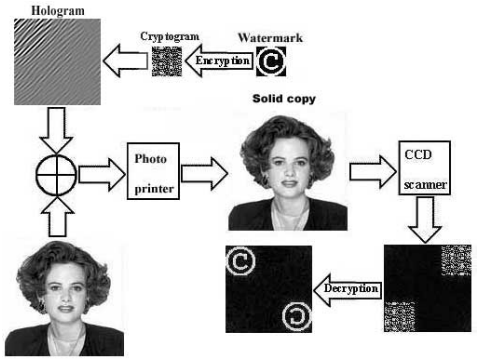
В основу метода встраивания, скрываемых данных, положен принцип интерференции. Сущность метода состоит в синтезе цифровой голограммы водяного знака и аддитивно-мультипликативном смешивании полученной голограммы с изображением-контейнером (смотри рисунок):



Для реализации обратной процедуры - процедуры восстановления водяного знака из голограммы, достаточно выполнить двумерное преобразование Фурье, если конечно известны параметры синтеза голограммы, и в частности пространственная несущая. В реальном времени, эта функция реализуется с помощью цифровых сигнальных процессоров (ЦСП). Например, ЦСП фирмы Texas Instruments, позволяют выполнить эту процедуру за доли секунды. В процессе восстановления водяного знака, можно наблюдать как восстановленный объект, так и его голографическое изображение (смотри рисунок):



Важнейшим элементом любой информационной системы является шифрование конфиденциальной информации. Рассматриваемый подход не является исключением - двумерные криптограммы органически встраиваются в цепочку преобразований двумерных изображений (смотри рисунок):



Стойкость шифра определяется исключительно стойкостью секретного ключа. Таким образом, аналоговое исполнение средства защиты объекта идентификации (фотографии владельца) и скрытый характер встраиваемых данных представляет собой малопривлекательный объект для цифрового взлома, а подключение криптографической подсистемы к стеганографической системе сокрытия данных обеспечивает мощный барьер несанкционированному вмешательству.

В заключение, стоит отметить, что предложенную технологию можно рассматривать как дополнительную степень защиты документов к существующим технологиям. И в этом смысле, на PhotoWaterMark возлагается защита фотографических материалов на аналоговом уровне, а за микрочипами остается их неоспоримое преимущество - простой и удобный способ работы с цифровыми массивами данных.

"TIME CARD" - БЕЗОПАСНОСТЬ ВАШЕЙ КОМПАНИИ В ВАШИХ РУКАХ!

Станислав ЖУК, Евгения ЗГАРДАН
Теоретический Лицей им. "Михаил Когэлничану"
(Республика Молдова)

Information security is the process of protecting information. It protects its availability, privacy and integrity. "TIME CARD" - the software for the account of working hours of the personnel of the company which possesses following advantages: gives possibility of automation of the account of working hours and protection against deliberate infringement of the data.

Кто владеет информацией, тот владеет миром! Пренебрежение этой истиной может обойтись в миллионы и миллиарды убытков. Даже в современной истории можно найти массу красноречивых примеров, когда один единственный файл или документ вершил судьбы сотен тысяч людей и целых корпораций. В силу этих причин защита информации сегодня многими бизнес структурами считается главным

направлением деятельности в области внедрения технологий корпоративной безопасности. Не смотря на это, многие бизнесмены считают, что защитить от кражи папку с бумагами можно, поставив надежный замок на сейф, а защита данных в электронном виде заключается лишь в установке пароля на компьютер. Тем не менее, любая система управления документами и защиты данных — это не просто ограничение доступа к файлам или бумагам. Это современные технологии, которые обеспечивают непрерывность бизнес процессов путем создания электронного архива, внеофисного хранения информации, а также других методов программного и аппаратного типа.

Безопасность информации сегодня не роскошь и не причуда руководства, а вопрос «обезопасить или не обезопасить?» даже не поднимается - ответ очевиден, как очевидна необходимость чистить зубы утром и вечером. Говорят лишь об уровнях безопасности, а они различны.

Насколько уязвим ваш бизнес и вы сами, когда кто-то посторонний имеет возможность доступа к вашей информации? Что сделают ваши конкуренты, журналисты, недруги и мошенники, получив конфиденциальную информацию о вашем бизнесе?

Информационная безопасность, как и защита информации, задача комплексная, направленная на обеспечение безопасности, реализуемая внедрением системы безопасности. Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач. Проблемы информационной безопасности постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем.

Мы предлогаем вам один из возможных способов решения этой проблемы. "Time Card"-программное обеспечение для учета рабочего времени персонала компании,которое обладает следующими преимуществами:

- Предоставляет возможность автоматизации учета рабочего времени;
- Полноценное ведение табельного учета в электронных табельных журналах, пользуясь всеми возможностями автоматического заполнения;
- Ограничение доступа пользователей к табелю согласно штатному расписанию компании.
- Защита от преднамеренного нарушения данных;
- Хранение табелей непосредственно в базе данных;
- Возможность получения оперативных отчетов по учету трудозатрат.

Защита от преднамеренного нарушения данных представленного нами продукта состоит в следующем:

После того как вы установили программу,вы получаете доступ к единой базе данных,единому архиву. И так, Вы директор компании Х. С помощью данного продукта, вы получаете возможность заполнения, редактирования и просмотра своего табеля рабочего времени, а также табелей подчиненных.

Для обеспечения эффективной защиты информации предусмотрен контроль на трех основных уровнях:

- контроль доступа к информации со стороны пользователей информационной системы;
- контроль физической сохранности баз данных и их непротиворечивости;
- контроль конфиденциальности передаваемых по сетям данных и работоспособности сетевой инфраструктуры.

Средства обеспечения безопасности.

1. Обычная практика предполагает аутентификацию (распознавание) пользователей с помощью паролей.
2. Проверка полномочий при доступе к бизнес-объектам.

Например, для конкретного бухгалтера на предприятии в соответствии с его ролью может быть открыта возможность доступа к выполнению проводки бухгалтерского документа, но только на уровне своей бизнес-единицы,по конкретной группе счетов или по операциям отдельных деловых партнеров.Если у пользователя нет необходимых полномочий, система отказывает в получении доступа к соответствующим транзакциям или документам.

3. Администрирование ролей пользователей.

Для того, чтобы упростить ведение детальных данных полномочий каждого пользователя, предусмотрен специальный инструмент – генератор профилей полномочий. Основная идея заключается в использовании стандартных ролей бизнес-пользователей в соответствии с их должностными ролями. Вы можете,например, присвоить отдельному сотруднику одну или несколько стандартных ролей, и этим полностью определить профиль его полномочий. При необходимости Вы можете отредактировать перечень функций, добавив или удалив один объект полномочий или целую группу функций.

Ограничения полномочий пользователя не являются гарантией корректности данных бизнес-документов. В случае, если все действия пользователя документируются и существует формальное подтверждение автора изменений, Вы можете контролировать источник данных и, как следствие, управлять ответственностью за конкретные действия пользователей.

4. Защита одновременного доступа к изменению данных.

“TIME CARD” также обеспечивают защиту одновременного доступа к объектам многопользовательской обработки с помощью механизмов блокировки.

Эти механизмы предотвращают одновременный доступ нескольких пользователей к одному и тому же объекту через транзакцию изменения, сохраняя, как правило, возможность просмотра объекта.

5. Физическая целостность данных.

Сохранность данных, накопленных в процессе деятельности компании, обеспечивается средствами копирования и восстановления информационной базы. С помощью механизмов планирования и выполнения фоновых заданий могут управляться автоматические операции создания резервных копий, а средства мониторинга параметров базы данных обеспечивают постоянный контрольтехнических аспектов эксплуатации данного продукта.

Примерно так выглядит краткое описание представленного нами продукта. TIME CARD позволит упростить рабочий процесс вашей компании,вести постоянный учет и в то же время это один из способов защитить свои данные от посторонних лиц.

В современных условиях любая деятельность сопряжена с оперированием большими объемами информации, которое производится широким кругом лиц. Защита данных от несанкционированного доступа является одной из приоритетных задач при проектировании любой информационной системы. Следствием возросшего в последнее время значения информации стали высокие требования к конфиденциальности данных.

Помимо систематического применения арсенала средств, описанных выше, необходимо использовать административные и процедурные меры, в частности регулярное изменение паролей пользователей, предотвращение доступа к физическим носителям информации и т.п.

Materialele Conferinței "Securitatea Informațională 2011"
sunt publicate în redacția autorilor.

Semnat pentru tipar 19.04.11.
Coli de tipar 8,26. Coli de autor 7,85.
Tiraj 25 ex.
Tipografia Departamentului Editorial-Poligrafic al ASEM