SECURITATEA INFORMAȚIONALĂ 2010

CONFERINȚĂ INTERNAȚIONALĂ,
(ediția a VII-a), 15-16 aprilie 2010

ACADEMIA DE STUDII ECONOMICE DIN MOLDOVA

LABORATORUL DE SECURITATE INFORMAȚIONALĂ

SECURITATEA INFORMAȚIONALĂ 2010

CONFERINȚĂ INTERNAȚIONALĂ
(ediția a VII-a)

15-16 aprilie 2010

Chișinău – 2010

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

Descrierea CIP a Camerei Naţionale a Cărţii

„Securitatea informaţională 2010", conf. intern. (2010 ; Chişinău). Securitatea informaţională 2010 : Conf. intern. (ed. a 7-a), 15-16 apr. 2010 / com. org.: Grigore Belostecinic, Tatiana Mişova, Sergiu Tutunaru [et al.] ; coord. ed. S. Ohrimenco. – Ch.: ASEM, 2010. – 114 p.

Antetit.: Acad. de Studii Econ. din Moldova, Lab de Securitate Informaţională. – Texte: lb. rom., engl., rusă. – Rez.: lb. engl. – Bibliogr. la sfârşitul art. şi în notele de subsol. – 25 ex.

ISBN 978-9975-75-509-2.

-- 1. „Securitatea informaţională 2010" – Conferinţă internaţională (rom., engl., rusă).
004.056(082)=135.1=111=161.1

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

ISBN 978-9975-75-509-2

ORGANIZATORII CONFERINȚEI:

Academia de Studii Economice din Moldova

Agenția pentru Inovare și Transfer Tehnologic

Partener media:	Partener informațional

SPONSORI:

Întreprinderea de Stat
Centrul de telecomunicații speciale

Cuprins:

INFORMATION SECURITY IN BUSINESS ENTITIES

Leszek F. Korzeniowski,
President European Association for Security (Poland)

The article focuses on the significance of information security in business entities. This problem has a large significance for the effectiveness of business entities and for the assessment of managers' activities. One can also acknowledge this problem to be of interest for scientific investigations.

Until the great revolutionary transformation at the beginning of the 1990s in European science there was domination of interest in the security of states and state enterprises.

From the introduction of market economy in 1989 in Poland, and then in other countries of Central and Eastern Europe, also the security of citizens and private economic organizations became a subject of interest for science.

Security also became an object of different scientific disciplines. Securitology which undertakes the analysis of security by investigation of the function of such factors, as[1]:

- **objective and subjective hazards**
- **internal and external hazards**
- **abstract and specific hazards**
- **potential and active hazards,**
- **constructive and destructive values,**
- **static and dynamic situation.**

Security of a human i.e. the human existence, the development and normal functioning is therefore a main objective through which one ought to consider the security of a business organization. The participation of information resources in the structure of the value of all resources of a firm can attain even 80%. Research of a group of 500 greatest American firms in 2000 showed that in every 6 dollars of the trading value of these firms 5 dollars represented invisible resources, not estimated in the assets (that is to say, first of all, information resources), and only 1 dollar is the value of material and financial resources[2].

Here we may draw the first conclusion that information resources became the most important factor in attaining targets of every economic

[1] Korzeniowski L.F. Securitologia. *Nauka o bezpieczeństwie człowieka i organizacji społecznych.* Kraków: EAS 2008. ISBN 978-83-925072-1-5. http://www.sbc.org.pl/dlibra/doccontent?id=13871&dirids=66 Until the great revolutionary transformation at the beginning of the 1990s in European science there was domination of interest in the security of states and state enterprises.

[2] Lev B.: *Knowledge Management: Fad or Need?* "Research Technology Management", September/October 2000, Vol. 43, Issue 5.

organization. They are indispensable in all functions of the management process: planning, organization, motivation and control.

A notion of an enterprise appeared in the economic literature around the middle of 18th century, introduced by a French economist **Richard Cantillon**, who gave a name of businessmen to merchants perceiving price differentials on different markets and being able „to buy cheap, and to sell dear". The Austrian economist **Joseph Schumpeter** defines a contemporary businessman as an innovator, a „creative destructor", involved in the process „of creative destruction" which disturbs the economic equilibrium and in this manner creates conditions for the new economic development.

The activity of this mechanism means that businessmen greedy for extraordinary profits constantly seek new, not practiced before combinations of productive factors (the innovation) and thus destroy equilibrium of economy, because the development takes place by means of „creative destruction", by destroying the equilibrium and releasing adjustment processes, which - by means of the mechanism of competition - eliminate ineffective uses of productive factors and propose new, effective ones.

Here we have another characteristics of entrepreneurship: it is not only the security (the existence, the development and the normal functioning) of the economic organization but also „the creative destruction" accompanying an enterprise. Secure existence and the development pertain to the subject as an entirety (of the system) wherein some component parts (subsystems) can be threatened. In axiological categories factors raising the security of the all system (economic) or some parts of this system (business entities) will be a source of threat for others.

It can be graphically represented comparing security of:

- economies (economic systems) of a socialist country in 1988 with central planning, wherein enterprise did not go bankrupt, but the whole system became bankrupt.
- economies of countries with the system of market economy in 2008, wherein enterprise go bankrupt, but the whole system is secure.

What results from research which has been carried out in Poland since 2001 by the Main Statistical Office in newly registered firms, is that in the first year of their functioning 1/3 ceased the activity, in the second year - 1/4 of remaining firms, in third year - 1/5 of the remaining ones. After three years 39,6% of businessmen registered in 2001 remained on the market (only 56% of businessmen in a form of a corporate body and 38% in a form of a natural person).

However, all economy in Poland reached the positive rate of development - +1% changes of the Product of the National Gross (GDP) in 2001, +1,4% in 2002 +3,8% in 2003 +5% in 2004.

Due to the criterion of the accessibility and protection, in the structure of the information class in an economic system (in an enterprise) one can separate the following categories:

- **State secret,** whose unauthorized disclosure can cause the essential threat for basic interests of the Republic of Poland (Classified Information Disclosure Act dated 22 January 1999).
- O**fficial secret**, the information whose unauthorized disclosure could threaten the state interest, the public interest or legally protected interest of citizens or an organizational unit
- **Classified information** is a secret defined by separate laws or contracts among parties: professional, fiscal, bank, medical, commercial, statistical etc.
- **Personal data**, meant as each information concerning a natural person, allowing for a qualification of the identity of this person.
- **Neutral information** for legal purposes whether it is the right to protection or duty to make it accessible.
- **Public information** which is to be made accessible by public authorities or other entities performing public tasks.

In management, good quality of information is essential.

By **the quality of information** one ought to understand **here the generality of the information proprieties relating to the ability of satisfaction of absolute or foreseen needs of a user of information - possibilities of attaining the targets of an organization (a business entity).**

So we arrive at the third conclusion, that **the information security** of a business entity means:

1) the possibility of unthreatened **gaining** of good quality information proper for making a decision and attaining the targets of a business entity),
2) and the **protection** of possessed information from its loss.

Decision making by **managers** is a key in functioning of business entities. Decisions are encumbered by an error resulting from a fact that:

1. the environment of the organization is variable and not homogenous,
2. people and other resources of the organization are deceptive,
3. the information is subjective, not an exact image of the objective reality.

From this model we arrive at the fourth conclusion that a manager (a businessman) needs incessantly to obtain the situational (about the state and condition in the enterprise, its environment, situation on the market etc.) information so that he is able to make decisions which are imparted as managerial information for executive bodies and basic organizational units of the enterprise.

References:

1. Dworzecki J.: *Podstawy prawne wykonywania zadań ochrony osób i mienia. Wybrane zagadnienia*, Gliwice: GWSP, 2009. ISBN 978-83-61401-20-9
2. Korzeniowski L.F. *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*. Kraków: EAS 2008. ISBN 978-83-925072-1-5. **http://www.sbc.org.pl/dlibra/doccontent?id=13871&dirids=66**
3. Lev B.: *Knowledge Management: Fad or Need?* "Research Technology Management", September/October 2000, Vol. 43, Issue 5.

DEVELOPING A STRATEGY AND POLICY FOR ELECTRONIC TRADING SECURITY

Rumen Varbanov,
D.A.Tsenov Academy of Economics (Bulgaria)

This study substantiates and elaborates on one of the crucial issues directly related to the success of every initiative regarding electronic trading - its **security**. This is accomplished along four key lines:

- Giving proof of the significance and trust for the successful development of electronic trading;
- Systematizing and analyzing the dangers in terms of electronic trading security;
- State of the art technologies for securing information security in electronic trading;
- Working out an approach towards the establishing of a policy of electronic trading in small- and medium-sized enterprises /SME/.

Many concrete data and figures are produced supporting the author`s thesis of the incessantly growing dangers in the Internet and of the need for systematic and purposeful work. The risks engendered by the continuous development of electronic trading on a world scale are growing so rapidly that the experts in information security are not relevantly capable of responding to them and assuring reliable functioning of the information systems. This entails urgent development of entirely new methods and technologies for securing the businesses` security in the Web.

We analyze the state of electronic trading security in Bulgaria and particularly the outcomes of the poll

survey conducted by the author with regard to SME.

We examine in detail the dangers to electronic trading at the stages of informing, contracting, delivering of the purchased merchandise, and servicing and maintenance from the perspective of three core aspects of security – confidentiality, data integrity and accessibility. The concrete manifestation of the various kinds of dangers as per their nature is classified in 5 key points: those related to the communication medium; affecting the system`s hardware components; the process of payment when purchasing a merchandise on-line; the cryptographic methods and technologies employed, and other types of danger. We take into special consideration the spam whose impact on electronic trading in the Internet as a whole is becoming incrementally negative and is a real impediment to the traffic in the Web.

Our studies indicate that a big portion of SME which are definitely ambitious to effectively perform in the Web, make effort primarily towards the development and functioning of the site, missing in their strategy the problems of the security of the on-line trading processes. Thus from the very beginning they leave unaccounted for several key requirements for successful electronic trading and as a consequence this has a negative impact on their endeavors. And there are many reasons for one to assert that the information environment of small- and medium-sized enterprises is more vulnerable in terms of security breaches.

We propose an approach for setting up a policy for electronic trading security in SME based on several fundamental assumptions: identification and authenticity; data preservation; processing of orders; gradualness and step-by step proceeding; implementing state of the art technologies and proven decisions based on products of leading firms in the relevant field; protection of investments; protection of transactions.

Finally, several key recommendations are laid out in view of establishing and optimizing a policy of electronic trading security.

ИНТЕЛЛЕКТУАЛЬНЫЙ СЧЁТЧИК ЭЛЕКТРОЭНЕРГИИ: АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ю.А. Пушняк, *независимый эксперт (Республика Молдова)*

The modern electricity smart meter can become a target for hacker attacks. In this report all potential threats are analyzed and the general requirements for meter data security are formulated.

Современный интеллектуальный счётчик электроэнергии может стать мишенью для хакерских атак. В докладе проанализированы все потенциальные угрозы и сформулированы общие требования к информационной безопасности счётчика.

Информационные технологии активно внедряются в область учёта бытового потребления энергоресурсов. Современный интеллектуальный счётчик электроэнергии уже способен выполнять десятки функций и поддерживать двусторонние коммуникации через распределённые сети связи. Эти качества открывают принципиально новые возможности в области учёта, позволяют поставщикам внедрять новые сервисы для потребителей и общими усилиями эффективно решать задачи энергосбережения.

Вместе с тем, возникают и принципиально новые проблемы. На фоне постоянного роста стоимости энергоресурсов и ожидаемого массового (порядка 10^8 точек учёта) распространения интеллектуальных счётчиков по всему миру – становится весьма актуальной и острой проблема обеспечения информационной безопасности. Дело в том, что современный счётчик электроэнергии – это по сути "маленький компьютер", включенный в распределённую сеть связи. Его предок – электромеханический счётчик – часто подвергался разного рода непосредственным атакам со стороны злоумышленников, недобросовестных потребителей. Теперь счётчик становится ещё и потенциальной мишенью для … хакерских атак через сеть связи [1].

Какие меры предпринимаются для решений этой проблемы? Прежде всего, усилиями ряда международных организаций формируется соответствующая нормативная база [2,3], но этот процесс еще далёк от завершения. Кроме того, по мнению автора, некоторые из уже опубликованных положений и рекомендаций имеют весьма спорный характер; среди разработчиков нормативных документов ощущается явная нехватка специалистов по информационной безопасности и криптографии.

Тем временем ведущие мировые производители счётчиков предлага-

ют свои собственные решения. Как правило, эти решения затрагивают лишь некоторые аспекты проблемы и имеют явную маркетинговую направленность. Дело в том, что встроенные средства обеспечения информационной безопасности обходятся производителю достаточно дорого. Они заметно повышают себестоимость счётчика, и, следовательно, либо приводят к его удорожанию, либо снижают долю прибыли при продаже счётчика по прежней цене. В то же время многие производители сознательно или подсознательно недооценивают степень "информационной" угрозы. А если угроза невелика, зачем идти на дополнительные расходы? Этим и определяется отношение большинства производителей к встроенным средствам информационной безопасности - да, формально они реализуются, но реализуются ровно настолько, насколько это необходимо для того, чтобы успокоить потенциального покупателя, который конечно же слышал об этой проблеме, но ничего в ней не понимает ("данные шифруются? – да, разумеется! – ну и замечательно, покупаю!").

Ниже приводится перечень общих требований по информационной безопасности к любому современному счётчику электроэнергии. Перечень был сформулирован автором на основе многолетнего личного опыта проектирования и эксплуатации систем учёта.

Требования:

1. Соответствие требованиям международных стандартов (IEC, DLMS/COSEM и др.)
2. Аутентификация источника при приёме/передаче сообщений
3. Шифрование сообщений
4. Помехоустойчивое кодирование
5. Поддержка режима предоплаты (опционально, для счётчиков с prepayment mode)
6. Безопасный локальный интерфейс для поддержки домашней сети связи
7. Периодическая проверка целостности резидентного программного обеспечения
8. Защита метрологического обеспечения от изменений в процессе эксплуатации
9. Доступ к резидентным программам и данным через оптический порт по паролю
10. Датчик вскрытия крышки счётчика
11. Датчик вскрытия крышки клеммника
12. Датчик наличия внешнего магнитного поля
13. Датчик температуры внутри корпуса
14. Встроенный журнал событий с регламентированным доступом
15. Поддержка аварийных сообщений
16. Безопасное управление настройками счётчика

17. Безопасное изменение резидентного программного обеспечения (upgrade)

В докладе подробно анализируются потенциальные информационные угрозы для счётчика и предлагаются встроенные аппаратные и программные средства, способные эффективно парировать эти угрозы.

Полученные результаты могут быть использованы в качестве справочного руководства при выборе системы централизованного учёта энергоресурсов. Кроме того, эти результаты могут служить основой (аналогией) при разработке аспектов информационной безопасности для других подобных систем, например – для защиты разнообразных оконечных устройств (user appliances) в рамках концепции "Умный дом".

Источники:

1. Bruce Schneier. Hacking Power Networks. CRYPTO-GRAM, February 15, 2008. http://www.counterpane.com
2. Electricity metering - Data exchange for meter reading, tariff and load control. Международные стандарты серии IEC 62056.
3. DLMS/COSEM for smart metering. http://www.dlms.com

ИНФОРМАЦИЯ КАК ТОВАР В XXI ВЕКЕ: АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ НАЦИОНАЛЬНЫМ РЫНКАМ

Анатолий Крапивенский, *ФГОУ ВПО «Волгоградская академия государственной службы» (Российская Федерация)*

The problem of national markets security in the segment of informational products is considered in the given article. Author investigates the phenomenal properties of information as a product and analyzes the paradigm of threats to national security in the above area.

В XXI столетии информация переходит в раздел наиболее востребованных товаров, предлагаемых к продаже или обмену. Современное состояние общества характеризуется лавинообразным ростом процесса "производства, потребления и накопления информации во всех отраслях человеческой деятельности" [1: 3]. Это объясняется объективным увеличением общего трафика информационного контента в соци-

уме; перманентной технологической революцией, практически ежедневно выдающей принципиально новые решения в области коммуникативно-информационных технологий (в первую очередь – интерактивных); все бóльшую зависимость любого производства от программного обеспечения, также базирующегося на современных информационных технологиях. Философский энциклопедический словарь подчеркивает, что "проблема информации является одной из наиболее актуальных и фундаментальных в условиях современной научно-технической революции, характеризующейся, в частности, передачей информационных функций от человека к машинам в самых широких масштабах" [2: 218].

В этой связи определим само понятие "информация", позволяющее считать ее товаром. Словарь терминов и определений по вопросам безопасности трактует информацию как "сведения о лицах, предметах, событиях, явлениях, процессах и объектах (независимо от формы их представления), используемые в целях … оптимизации принятия решений и управления объектами" [3: 123]. Разумеется, в условиях рыночной экономики, сведения, используемые для оптимизации принятия решений и управления объектами, являются не чем иным, как товаром. Однако собственно "информация" является не совсем обычным товаром. Это отмечает, в частности, Р. Дж. Нолл: "информацию необходимо каким-то образом доводить до последующих потребителей, и распространение ее может даже стоить дороже, чем повторное создание, - это, например, относится к простейшим компьютерным программам. Или, например, информацию можно приватизировать, причем стоить это будет очень недорого, так что свойство информации служить общественным благом не внесет значительной неэффективности в систему ее рыночного распространения. Тем не менее, публичность информации – это серьезная проблема" [4: 109]. Отметим также такое товарное свойство информации, как универсальность. Информация в той или иной форме присутствует во всех без исключения видах товаров, создавая, таим образом, либо дополнительную информационно-техническую, либо дополнительную эстетическую стоимость.

Следовательно, присутствуя в качестве товара на любом из национальных рынков, информация не может не создавать потенциальных угроз их информационной безопасности. Под национальным рынком в данном случае понимается генеральная "совокупность социально-экономических отношений" [5: 518], существующих в том или ином государстве.

При этом различают внешние и внутренние угрозы информационной безопасности. К внешним

угрозам относят доминирование иностранных информационных продуктов и источников распространения информации на внутреннем национальном рынке; ограничение доступа национальных информационных технологий и продуктов на международные рынки; противодействие созданию конкурентоспособных национальных информационных технологий. Данные угрозы воплощаются в так называемое "цифровое неравенство" - "вид социальной дифференциации, вытекающий из разных возможностей использования информационно-коммуникативных технологий" [6: 20]. Внутренние угрозы заключаются в критическом состоянии национальных отраслей промышленности, производящих информационные продукты и технологии; сращивание государственных и криминальных структур в информационной сфере; недостаточная разработанность нормативно-правовой базы в информационной сфере; недостаточная правоприменительная практика; недостаточное государственное финансирование мероприятий по обеспечению национальной информационной безопасности.

Следует отметить, что под угрозами безопасности национальным рынкам в секторе информационных продуктов надо понимать не только непосредственно нанесение экономического ущерба, но и так называемый ущерб косвенный, проявляющийся в комплексе мероприятий и технологий, направленный на снижение критичности восприятия национальным потребителем качества потребляемой информации и ее герменевтического восприятия. Однако указанный косвенный ущерб в конечном счете, опять-таки, ведет к существенным экономическим потерям для национальной экономики.

Глобализация, основой которой стали "информатизация всех областей социальной деятельности, интеграция информационных систем различных государств в единую общемировую информационную сферу, формирование единого информационного пространства, создание глобальных информационно-телекоммуникационных сетей, интенсивное внедрение новых информационных технологий" [7: 8], с точки зрения национальных интересов в любой сфере деятельности, не является сугубо положительным фактором. Национальные рынки, как объект приоритетного национального интереса, нуждаются в защите со стороны государства. Этот вывод в полной мере относится к такому жизненно важному и стратегическому виду товара, каким является информация. При защите национальных рынков, разумеется, нельзя обеспечивать их суверенитет исключительно за счет интересов потребителей – коллективного социального актора, "занимающего центральное место в системе уп-

равления качеством" [8: 15] любого товара. В данном процессе необходимо соблюдать баланс интересов общества, государства, корпорации и личности. Только в этом случае обеспечивается "динамическое равновесие охраняемой системы. При таком подходе понятие безопасности сближается с понятием стабильности, выполняющей функцию сохранения неизменности социальных взаимодействий" [9: 40].

Литература:

1. Башлы П.Н. Информационная безопасность. – Ростов н/Д: Феникс, 2006.
2. Философский энциклопедический словарь / Гл. редакция: Л.Ф. Ильичев, П.Н. Федосеев, С.М. Ковалев, В.Г. Панов. – М.: Советская Энциклопедия, 1983.
3. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Словарь терминов и определений. 2-е изд. – М.: Знание, 1999.
4. Нолл Р. Дж. Массовые коммуникации // Экономическая теория / Под ред. Дж. Итуэлла, М. Милгейта, П. Ньюмена: Пер. с англ. – М.: ИНФРА-М, 2004.
5. Хилл П. Рынки как места торговли // Экономическая теория / Под ред. Дж. Итуэлла, М. Милгейта, П. Ньюмена: Пер. с англ. – М.: ИНФРА-М, 2004.
6. Лунев А.П. Информационная культура населения – основа социально-устойчивого развития общества // Электронная культура. Информационные технологии будущего и современное электронное обучение «MODERN IT & (E-) LEARNING»: Материалы международной научной конференции. – Астрахань: ООО «Типография «НОВА», 2009.
7. Федоров А.В. Информационная безопасность в мировом политическом процессе. – М.: МГИМО-Университет, 2006.
8. Хилл Н., Сельф Б., Роше Г. Измерение удовлетворенности потребителя по стандарту ИСО 9000:2000. – М.: Издательский Дом «Технология», 2004.
9. Зинченко Н.И. Социально-правовые институты обеспечения национальной безопасности России: состояние и перспективы развития (социологический аспект): автореф. дисс. на соиск. уч. ст. доктора соц. наук. – М.: РГТЭУ, 2006.

ЦЕЛЕСООБРАЗНОСТЬ И ВОЗМОЖНОСТЬ ИСПОЛЬЗОВАНИЯ НЕЧЕТКОГО МОДЕЛИРОВАНИЯ ДЛЯ ОЦЕНКИ РИСКОВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Владимир Чернов,
Владимирский государственный университет
(Российская Федерация)
Александр Дорохов,
Харьковский национальный экономический университет
(Украина)

The problem of the analysis, modelling, forecasting of risks in information systems has been examined. Necessity and an opportunity of application of the fuzzy sets theory for studying risks of development, introduction and operation of information systems has been proved. Application of specialized software, such as Matlab Fuzzy Toolbox, Fuzzytech and Fuzicalc, for studying and modelling of corresponding risks in information systems has been offered.

Изучение разнообразных процессов, этапов и составляющих разработки, внедрения, эксплуатации информационных систем, включая финансово-экономические составляющие, техническую, информационную, экономическую безопасность, надежность и устойчивость работы, сохранения и обработки информации, корректности и адекватности продуцируемых управленческих решений, требует использования новых, научно обоснованных, математически формализованных подходов и методов.

Одним из современных средств изучения информационных системних являются методы и приемы анализа рисков, позволяющие достичь максимальной эффективности использования информационных систем в условиях рыночной экономики, поскольку под действием законов рынка в условиях конкуренции результаты внедрения и эксплуатации этих систем в значительной степени связаны с различными рисками и неопределенностью, которые следует учитывать, измерять и оценивать влияние.

Анализ и программирование рисков особенно необходимы для ИТ-компаний, специфика деятельности многих из которых заключается в наличии нескольких рыночных элементов, сегментов (заказчиков, покупателей, потребителей, пользователей) со слабоопределенными

колебаниями объема и структуры спроса в условиях недостатка маркетинговой информации, высокой степени риска при проведении коммерческих операций.

С другой стороны, информационное обеспечение при оценке и программировании риска служит не только в качестве источника данных для анализа, но и само по себе является средством снижения риска. Однако доступ к информации, на основе которой принимаются решения, связанные с выявлением и оценкой текущих и перспективных тенденций в условиях рынка, ограничен, так как получение данных о работе других ИТ-компаний часто затруднено существованием коммерческой тайны, способностью каждой компании в любой момент принять любое решение, непредсказуемое для оценивающего окружающую среду субъекта, что порождает неопределенность при выборе линии поведения и прогнозирования риска.

С позиций системного анализа это означает, что существует многообразие реально существующих и взаимодействующих друг с другом систем, есть вероятность неблагоприятных внешних воздействий, и, следовательно, внешняя среда постоянно создает риски наступления неблагоприятных событий. Совокупность этих систем образует многомерное пространство их взаимодействия в котором находится все многообразие существующих рисков - многомерное пространство рисков. В нем каждому виду деятельности, касающейся информационных технологий, соответствует свое подпространство рисков.

Подпространства рисков, касающихся информационных технологий, формируются в зависимости от вида или типа информационной системы, стадии ее жизненного цикла (проектирование, разработка, внедрение, эксплуатация, модернизация, ликвидация и так далее), финансовых, социальных, общественных условий и ограничений, отрасли использования, региона, стратегии поведения действующих лиц и принимаемых ими решений. На каждый из рисков оказывает (или может оказывать) влияние своя система факторов. Таким образом, оценивание и программирование рисков для информационных систем - это многофакторная задача, специфика которой заключается в том, что действующие факторы сами по себе могут и не провоцировать развитие рисковой ситуации, но при некоторых сочетаниях, которые не всегда можно предвидеть, могут привести к крайне негативным.

Очевидно, что подпространство рисков, в котором происходит любой рассматриваемый вид деятельности, нуждается в создании систем классификации рисков и влияющих на них факторов. Существуют варианты такой классификации и для информационных систем.

Не останавливаясь подробно на этих вариантах, отметим одно существенное обстоятельство. При создании такой классификации фактически происходит замена сложной системы рисков, реально существующих в рассматриваемом подпространстве (т.е. объективной системы), на субъективное и всегда упрощенное отражение этой системы рисков некоторой моделью с целью их практического изучения и анализа.

Использование значительной доли субъективных оценок приводит к тому, что результат анализа риска, связанного с информационными системами, в большой степени имеет характер субъективного исследования, получаемого с различной степенью достоверности, у которой значение не меньшее, чем сама полученная результирующая величина (оценка) риска.

На практике приходится иметь дело с конкретной системой рисков конкретной информационной системы. Явно выраженный динамический характер этой ситуации приводит к тому, что во временном смысле области оценка рисков для любой информационной системы связана с задачей прогнозирования, что также предопределяет неопределенность в полученных результатах.

Общий жизненный цикл любой информационной системы от формирования бизнес-идеи до завершения эксплуатационной фазы сопровождается появлением и развитием различных рисков, поэтому вполне правомерно говорить о существовании целостной и весьма сложной пространственно-временной системы рисков, в рамках которой происходит разработка, внедрение, эксплуатация информационной системы. При этом отдельные риски или их подмножества, объединенные взаимозависимостями, подчиняются своим внутренним, объективным законам, абсолютное познание которых чрезвычайно затруднено.

Все изложенное выше позволяет с полным основанием увязать понятие «риска» в информационных системах с понятием «неопределенность». При этом следует отметить, что очень часто в исследованиях, посвященных различным рискам, понятие «неопределенность» заменяется (не всегда достаточно обоснованно) более узким - «случайность». Ведь только при таком упрощении возможно использовать для оценки рисков в информационных системах методы классической теории вероятностей. Однако остаются до конца не решенными проблемы корректного применения этих методов.

В то же время можно говорить о существенных преимуществах применения теории нечетких множеств (разработки соответствующих многокритериальных моделей и их реализации в специализированных программных продуктах) для оценки рисков в информационных системах.

Основное преимущество такого подхода определяется тем, что аппарат теории нечетких множеств требует от лица, принимающего решения, задания не точечных вероятностных оценок, а интервальных, образующих расчетный коридор значений прогнозируемых параметров. Отсюда вытекает удобство этих методов, проявляющееся в повышенной степени обоснованности, поскольку здесь учитываются все возможные сценарии развития, образующие непрерывный спектр, в отличие, например, от метода Гурвица, рассчитанного на дискретное множество сценариев.

При этом оценки рисков могут быть получены в двух вариантах. Первый - это величина финансовых, информационных и других потерь, которые возможны в случае нежелательного развития ситуации. Второй - это некоторый числовой или нечисловой показатель, характеризующий уровень риска, присущий анализируемой информационной системе, как степень неопределенности относительно будущего развития позитивных и негативных сторон ее функционирования и окружающей среды. Соответствующие методы оценки и программирования рисков нами в настоящее время развиваются с использованием программного обеспечения Matlab Fuzzy Toolbox, Fuzzytech и Fuzicalc и будут представлены в дальнейших публикациях.

POLICY OF PERSONAL DATA SECURITY

Łukasz Kister,
European Association for Security (Poland)

This article focuses on procedures of drawing up and bringing into effect a document which describes essential rules for personal data security. Possession of such a document is legal obligation to any organization that processes personal data on territory of the Republic of Poland.

1. Introduction

Once Poland run for joining the European Union structures it had to conform its national legal system to meet the international standards within the area of civil rights and obligations. At level of personal data security, all EU countries are obliged to implement *Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (WE L 281)*. Poland im-

plemented the directive on 29 August 1997 by authority of the Act on the Protection of Personal Data (Journal of Laws No. 133 item 883).

Currently binding legal system in this area was established upon amendments passed to earlier legal acts in 2004 (Journal of Laws No. 25 item 219 with amendments) which in particular applied to mandatory organizational and technical means ensuring security of processed personal data.

2. Basic expressions in personal data security

In order to keep argument in the article correct, it is necessary to introduce some major expressions related to personal data security.

Personal data is any information concerning an identified or identifiable person. Modifier *any information* indicates wide range of the expression "personal data", that includes not only language signs but also images, sounds and, getting more important, biometrics as well. It is important that biometric data is finger prints or retina pattern as well as structure of face, voice projection, geometry of a hand, pattern of veins and even habits or acquired skills (e.g. walk style, handwriting, etc.).

Personal data processing is any operation made over personal data, especially in IT systems, such as collecting, saving, storing, editing, modifying, sharing and erasing data. Determining particular operations which are part of personal data processing, does not make the catalog of such operations closed. It specifies time frames of data processing, from collecting to erasing data, what gives frames for obligation of personal data security.

3. Documentation of personal data security

3.1 Definition

The legislature did not define expression "Policy of Personal Data Security" [further called: the Policy] therefore help of scientists and experts was necessary to make clear and precise definition of it.

Policy of Personal Data Security is a set of laws, regulations and practical experience that determine a way of management, protection and distribution of personal data inside and outside of an institution. The set is directly related to security of personal data processed traditionally as well as in IT systems.

3.2 Contents

Contents of the Policy document is described in the executive decree to the mentioned earlier Act, nevertheless almost all independent experts and researchers claim that it is not extensive enough to cover all legal obligation for personal data security. Therefore, according to the international standards ISO 27001 and ISO 17799, the Policy is supposed to include below listed elements:

- Declaration of an institution management;
- General statements (definitions, goals, extent);

- Structure of management;
- Strategy of organizational and technical security measures, including:
  - personnel security;
  - access control;
  - hardware protection;
  - access to IT systems;
  - notebooks and on-line work (remote access);
  - electronic information storage devices;
  - access to the Internet;
  - e-mail;
  - antivirus protection;
  - cryptographic protection;
  - emergency data back-up;
  - withdrawal from use and utilization of hardware and storage devices;
  - security audits;
  - trainings;
  - access to personal data for personnel from the outside.
- Registering of personal data sets;
- Audit and updating of documentation
- Final statements.

and also elements described in the executive decree:

- List of buildings, rooms and parts of room that make area in which personal data is processed;
- List of personal data sets with software used to processed the data;
- Description of structure of the data sets which shows contents of data records and relations between records;
- Algorithm of data flow between particular systems.

It is also important to indicate necessity of implementation into the Policy procedures for crisis management in personal data security system.

3.3 Preparation of the Policy

Documentation that specifies rules of security for processing personal data, apart from other detailed requirements, **must be adequate to reality** when treats actual state of its conformity with the law. Preparation of the Policy should be preceded by audit in a company that allows to collect all information needed to create the Policy.

Formally, the Policy may consist of one or few documents describing process of personal data security. According to the legal requirements, the Policy has to be prepared in a traditional way (hard copy).

4. In conclusion

Properly prepared and implemented in a company Policy of Personal Data Security makes procedures that allow to manage data of specific value professionally. Beside meeting legal requirements, the Policy creates long-term image of safe partner in business, client, employer, organization etc.

References:

1. Buller L.J.: *Influencja*, Stalowa Wola: KUL, 2008. ss. 165. ISBN 978-83-61307-08-2
2. Drozd A.: *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa: LexisNexis, 2007. ss. 499. ISBN 978-83-7334-784-7
3. Dworzecki J.: *Podstawy prawne wykonywania zadań ochrony osób i mienia. Wybrane zagadnienia*, Gliwice: GWSP, 2009. ss. 138. ISBN 978-83-61401-20-9
4. Kister Ł.: *Polityka bezpieczeństwa danych osobowych*, Ochrona mienia i informacji, nr 6, 2009, s. 14-16. ISSN 1732-5951
5. Kister Ł., MACH V.: *Bezpieczeństwo przedsiębiorstwa informacyjnego*, Securitologia, nr 9, 2009, s. 19-28. ISSN 1898-4509
6. Korzeniowski L.F.: *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*, Kraków: EAS, 2008. ss. 311. ISBN 978-83-925072-1-5

ЭЛЕКТРОРАЗРЯДНАЯ ЗАЩИТА ОТ ПОДДЕЛКИ БУМАЖНЫХ ДОКУМЕНТОВ

Шкилёв Владимир, Недиогло Виктор, Адамчук Аркадий
Министерство информационных технологий и телекоммуникаций (Республика Молдова)

Is presented new information technologies at manufacturing paper documents with high level of protection. The way of formation a database of documents on the basis of association of the wave and digital information is offered.

Идея использования процессов, даже теоретически не поддающихся полному расчету и управлению, для высокоуровневой защиты документов не нова. Ещё в конце 60-годов С.Виснер предложил использовать фотоны с заданными поляризованными состояниями [1]. И хотя технологически идея не реализуема и по сей день, тем не менее, идея С.Виснера действительно была блестящей, хотя бы потому, что из нее со временем развились новые подходы в криптографии, которые дают надежду разработать, рано или поздно, простые и дешевые технологии изготовления бумажных документов с высочайшим уровнем защиты.

А теперь обсудим не технологию защиты бумажных документов, а физический эксперимент, проведенный в 1989 году, с помощью которого была еще раз подтверждена интерференция электронов [2]. В этом эксперименте сотрудники, возглавляемые А.Тономурой из Лаборатории перспективных исследований фирмы Хитачи и Университета Гакушуин в Токио, пропускали поток электронов через проницаемый барьер, эквивалентный экрану с двумя щелями. После прохождения через барьер каждый электрон попадал на флуоресцентный экран, вызывая короткую вспышку света. Наблюдая за каждой вспышкой, японские экспериментаторы могли фиксировать место попадания каждого электрона. Полученные результаты, подтверждающие волновую природу материи, приведены на рис.1.

Вначале *(рис. 1а – 10 попаданий электронов в мишень, рис. 1б -100 попаданий)* кажется, что эти вспышки распределены более или менее равномерно по мишени-экрану. Но со временем начинают появляться намеки на определенную картину *(рис. 3в – 3000 попаданий).* Возникают ощущения, что вспышки предпочитают появляться в одних местах и избегать другое места экрана. На четвертой и пятой экспозиции *(рис. 1г и рис. 1д – 20.000 и 70.000 соответственно число попаданий электронов в экран)*, ощущения превращаются в экспери-

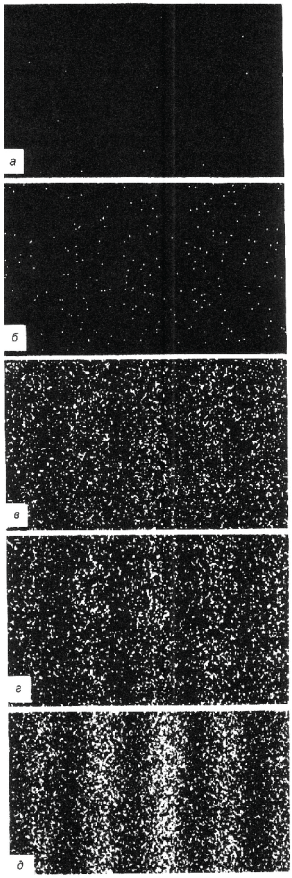


***Рис.1* Экспериментальное подтверждение существования волн материи**

ментальный факт – на мишени появляется чередующий ряд параллельных полос, подтверждающих интерференцию электронов.

Данный физический эксперимент, даёт намек на то, в какую сторону нужно развивать технологию, но с учетом того, что технология

изготовления документов должна быть в тысячи раз более дешевой.

Результаты и обсуждение.

А теперь перейдем к описанию другого физического эксперимента [3], который действительно открывает в перспективе путь к созданию новой технологии.

Схема проведения эксперимента чрезвычайно проста. В бумаге электроразрядным способом пробиваются небольшие отверстия. Затем полученные образцы сканируются на просвет на обычном сканере и сохраняются в базе данных. Полученные картинки обсчитываются на компьютере, и вычисляется ряд параметров в расположении пятен.

Большинство экспериментальных работ в этой области [4] описывает особенности физических процессов в межэлектродном промежутке, внимание исследователей на информационные возможности этих технологий [5] ранее практически не обращалось.

Типичный документ, содержащий индивидуальный цифровой код и индивидуальную картинку, полученную с помощью электрических пробоев, выглядит следующим образом (рис. 2). При отсутствии индивидуального цифрового кода сложно построить базу данных из-за серьезных математических трудностей, возникающих при использовании распознания образов. База данных строится на совмещении цифровой и волновой (индивидуальной матрицы) информации. По цифровому коду находится документ в базе данных, а по индивидуальной матрице проверяется подделный документ или нет.

На рис.3 приведена типичная индивидуальная картинка *(без цифрового кода)*, из которой следует не только индивидуальность картинки в целом, но и неповторимость каждого из пятен.

***Рис.2* Документ строгой отчетности с защитой индивидуального цифрового кода электроразрядной технологией**

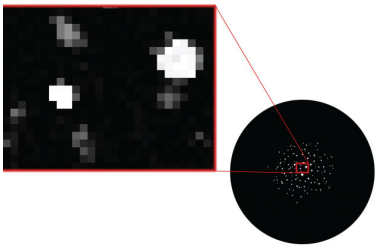


***Рис.3* Типичная индивидуальная картинка, экспериментально полученная с применением электроразрядной технологии**

Эта типичная картина *(рис. 3)* мало отличается от рис. 1б. Отличие в том, что эксперимент предельно прост и технологичен, а результаты реализуются не на экране дисплея, а непосредственно на бумажном носителе.

Теоретически вероятность повтора матрицы при индивидуальной обработке оценивалась в 10^{-400}. С позиции уровня защиты эта величина равна бесконечности. Технологический аспект проблемы показывает, что бесконечность и 10^{-400} слабо отличимые понятия.

Заключение

Предложена принципиально новая технология защиты бумажных документов с высоким уровнем защиты.

Литература:

1. Wiesner S. Conjugate coding // Sigact News. –1983. –Vol.15, №1. –P.78-88.
2. Тономура А., Ендо Ј., Matsuda T., Kawasaki T., and Exawa H. Demonstration of single – electron buildup of an interference pattern. Amer. J. Phys. Vol. 57. pp. 117-120. 1989.
3. 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.
4. Г. Ретер. Электронные лавины и пробой в газах. Перевод с английского под редакцией В.С. Комелькова, Издательство «Мир». Москва, 1968, -390 с.
5. Шкилев В.Д. и др. Патент Республики Молдова № 3389 «Способ идентификации объектов». MD-BOPI №8, 2007, с. 51.

ОРГАНИЗАЦИЯ ДОСТУПА К РЕСУРСАМ ВУЗА НА ОСНОВЕ ID-КАРТ

Жека Александр, *"Intexnauca" S.A. (Республика Молдова)*

Activities of the modern university are multidisciplinary in nature, and management of the university on the basis of information technology is a complex task. In this regard, the key events in the development of IT become a reliable and efficient infrastructure of informatization, the introduction of unified methods of access to corporate data based on ID-cards, improvement of the controllability of the full range of information resources, as well as ensuring that the IT infrastructure meets the strategic objectives of the university.

В вопросах информатизации университета можно выделить несколько проблемных областей, или контуров информатизации вуза, - административное управление и управленческий учет, финансы, уп-

равление учебным процессом, управление информационными ресурсами, собственно образовательный процесс, научные исследования. Как правило, интеграция объектов информатизации каждого контура выполняется на основе создания корпоративной информационной среды вуза в целях обеспечения единства учебных и управленческих процессов в вузе, а также реализации универсальных способов доступа к информации, что послужит основой формирования полноценной корпоративной системы управления знаниями. Если говорить об управлении в вузе, то для него информационные технологии (ИТ) являются основным средством, которое позволит создать преимущества в конкурентной среде. В этой связи ключевыми мероприятиями в развитии ИТ становятся создание надежной и эффективной инфраструктуры информатизации, внедрение унифицированных способов доступа к корпоративным данным на основе **ID-карт**, улучшение управляемости всего комплекса информационных ресурсов, а также обеспечение соответствия ИТ-инфраструктуры стратегическим целям вуза. Комплексная реализация данных мероприятий может быть увязана с формированием **корпоративной информационной среды** (КИС) вуза, что обеспечит интеграцию информационных ресурсов и позволит создать информационную инфраструктуру вуза в соответствии с действующей организационной структурой и принятыми бизнес-правилами.

Особенности университета как объекта информатизации связаны с многопрофильным характером деятельности, обилием форм и методов учебной работы, пространственной распределенностью инфраструктуры (филиалы, представительства), многообразием источников финансирования, наличием развитой структуры вспомогательных подразделений и служб (строительная, производственная, хозяйственная деятельность), необходимостью адаптации к меняющемуся рынку образовательных услуг, потребностью анализа рынка труда, отсутствием общепринятой формализации деловых процессов, необходимостью электронного взаимодействия с вышестоящими организациями, частым изменением статуса сотрудников и обучаемых. Несколько облегчает проблему то, что вуз представляет собой стабильную, иерархическую по функциям управления систему, обладающую всеми необходимыми условиями жизнедеятельности и действующую на принципах централизованного управления (последнее означает, что в управлении задачами информатизации может активно использоваться административный ресурс).

Во многих задачах управления университетскими ресурсами возникает вопрос, связанный с иден-

тификацией пользователя. Обычно идентификация необходима для получения персонифицированного регламентированного доступа к ресурсам вуза. В рамках описываемой задачи можно разделить ресурсы на две категории:

- информационные ресурсы, имея в виду ресурсы, доступ к которым осуществляется через компьютер;
- материальные ресурсы, доступ к которым осуществляется непосредственно.

К ресурсам *первой категории* можно отнести корпоративную вычислительную сеть вуза, файловые серверы, корпоративные порталы, различные корпоративные системы и сервисы информационной среды вуза.

Ресурсами *второй категории* могут являться доступ в помещения вуза, в том числе в общежития, библиотечные ресурсы, товары в специализированных магазинах университета, и даже общественный транспорт.

Для ресурсов первой категории используются учетные записи пользователей сети вуза и корпоративных порталов. Для ресурсов второй категории чаще всего используются идентификационные пластиковые карты (ID-карты).

ID-карты различаются по технологическим решениям. На простейшие ID-карты требуется нанести некоторый идентификационный код, однозначно характеризующий владельца. Считывание с таких ID-карт является контактным. Технология других ID-карт позволяет «прошить» идентификационный код на карте и связывать этот код с пользователем ресурсов.

Другой тип ID-карт – smart-карты, позволяют программировать эти карты, прошивая, например, срок их действия до конца обучения в университете. Таким образом, отпадает необходимость отслеживать действительность карты при анализе на обрабатывающих устройствах. Необходимая информация уже есть на самой карте.

Последняя описываемая технология уже действует в течение нескольких лет в некоторых Европейских и Американских университетах, но опыт их использования свидетельствует о многочисленных сложностях с оборудованием и собственно картами. Поэтому на текущий момент наиболее приемлемым выбором с точки зрения цена/эффективность в молдавских вузах можно считать ID-карты с прошитым кодом, но без возможности программирования. К таким ID-картам можно отнести проксикарты, соответствующие стандарту EM-MARINE.

Прокси-карты бесконтактного считывания имеют и те преимущества, что они не изнашиваются, не боятся загрязнения и влаги, имеют высокую степень защиты от копирования. На эти карты могут быть

нанесены дополнительные сведения о пользователях. В том числе – ФИО, фотография, статус, штрихкод, позволяющий использовать ту же карту и в устройствах контактного считывания. Для дополнительной защиты при идентификации возможно использования PIN-кода, при этом необходимо использовать специализированные считыватели с клавиатурой.

В настоящий момент, для ВУЗов могут быть разработаны и внедрены сервисы с использованием прокси ID-карты для:

- доступа студентов и сотрудников в общежития университета;
- доступа сотрудников в некоторые помещения;
- доступа учащихся и сотрудников на охраняемую территорию;
- выдачи/приема ключей от аудиторий на вахтах университета;
- фиксирования посещаемости студентов на лекционных занятиях;
- использования в библиотеке вуза в качестве читательских билетов.

Использование ID-карт и специализированного программного обеспечения, интегрированного с корпоративными данными, для доступа к ресурсам позволит упорядочить доступ в общежития, на территорию и в помещения университета и к ресурсам библиотеки. Поддержка данных по студентам, сотрудникам, помещениям в актуальном состоянии обеспечит высокий уровень безопасности такого доступа.

Список источников:

1. *Крюков В.В., Майоров В.С., Шахгельдян К.И.* Реализация корпоративной вычислительной сети вуза на базе технологии Active Directory // Труды Всерос. науч. конф. «Научный сервис в сети Интернет». Новороссийск, 2002. С. 253–255.
2. *Гмарь Д.В., Крюков В.В., Майоров В.В., Шахгельдян К.И.* Единая система регистрации и управления доступом к информационным ресурсам вуза // Труды Всерос. науч. конф. «Научный сервис в сети Интернет». Новороссийск, 2003. С. 135–138.
3. http://www.vvsu.ru/

НЕКОТОРЫЕ ПОДХОДЫ К СОЗДАНИЮ СИСТЕМ УПРАВЛЕНИЯ ЗНАНИЯМИ КОМПАНИЙ

Ольга Петрова, *"Compania Dekart" SRL (Республика Молдова)*

Успешность деятельности той или иной компании зависит от различных факторов. Одним из основных является уровень подготовки сотрудников, их квалификация и опыт.

1. Квалификация любого сотрудника нуждается в регулярном повышении
2. Опыт, который не передается другим, теряет половину своей ценности поскольку при этом не происходит накопления знания другими сотрудниками. Кроме того, увольнение сотрудника ведет к потери этого знания для компании, а переход сотрудника к конкурентам приведет к тому, что эти знания возможно будут работать на пользу других.

Цель работы – создать систему, позволяющую решить одновременно две задачи. Во-первых, создать сотрудникам эффективный доступ к информационным ресурсам компании. А во-вторых, обеспечить защиту интеллектуальной собственности компании, ее коммерческой тайны.

Противодействие угрозам, связанным с несанкционированным доступом к информации

1. Всю совокупность информации, накопленную компанией и постоянно обновляемую, следует классифицировать по различным признакам.
   a. По области применения – финансовая информация, технологические сведения, сведения о безопасности предприятия и т.п. (F_1, …, F_n).
   b. Внутри каждого тематического раздела информация должна быть разделена по уровню доступности – общедоступная (IR_f), доступная представителям отдельных групп (IR_g), доступная отдельным работникам (сотрудникам) (IR_p).
2. Штат (штатное расписание) компании разбивается на группы по профессиональной принадлежности и т.п.
3. Формируется матрица соответствия сотрудника и информационных ресурсов, доступных ему для чтения.
4. Создается LDAP-хранилище с персональными данными сотрудников, необходимыми для аутентификации в системе и персональный список доступных информационных источников – например, $P_1 \leftrightarrow\{(F_1, IR_f), (F_1, IR_p), (F_2, IR_f), (F_2, IR_g), \ldots, (F_n, IR_f), (F_n, IR_g)\}$, $P_2 \leftrightarrow$

{(F_1 , IR_f), (F_1, IR_g), (F_2, IR_f), (F_2, IR_p), …, (F_n, IR_p)}.

5. Доступ к информационной системе осуществляется только после аутентификации. При обращении к системе после аутентификации сотруднику получает доступ к информации (выдается список всех доступных источников или последний читаемый документ или список изменений в базе знаний или авто-напоминание).

6. Для доступа к особо важной информации вместо обычной аутентификации может применяться усиленная аутентификация.

Противодействие угрозам, связанным с нарушением процедуры размещения информации

1. Так же как и в предыдущем разделе, вся совокупность информации, необходимая компании, классифицируется по различным признакам F_1, …, F_n.
2. Внутри каждого тематического раздела информация разделяется по уровню ответственности – IW_g, когда право на запись есть у представителей отдельных групп, IW_p, когда право на запись есть только у отдельных работников.
3. Аутентификация для доступа к соответствующим разделам базы знаний осуществляется только после предъявления сертификата открытого ключа конкретного сотрудника.
4. Запись информации производится только при наличии цифровой подписи для подтверждения неизменности и неотрекаемости.

В целях реализации вышеперечисленных мер в компании должно быть предусмотрено использование инфраструктуры защиты информации на основе открытых ключей. Компания может развернуть собственный Центр сертификации открытых ключей либо воспользоваться услугами уже существующих Центров. Каждый из сотрудников генерирует свою пару ключей (секретный и открытый) и получает в Центре сертификации сертификат своего открытого ключа. Данный сертификат может быть использован для аутентификации сотрудника при обращении к базе знаний и для проверки цифровой подписи под размещенной там информацией.

Защита интеллектуальной собственности авторов

Для защиты прав авторов (их интеллектуальной собственности) предлагается один из разделов базы знаний превратить в интеллектуальный репозиторий. Авторы могут размещать свою информацию в данном разделе, заверяя ее своей цифровой подписью. Причем могут сохраняться не только законченные результаты, но и промежуточные, а также варианты решений. Законченные работы могут быть (и должны!) перенесены в основную базу знаний компании. При переносе документ подписывается (с помощью цифро-

вой подписи) лицом, осуществляющим данную операцию.

Обучающая составляющая системы знаний

Любое обращение к базе знаний компании должно быть запротоколировано в специальном файле – журнале операций. Данный модуль решал бы двуединую задачу – информационной безопасности компании и стал бы одной из компонент автоматизированного помощника самого сотрудника. На базе экспертных оценок подготовить авто-советника для сотрудников с целью повышения уровня их знаний.

Система контроля знаний

Выявление знания-незнания возможно за счет использования различных тестов. Тестирование может проходить как на добровольной основе, так и быть предусмотрено должностными обязанностями. Регулярность процедуры, размер теста и его уровень могут быть заданы исходя из сложности проблематики решаемых тем или иным специалистом вопросов, стажем работы в компании, ответственности при принятии решений, уровнем образования и т.д.:

1. ежемесячно, ежеквартально, раз в полгода, раз в год;
2. исходя из того, к каким разделам информационной базы сотрудник имеет доступ, составляется перечень тестов, их очередность, регулярность и уровень сложности;
3. если произошло обновление информационной базы, то можно после ознакомления с ней проводить мини-тест для определения степени усвоения материала;
4. при накоплении данных о том какие части информационных ресурсов посещаются сотрудником и с какой регулярностью программа-робот может предложить пройти тестирование по данным частям, а также по тем, которые посещаются гораздо реже либо не посещаются вовсе;
5. открытый вопрос о принудительности прохождения того или иного теста. Возможно имеет смысл применять тонкую интеллектуальную настройку системы управления знаниями. Например, не разрешать просматривать информацию из базы знаний, если не пройден тест, либо тест пройден с неудовлетворительным результатом. Второе предложение – автоматически открывать тот раздел базы знаний, по которому сотрудник не смог пройти тестирование.

ОБ УНИВЕРСАЛЬНЫХ МЕТОДАХ ИДЕНТИФИКАЦИИ МАТЕРИАЛЬНЫХ РЕСУРСОВ И О ФИЛОСОФСКОМ ПОНИМАНИИ ВЗАИМОДЕЙСТВИЯ ЛЕГАЛЬНОЙ И ТЕНЕВОЙ ЭКОНОМИКИ

Шкилев В.Д., Адамчук А.Н., Мартынюк. Н.П.
Министерство информационных технологий и телекоммуникаций, Технический университет (Республика Молдова)

The universal method of identification of material resources is offered.

Причина возникновения теневой экономики лежит в двойственности всего сущего. Весь феноменальный мир [1] в котором человечество строит свою цивилизацию путем выстраивания экономических отношений, есть бесконечное выстраивание сочетаний двух известных начал Мироздания – Духа и Материи. Из этой проявленной двойственности *(биполярности или дуальности)* проистекает двойственность всего Мироздания. Все существа, и человек в том числе, все понятия и вещи – это дуальности *(или бинеры)*, обладающие двумя полюсами одной и той же силы и одного и того же явления. Наличие левого и правого полушарий в нашей голове, позволяющего воспринимать Мироздание, как с логических, так и чувственных позиций, предполагает всякое понятие воспринимать через противопоставление. И не только воспринимать, но и выстраивать в соответствии с этой логикой экономические отношения. Лишь из составления этих крайних экономических понятий *(теневая и легальная экономики)* рождается истинное понимание экономики в целом. Человеческий Разум, по своей природе способен воспринимать лишь разности экономических явлений, но не их действительную сущность. Каждое внутриэкономическое понятие мы воспринимаем через комплекс более простых противопоставлений. Человеческий разум постигает Мироздание в целом, и экономику в частности, только через бинеры *(противопоставления)*.

Рис. 1. **Монада как символ единства и борьбы противоположностей (теневой и легальной экономики)**

В экономических обзорах, а особенно в представлениях налоговых служб, теневую экономику представляют как зло, порождающее коррупцию. Если бы все было так просто, нашли первопричину коррупции и быстро победили Зло. Все устроено более красиво и не однозначно. Легальная и теневая экономика в некотором смысле равноценны и равнозначны и являются полюсами одного и того же явления – экономики в целом. Легальная экономика без теневой – ничто, лишь их соединение дает экономике жизнь, и противопоставление их дает эволюцию в экономике. Стоит «победить» теневую экономику и умрет вся экономика. Означает ли это бессмысленность или даже вредность в работе налоговых служб? Конечно нет, задача у налоговой службы благородная, правда задача у налоговых служб вовсе не в победе над теневыми структурами *(такая победа в принципе невозможна)*, их задача более тонкая – в плавном вытеснении структур теневой экономики в легальную, именно в этом смысл эволюционного развития экономики. Теневая экономика – это зло для одних и добро для других. Теневую экономику можно представить в виде тени света, без которой свет не существовал бы даже в нашем представлении. Разъединить теневую и легальную экономику, отсечь одну от другой, и они обе умрут. Для того чтобы получить живую и эволюционирующую экономику нужно познать и оценить каждую из них. Все что дано для жизни природой, не дурно и не хорошо, но становится дурным или хорошим в зависимости от того, как человек ими пользуется. Мы привыкли к методологии разъединения теневой и легальных экономик, в то время как более гармоничным подходом можно признать их как две стороны одного и того же.

Может ли выжить вновь создаваемое малое предприятие в режиме легальной экономики? Нет, не может. Законодательство любой страны создано таким образом, что осуществление всех платежей на ранней стадии приводит это предприятие к естественному банкротству. Идея инновационного инкубатора, создающего для вновь создаваемого малого предприятия тепличные *(в том числе и законодательные)* условия, является косвенным признанием законодательного несовершенства. Можно ли создать такое законодательство, которое бы не допускало существование теневой экономики? Не обольщайтесь, и не требуйте этого от законодателей, этого в принципе сделать невозможно.

Любой политик, принимающий экономические решения из самых лучших побуждений *(вспомним афоризм бывшего премьера РФ Черномырдина В. – хотели как лучше, а*

получилось как всегда) не может принимать гармоничные решения исходя из официальной экономической отчетности, не учитывающей экономические результаты теневой экономики. Из-за отсутствия в нашем обществе механизма объективного разделения экономических показателей теневой и легальной экономик и вытекает политическая беспомощность. Создать такой механизм можно с помощью идентификационных технологий [2-4] и путем создания автоматизированных систем управления способных отличать легальные и контрафактные товары, но пользоваться таким механизмом может только высокодуховный и образованный политик. Окончательная победа в противоборстве легальной и теневой экономиках реализуется не с помощью автоматизированных систем управления (это всего лишь вспомогательный инструментарий), а с помощью эволюционного развития нашего Сознания.

Любое ускоренное вытеснение теневой экономики на «свет» может дать противоположный результат и нанести удар по легальной экономике. Вспомним исторический пример из нашего прошлого – ускоренную коллективизацию и к чему она привела.

Разработка универсальных принципов идентификации для автоматизированных систем управлении требует разработки идентификационных меток, способных отличать легальные и контрафактные ресурсы, находящиеся в любом фазовом состоянии.

Литература:

1. Шкилев В.Д., О философском понимании генезиса коррупции. Материалы XVII симпозиума по эниологии, 2008, с. 118-122.
2. Шкилев В.Д. Каранфил В.Г., Фотенко В.М. и др. Патент РМ №3328. Способ и устройство для спектральной идентификации материальных ресурсов.
3. Шкилев В.Д. Патент РМ №39612. Индивидуальная маркировка, штрихкод и способ его изготовления.
4. Шкилев В.Д. Патент РМ №3968. Способ формирования идентификационной метки на бумажном носителе.

ANALYSIS OF THE "HUMAN FACTOR" AS AN INFORMATION THREATH TO TRADE SECRETS AND COUNTERACTIONS – SPYING IS IN!

Tamara Jovanov, *MSc*
Faculty of Economics, "Goce Delcev" University — Stip,
(Republic of Macedonia)

"Economic espionage and trade secret theft threaten our nation's national security and economic well being."[1]
Since the 1970s brought the explosion of the Information Revolution and the rise of personal computers, we've become even more interested in the brain and how it works. We shouldn't be aware of Artificial Intelligence and the smart machines of the 21st Century, but of the people in our surroundings and their ability to be corrupted from our competitors. How can we know who is really working for us and who is on the other side from inside!? The changing business environment is putting a huge pressure on the everyday activities of the corporations and has pushed them into a corner, where they do not choose the means of their survival. People - spies - companies, and even countries are after your company's property…

The flying heads of once well established managers and corporate directors are a consequence of poorly protected corporate secrets and installed moles among the loyal company workers. Virtually no company is immune to the risk of economic espionage. If you think economic espionage happens only to the Fortune 500 giants who have huge secrets to steal and operate on a global basis, think again! While all companies are at risk, the biggest victims of economic espionage are typically smaller businesses. And why? Because these companies have the largest number of competitors, which translates into the largest number of possible spies. Globalization as well has raised their profile significantly. This may make them a target of someone's espionage scope. If the company has confidential "secret" information, legally referred to as a trade secret (it doesn't matter whether it is chemical formula, patent application, marketing plan, business expansion plan, customer list, pricing information, new product launch information, new technology drawing, etc.), which is one type of intellectual property, that has independent economic value, which you have made a reasonable effort to keep secret, and someone illegally gets a copy of it, you have been a victim of economic espio-

[1] President Bill Clinton, Upon signing the Economic Espionage Act, October 11, 1996

nage. Companies are under attack and at enormous risk every day from the global threat of economic espionage, but that risk can and should be lowered and managed. If we don't take for granted the fact that the companies are constituted by people, we can admit that the most common factor of information leaking is the human factor. But why do they do it? It is luxury question to ask if noted that the answers can be various and very individual. Many of the espionage spies do it for money, for greed, for revenge, for their native countries, for opportunity or just because of their huge egos. So it is therefore possible to assume that the anatomy of the spy can be well put in a several counts: young, well educated individual, male or female, with high intellectual potential, ambitious, with money issues, neglected from the company, with troubled childhood, loyal to higher goals. Thanks to the modern age they also have the gadgets to do the job: micro stick - an mini compact audio and video recorder; wrist watches which can record even an rustling conversations with it's hidden voice recorder; dime-size "contact bugs," which anyone could stick to the outside of a conference room window and matchbox-size "SIM bugs"; listen-only cellphones that don't ring or light up, that can be activated by a phone call an hour, a week or a month later; innocuous-looking ballpoint pen with a voice-activated audio recorder; Keyghost; etc. Proprietary and trade secret information are the lifeblood of every company in every industry group. Given how valuable trade secrets are, you would think that companies would bend over backwards to protect them, but that is not the case. If the Pareto rule should be applied, than we could say that 80 percent of the risk comes from inside the company, and only 20 percent from outside the company. Opposite of what it is, the focus on reducing risk of trade secret theft should be on education and ethics, not physical security, but the majority of money spent on protecting a company's assets is spent on protecting the physical assets, and it is spent largely to protect the company from only 20 percent of the risk—from outsiders. Think how tough it sometimes is just to get into some buildings as a visitor. You often have to sign in and be issued a badge. At some locations, visitors have to be escorted in certain sensitive areas. You need to know and then punch in on a keypad special door combinations or have card keys to open doors or have elevators stop at specific floors. Security guards greet and watch you when you arrive in the lobby or walk around or enter or leave the parking lot. Closed circuit TV cameras are mounted in ceilings or some other inconspicuous locations keeping an eye on you. In most cases, what is actually being protected is physical property from outsiders, not trade secrets from insiders. Typical security people in

office buildings are concerned with guarding against thieves walking off with a computer; they wouldn't know a trade secret if their lives depended on it. Given that some 80 percent of trade secret theft is perpetrated by employees or other insiders, most companies simply do not properly address the issue of protecting trade secrets. This lapse only increases a company's risk that an employee, ex-employee, or some other insider will walk off with a valuable trade secret, whether intentionally or not. A trade secret that gets out into the marketplace accidentally can cause every bit as much harm as those that are breached by true spies. The question is: Can anything be done to stop economic espionage and secure the informations? - It is impossible to stop it, but it can be reduced! Information protection should be based on eight major elements:[2]

1. Information protection should support the business objectives or mission of the enterprise – the position of the ISSO (Information Systems Security Officer) has been created to support the enterprise, not the other way around;
2. Information protection is an integral element of due care – the senior management is required to protect the assets of the enterprise and make informed business decisions (an effective information protection program will assist in meeting these duties);
3. Information protection must be cost effective (implementing controls based on pre identified significant risk existence);
4. Information protection responsibilities and accountabilities should be made explicit (it is necessary to publish an information protection policy statement where the roles and responsibilities of all employees would be identified);
5. System owners have information protection responsibilities outside their own organization (monitoring the usage of the information to insure that it complies with the level of authorization granted to the user);
6. Information protection requires a comprehensive and integrated approach (information protection issues should be a part of the system development life cycle and during the initial or analysis phase, information protection should receive as its deliverables a risk analysis, a business impact analysis and an information classification document. Additionally, because information is resident in all departments throughout the enterprise, each business unit

[2] Thomas R. Peltier, Justin Peltier, John Blackley, "Information Security - Fundamentals", CRC Press LLC, USA, 2005, p.1-2

should establish an individual responsible for implementing an information protection program to meet the specific business needs of the department);

7. Information protection should be periodically reassessed (due to the dynamic of the process it must be reassessed at least every 18 months);
8. Information protection is constrained by the culture of the organization (the ISSO must give each business unit the latitude to make modifications to meet specific needs).

The conducting of a "walk – about" for a measurement of the current attitude toward information protection should be focused on five basic control activities:[3]

1. Offices secured;
2. Desk and cabinets secured;
3. Workstations secured;
4. Information secured;
5. Diskettes secured.

The typical office environment will have a 90 to 95 percent noncompliance rate with at least one of these basic control mechanisms.[4] In business, having an effective information protection program is usually secondary to the need to make a profit, and the main reason we don't hear so much about its weaknesses and trade secrets theft in public is because the principals do not want the stockholders or the press getting a hold of the fact that company secrets were leaked because of what that would do to the company's stock price.

References

1. Hedieh Nasheri , "Economic Espionage and Industrial Spying", Cambridge University Press, USA, NY, 2005;
2. John Aycock, "Computer Viruses and Malware", Springer Science+Business Media, LLC, 2006, Canada;
3. Khaled Khan & Yan Zhang, "Managing Corporate Information Systems Evolution and Maintenance", Idea Group Inc., USA, 2005;
4. Mark Osborne, "How to Cheat at Managing Information Security", Syngress Publishing, Inc., Canada, 2006;
5. Mark Stamp, "Information Security – Principles and Practice", John Wiley & Sons, Inc., New Jersey, 2006;
6. Steven R. Barth, "Corporate Ethics – The Business Code of Conduct for Ethical Employees", Aspatore Books, Inc., USA, 2003;
7. Thomas R. Peltier, Justin Peltier, John Blackley, "Information Security - Fundamentals", CRC Press LLC, USA, 2005;

[3] Ibid., p.3

[4] Ibid.

ЗНАЧЕНИЕ ИНФОРМАЦИОННОЙ КУЛЬТУРЫ ЛИЧНОСТИ И ОБЩЕСТВА, ПРИ ФОРМИРОВАНИИ ПОЛИТИКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Денис Блудов, *Ставропольский институт им. «В.Д.Чурсина» (Российская Федерация)*

«Впервые человеческая культура и человеческие ценности формируются электронными средствами информации»
Л. Туроу

Информация, была, есть и будет продуктом, который можно продать, купить, обменять, а следовательно она всегда вызывает интерес как со стороны людей пытающихся ею завладеть, так и со стороны тех кто создает системы по ее защите.

На современном этапе развития мира обмен информацией осуществляется при помощи электронных средств, связи. Которые в разы увеличивают скорость, и качество передачи данных. Однако этот подарок прогресса имеет свою ахиллесову пяту, теперь завладеть необходимой информацией и использовать ее по своему корыстному усмотрению, можно при помощи компьютерной техники, находясь за тысячи километров от источника информации, и получив нужные сведения тихонько «скрыться», и как следствие остаться безнаказанным. В связи с этим для полноценного использования возможностей прогресса, необходимо пользоваться информационной культурой, которая является своего рода гарантом безопасности.

Однако информационная культура, как всякая другая, имеет и обратную сторону, она может служить и добру и злу. Свободное развитие личности здесь совмещаются с автоматизацией человека, обилие информации с определенным мышлением, возрастание коммуникативных возможностей с изоляцией индивида и элитарным знанием, преодоление кризисных явлений в обществе с упрощением жизни. С социально-психологической точки зрения информатизация изменяет традиционные циклы жизнедеятельности людей и сам ритм их жизни; с моральной – вытесняет ценность межличностного общения, заменяет реальный мир виртуальным; с политической – усиливает возможности манипулирования индивидуальным и массовым сознанием.

Итак, появление информационной культуры общества и личности в

России отрицать нельзя, но она имеет два основных назначения с одной стороны это один из основных источников дающий огромный поток информации с другой способный этот же информационный массив обработать и найти необходимое.

К сожалению, уровень информационной культуры большинства людей в России низок.

С одной стороны, это объясняется все еще недостаточным внедрением информационных технологий во все сферы жизни и деятельности человека. А с другой стороны - отсутствием системы подготовки грамотных пользователей информационных систем и потребителей информации.

Начало преподаванию информатики в школах России, приходится на 1985 год, когда были приняты соответствующие правительственные решения. Но эти решения имели чисто политический характер и не были подкреплены материально. В 1992 году из 66,8 тыс. школ России только 17 тыс. имели компьютеры (в США 98% школ имеют компьютеры). Однако компьютеризация не оказала заметного влияния на уровень образования ввиду отсутствия педагогических программ и использования явно устаревшей техники (70 % «пентиумов», которыми оснащены наши школы сегодня уже устарели.). Дело ограничилось простейшими программами типа текстового и графического редакторов, электронных таблиц, практических упражнений и простейших головоломок, программ обработки данных.[1]

Все же тот образовательный процесс который ведется, имеет однобокое развитие, а именно при обучении компьютерщиков очень редко можно услышать слово «этика». Основное внимание уделяется математическому образованию, взаимодействию с компьютером как средством решения тех или иных задач. При этом игнорируется то обстоятельство, что взаимоотношение человека с компьютером происходит в определенной культурной среде. Лишенный нравственных ориентиров, человек начинает и себя воспринимать как умную машину, переносит техническое обращение с компьютером на отношения между людьми, что ведет к далеко идущим последствиям – антигуманной деформации всей культуры информационного общества. Не случайно Р. Уиден в своем выступлении перед конгрессменами США заявил, что «некоторые из вполне достойных молодых людей оказываются неспособными оценить этические и моральные последствия своих действий. Я убежден, например, что очень многие, если не все молодые хакеры в нашей стране даже помыслить не могут о том, чтобы на улице силой отнять деньги у старой жен-

[1] Негодаев И.А. «На путях к информационному обществу» Ростов-на-Дону 1999.,с 274.

щины. Но, с другой стороны, весьма реально, что простым нажатием нескольких клавиш компьютера они легко лишат ее всех сбережений»[2]

Из всего сказанного получается, что сложившаяся информационная культура в нашей стране, к сожалению относится пока еще не к массовой, а к субкультуре отдельных индивидов которые благодаря своих глубинным знаниям в этой сфере и наличием также правовой неграмотности противоположной стороны которая заключается в неспособности осознать что они стали жертвой преступления и понесли имущественный вред,[3] могут свободно совершать преступления с использованием компьютерных технологий и оставаться безнаказанными. Это касается, например, такого способа преступной деятельности в сфере компьютерной информации, как кража компьютерного времени, компьютерное мошенничество[4] и другие (в Уголовном Кодексе Российской Федерации ответственности за эти виды преступлений даже не предусмотрено).

Отсюда следует, что бы стабилизировать ситуацию, государству необходимо создавать нормативно правововые базы направленные на урегулирование отношений в данной сфере и защиты всех прав участников задействованных в этом процессе. Создание социальных программ направленных на повышение информационной и правовой грамотности. Своевременная переориентация направлений развития компьютерной техники согласно требованием современности. В результате всех этих консолидированных действий личности общества и государства находящихся, в тесной взаимосвязи и сотрудничестве, как элементов, дополняющих друг друга, будет создана информационная культура в которую будут входить все члены современного российского общества .

---

[2] Батурин Ю.М. Право и политика в компьютерном круге. М.,1987, с. 56.

[3] Сабадаш В. «Компьютерная преступность - проблемы латентности». Источник: crime-research.ru

[4] Волеводз А.В. «Противодействие компьютерным преступлениям» М., 2002., с.98.

ОБ ОДНОМ КРИПТОГРАФИЧЕСКОМ ПРОТОКОЛЕ

В.В. Койбичук
Украинская академия банковского дела
Национального банка Украины (Украина)

Description of the cryptosystems, use of Kerberos crypto protocol for the information transfer protection in the shared distributed systems.

Сейчас для любой компании, государственной организации или отдельного индивидуума, которым требуется защитить данные, транзакции, репутацию, и даже самих себя, как никогда важны безопасность и проверка идентификации. Информация – это актив, который, подобно другим активам организации, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Информационная безопасность – механизм защиты, обеспечивающий: конфиденциальность (доступ к информации только авторизованных пользователей), целостность (достоверность и полноту информации и методов ее обработки), доступность (доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости).

Использование криптографических протоколов – один из способов защиты информации в открытых распределенных системах. Каждая криптосистема характеризуется такими понятиями, как шифрование (расшифровка), ключ шифрования (расшифровки), аутентификация. ***Шифрование*** (***кодирование***) – процесс преобразования порции информации в непонятный вид. Исходную информацию называют ***открытым текстом***, а результат преобразования – ***зашифрованным текстом (криптограммой)***. ***Декодирование (расшифровка)*** – обратный процесс преобразования зашифрованного текста в открытый. Открытый и зашифрованный текст образуют пару взаимосвязанных понятий: открытый текст поступает на вход алгоритма шифрования, а зашифрованный текст является его результатом. В ***симметричной криптосистеме*** (***системе с общим ключом*** (shared-key system)) используются одинаковые (или практически одинаковые) ключи. В ***асимметричной криптосистеме*** (***криптосистеме с открытым ключом*** (public-key cryptosystem)) используются два разных ключа: ***ключ шифрования*** и (соответствующий) ***ключ расшифровки (секретный)***. Под понятием ***аутентификация*** понимается процедура установления соответствия параметров, характеризующих пользователя, процесс или данные задан-

ным критериям. В качестве критерия соответствия обычно используется совпадение заранее введенной в систему и поступающей в процессе аутентификации информации, например, о пароле пользователя, его отпечатке пальца или структуре сетчатки глаза.

Аутентификацию можно разделить на три вида: ***аутентификация источника данных*** (***аутентификация сообщения***), ***аутентификация сущности*** и ***генерация аутентифицированных ключей.*** Первый вид аутентификации означает проверку объявленного свойства сообщения и обязательно связан с каналами связи. Она представляет собой службу безопасности получателя, предназначенную для верификации источников сообщений. Аутентификация сущности – это процесс обмена информацией (т.е. протокол), в ходе которого пользователь устанавливает подлинность другого пользователя. Часто слово «сущность» опускают. Третий вид аутентификации предназначен для организации защищенного канала обмена секретными ключами.

В качестве примера рассмотрим один из наиболее распространенных и эффективно применяемых для защиты передающейся информации, криптографический протокол Kerberos версии 5.

Участниками безопасной связи являются клиент, сервер и центр распределения ключей (KDC – Key Distribution Center), который выступает в качестве доверенного посредника.

Когда клиенту нужно обратиться к серверу, он изначально направляет запрос в центр KDC, который в ответ направляет каждому участнику предстоящего сеанса копии уникального сеансового ключа (session key), действующие в течение короткого времени. Назначение этих ключей – проведение аутентификации клиента и сервера. Обмен сообщениями происходит следующим образом:

***Сообщение 1*:**

$$A \rightarrow S : A,B\,.$$

***Сообщение 2*:**

$$S \rightarrow A:\{T_s, L, K_{ab}, B, \{T_s, L, K_{ab}, A\}_{K_{bs}}\}_{K_{as}}\,.$$

***Сообщение 3*:**

$$A \rightarrow B:\{T_s, L, K_{ab}, A\}_{K_{bs}}\ \{A, T_a\}_{K_{ab}}.$$

***Сообщение 4*:**

$$B \rightarrow A:\{T_a+1\}_{K_{ab}}.$$

Здесь *A*, *B* – принципалы (люди, компьютеры, устройства), *S* – доверенный по средник (сервер аутентификации), *T* – метка времени, *L* – срок годности мандата, K_{ab} – общий ключ для *A* и *B*. Как видно из сообщения 2, сервер генерирует сеансовый ключ, общий для *A* и *B*, скрытно доставляет его (спрятан внутри двух мандатов), шифруя долговременными секретными ключами, который он разделяет с *A* и *B* (K_{bs} , K_{as}).

Получив протокольные сообщения от *Сервера*, пользователи (принципалы) могут обнаружить, что их послания остались без ответа, про-

верив неравенство $|Время - T| < \Delta t_1 + \Delta t_2$. Здесь *Время* означает локальное время получателя, Δt_1 – интервал, представляющий допустимую разницу между временем Сервера и локальным временем, Δt_2 – ожидаемая временна́я задержка. Если часы всех клиентов сверены по эталону, то величина Δt_1, равная одной-двум минутам, вполне допустима. Главное допущение протокола Kerberos – это то, что часы принципалов работают синхронно с часами сервера.

Таким образом, рассмотрев основные концепции протокола сетевой аутентификации Kerberos 5, нельзя полагать, что Kerberos это централизованное решение, способное решить все проблемы сетевой безопасности. В основе данного протокола лежит принцип наследования: клиент доверяет Kerberos, если система корректно предоставляет клиенту ключ шифрования. Приложение доверяет клиенту, если клиент успешно предоставил квитанцию, зашифрованную ключом сервера. В этом доверии и кроется уязвимасть системы (Kerberos). Иначе говоря, секретные ключи должны как и полагается, храниться в секрете. Если взломщик каким-либо образом получит ключ инициатора запроса, то он сможет его сымитировать. Kerberos не защищает от атак типа «подбора пароля». Если пользователь использует несложный пароль, то атакующий может спокойно подобрать его атакой по словарю.

Не смотря на эти недостатки, следует отметить, что данный протокол отличается гибкостью и эффективностью использования, а также обеспечивает повышенный уровень безопасности. Kerberos положен в основу аутентификации пользователей операционных систем Windows 2000/XP/2003.

В заключение, следует отметить, что при разработке и реализации систем защиты, нужно руководствоваться следующими принципами.

1. Ясно формулировать все необходимы предположения. Система защиты информации взаимодействует с окружением, и следовательно, это окружение должно удовлетворять определенным условиям.
2. Явно и точно указывать все предполагаемые услуги по защите информации (обеспечение конфиденциальности, доказательство знания, аутентификация, невозможность отречения, фиксация).
3. Явно выделять частные случаи математических задач (может существовать частный случай трудноразрешимой задачи, который относительно просто решить).

«МЕНЕДЖМЕНТ ИНЦИДЕНТОВ В СИСТЕМЕ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

Анна Милованова, *IT&IS Management SRL*
(Республика Молдова)

Одним из важных процессов в системах управления ИТ-деятельностью является управление инцидентами, оказывающих непосредственное влияние на стабильность работы информационных систем. Это обусловлено увеличением масштаба и функционала систем. Даже после внедрения защитных мер в большинстве случаев остаются слабые места, что делает обеспечение информационной безопасности неэффективным, и, следовательно, инциденты - возможными.

Управление инцидентами обеспечивает уменьшение/ исключение отрицательного воздействия нарушений в предоставлении ИТ-услуг, что является актуальным в особенности для финансово-кредитных организаций и телекоммуникационных компаний. Решение данной задачи требует тесного взаимодействия с пользователями клиентами посредством функции Service Desk.

Сам процесс управления инцидентами связан со многими другими процессами, например, управлением рисками, мониторингом/ аудитом, управлением изменениями, управлением доступом, управлением непрерывностью. Другими словами, процесс управления инцидентами является своеобразным «мотором» жизненного цикла системы безопасности.

Исходя из практики, можно отметить тот факт, что основными типами инцидентов являются:

- функциональная неработоспособность основных модулей или информационных систем целиком;
- недоступность к значимым сервисам, приложениям или к информационным системам в целом;
- ошибочная обработка информации в информационных системах и приложениях;
- сбои в работе приложений, влияющих на эффективность ведения деятельности;
- неисправность, выход из строя аппаратных средств;
- отсутствие доступа к открытым Интернет-ресурсам;
- некорректная работа информационных систем;
- перегрузка в сети.

При управлении инцидентами по всем выявленным инцидентам следует проводить анализ потенциального или реального негативного

воздействия инцидента информационной безопасности на деятельность организации. В качестве примеров основных категорий последствий, которые могут повлечь за собой инциденты, можно отметить:

- финансовые убытки/разрушение бизнес-операций;
- ущерб коммерческим и экономическим интересам;
- ущерб для информации, содержащей персональные данные;
- нарушение правовых и нормативных обязательств;
- потеря/ущерб репутации организации.

Для любой организации, серьезно относящейся к информационной безопасности, основой менеджмента инцидентов должно быть применение структурного и планового подходов с целью минимизации рисков информационной безопасности. Суть данных подходов заключается в осуществлении следующих действий:

- обнаружение, оповещение об инцидентах информационной безопасности и их оценка;
- реагирование на инциденты информационной безопасности, включая применение защитных мер для предотвращения, уменьшение последствий и восстановление после негативных воздействий;
- извлечение уроков из инцидентов информационной безопасности, введение превентивных защитных мер и улучшение общего подхода к управлению инцидентами информационной безопасности.

Менеджмент инцидентов информационной безопасности включает следующие этапы:

- обнаружение и регистрация инцидентов - осуществляется на основании показаний систем мониторинга доступности ИТ-услуг, обращений пользователей, а также осуществляется в системе регистрации и обработки инцидентов;
- классификация и приоритезация инцидентов - идентификация причин инцидента и соответствующих действий для его решения, и определение критичности инцидента для деятельности компании;
- эскалация инцидентов – осуществляется помощь в своевременном разрешении инцидента;
- обработка инцидентов – разрешение инцидента и восстановление ИТ-услуг;
- мониторинг инцидентов – осуществляется контроль качества обработки и разрешения инцидентов с целью выявления несоответствий и подготовки рекомендацией по управлению инцидентами;
- закрытие инцидентов.

Этапы менеджмента инцидентов могут меняться каждой органи-

зацией в зависимости от ее внутренних потребностей ведения бизнеса. Рекомендуется руководствоваться требованиями по управлению инцидентами, прописанными во многих международных стандартах и практиках, среди которых можно отметить следующие:

- ISO 17799 Информационная технология - методики Безопасности - Практическое руководство для информационного управления безопасности;
- ISO 18044-2007 Информационная технология – Методы и средства обеспечения безопасности – Менеджмент инцидентов информационной безопасности;
- лучшие практики IT Infrastructure Library (Библиотека передового опыта организации ИТ).

Применение данных стандартов и практик позволит сократить возможные последствия и снизить риски, возникающие при реализации инцидентов, что еще раз доказывает важность вопросов менеджмента инцидентов в рамках управления ИТ функциями. Это обеспечивает необходимость принятия эффективных мер по сокращению появляющихся инцидентов. Эффективность управления инцидентами должна выражаться в измеряющихся и оценивающихся показателях. Такими показателями, например, могут выступать:

- тенденции в изменении общего количества инцидентов;
- среднее фактическое время, затраченное на разрешение инцидента;
- процент инцидентов, обработанных в рамках согласованного времени реакции;
- средние затраты на решение инцидента;
- процент инцидентов, закрытых без обращения к специализированным группам поддержки;
- количество и процент инцидентов, разрешенных удаленно.

Таким образом, эффективный менеджмент инцидентов позволит обеспечить быстрое восстановление нормального функционирования информационных систем, минимизировать неблагоприятное воздействие на бизнес, снизить финансовые потери, а также поддерживать процессы управления рисками.

Литература и интернет источники:

1. IT Infrastructure Library (Библиотека передового опыта организации ИТ);
2. www.iso27000.ru;
3. www.itsec.ru;
4. www.connect.ru.

МЕНЕДЖМЕНТ ИНФОРМАЦИОННЫХ РИСКОВ С ИСПОЛЬЗОВАНИЕМ АВС-АНАЛИЗА

Юрий Копытин
Одесская национальная академия связи им. А.С. Попова (Украина)

Проблем утраты таких важных свойств информации, как конфиденциальность, целостность и доступность, избежать невозможно. Однако ими можно управлять путем менеджмента рисков - полного процесса идентификации, контроля, устранения или уменьшения последствий опасных событий, которые могут оказать влияние на ресурсы информационно-телекоммуникационных технологий [1]. Для осуществления менеджмента информационными рисками используют специально разработанные стандарты, методики и рекомендации. Наиболее известные: ISO/IEC 17799 (BS7799), ISO/IEC 27001, ISO/IEC TR 13335-3, BSI, NIST 800-30, MITRE и др..

Цель доклада – продемонстрировать целесообразность использования АВС-анализа в вопросах выбора защитных мер при проведении менеджмента информационными рисками.

Процесс менеджмента информационным риском состоит из следующих основных этапов: 1) идентификации активов; 2) оценки активов и установления зависимостей между активами; 3) оценки угроз и уязвимостей; 4) идентификации существующих/планируемых мер безопасности; 5) оценки рисков; 6) выбора защитных мер; 7) оценки остаточных рисков.

На первом этапе производится идентификация активов информационной системы. К ИТ активам относятся: информация/данные, аппаратные средства, программное обеспечение и т.д. Полный перечень активов в [2].

На втором этапе определяется ценность идентифицированных активов (выраженная в деньгах), а также устанавливаются зависимости одних активов от других, поскольку наличие таких зависимостей может оказать влияние на оценку активов.

На третьем этапе производится идентификация угроз и уязвимостей, вызывающих эти угрозы, характерных данной информационной системе. Для описания угроз и уязвимостей используют классификации угроз и уязвимостей (OCTAVE (США), BSI (Германия), DSECCT (Россия), ISO/IEC TR 13335-3 и др.).

На четвертом этапе создается перечень действующих и планируемых мер безопасности с указанием статуса их реализации и использования.

На пятом этапе определяется величина риска каждого информационного актива. Величина риска

может быть представлена в качественных, количественных, одномерных и многомерных терминах [3]. Результаты анализа величины рисков могут быть использованы при оценке остаточного риска, выборе мер по предотвращению или устранению рисков, оценке затрат на обеспечение поддержания безопасного состояния.

На шестом этапе производится выбор защитных механизмов. Автором доклада предлагается методика определения уровня опасности угроз с использованием АВС-анализа для выбора эффективных защитных механизмов.

Метод «АВС-анализа» можно применять практически в любых областях деятельности с целью выявления первоочередных проблем, которые необходимо устранить, определив их приоритетность.

Согласно [4] АВС-анализ представляет собой следующую последовательность действий: 1) определение цели анализа; 2) определение объектов анализа; 3) определение факторов для дифференциации объектов анализа; 4) формирование информационного массива для анализа; 5) оценка объектов анализа по выделенным факторам; 6) ранжирование показателей; 7) разделение объектов на группы; 8) интерпретация результатов анализа.

Целью АВС-анализа является определение уровня опасности угроз информационной системе для дальнейшего выбора эффективных защитных механизмов.

Объектами анализа выступают активы информационной системы, идентифицированные на первом этапе.

В качестве анализируемого фактора выступает выведенный коэффициент опасности угрозы K_{on}, вычисляемый по формуле:

$$\boldsymbol{K}_{on} = \frac{\sum_{i=1}^{N} \boldsymbol{Y}_i}{\boldsymbol{N} * 10} \qquad (1)$$

где: $\boldsymbol{Y}_i$ - значения базовых показателей от 1 до 10, $\boldsymbol{N}$ - количество базовых показателей.

К базовым показателям относятся: возможность предотвращения угрозы, возможность обнаружение угрозы, частота появления, потенциальная опасность, простота реализации, потенциальное наказание в рамках существующего законодательства, степень защищенности от угрозы и т.п. Количество показателей выбирается в зависимости от степени детализации.

Информационный массив для анализа создается на основе присвоения идентифицированным на третьем этапе угрозам и уязвимостям числовых значений базовых показателей.

В дальнейшем производится: оценка вклада каждого объекта по выбранному фактору; ранжирование объектов в порядке уменьшения анализируемого фактора; вычисление нарастающего общего вклада объекта к общему количеству объ-

ектов в процентах и вклада объекта в общий результат в процентах.

Разделение полученных результатов осуществляется на три группы (A,B,C) при помощи одного из методов. Например: эмпирического метода, метода сумм, метода петли. Группу А составляют очень опасные угрозы; группу В - опасные угрозы; группу С -неопасные. При этом под: неопасными угрозами понимаются те, которые легко предотвращаются или обнаруживаются, нейтрализуются и устраняются; опасными - те, для которых процессы предотвращения, обнаружения и нейтрализации, с точки зрения технологии, не отработаны; очень опасными - те, которые обладают максимальными оценками по всем показателям и реализация процессов противостояния сопряжена с огромными затратами [5].

Суть проведенного АВС-анализа сводится к тому, что максимальный эффект при выборе защитных механизмов достигается при первоочередном закрытии угроз, относящихся к группе А.

На седьмом проводится измерение остаточных рисков, которые всегда имеют место, поскольку система не может быть абсолютно безопасной. Эти риски оцениваются организацией как приемлемые или неприемлемые.

В заключение отметим, что использование АВС – анализа на этапе выбора защитных мер безопасности предоставляет возможность: значительно повысить качество менеджмента информационных рисков; выбрать оптимальные меры безопасности, которые обеспечивают защиту от опасных угроз для конкретного объекта; осуществить легко, быстро и удобно адаптацию систем защиты к изменяющимся условиям.

Литература:

1. ISO/IEC 13335-1:2004 “Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management (IDT)”.
2. ISO/IEC TR 13335-3:1998 “Information technology - Guidelines for the management of information technology security - Part 3: Techniques for the management of information technology security”.
3. *В.В. Домарев*. Безопасность информационных технологий. Системный подход. - ТИД «ДС», 2004. - 992 с.
4. *Фишер Андрей*. Методы выделения групп в АВС анализе [Електронний ресурс]: - Режим доступа: http://www.transmap.ru/articles/view/169
5. *Черней Г.А.* Оценка угроз безопасности автоматизированным информационным системам [Електронний ресурс]: - Режим доступа: http://security.ase.md/publ/ru/pubru01.html

АЛГОРИТМ РАЗГРАНИЧЕНИЯ ДОСТУПА ПО РАДУЖНОЙ ОБОЛОЧКЕ ГЛАЗА ДЛЯ РЕШЕНИЯ ЗАДАЧ КОНТРОЛЯ ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ

Иван Третьяков, Наталья Минакова
Алтайский государственный университет
(Российская Федерация)

The algorithm of differentiation of access on an eye iris of the eye is described. For identification matrix calculations are used. Advantages of consideration of a neural network as a mathematical matrix are shown

В современных условиях обеспечение безопасности информационных ресурсов представляет собой чрезвычайно актуальную задачу. Формирование политики безопасности информационных систем требует продуманности, сбалансированности защиты, разработки эффективных организационно-технических мер и обеспечении контроля над их исполнением. Одно из направлений формирования политики безопасности информационных систем - разработка простой и эффективной процедуры ограничения и контроля доступа к информационным ресурсам.

Для управления и реализации политики безопасности широко применяется парольная система идентификации. Широкая апробация парольной идентификации выявила ряд недостатков: пароли используются третьими лицами для несанкционированного доступа, восстановление пароля во многих случаях затруднено невозможностью дистанционной идентификации и аутентификации человека, обращающегося к службе поддержки, требуются дополнительные затраты времени для ввода идентификатора пользователя, дополнительная нагрузка возлагается пользователей, администраторов, сотрудников службы безопасности и т.д.

В связи с возросшими требованиями к информационной безопасности получают широкое распространение методы биометрической верификации и идентификации человека. Их использование облегчает деятельность специалистов по защите информации, одновременно обеспечивая существенный рост уровня информационной безопасности. При использовании биометрии проверка подлинности производится по уникальным признакам пользователей: отпечатки пальцев, форма лица, сетчатка и радужная оболочка глаза и т.д.

В представленной работе биометрическим признаком выбрана радужная оболочка глаза. По мнению специалистов в области биометрических систем, средства идентификации человека по радужной оболочке глаза способны заменить ключи и персональные идентификационные номера. В отличие от других биометрических систем контроля доступа идентификация по рисунку радужки допускает полностью бесконтактную реализацию. Данная область широко изучается, разработаны различные системы идентификации человека, такие как: метод основанный на вейвлет-преобразованиях, методы Нох, преобразования Эрмита, система Даугмана и т.д. [1]. Их анализ показал, что обычно привлекается сложный математический аппарат, как при составлении кода, так и при процессе идентификации. Это затрудняет реализацию и требует значительных вычислительных затрат.

Была поставлена задача разработки простого и эффективного алгоритма идентификации человека по радужной оболочке глаза. Для решения задачи распознавания радужной оболочки глаза выбраны искусственные нейронные сети.

Как известно, качество распознавания зависит от того, как будет использоваться нейронная сеть. Для идентификации было решено использовать обычные матричные вычисления. В основу алгоритма положен следующий подход. Пусть имеется некоторое множество B. Каждый элемент множества имеет некоторый признак t. Множество всех значений признака t обозначим как T. Признак является идентифицирующим, если $\forall \in t \in T \ \exists! \ b \in B$.

Известны два метода идентификации элементов по признаку t [2]:

1. Создать одну нейронную сеть, при этом для каждого элемента из A создаётся отдельный выход.
2. Для каждого элемента $b \in B$ создаётся нейронная сеть с одним выходом.

В обоих случаях на вход нейронной сети подаются данные параметра, а на выходе значение вероятности, с которой данный параметр соответствует элементу $b \in B$.

Предварительные численные эксперименты показали, что первая схема менее предпочтительна поскольку:

1. Добавление новых элементов во множество потребует переобучения нейронной сети и изменения её структуры.
2. Сеть должна содержать довольно большое число нейронов, чтобы сохранить в себе информацию об элементах множества B.
3. Сложности с распараллеливанием вычислений.

Для упрощения расчетов перед передачей данных нейронным сетям на подтверждение необходимо:

1. Выделить ключевые части данных.

2. Максимально уменьшить множество элементов, для которых будет проводиться проверка с помощью нейронной сети.

Значения входных данных предварительно нормировались в интервале (-1, 1). На выходе нейронной сети значение изменяется в диапазоне (-1, 1).

Рассмотрение нейронной сети в качестве математической матрицы дает возможность оперировать векторами и матрицами: элементы матрицы – синапсы, слой – вектор (часть вектора-результата). Подобная реализация позволяет легко задать связь между синапсами между слоями (задаются коэффициенты хранимой для каждого пользователя матрицы).

Алгоритм создания вектора входных значений формируется из нулевого слоя, далее добавляется выход с первого слоя (с предыдущего подсчёта) и т.д. (добавляется выход с n-ого слоя). Особенностью данного вычисления является следующее: пока не будут вычислены новые значения для всего слоя (на каждом этапе), значения не переносятся во входной вектор. На каждом этапе умножения на новый слой, полученное значение передаётся пороговой функции, результат передаётся в вектор-результат. Полученный после всех пересчётов вектор – умножается на матрицу с синапсами. Результат первого этапа обучения - выходной вектор из ячеек.

Матрица формируется для каждого зарегистрированного пользователя, Однако её хранение заняло бы большой объём данных. Анализ результатов вычислений позволил сделать следующий вывод: коэффициенты, лежащие ниже дополнительной диагонали, не имеют определяющего значения, так как их использование не влияет на результат вычислений. Это связано с тем, что перемножаемый вектор хранит в себе результаты текущих вычислений. Дополнительно считаем, что в модели отсутствует обратная рекурсивность, поэтому коэффициенты выше вспомогательной диагонали не информативны, если исходить из предположения что синапсы связываются только с элементами из соседнего слоя и не связываются со следующими, минуя рядом стоящий слой. Тем самым число хранимых элементов резко уменьшается.

Конечная матрица представляет собой код идентификации. На первоначальном этапе проводится обучение сети. В дальнейшем нейронная сеть будет обучаться сама. Входные данные $(x_1, ..., x_q)$ сравниваются с имеющейся выборкой, высчитывается вероятность совпадения полученных коэффициентов с имеющимися эталонными коэффициентами.

Таким образом, представленный алгоритм реализации нейронной сети из-за указанных выше особенностей позволяет упростить расчеты, соответственно, дает возможность ускорения доступа легальных пользователей к ресурсам информационной системы.

Библиографический список

1. Дегтярева, А. Методы идентификация личности по радужной оболочке глаза / А. Дегтярева, В. Вежневец // Компьютерная графика и мультимедиа. – [Электронный ресурс] – электрон. дан. – Вып. № 2 (6). – 2004. – Режим доступа: http://www.cgm.computergraphics.ru/content/view/61.
2. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. Монография. — Пенза: Изд-во Пензенского государственного ун-та, 2000. – 188 с.

PROBLEMS OF INFORMATION SECURITY

Kostadinka Cabuleva, *MSc*
Faculty of Economics, "Goce Delcev" University - Stip
(Republic of Macedonia)

We know that information security have economic impact on organizations. Collection, aggregation and access to information in today's organizations is based on innovation, which in turn create conditions for a positive feedback cycle of development. Speed and accuracy in the flow of information processes determine the rate of development and degree of certainty. Information security has as its sole purpose to protect the information resources of the organization, without being in conflict with the safety of staff, norms and generally accepted moral principles.

Information risk and the economics of managing security is a concern of private-sector executives, public policy makers, and citizens.[1] Information is an asset that, like other important business assets, adds value to the business of the company (organization) and therefore should be protected. Information security protects information from a number of threats in order to ensure continuity, to minimize damage to the company (organization) and to maximize return on investment and business opportunities.

Today, the reliability of information systems and services makes companies and organizations more vulnerable to security threats. The reasons are many but the basis is the very nature of cybercrime-they are more hidden and more complex, making their detection difficult. The company management should en-

[1] M. Eric Johnson "*Managing Information Risk and the Economics of Security*", Center for Digital Strategies Tuck School of Business at Dartmouth Hanover, NH, USA, 2008.

gage in the process of evaluation of resources for safeguards. Even in cases where the level of information security is clearly insufficient technical specialists have trouble justifying to senior management of the necessary funding. If the information is valuable in practice there is no threat to information assets of the company's potential losses are minimal (manual confirms it) and you can forget about security systems. However, if the information has a particular value, threats and potential losses are clear, then the budget (with the absolute conviction of this manual) should include funds for the security subsystem. Information security is ensured by a set of measures at each stage of the life cycle of information system, the value of specialized subsystem in the general form of the cost of design work, purchase and setup of software and technical resources, incl. internetwork screens, cryptographic tools, antivirus systems, means of authentication, authorization and administration costs to physical safety, staff training, management, maintenance and periodically update the system. It is interesting that the main causes of damage, especially in the financial sector are employees in the company followed by former employees, while the damages from outsiders are contributing much less. The types of attacks can be summarized in: stealing passwords - methods to obtain other user passwords; social engineering - the acquisition of information to which they have access; errors and black door (bugs and backdoors) - destination (use) of benefits through the use of systematic errors; opportunities for authentication - the use of defects (inconsistency and incompleteness) of the authentication mechanisms; errors (failures) in some protocols - protocols with errors in design and implementation; leaks - use of systems such as system signature (finger) or a named system (DNS) information needed by administrator or necessary for the functioning of the network, but which can be used for network attacks; denial of service - attempts to deprive consumers of the services of their computer system.

Also fraud by phone, online or by mail continue to grow and is on the rise. Such types of fraud where the true owner of the card is not present when the transaction shows an increase of 5 percent annually. Banks have reduced losses by two thirds of investment in new technology and upgrading systems for information security. Thus, the efforts of banks to fight criminals and frauds with credit cards and bank accounts are successful and show excellent results. In America banks cooperate with police, with special sections on financial fraud, but also invest in software and identification of fake websites that timely prevent abuse of the bank accounts of us-

ers (various benefits of lottery, offering online job offering rate for transferring money to your account various types of heritage). However, most studies show that 40 percent of banks do not report incidents to protect their reputation and trying internally to cope with problems.

In the modern market economy each firm is forced to work in conditions of fierce competition. When possible use by competitors of confidential information obtained in ways not entirely legitimate. This leads to obvious violations of rights of owner of industrial or intellectual property rights. Subject of harm may be know-how, trade and financial secretions, interference in the privacy of the citizen and the others. Security policy is the set of rules and practices that govern how an organization manages, protects and distributes information.

The problem of information security is the world's number one priority, and its solution should lead to maximum security for network resources with minimal impact on user access and productivity. Consequences of breaches of information security: loss of revenue; reducing investor confidence; reduce the confidence of customers; disclaimer consequences; deterioration of goodwill; loss or compromise of data; violation of business processes.

Price decisions against major security issues: - limiting functionality for improved security; -compromising the ease of use of the Internet; - need for investment of considerable human and financial resources.

References

1. Bogetoft, P., Damgaard, I., Jacobsen, T., Nielsen, K., Pagter, J. and Toft, T. "Secure Computing, Economy, and Trust - a Generic Solution for Secure Auctions with Real-World Applications," Report RS-05-18, Basic Research in Computer Science. 2005.
2. L. Jean Camp and Stephen Lewis "Economics of Information Security (Advances in Information Security)" Kluwer Academic Publishers, 2008
3. M. Eric Johnson, "Managing Information Risk and the Economics of Security" Springer, 2008
4. Mark Stamp, "Information Security – Principles and Practice", John Wiley & Sons, Inc., New Jersey, 2006;

КОНЦЕПЦИЯ РАЗРАБОТКИ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА СОТРУДНИКА СЛУЖБЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Евдокимов Д. А., Файзуллин Р. Т.,
ГОУ ВПО Омский государственный университет им. Ф. М. Достоевского (Российская Федерация)

В настоящей работе представляется концепция автоматизированного рабочего места (АРМ) сотрудника службы информационной безопасности (ИБ) предприятия. Для выполнения своих функциональных обязанностей сотрудник службы ИБ должен обладать широкими знаниями в области международных и отечественных стандартов в области ИБ для построения эффективной системы информационной безопасности. Сотрудник должен постоянно поддерживать систему ИБ на должном уровне, чтобы она отвечала актуальным угрозам безопасности, для этого необходимо регулярно проводить аудит системы ИБ с целью ее оценки и минимизации рисков.

Применение автоматизированных систем при проведении аудита ИБ способствует улучшению качества исследования, уменьшает влияние человеческого фактора, позволяет специалисту использовать более широкий арсенал критериев оценки ИБ. Модель проведения оценки защищенности объект информатизации (ОИ) предприятия при помощи автоматизированного рабочего места (АРМ) основана на формировании опросов для специалистов по информационной безопасности, производящих аудит. Процесс заполнения опроса основан на информации, которая не всегда может быть точной, например, в случае самооценки. Учитывая возможные неточности в исходной информации, в представляемой концепции для обработки результатов аудита применяется модель оценки, основанная на теории нечетких множеств (ТНМ).

Одной из задач разработки АРМа является разработка опросной анкеты по определенным критериям и стандартам информационной безопасности, а это влечет необходимость проведения исследования по актуальным, для специфики исследуемой

информационной системы, требованиям в данной области. Предлагаемая концепция предусматривает наделение АРМа свойством масштабируемости, которое достигается путем применения метода лексического анализа текстовых документов с целью получения опросной анкеты, которая изначально не закладывается в код программы на этапе разработки.

На рисунке 1 представлена концептуальная схема алгоритма работы программы на этапе формирования анкеты и проведения классификации.

Лексический анализ - процесс аналитического разбора входной последовательности символов с целью получения на выходе последовательности символов, называемых «токенами». При этом, в процессе лексического анализа производится распознавание и выделение лексем из входной последовательности символов [1].

Традиционно принято организовывать процесс лексического анализа, рассматривая входную последовательность символов, как поток символов. При такой организации, процесс самостоятельно управляет выборкой отдельных символов из входного потока[2]. Входной поток формируется из библиотеки документов, содержащих методики и критерии оценки информационной безопасности предприятия. При добавлении документа в библиотеку ему присваивается метка ***T***, определяющая его принадлежность к тому или иному разделу исследования, если ранее существовал данный раздел, иначе создается новый раздел. В качестве метки ***T*** принадлежности к определенному критерию ***K*** используется заголовок документа, в котором прописывается номер ***K***-го критерия из списка.

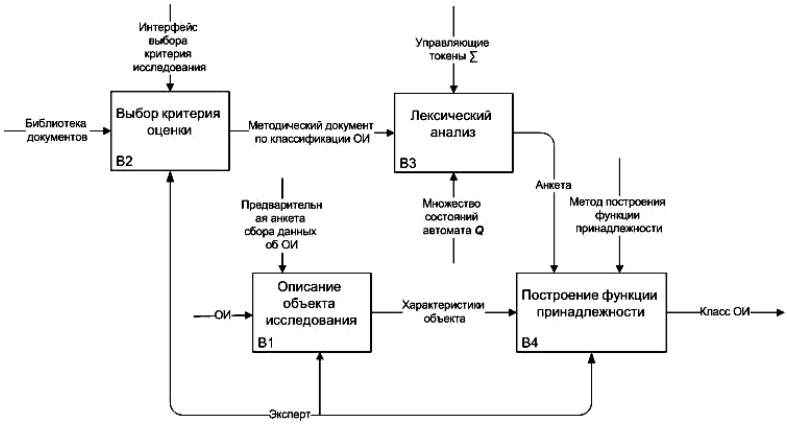


Рисунок 1 **- Алгоритм формирования опросных анкет проведения оценки защищенности ОИ предприятия.**

Для достижения масштабируемости АРМ по использованию критериев оценки, применяется метод лексического анализа библиотеки документов. Выбор критерия исследования $\boldsymbol{K_i}$ пользователем программы определяет перечень документов таких, что $\boldsymbol{T_j = K_i}$. Для любого исследования будет два и более документов. Лексический анализ первого документа формирует опросную анкету для определения класса в рамках выбранного критерия, второго - анкету оценки выполнения требований. Структура анкеты и содержание формируется в результате распознавания лексем конечным автоматом

$$\boldsymbol{M = (Q, \Sigma, \delta, q_0, F),} \qquad (1)$$

где Q - конечное множество состояний автомата; q_0 - начальное состояние автомата $q_0 \in Q$; F - множество заключительных (или допускающих) состояний, таких что $F \subset \sum Q$; $\sum$ — допустимый входной алфавит (конечное множество допустимых входных символов), из которого формируются строки, считываемые автоматом; δ — заданное отображение множества $Q \times \sum$ во множество $P(Q)$ подмножеств Q:

$$\boldsymbol{\delta : Q \times \sum \rightarrow P(Q)} \qquad (2)$$

На выходе алгоритма автомат выдает анкету для классификации либо оценки ОИ в зависимости от выбранного входного документа. Анкета формируется отображением δ множества $Q \times \Sigma$ во множество $P(Q)$ подмножеств Q.

Следующие этапы исследования – классификация и/или оценка исследуемой системы по выбранной методике с применением математического аппарата ТНМ. Пользователь АРМ проводящий оценку защищенности ОИ определяет метод оценки, на выбор предлагается два метода ТНМ: на основе балльной шкалы и на основе лингвистической шкалы[3].

Литература

1. Джон Хопкрофт, Раджив Мотвани, Джеффри Ульман Введение в теорию автоматов, языков и вычислений = Introduction to Automata Theory, Languages, and Computation. — М.: «Вильямс», 2002. — С. 528.
2. Касьянов В.Н. Лекции по теории формальных языков, автоматов и сложности вычислений. - Новосибирск: НГУ, 1995. - С. 112.
3. Батыршин И.З., Недосекин А.О., Стецко А.А., Тарасов В.Б., Язенин А.В., Ярушкина Н.Г. Теория и практика нечетких гибридных систем. Под ред. Н.Г. Ярушкиной. М.: Физматлит, 2007.

SECURITY, PROTECTION AND PRIVACY OF INFORMATION IN HEALTHCARE

Radmila Jovanova,
Faculty of Economics, "Goce Delcev" University - Stip,
(Republic of Macedonia)

The development of information technologies which are based on the production and application of electronic systems for data processing, telecommunications equipment and other suitable equipment opens the opportunity for unlimited data concentration, their grouping and search based on various characteristics. This causes a massive use of data for individuals in different organizations, registries, etc. Patients and the public must be confident that their information is kept by all security measures and are exchanging under the law, legal, ethical and technological processes.

Before we start to talk about privacy and protection of health information, we must define what exactly personal data is, because the health information is some kind of their subcategory.

1. Personal data is any information relating to the identified person or individuals who can be identified.[1] Of special importance are name, surname, ID number, phone number, sexual orientation etc;

2. Health information can be defined quite broadly as information that is created or received in any form or medium by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse, and that "relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for health services provided to an individual".[2] For example, diagnosis, blood test results, blood group, medical treatment etc.

Almost every time we go to the doctor, we are sharing our personal data and information about our health. All of them in some way can be abused and can be threat for patient's privacy. The main question here is who can accede to this information? First of all, it is the whole medical personnel that the patient comes in contact with, when he is going to doctor. People, who carry out their practice in healthcare organizations, also have access to these data. If they don't know to keep the professional secrets, there could be a possibil-

[1] http://www.dzlp.mk/files/uploads/global/ZZLP_Precisten%20tekst.pdf, 17.02.2010

[2] William H. Roach, Medical records and the law, Jones & Bartlett Publishers; 4 edition , USA, April 24, 2006, page 125

ity to be undermined patient's privacy, reputation and honor. Privacy of health information can be defined as a professional obligation of doctors, nurse, non-medical researchers and other public health professionals. Privacy is right of any individual or institution to decide when and to what extent will share information about themselves and others. In any system of data protection must not neglect the human factor. It is important to know that non - medical employees must be motivated to adhere to the same principles of professional confidentiality which are required for healthcare employees.

Security of information is a result of various measures which contribute for information protection from unwanted things, such as modifications, deleting or loosening personnel and other data which are defining the patient. From one side, security is related to protection of the integrity of data, and from the other side, on serving privacy on the patient and the doctor.

For how long the information should be kept? [3]

1. Personal data should not be kept longer than necessary to fulfill the purposes for which are collected;

2. In healthcare organizations, basic medical documentation is kept for 15 years from the last data entry;

3. Medical history of the disease is kept 15 years after the death of the patient.

Information security deals with the protection of information within a given domain. In this context it is usually expanded into tree different directions:[4]

- Confidentiality - assurance that particular information is accessible (read, write or execute) by authorized personal only
- Integrity - assurance that during processing no unauthorized changes of information are possible.
- Availability - assurance that information can be used at will.

Issues which are related on the organizational measures and rules for data protection include:

1. Format and authority of a special organization which are entrusted to implement the law and the other measures for data protection.
2. Technical standards for handling with the computer center and using of programming techniques in the operating systems.
3. Taking precautions relating to computer equipment.
4. Training of the persons who will processing the data and more.

[3] http://dzlp.mk/FILES/1164/PUBLIC/CONTENT/4282378027296612126011011481_ FILES/Preporaki% 20za%20graganite% 20zdravstvo.pdf, 17.02.2010

[4] http://books.google.com/books?id=Z6azHX3wJKUC&pg=PA50&dq=security+of+health+information&cd=1#v=onepage&q=security%20of%20health%20information&f=false,17.02.2010

Today, many countries in the world that have laws which are regulating the issues of data protection, namely the right to privacy. Hence, the problem of privacy is the subject of many resolutions, guidelines, directives, recommendations are adopted by the Council of Europe, Economic and Social Council, the UN office in Geneva, the European Parliament and Council of the European Union. In these documents are determined the basic goals and principles of data protection of the individuals, criterions related to quality and legitimacy of data processing for individuals, especial categories of data, exceptions and limitations to these rights and other similar issues. International organizations especially World Health Organization (WHO) and Organization for Economic Co-operation and Development (OECD) have long time experience in accumulation, distribution and using data health to inform public health and to understand the whole public health systems.

As a conclusion of all this, we can say that all public health organization should have an integrated electronic system who will restrict the information access to the patient's personal information. For example, the guard cannot access into clinical information, and the medical personnel cannot access into the data for invoices.

References

1. Adi Armnoni, *Healthcare information system: Challenges for the new millennium,* Idea group publishing, USA, 2000;
2. Computer science and telecommunications board national research council, *For the Record : Protecting Electronic Health Information*, National Academies Press, USA, 1997
3. William H. Roach, *Medical records and the law*, Jones & Bartlett Publishers, 4 edition , USA, April 24, 2006;

Web sources

1. http://dzlp.mk/FILES/1164/PUBLIC/CONTENT/428237802729661212626011011481_FILES/Preporaki%20za%20graganite%20zdravstvo.pdf;
2. http://www.dzlp.mk/files/uploads/global/ZZLP_Precisten%20tekst.pdf;
3. http://books.google.com/books?id=Z6azHX3wJKUC&pg=PA50&dq=security+of+health+information&cd=1#v=onepage&q=security%20of%20health%20information&f=false;
4. http://www.scribd.com/doc/12391658/Security-in-health-information-systems;
5. http://www.scribd.com/doc/18429810/Dictionary-of-Health-Information-Technology-and-Security;
6. http://www.himss.org/content/files/PrivacySecurity/PIIWhitePaper.pdf.

ОЦЕНКА И УПРАВЛЕНИЕ РИСКАМИ ВНЕДРЕНИЯ КИС НА ПРЕДПРИЯТИЯХ

Екатерина Авдеева
Владимирский государственный университет (Российская Федерация)

In this article features of enterprise information systems introduction at the enterprises were observed. The basic risk evaluation methods were researched, the procedure of risk expert evaluation method during the introduction of enterprise information systems was submitted and the analysis of expert evaluations co-ordination was considered. The methods of critical project risks determination were researched.

Корпоративные информационные системы представляют собой весьма эффективный инструмент управления предприятием, который позволяет не только оптимизировать процесс принятия решений и оперативно получать достоверную и целостную информацию в режиме реального времени, но и снижает затраты за счет увеличения гибкости и позволяет адаптироваться к изменениям бизнеса. Предприятие, внедряющее КИС, действительно может добиться значительных результатов и получить стратегические преимущества, но только в случае успешного внедрения системы, которое является дорогостоящим и трудоемким процессом.

Успех внедрения КИС на предприятии зависит от многих факторов: тщательного планирования и грамотного выполнения проекта внедрения, готовности предприятия к изменениям, участия и заинтересованности руководства в проекте, обучения команды внедрения, участия внешних консультантов и т.д. Несоблюдение этих факторов часто приводит к тому, что проект завершается неудачей. Кроме того, поскольку внедрение КИС влечет за собой значительные изменения в деятельности компании, то оно всегда сопровождается различными трудностями и рискам, которые необходимо заранее определять, оценивать и которыми нужно управлять. Поэтому не маловажным при внедрении КИС на предприятии является грамотное управление рисками проекта, результат которого в значительной степени влияет на реализацию проекта внедрения и определяет его успех.

Основными показателями проекта внедрения КИС, с помощью которых можно оценить его успех или неудачу, являются бюджет, сроки и качество. Главная задача руководителя проекта внедрения – уложиться в выделенный бюджет и заданные сроки и обеспечить требуемое качество имеющимися ресурсами. Сбалан-

сировать эти показатели всегда довольно трудно: нельзя добиться желаемого качества за сжатые сроки и при ограниченном бюджете, но увеличение сроков проекта неизбежно влечет превышение бюджета. Поэтому общими рисками, характерными для любого проекта внедрения КИС, являются риск низкого качества результатов проекта; риск превышения сроков проекта; риск увеличения бюджета проекта. В самом худшем случае возникает риск остановки проекта, когда кардинальным образом изменяются условия и масштабы проекта.

Кроме общих рисков, можно выделить частные риски, характерные для конкретного проекта внедрения и которые также влияют на бюджет, сроки и качество проекта. К частным рискам можно отнести такие наиболее часто встречающиеся риски, как риск перехода на новую систему (или риск непринятия системы пользователями), риск, связанный с поддержкой руководства (незаинтересованность или неучастие в проекте высшего руководства предприятия), а также риск несоответствия поставленным целям проекта.

Каждый из частных рисков имеет соответствующие ему факторы или причины возникновения. Так, например, основными факторами риска перехода на новую систему являются слабое участие операционного персонала (либо он вообще не участвует в проекте); отсутствие или слабая информированность сотрудников предприятия; недостаточное обучение персонала или оно вообще не проводится, а также низкая мотивация.

Поскольку конкретной методики оценки рисков, возникающих при внедрении корпоративных информационных систем, которую предприятие могло бы использовать самостоятельно, не существует (имеются частные методики оценки рисков, разработанные отдельными консалтинговыми компаниями), было проведено исследование основных методов оценки проектных рисков: вероятностного анализа, экспертных оценок, метода аналогов, анализа чувствительности, анализа сценариев развития проекта, метода построения дерева решений проекта и имитационного моделирования с помощью метода Монте-Карло.

Анализ перечисленных методов оценки рисков позволяет сделать вывод, что вероятностный анализ, метод аналогов и имитационное моделирование трудно использовать для оценки рисков при внедрении КИС потому, что для применения этих методов необходимы статистические данные, которые отсутствуют, так как при внедрении КИС на предприятиях используется информация, актуальная на момент внедрения.

Учитывая достоинства и недостатки остальных методов оценки, наиболее предпочтительным методом оценки рисков, возникающих

при внедрении КИС на предприятиях, являются экспертные оценки, так как они позволяют получить быструю и комплексную оценку рисков даже при недостаточном объеме исходной информации о проекте.

Порядок проведения экспертной оценки рисков, возникающих при внедрении КИС на предприятиях, состоит в следующем: сначала каждый эксперт оценивает факторы риска по вероятности их наступления и опасности. Далее на основе средних оценок факторов риска определяется величина каждого риска, а также вычисляется общий риск проекта внедрения. В результате на основе полученной общей оценки риска проекта можно определить, как изменяться основные показатели проекта внедрения, т.е. определить влияние величины риска на бюджет, сроки и качество проекта.

При проведении экспертных оценок особое внимание следует уделять анализу согласованности оценок факторов риска, так как экспертные оценки носят субъективный характер и могут сильно отличаться друг от друга. Основными показателями, с помощью которых можно проанализировать согласованность экспертных оценок, являются коэффициент ранговой корреляции Спирмена и коэффициент конкордации Кендалла. Общей особенностью этих коэффициентов является то, что перед их вычислением необходимо проранжировать полученные от экспертов оценки факторов риска. Разница между коэффициентами заключается в следующем: коэффициент ранговой корреляции Спирмена используется для анализа согласованности оценок, полученных от двух экспертов. Когда экспертов несколько используется коэффициент конкордации Кендалла.

Еще одной задачей при управлении рисками является определение критических рисков проекта, т.е. таких рисков, которые в большей степени влияют на выполнение проекта, его цели и результаты. Сравнительный анализ таких методов определения критических рисков проекта, как ранжирование, метод непосредственной оценки, метод последовательных сравнений и метод парных сравнений, позволяет сделать вывод, что наиболее предпочтительным методом является метод парных сравнений, в котором эксперты для определения критического риска проекта сравнивают риски попарно, что позволяет получить более точный и надежный результат.

Оценка проектных рисков является важным этапом в процессе управления рисками. Различные методы оценки позволяют определить наиболее критические и значимые риски проекта и выявить степень их влияния на развитие проекта. На основе оценки рисков можно определить слабые места проекта и выбрать наиболее подходящую

стратегию его развития, которая позволит минимизировать потери и достичь поставленных целей.

Своевременное управление рисками, которые возникают при внедрении корпоративных информационных систем на предприятиях и негативно влияют на реализацию проекта внедрения, позволит устранить недостатки проекта, тем самым повысить его эффективность и результаты.

МЕТОДЫ РАСЧЕТА ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

***Солоненко Олег**, Молдавская Экономическая Академия (Республика Молдова)*

In this work were present methods for calculating cost-effectiveness of information security system.

Введение. Сегодня не вызывает сомнений необходимость вложений в обеспечение информационной безопасности современного бизнеса. Основной вопрос современного бизнеса - как оценить необходимый уровень вложений в ИБ для обеспечения максимальной эффективности инвестиций в данную сферу. Для решения этого вопроса существует только один способ – применять системы анализа рисков, позволяющие оценить существующие в системе риски и выбрать оптимальный по эффективности вариант защиты. Для расчета можно выбрать одну из перечисленных в [1] методик.

Расчет затрат на информационнцю безопасность

Для количественной оценки предварительно необходимо рассчитать затраты на:

- приобретение и ввод в эксплуатацию программно-технических средств: серверов, компьютеров конечных пользователей, периферийных устройств и сетевых компонентов.
- приобретение, настройку, плановые и внеплановые проверки и испытания средств защиты информации;
- содержание персонала, стоимость работ и аутсорсинг;
- формирование политики безопасности предприятия и контроль за ее соблюдением;
- проверку навыков эксплуатации средств защиты персоналом предприятия;
- выявление причин нарушения политики безопасности, организационные и прочие расхо-

ды, которые непосредственно связаны с предупредительными мероприятиями;
- осуществление технической поддержки производственного персонала при внедрении средств защиты и процедур, а также планов по защите информации;
- проверку сотрудников на лояльность, выявление угроз безопасности;
- ликвидацию последствий нарушения режима информационной безопасности;
- организацию взаимодействия и координации между подразделениями для решения конкретных повседневных задач;
- проведение внутреннего и внешенго аудита безопасности
- идентификацию угроз безопасности,уязвимостей и оценке степени риска
- восстановление системы безопасности до соответствия требованиям политики безопасности;
- установка патчей или приобретение последних версий программных средств защиты инфомрации;
- восстановление баз данных и прочих информационных массивов;
- проведение расследований нарушений политики безопасности
- обновление планов обеспечения непрерывности деятельности службы безопасности.
- внедрение дополнительных средств защиты, требующих существенной перестройки системы безопасности;
- выполнение обязательства перед государством и партнерами
- юридические споры,выплаты компенсаций и потери в результате разрыва деловых отношений..
- организацию системы допуска исполнителей и сотрудников конфиденциального делопроизводства с соответствующими штатами и оргтехникой.
- поддержание системы резервного копирования и ведения архива данных;
- контроль изменений состояния информационной среды предприятия;
- повышение квалификации сотрудников предприятия в вопросах использования имеющихся средств защиты, выявления и предотвращения угроз безопасности;
- проведение инженерно-технических работ по установлению сигнализации, оборудованию хранилищ конфиденциальных документов, защите телефонных линий связи, вычислительной техники и т.п.

Приведенный список затрат является не полным и может быт дополнен из [2].

TCO можно расчитать по формуле:

$$\mathbf{TCO(E) = cost0(E) + \sum_{t=1}^{t=n} cost\ t(E) / T,}$$

где, cost0(E) единовременне затраты (закупка, установка и тд.), cost t(E) текущие затрат в течении времени эксплуатации (операционные и прочие), T – время эксплуатации. [3]

Метод расчета ROSI можно представить так.

1. Определяется ожидаемая потеря денежных средств за год по причине возникновения инцидента ИБ - Annual Loss Expectancy (ALE). Показатель ALE вычисляется как произведение ущерба от некоего инцидента ИБ в денежном эквиваленте на количество возникновений (или вероятность возникновения) этого инцидента в течение года.
2. Применение меры защиты предполагает снижение вероятности возникновения инцидента ИБ, поэтому определяется также так называемый модифицированный показатель ALE (mALE), как произведение ущерба от инцидента ИБ в денежном эквиваленте на количество возникновений (или вероятность возникновения) этого инцидента после применения средств защиты.
3. Разница между ALE и mALE, за вычетом стоимости всех затрат перечисленных выше и есть ROSI.

Вывод

Единого рецепта на все случаи жизни не существует. Многое зависит от того, как воспринимает проект бизнес-руководство. Каждый из методов обладает своими достоинствами и недостатками и имеют свои предпочтительные области применения.

Иинфраструктурный проект может быть оценен прежде всего с помощью TCO, ALE. Оценка бизнес-проектов — это, прежде всего, оценка отдачи для бизнеса, и ее лучше делать при помощи ROI, EVA. Для финансовой оценки аутсорсинговых проектов подойдут ROI, TCO, ALE. Если принята программа создания нового бизнеса в сфере аутсорсинга то можно применять EVA, усиленную оценкой рисков и возможностей на основе ROI.[4]

Литература

1. Базаров Р. Во всех измерениях журнал “CIO World”№9; http://www.cio-world.ru/offline/2006/52/286650/
2. Козаченко В. - Управление общей стоимостью владения КИС http://www.cfin.ru/itm/kis/kis_tco.shtml

3. Robinson Ph., Stephenson B. - "TCO-aware provisioning of information security infrastructure" HP Labs, http://www.hpl.hp.com/techreports/2008/HPL-2008-195.pdf
4. Полякова М. - "ИТ и деньги"; http://www.osp.ru/titles/cw/article/article_9491929.html

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ И ПЕРСПЕКТИВЫ КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ

Константин Андроник, Василий Власов
Славянский университет (Республика Молдова)

Some modern possibilities of use computer стеганографии for the decision of problems of information safety are considered. Development prospects are defined.

Компьютерные технологии придали новый импульс развитию и совершенствованию стеганографии (от греческого «тайнопись»), появилось новое направление в области защиты информации - компьютерная стеганография (КС). Современный прогресс в области глобальных компьютерных сетей и средств мультимедиа привел к разработке новых методов, предназначенных для обеспечения безопасности передачи данных по каналам телекоммуникаций и использования их в необъявленных целях. Эти методы, учитывая естественные неточности устройств оцифровки и избыточность аналогового видео или аудио сигнала, позволяют скрывать сообщения в компьютерных файлах (контейнерах). Причем, в отличие от криптографии, данные методы скрывают сам факт передачи информации [2].

Основными положениями современной компьютерной стеганографии являются следующие [1, 3]:

I. Методы скрытия должны обеспечивать аутентичность и целостность файла.

II. Предполагается, что противнику известны все возможные стеганографические методы.

III. Безопасность методов основывается на сохранении стеганографическим преобразованием основных свойств открыто передаваемого файла при внесении в него секретного сообщения и некоторой неизвестной противнику информации - ключа.

IV. Даже если факт скрытия сообщения стал известен противнику

через сообщника, извлечение самого секретного сообщения представляет сложную вычислительную задачу.

Анализ информационных источников компьютерной сети Internet позволяет сформулировать перечень предметных областей использования стеганографических систем:

1. Защита конфиденциальной информации от несанкционированного доступа. Так, например, только одна секунда оцифрованного звука с частотой дискретизации 44100 Гц и уровнем отсчета 8 бит в стерео режиме позволяет скрыть за счет замены наименее значимых младших разрядов на скрываемое сообщение около 10 Кбайт информации. При этом изменение значений отсчетов составляет менее 1 %. Такое изменение практически не обнаруживается при прослушивании файла большинством людей [1].

2. Преодоление систем мониторинга и управления сетевыми ресурсами промышленного шпионажа. Стеганографические методы позволяют противостоять попыткам контроля над информационным пространством при прохождении информации через серверы управления локальных и глобальных вычислительных сетей [2].

3. Камуфлирование программного обеспечения (ПО). В тех случаях, когда использование ПО незарегистрированными пользователями является нежелательным, оно может быть закамуфлировано под стандартные универсальные программные продукты (например, текстовые редакторы) или скрыто в файлах мультимедиа (например, в звуковом сопровождении компьютерных игр) [4 - 8].

4. Защита авторских прав от пиратства - использование стеганографии позволяет наносить на компьютерные графические изображения специальную метку, которая остается невидимой для глаз, но распознается специальным ПО. Такое программное обеспечение уже используется в компьютерных версиях некоторых журналов и предназначено не только для обработки изображений, но и для файлов с аудио- и видеоинформацией и призвано обеспечить защиту интеллектуальной собственности [3].

Анализ тенденций развития КС показывает, что в ближайшие годы интерес к развитию методов КС будет усиливаться всё больше и больше. Предпосылки к этому уже сформировались сегодня. В частности, общеизвестно, что актуальность проблемы информационной безопасности постоянно растет и стимулирует поиск новых методов защиты информации (ЗИ). С другой стороны, бурное развитие информационных технологий обеспечивает возможность реализации этих новых методов ЗИ. И, конечно, сильным катализатором этого процесса является лавинообразное развитие компьютерной сети общего пользо-

вания Internet, в том числе такие нерешенные противоречивые проблемы Internet, как защита авторского права, защита прав на личную тайну, организация электронной торговли, противоправная деятельность хакеров, террористов и т.п.

Весьма характерной тенденцией в настоящее время в области ЗИ является внедрение криптологических методов. Однако на этом пути много ещё нерешенных проблем, связанных с разрушительным воздействием на криптосредства таких составляющих информационного оружия как компьютерные вирусы, логические бомбы, автономные репликативные программы и т.п. Объединение методов компьютерной стеганографии и криптографии явилось бы хорошим выходом из создавшегося положения. В этом случае удалось бы устранить слабые стороны известных методов защиты информации и разработать более эффективные новые нетрадиционные методы обеспечения информационной безопасности.

В последние годы в связи с интенсивным развитием мультимедийных технологий очень остро встал вопрос защиты авторских прав и интеллектуальной собственности, представленной в цифровом виде. Особенно актуальной эта проблема стала с развитием общедоступных компьютерных сетей, в частности, сети Internet. С учетом этого в настоящее время задачи защиты от копирования и обеспечения аутентификации решаются, помимо мер организационно-юридического характера, с использованием технологий цифровых водяных знаков (ЦВЗ). Необходимо отметить, что наибольшие достижения стеганографии в прошедшем десятилетии были достигнуты именно в области развития цифровых водяных знаков. Эти достижения вызваны реакцией общества на актуальнейшую проблему защиты авторских прав в условиях общедоступных компьютерных сетей.

Проводя подробный анализ стеганографических программ, нельзя не отметить, что в настоящее время на рынке широко представлены следующие программы и приложения: DiSi-Steganograph (DOS-приложение, прячет данные в графических файлах PCX); StegoDOS (DOS, графические форматы); Gif-It-Up (Win95, прячет данные в Gif-файлах); EZStego (Java-приложение, метод LSB для форматов GIF и PICT); Contraband (Win95, формат BMP); FFEncode (DOS, формат ASCII); Isteg (DOS, JPEG); Steganography Tools 4 (шифрует информацию алгоритмами DEA, MPJ2, DES, TripleDES, NSEA и затем прячет ее в графических и звуковых файлах, а также в секторах дисков); Winstorm (DOS, OS/2, PCX) и др. [5 - 8].

Таким образом, в настоящее время одна из наиболее древних наук стеганография становится основой для создания перспективных систем

защиты информации, оперативно-технические характеристики которых определяются новыми информационными технологиями. Сегодня стеганография позволяет не только успешно решать основную задачу – скрытно передавать информацию, но и решать целый ряд других актуальнейших задач, в том числе, помехоустойчивой аутентификации, защиты от несанкционированного копирования, мониторинга информации в сетях связи, поиска информации в мультимедийных базах данных и др.

Литература:

1. Грибунин В.Г. и др. Цифровая стеганография. - М.: СОЛОН-Пресс, 2002. - 299 с.
2. Карасев Андрей. Компьютерная тайнопись – графика и звук приобретают подтекст. – //Мир ПК. - № 1/2007. – С.132-134.
3. Специальная техника//№№ 5/1998, 6/1999, 6/2000, 3/2002.
4. Тигулев Максим. Стегонозавр или тайнопись на компьютере. - //Internet журнал http://www.gagin.ru/internet/8/12.html
5. Privacy Guide: Steganography. http://www.all-nettools.com/privacy/stegano.htm
6. http://www.citforum.ru/internet/securities/stegano.shtml
7. http://www.securitylab.ru/analytics/216270.php
8. http://st.ess.ru/publications/articles/steganos/steganos.htm

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РОЛЬ ЧЕЛОВЕКА В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Александр Каминский,
эксперт (Республика Молдова)

This work describes the global and local problems of information security, as well as man's role in the common information system.

Централизация знаний и информации происходит на высших уровнях. Идеи и мысли, всё тщательным образом отфильтровывается и обрабатывается, сохраняется и используется для управления низшими звеньями. Тут, применимо высказывание, принадлежащее философу Френсису Бэкону, которое в своё время употребили и приме-

няли на практике Ротшильды: «Кто владеет информацией - владеет миром». Так значит, защищаться, защищать и нападать может лучше тот и те, кто обладает большим количеством качественных знаний и владеет нужной информацией. Нам, если мы хотим создать защищенную систему, нужно карабкаться и рваться вверх по лестнице знаний, находить решения глобального характера, а не зацикливаться только на специфики своей деятельности.

Защиту любой структуры или обычных людей можно сравнить с волнорезами в портах и гаванях. Волнорез обычно строят чуть выше уровня моря, так и организации стараются защитить свою систему чуть выше ныне существующих угроз, чуть «выше уровня моря», но это только создаётся иллюзия безопасности. Многим приходилось, наверно, видеть как во время шторма в море волны свободно перегибают высоту волнореза и в спокойной до того гавани, начинаются колебания и волнения. Если в идеальных условиях волнорез в крупном порту может и не удастся разрушить волной, только разве цунами. То после продолжительного и изощренного шторма на «волнорез» информационной системы, да и на любую другую систему организации, в защите могут появиться сильные пробоины и тогда итог может быть ещё либо известен, либо уже не известен. Примером такого «шторма», в реальности, может быть масштабная атака не только на одну компанию, но и на прилегающие к ней инфраструктуры. Этот процесс может коснуться не только защищающей системы, но и отдельных участников информационной системы. Так можно «оградиться огромнейшими сооружениями» создать идеальную политику безопасности, обучать, наказывать и поощрять членов информационной системы (ИС), но слабейшим звеном остаётся, как бы ни было обидно, сам Человек, инсайдер.

Компьютерные программы и системы, пока они не обладают Искусственным интеллектом, способны действовать только в рамках поставленных на них задач придерживаясь строгих алгоритмов и логики, и только человек может изначально изменить эту логику и соответственно задачи, или в процессе выполнения задачи нарушить логику и алгоритм работы системы.

Построение любой системы начинается с изучения и рассмотрения регламентирующей и законодательной документации, придерживаясь строгих стандартов, если производство большое возможна разработка собственных стандартов. В сфере ИТ, а в частности в ИБ существуют строго регламентированные стандарты такие как: международные стандарты ИБ *ISO/IEC 17799* и ***ISO13335***, а также серия стандартов управления

ИБ ***ISO27000***. Это очень хорошо что «велосипед уже создан», и нам остаётся только использовать и придерживаться этих стандартов и рекомендаций в своей деятельности. Но и злоумышленники придерживаются в своей неблагородной деятельности этих же стандартов. Если все принципы, на которых основывается безопасность ИС, заранее известны, то инструменты как нарушить безопасность системы можно подобрать.

Заботясь о своей национальной безопасности или защищая свою информационную - корпоративную систему, здравым смыслом было бы разрабатывать и использовать собственные принципы защиты, строить безопасность и информационные системы таким образом, чтобы они имели определённую неизвестную специфику. А когда нам «сверху» диктуют как и что, и у кого мы должны покупать, как мы должны защищаться, какие средства защиты на сегодня самые надёжные, какую операционную систему использовать, то о какой специфике и индивидуальности нашей системы может идти речь. Не ужели, более 90% использования операционных систем одной корпорации, и более 50% всех поисковых запросов другой корпорации, в мире в общем - это чистая случайность? О какой глобальной, национальной и тем более корпоративной и личной безопасности может идти речь, когда мы все одинаковые? Мы все сидим на «дырявом» софте, пользуемся прослушивающими сервисами и самое страшное, что мы это всё пускаем в свою корпоративную систему и частную жизнь.

Защита интересов бизнеса и граждан, должна исходить в первую очередь от государства, оно должно на законодательном и исполнительном уровне защищать свои национальные интересы, а не интересы бизнеса других стран. Это если говорить на глобальном и государственном уровне.

А если придерживаться границ частного бизнеса, то защита на этом уровне должна складываться из:

- поиска существующих угроз, реальных для этого сегмента рынка и деятельности организации. Не стоит перегибать палку и приписывать себе угрозы которые могут и не коснуться вас.
- оценки и управления рисками, которые может понести ИС и бизнес в результате действия угроз.
- выбрать оптимальную защиту, и построить ИС таким образом чтобы затраты на защиту были оправданы возможным риском.

Можно сказать, что никогда не будет создана идеальная система защиты, так как знания защищающейся стороны, и тех сторон которые её защищают будут ниже возможных ре-

альных угроз, которые ещё не известны или известны были заранее, но их преднамеренно скрывали. Но попытаться сделать что-то своё всё таки стоит, не стоять на месте, а двигаться вперёд, вверх по лестнице знаний.

Литература и интернет ресурсы:

1. http://ru.wikipedia.org/
2. http://www.intuit.ru/
3. http://www.securitylab.ru/
4. http://security.ase.md/

BPMS – ОСНОВА РЕИНЖИНИРИНГА БИЗНЕС-ПРОЦЕССОВ ПРЕДПРИЯТИЙ

К. Шишманов,
Экономическая академия им. Д.А.. Ценов (Болгария)

Согласно результатам исследований ведущих исследовательских учреждений системы управления бизнес-процессов (Business Process Management System – BPMS или BPM) в настоящий момент являются одним из самых актуальных задач для большинства информационных подразделений предприятий. В связи с этим аналитики IDC ожидают, что к 2011 году продажи систем BPM будут составлять около 5,5 млрд. $ и это примерно 40 % роста в год[1].

BPM системы помогают моделировать процессы, основываясь на анализе потребностей предприятия, для преобразования реальных исполняемых процессов. Уровень развития технологии организации в большой степени определяет и уровень применения BPM. Этот вопрос индивидуального выбора. Некоторые предприятия применяют инструменты моделирования и обмена данными, другие внедряют системы активного контроля рабочих процессов (workflow), третьи обеспечивают трасляцию построенных моделей в новые исполняемые процессы без дополнительного программного кода и т. д. В зависимости от того, какими процессами следует управлять, могут применяться все функции современных BPMS или их часть для решения локальных проблем.

Эмпирический анализ BPM только с точки зрения информационных технологий позволяет сделать следующие выводы:

[1] http://cio.bg/2334_klyuchovi_aspekti_pri_vnedryavaneto_na_bpm

1. В первую очередь BPM рассматривается как платформа для интеграции. Применяемая система обеспечивает соединение различных приложений, но не уделяет внимания моделированию бизнес-процессов. В результате получается так, что процессы не связаныс приложениями, а только найдено решение с управлением данных, которое в целом не улучшает управления предприятием.
2. Во-вторых, BPM рассматривается как инструмент для автоматизации рабочих процессов. В этом сценарии использование предлагаемого решения обычно находится в пределах отдельного подразделения предприятия и только для ограниченного круга задач. В результате наиболее ценные возможности BPM остаются нереализованными.

Особенности современного бизнеса обуславливают необходимость смещения акцентов с управления отдельными ресурсами соответствующих функциональных подразделений предприятия на управление сквозными бизнес-процессами, связывающих воедино деятельность подразделений предприятия. Обычные представления о хорошем предприятии как о монолитной, устойчивой централизованно-управляемой организации уступают место идеям о самоорганизации предприятия как формам адаптации к быстроменяющимся требованиям рынка.

Наиболее полно концепция управления бизнес-процессами в настоящее время реализована в реинжиниринге бизнес-процессов, цель которых заключается в системной реорганизации материальных, финансовых и информационных потоков, направленных на упрощение организационной структуры, перераспределение и минимизацию использования различных ресурсов, сокращение сроков исполнения заказов потребителей, повышение качества их обслуживания.

Сложность реинжиниринга бизнес-процессов обусловлена необходимостью оптимального распределения ресурсов, а также реализацией задач перепроектирования организационно-экономической и информационной системы.

МЕТРИКИ БЕЗОПАСНОСТИ

Денис Салтыков,
Молдавская Экономическая Академия (Республика Молдова)

This article presents general information about security metrics. Also, here will be described common classification and the main goal of security metrics with advice for the best choice of special security metrics.

Цели использования метрик безопасности.

Тема метрик безопасности является современной и актуальной, так как настоящее время можно охарактеризовать как эпоху информации, когда информация является без преувеличения самой важной основной ценностью в обществе. Таким образом, не менее актуальным является вопрос информационной безопасности и защиты информации. Метрики информационной безопасности, правильный подбор нужных метрик и методов их расчета отражают эффективность системы защиты информации и позволяют на их основе улучшать характеристики системы.

Актуальность данной темы подтверждают результаты опроса ISACA – "Critical Elements of Information Security Program Success".. Как вывод были выведены 5 основных критериев успеха:

1. Общий язык. Бизнес первичен.
2. Процесс взаимодействия. Двусторонняя связь.
3. Система убеждения. Маркетинг и PR.
4. Выход на руководство. Сила и влияние.
5. Метрики. Что и как измерять.

Можно задать вопрос: можно ли вообще измерять? Если что-то лучше, значит, есть признаки улучшения. В таком случае улучшение можно наблюдать, наблюдаемое улучшение можно посчитать. То, что можно посчитать, можно измерить, а измеренное – оценить и продемонстрировать. Таким образом, можно сделать вывод, что тема метрик информационной безопасности актуальна, так как явно отображает безопасность на уровне бизнеса, а значит, помогает увеличить экономическую эффективность работы любого предприятия в любой отрасли.

Метрики необходимы для того, чтобы:

* показать, каким образом деятельность вносит непосредственный вклад в достижение целей;
* измерить, как изменения в процессе отражаются на достижении целей;
* выявить существенные ано-

малии в процессах и принять обоснованные решения по исправлению или улучшению процессов.

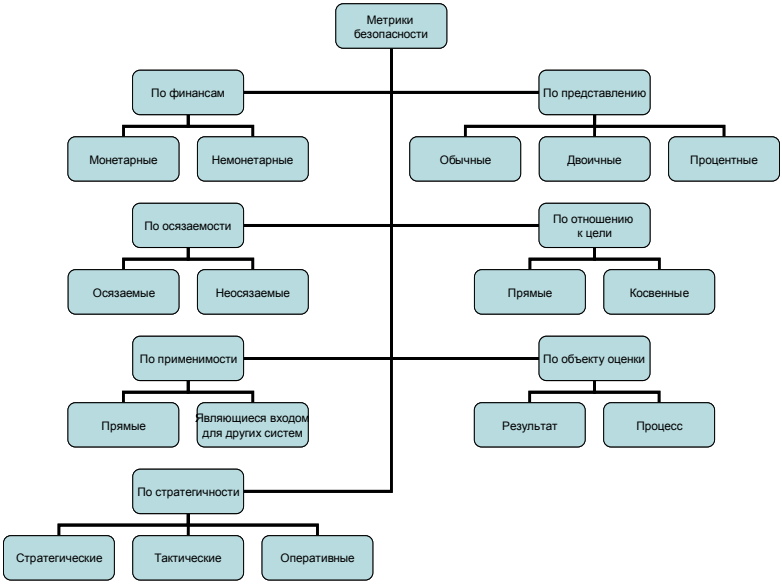
Выбор правильных метрик.

Следует отметить, что стандартного набора метрик безопасности, который подошёл бы на все случаи жизни не существует. Любой объект обладает собственной спецификой, так что в каждом конкретном случае рассчитывается специальный набор метрик, который должен оптимально соответствовать ситуации.

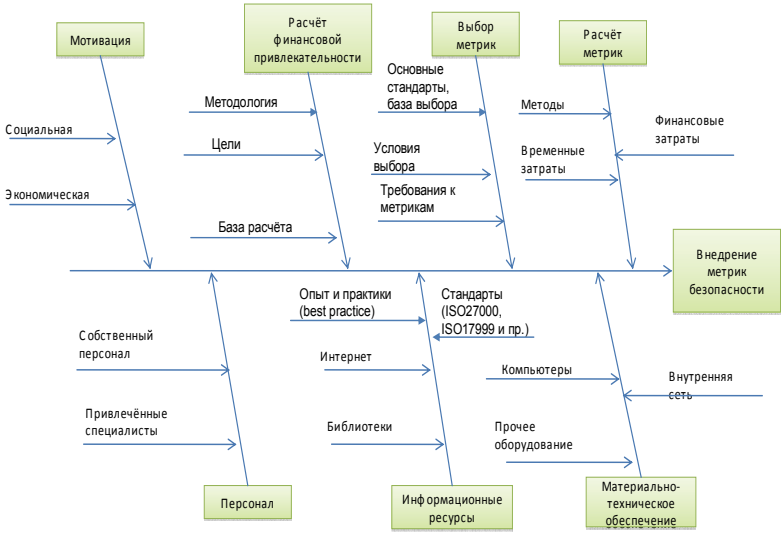
Следует также дать ответ на вопрос, какие метрики подойдут лучше: для целей или для результатов процесса. Отсутствие инцидентов в течение длительного времени приводит к ощущению безопасности, но предотвращённые инциденты не могут быть измерены так же, как реально произошедшие.

Метрики для целей не только трудно найти, они, кроме всего прочего, еще и не очень полезны для управления безопасностью. Это связано с отсутствием прямой связи между деятельностью по безопасности и, собственно, целями безопасности. Вы никогда не сможете сказать, действительно ли Вы приблизились к целям безопасности, оказав определенное воздействие на процессы безопасности.

Классификация метрик безопасности.



Если метрики для целей трудно получить, и они не очень полезны, то измерение результатов процесса обеспечения безопасности не только возможно, но и крайне полезно, так как результаты прямо или косвенно связаны с обеспечением безопасности, уверенности и достоверности.



Литература:

1. Астахов А. Искусство управления информационными рисками, Москва, ДМК Пресс, 2010.
2. Мельников В. П., Клейменов С. А., Петраков А. М.. Информационная безопасность и защита информации, Москва, Издательский центр «Академия», 2008.
3. Блог Алексея Лукацкого. http://lukatsky.blogspot.com/

СОГЛАШЕНИЕ ОБ УРОВНЕ ОБСЛУЖИВАНИЯ

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

Соглашение об уровне обслуживания (Service Level Agreement, SLA) является достаточно новым для нашего рынка понятием. Основное назначение SLA — определить уровень услуг, оказываемых клиенту поставщиком согласно взаимной договоренности.

В настоящее время не существует стандартных норм для регулирования качества предоставляемых информационных сервисов, поэтому SLA является единственным путем для установления взаимных прав, обязанностей, гарантий и компенсаций.

В ИТ подразделениях наиболее динамичных и технологичных компаний работает минимум сотрудников, которые осуществляют лишь мониторинг и координацию всех процессов, а всю технологическую поддержку и развитие ИТ проектов обеспечивают провайдеры информационных сервисов.

Дополнительной гарантией высокого качества сопровождения информационных сервисов является наличие у провайдера услуг сертификата качества, например, ISO, а также сертификации процесса предоставления ИТ услуг. Если же еще и потребитель сертифицирован по стандартам ISO или строит свою деятельность в соответствии с данными стандартами, то возможность некачественного сопровождения сводится практически к нулю, поскольку обе стороны оперируют едиными понятиями и действуют в рамках единой методологии.

Многие аутсорсинговые компании формируют SLA на основании бизнес-требований конкретного клиента в соответствии с его потребностями. Экспертные организации по всему миру разрабатывают унифицированные системы материальной оценки качества услуг в сфере ИТ.

Концепция SLA должна включать следующие разделы:

- Содержание предоставляемого информационного сервиса и стороны, вовлеченные в соглашение;
- Срок действия соглашения;
- Место предоставления информационного сервиса;
- Время предоставления информационного сервиса - дни и часы предоставления сервиса, включая тестирование, поддержку и модернизации;
- Регламент доступности сервиса, включая время, потраченное на тестирование, текущую поддержку и модернизацию. Также оговаривает-

ся число конечных пользователей услуги и обслуживаемое или задействованное в обслуживании оборудование;

- Алгоритм предоставления информационного сервиса, который детально описывает процедуры мониторинга, устанавливает график отчетности о сервисе и о методах устранения неполадок, указывает способы модернизации и эволюции сервиса, если его предоставление рассчитано на длительный срок;
- Спецификации целевых уровней качества сервиса, включая:

a) средняя доступность, выраженная как среднее число сбоев на период предоставления сервиса;
b) минимальная доступность для каждого пользователя;
c) среднее время отклика сервиса;
d) максимальное время отклика для каждого пользователя;
e) средняя пропускная способность;

- Перерывы в предоставлении услуги: согласованные перерывы в предоставлении услуги и исключения;
- Описание платежей, связанных с сервисом - установление единой цены за весь сервис или с разбивкой по уровням сервиса. Здесь также определяется ответственность заказчиков при использовании сервиса (подготовка, поддержка соответствующих конфигураций оборудования, ПО или изменения только в соответствии с описанной процедурой изменения);
- Ответственность пользователей при использовании сервиса (подготовка, поддержка соответствующих конфигураций оборудования, программного обеспечения или изменения только в соответствии с процедурой изменения);
- Процедура разрешения рассогласований, связанных с предоставлением сервиса.
- Безопасность - при выполнении работ внешними специалистами изменяется уровень безопасности в компании, с учетом того что у компаний есть свои секреты, «ноу-хау», позволяющие опережать конкурентов.

При предоставлении услуг поставщик может руководствоваться следующими вариантами политики в отношении SLA:

- Не применять;
- Заключать SLA индивидуально по требованию клиента (в основном это самые крупные и выгодные клиенты);
- Ззаключать по требованию клиента типовое SLA;
- Заключать типовое SLA со всеми клиентами, которое в

этом случае является неотъемлемым атрибутом договора на предоставление услуг;
- Предлагать дифференцированные варианты SLA, отличающиеся качеством обслуживания и ценой.

Предоставление ИТ-услуг между структурными подразделениями компании должно быть направлено на улучшение взаимодействия между ИТ и бизнес пользователями для достижения стратегических и тактических задач пользователей. Целью Соглашения об уровне обслуживания является предоставление качественного и количественного описания предоставляемых услуг, как с точки зрения поставщика услуг, так и с точки зрения клиента.

Основными стратегическими шагами при разработке SLA должны быть:
- Четкое формирование требований компании;
- Установление приоритетов предоставляемых сервисов, оказание внимания защите важных компонентов;
- Четкое определение терминов - определение понятий, относящихся к качеству сервиса;
- Учет наилучших и наихудших сценариев развития событий;
- Определение адекватной компенсации;
- Обязательная модернизация - условия долгосрочных SLA должны периодически пересматриваться.

Продуманное SLA является выгодным как для провайдера услуг, так и для клиента. Провайдер услуг твердо знает, что конкретно он может дать, и таким образом может не опасаться нереальных запросов, удовлетворить которые будет технически невозможно или экономически нецелесообразно. Клиент в свою очередь получает приемлемый для него гарантированный уровень сервиса.

Корректно составленное Соглашение об уровне обслуживания отличает несколько особенностей, главная из которых — достижимость и измеримость условий соглашения.

Список нормативной и научной литературы:

1. ITIL (IT Infrastructure Library) - библиотека инфраструктуры информационных технологий;
2. Рекомендация E.860 “Framework of a Service Level Agreement”, 2002 г;
3. Рекомендация E.801 “Framework of a Service Quality Agreement”, 2005 г.;
4. ETSI – EG 202 009-3 “User Group; Quality of telecom service; Part 3: Template for Service Level Agreements”, 2002 г.

АНАЛИЗ УЯЗВИМОСТЕЙ И ИНСТРУМЕНТОВ ОСУЩЕСТВЛЕНИЯ СЕТЕВЫХ АТАК

Василий Гусликов, Михаил Стеркул
Славянский университет (Республика Молдова)

The counteraction problem to network attacks Is investigated. The characteristic is given attacks of type DoS and DDoS, intended for a conclusion out of operation operating system services. Questions of security of network resources on the basis of tools of operating system Windows XP are considered.
Ключевые слова: *операционная система, защита, сетевые атаки, DDoS, DoS.*

Актуальность темы заключается в том, что наряду с растущей популярностью операционная система Windows все в большей степени привлекает взломщиков, хакеров или просто любителей ради баловства написать программы взлома, вирусы именно для этой операционной системы. **Целью работы** явилось исследование возможностей сетевых атак на примере ОС Windows XP и разработка рекомендаций по их преодолению. **Предметом исследования** выступали сетевые инструменты Windows XP и их уязвимости при сетевых атаках.

Конечно, существуют вредоносные программы и для других ОС, но их значительно меньше. Главная причина этому, то, что такие ОС как Linux, Unix, FreeBSD и другие, как правило, контролируются опытными администраторами, которые полностью проверяют работоспособность как внутренней сети, так и каждой машины. Кроме того, сеть может быть защищена брандмауэром и даже если какой-то программе удастся преодолеть защиту, администратор сразу заметит активности и легко разберется, откуда исходит опасность по исходящему ICMP или UDP трафику [5].

Основная опасность грозит тем системам, которые управляются обычными пользователями, их компьютеры часто не имеют защиты или имеют, но не умеют пользоваться своими брандмауэрами. Кроме того, компания Microsoft наградила операционную систему Windows XP очень мощными инструментами, которыми не стесняются пользоваться хакеры. В частности самая популярная версия Windows поддерживает механизм SOCK_RAW, который является очень мощным инструментом и открывает большие возможности для взлома.

Этот тип “гнезд” обеспечивают доступ к протоколам наиболее низкого уровня и даже к сетевым

интерфейсам. В частности, в системе Unix raw sockets пользуются инструментом getethers, предназначенным для сбора информации о компьютерах, подключенных к сети Ethernet. Один из побочных эффектов поддержки raw sockets - возможность замены обратного адреса в IP- и ICMP-пакетах [3].

В далеком 2001 году, когда только должна была выйти операционная система Windows, разгорелись споры о том, нужна ли в ОС поддержка sockets raw. Тогда президент компании Gibson Research Corporation, Стив Гибсон обратился к компании Microsoft с предложением убрать этот мощный инструмент и не давать хакерам в руки столь мощное оружие. Но компания Microsoft не восприняла слова известного специалиста по компьютерной безопасности и заявила, что задуманное будет воплощено в жизнь. Во-первых, аргументируют они «raw sockets уже были реализованы в Windows 2000, и, как говорится, ничего страшного не произошло. Во-вторых, безопасность за счет отклонения от стандартов - порочная практика».

Именно с этого момента пользователи самой популярной ОС стали грозным оружием в руках сообразительных хакеров. Сами того не зная, вы можете быть одним из воинов многочисленной армии, так называемых «зомби» - компьютеров, которые атакуют заданную цель [1].

Атаки, предназначенные для вывода из строя служб операционной системы, подразделяются на два типа DoS и DDoS.

Атака DoS - Denial of Service, этот тип атак известен давно, его применяют не только для того, чтобы отключить службы или положить сервер, но часто прикрываются такой атакой при взломе сервера. Подобные действия хакеры называют «наводнением». Сервер закидывается запросами о соединении, при этом атакующий компьютер не отвечает, а посылает запрос снова и снова. Это продолжается до тех пор, пока буфер не будет переполнен. Когда это случится соединение с сервером станет невозможным [1].

Атака DDoS - Distributed Denial of Service, является модификацией DoS и отличается тем, что при проведении атаки используются скоординированные действия многочисленных компьютеров-посредников, которые играют активную роль. Для этого на машины внедряются специальные программы – «зомби», поддерживающие связь с неким управляющим центром. По его команде «зомби» начинают генерировать ICMP или UDP пакеты и передают их по адресу жертвы [1].

Подобные атаки сейчас часто применяются хакерами, даже существует негласный сервис, которым может воспользоваться каждый.

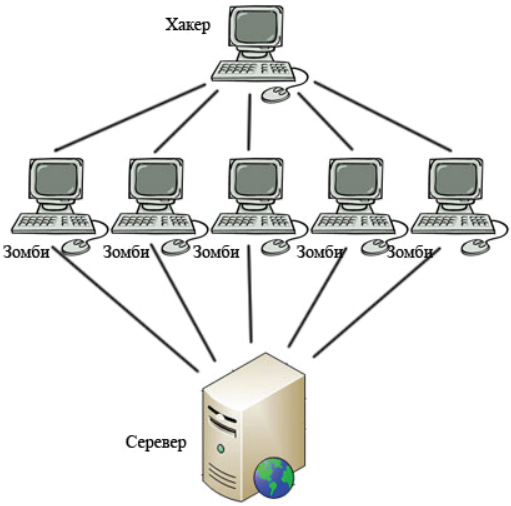


Рис. 1. **Пример DDoS атаки**

Конечно, всего этого не стоит опасаться, если установить и обновлять на компьютере антивирусные системы и брандмауэр. Таким образом, можно на 90% исключить возможность того, что компьютер станет еще одной боевой единицей армии «зомби». Но, в принципе, любой хакер может воздействовать на персональный компьютер пользователя на еще более низком уровне - разработав драйвер, который, по сути, будет троянской программой, открывающей доступ к информации и ресурсам. Именно по этой причине для обеспечения уверенности в 100% защите компьютера рекомендуется приобретать и устанавливать только лицензионное программное обеспечение

Литература:

1. Крис Касперски. Техника сетевых атак. Приемы противодействия. – М.: СОЛОН-Р, 2001. – стр. 311, 313, 315
2. Тим Паркер, Каранжит Сиян. TCP/IP. Для профессионалов. – М.: Питер, 2005. – 859 с.
3. Р. Элсенпитер, Т. Дж. Велт. Windows XP Professional. Администрирование сетей. – М.: Эком, 2006. – стр. 275
4. Вильям Столингс. Network Security Essentials. Applications and Standards. – М.: Вильямс, 2002. – 432 с.
5. http://ru.wikipedia.org DoS-атака

РАССЛЕДОВАНИЕ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ В СФЕРЕ ЭЛЕКТРОННОЙ КОММЕРЦИИ И ЭЛЕКТРОННЫХ ПЛАТЁЖНЫХ СРЕДСТВ

Иван Бабенко,
эксперт (Республика Молдова)

This article will provide a general overview on electronic commerce crimes investigation and on related Forensic. Also, you can find here general investigative methods and improvement recommendations at the level of issuing companies, and at the state level.

С развитием информационных технологий и коммерческих отношений привычные нам денежные операции переходят в электронный формат, предоставляя человеку удобный и эффективный инструментарий электронной коммерции.

Электронная коммерция (ЭК) - предпринимательская деятельность по осуществлению коммерческих операций с использованием электронных средств обмена данными. К объектам электронной коммерции относят различные товары, услуги и информацию. В качестве основного платёжного инструмента используются, электронные деньги.

Электронные деньги (ЭД) — это денежные обязательства эмитента в электронном виде, которые находятся на электронном носителе в распоряжении пользователя, базируются на не меньшем количестве *традиционных* денежных средств, находящемся в распоряжении эмитента и принимаются в качестве оплаты третьими лицами.

По данным отчёта IC3 за 2008 г. основная часть киберпреступлений (около 92%) происходят с использованием инструментария электронной коммерции.

Как средство для совершения преступления ЭД можно разделить на 3 условные группы:

- **пластиковые дебетовые или кредитные карты.** *Обычно служат злоумышленникам для совершения преступлений с банковскими счетами. Чаще всего такие преступления затрагивают относительно малое число пострадавших, но при этом ущерб на одного пострадавшего составляет достаточно крупные суммы денег.*
- **валюты систем для Интернет-платежей.** *Чаще всего используются для разовых платежей при мошенничестве в Сети, а также для сокры-*

тия следов киберпреступлений. Здесь преступникам помогает возможность автоматизации транзакций, а также конфиденциальность открываемых в таких системах счетов.

- **микроплатежи;** *Используются для масштабных по количеству пострадавших преступлений, но при этом с минимальным ущербом для одной жертвы, регистрация таких преступлений и обращение пострадавшего в правоохранительные органы происходит редко. Но, тем не менее, по общей сумме денег преступление может быть достаточно крупным и значимым.*

Отличительными чертами киберпреступлений в области ЭД и ЭК являются:

- целенаправленный характер;
- организованность и высокая координация при совершении преступления;
- групповой характер;
- международный состав, как преступной группы, так и пострадавших;
- почти всегда, предпринимаются действия по сокрытию следов преступления;
- чаще всего, требуют особых знаний и навыков, часто одним из соучастников является злонамеренный инсайдер, а также осуществляется квалифицированное юридическое сопровождение;
- трудно доказать преступный состав действий, даже если эти они носят явно асоциальный/преступный характер;

Невозможно дать исчерпывающий перечень способов совершения преступлений в области ЭК и ЭД, так как наряду с известными способами, постоянно появляются новые, более изощрённые и комбинированное использование известных способов.

Рассмотрим перечень наиболее часто встречающихся преступлений:

- фишинг - представляет широкий спектр преступлений. Используется в качестве основного или вспомогательного средства в подавляющем большинстве случаев
- фальсификация электронных платёжных средств;
- мошенничество с использованием пластиковых карт;
- удалённый НСД к серверам платёжной системы и доступ с использованием служебного положения;
- перехват трафика, чтение почты, а также вирусы и троянские программы для сбора платёжной информации и ключей доступа;
- скиминг – получение данных пластиковых карт посредством физической установки на банкоматы специальных накладок для считывания данных карт и PIN-кодов;

- взлом интернет-магазинов и плохо защищённых платёжных систем;
- фиктивные покупки в Интернет-магазинах и -казино;
- легализация незаконно приобретённых денежных средств;
- сбор и торговля конфиденциальной информацией или незаконными товарами и услугами, используя сервера страны с более "свободным" законодательством и правовой обстановкой;
- преступная небрежность при функционировании точек продаж ЭК;
- продажа заведомо некачественных/не соответствующих описанию/несуществующих товаров;

и многие другие виды и подвиды преступлений…

Основным мотивом для рассматриваемого класса преступлений является материальная заинтересованность злоумышленника. Другие мотивы не исключаются, но чаще всего объектом являются именно деньги, либо товары и услуги которые можно приобрести путём злонамеренных действий.

ОРМ по киберпреступлениям, *совершающимся при помощи коммуникаций и каналов связи удалённо* могут содержать:

1. Исследование и перехват трафика по установленным каналам связи;
2. Поиск следов на сервере и системе (месте преступления);
3. Установление иных коммуникационных средств, вовлечённых в преступление;
4. Установление принадлежности IP-адреса или домена злоумышленника ;
5. Поиск следов подготовки преступления во внешней среде;
6. Установление лиц имевших доступ к системе, либо располагавших сведениями о недостатках системы;
7. Установление текущего местоположения незаконно полученных денежных средств и проверка цепочки операций, совершённых с ними после преступления;
8. При необходимости, расследование преступления в международном масштабе, если есть причины полагать, что преступник действовал не только в рамках государства, а и за его пределами, обычно так и происходит в случаях крупного мошенничества и хищения.

ОРМ по киберпреступлениям, *совершающимся при физическом контакте с оборудованием или коммуникационными сетями платёжных систем,* могут содержать:

1. анализ системы пропусков и системы слежения за оборудованием, при их наличии;
2. поиск следов на сервере и в системе;

3. анализ предшествующих инцидентов, зарегистрированных в платёжной системе;
4. исследование, оставленных на месте преступления следов монтажа, оборудования, исходящих каналов передачи данных;
5. исследование вещественных доказательств и, в случае если они были произведены промышленным путём, установление производителя;
6. установление лиц, имевших отношение к разработке аппаратно-программного комплекса для работы платёжной системы.

Предотвращение преступлений в ЭК может быть очень эффективным при использовании общих и специальных стандартов *(стандарты серии ISO/IEC, PCI/PA DSS, PCI PED и т.д.)*. Для всех преступлений в ЭК внедрение стандартизации может значительно снизить риски возникновения инцидентов. На уровне государства это должно решаться принятием национальных законов об регламентации отношений в области ЭК и законов, касающихся информационной безопасности в соответствии с действующими международными стандартами и Конвенцией Совета Европы по борьбе с киберпреступностью.

Закалючение

Для борьбы с преступностью в сфере ЭК *платёжным системам и банкам* необходимо эффективно внедрять общеотраслевые и внутренние корпоративные стандарты безопасности и постоянно осуществлять контроль конфиденциальности, целостности, доступности и аутентификации при работе с информацией, а также регулярно проводить внешний и внутренний аудит безопасности и тщательно расследовать каждый инцидент.

В государственных масштабах необходимо позаботиться о правовой ситуации, а также вывести процедуру расследования преступлений в сфере ЭК на должный уровень, что поможет повысить их раскрываемость, а также снизит скрытую преступность. А международное сотрудничество в сфере расследования киберпреступлений может значительно повлиять на эффективность работы по раскрытию преступлений.

Литература

1. Закон РМ Nr. 284 от 22.07.2004 об электронной торговле
2. *Юрасов А.В.*, Основы электронной коммерции. Учебник для вузов. Телеком, 2008.
3. *Евтодиенко. Д.*, Пластиковые Карточки – один из способов Интернет-мошенничества *http://www.ase.md/~osa/publ/ru/pubru107/Evtodienco_D.pdf*

РАЗРАБОТКА СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ирина Балина, Станислав Панчёхин,
Славянский университет (Республика Молдова)

Problems of maintenance of information safety and system engineering of its protection, various variants of management by access to the information are investigated.

Актуальность выбранной темы обусловлена тем, что защита конфиденциальной и ценной информации от несанкционированного доступа и модификации призвана обеспечить решение одной из наиболее важных задач защиты имущественных прав владельцев и пользователей компьютеров, защиту собственности, воплощенную в обрабатываемой информации от всевозможных вторжений и хищений, которые могут нанести существенный экономический и другой материальный и нематериальный ущерб [1, 2].

Целью являлось исследование проблемы обеспечения информационной безопасности (ИБ) компании и разработка системы её защиты. **Новизна** работы определяется тем, что внедрению процедур и норм по обеспечению безопасности информационных процессов на предприятии будет способствовать разработанная База данных (БД) организации доступа к конфиденциальной информации сотрудников (Рис. 1), в которой каждый уровень доступа распознаётся как учетная запись и ей заданы соответствующие настройки безопасности (Рис. 3). Каждому уровню присвоен свой пароль (Рис. 2).

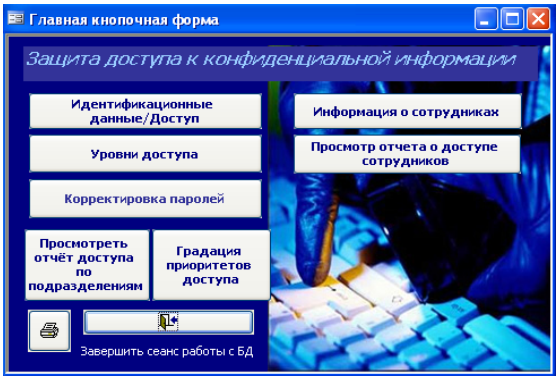
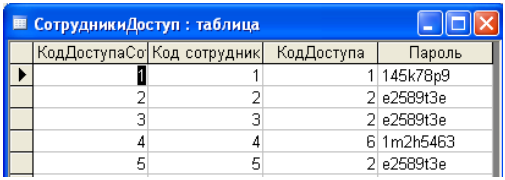


Рис. 1 **Главная форма БД организации доступа к конфиденциальной информации сотрудникам**



СотрудникиДоступ : таблица

КодДоступаСо	Код сотрудник	КодДоступа	Пароль
1	1	1	145k78p9
2	2	2	e2589t3e
3	3	2	e2589t3e
4	4	6	1m2h5463
5	5	2	e2589t3e

***Рис. 2* Таблица «Сотрудники. Доступ» (фрагмент)**

КодДоступа	Описание задачи	Заметки
1	Минимальный	Ограничение доступа пользователей к операциям над документами и справочниками, а также к содержанию (конкретным полям) документов и справочников производится через систему логических рабочих мест
2	Частичный	Возможна работа с конфиденциальными документами по указанию
3	Ограниченный	Доступ к конфиденциальной информации запрещен
...		
7	Повышенные привилегии	Администратор системы контролирует штатные пользовательские командные интерпретаторы, ограничивая возможности пользователя записями в файле "максимальные привилегии".

***Рис.3* Описание ко дов доступа (выборочно)**

Анализ современных технологий зашиты информации позволяет разработать рекомендации по совершенствованию системы безопасности предприятия:

1. Администрирование установок и ограничений работы пользователей: средствами операционной системы, специальных программ и утилит regedit.exe и XP Tweaker- на рабочих станциях (PC) всех сотрудников – прописать учётные записи пользователей, ограничить доступ к дискам и меню задач и др.

2. Постоянный контроль за действиями сотрудников при обработке информации за ПК: контроль в удалённом режиме работы за PC, запуск приложений, содержимое буфера обмена, сетевые подключения и др.

3. Использование возможностей современных криптографических систем – на сервере головного офиса ежедневное шифрование и обновление логического диска для хранения сводной отчётности фирмы, по требованию – производить шифрование текста и (или) файлов при обмене данными с удалёнными пользователями.

4. Установить разработанную СУБД настроек учётных записей всех сотрудников, имеющих доступ к средствам вычислительной техники. Корректировать настройки по мере увольнения/ приёма на работу новых работников/ изменений в штатном расписании и т.д. Разграничить 7 уровней доступа от минимального до повышенных привилегий.

На основании выполненных исследований можно сделать следующие **выводы**:

I. В области понимания информационной безопасности - на сегодняшний день на рынке отсутствует понимание ИБ как таковой. Обычно ИБ сводится к компьютерной

безопасности. При решении, какие услуги предлагать необходимо провести предварительные маркетинговые исследования и выяснить, на что ориентироваться [4].

II. Следствием низкого уровня развития информационных технологий является отсутствие обеспечения информационной безопасности бизнеса. Это приводит к тому, что большинство фирм являются потенциальными целями для умышленного постороннего вмешательства в их нормальную деятельность, со всеми вытекающими отсюда последствиями.

III. При организации работ по совершенствованию информационной безопасности необходим анализ клиентской базы - при внедрении на молдавский рынок услуг, связанных с информационной безопасностью, необходимо четко представлять, на какой круг потребителей можно ориентироваться.

IV. Одним из основных требований к формируемой системе управления безопасностью сетей является то, что данная система должна быть практически действующей и способной выявлять возможные события безопасности, разрабатывать своевременные мероприятия по снижению угроз уничтожения важной информации и выводу из работы системы в целом, вероятности наступления сбоев в работе информационных технологий, рисковых событий или минимизации последствий [3].

V. При внедрении разработанных неформальных (программно- аппаратных) мер защиты по обеспечению информационной безопасности предприятия следует помнить, что они должны быть совмещены с физическими (препятствие – ограничение доступа на предприятие) и с формальными средствами. К ним можно отнести: организационные (регламентация работы сотрудников), законодательные (принуждение в соответствии с законодательством РМ, Международными соглашениями) и морально – этические средства защиты информации (побуждение).

Литература:

1. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей. - М.: Академия, 2006.-240с.
2. Клейменов С.А., Мельников В.П., Петраков А.М. Информационная безопасность и защита информации. - М.: Академия, 2008.-336с.
3. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. М.: Феникс, 2008.-173с.
4. Балина И.В. Международные аспекты защиты информации в экономических информационных системах. // Тр. Межд. научно-практ. конф. «Экономические аспекты развития современного общества». К.: УЛИМ, 2008, стр. 56 – 62

КЛАССИФИКАЦИЯ ИНСАЙДЕРОВ

Григорий Бортэ,
Молдавская Экономическая Академия (Республика Молдова)

The aim of this article is to study the ways of classifying insiders into different categories. Persons who give confidential information away from the company they work in are the object of this article.

Практически три четверти преступлений в сфере информационных технологий приходится, по статистике, на внутренние угрозы. Поэтому обеспечение внутренней безопасности становится одной из приоритетных задач практически любого учреждения.

Целью данной работы является исследование методов разделения внутренних нарушителей на группы.

Объектом исследования являются лица преднамеренно или непреднамеренно выдающие информацию, доступную узкому кругу лиц вовне.

Инсайдер – работник организации, имеющий доступ к конфиденциальной информации, недоступной другим лицам, или широкому кругу лиц. Также, слово может нести негативный оттенок. Например, лицо, опубликовавшее конфиденциальную информацию, или передавшее её лицам, не имеющим доступ к данной информации.

Виды инсайдеров по преследуемым целям:

- Непреднамеренные инсайдеры
- Использующие полномочия и доступ в личных целях
- Продающие конфиденциальную информацию вовне
- Сами использующие доступ и положение для получения материальных выгод

Непреднамеренных инсайдеров можно подразделить на:

- Манипулируемых
- Самостоятельных

Обе эти категории проявляют неосторожность по отношению к информации. В первом случае существует какой-либо движущий механизм, возможно, осуществляется попытка доступа к конкретным данным. Во втором случае работник сам выдаёт какие-либо данные, которые злоумышленник впоследствии «находит». К данным категориям применим термин «социальная инженерия».

Использующих полномочия и доступ в личных целях можно подразделить на:

- Желающих отомстить
- Любопытных

К первой категории могут относиться уволенные или каким-ли-

бо другим способом ущемлённые работники. Обычно, данный вид злоумышленников стремится нанести как можно больший вред компании, а не получить какие-либо материальны блага или ценности. Ко второй категории относятся люди, преднамеренно злоупотребляющие своими полномочиями с целью получения доступа, как к корпоративным, так и личным тайнам коллег. Часто, представители обоих категорий преследуют в качестве цели повышение чувства собственного достоинства.

Работники, продающие конфиденциальную информацию вовне, являются классическим примером инсайдеров. Их можно подразделить на 2 типа:

- Мотивированные
- Планирующие использовать информацию

К первому типу относятся люди, получившие конкретные предложения по покупке информации. Примером может служить бывший сотрудник лихтенштейнского банка LGT Хайнрих Кибер в феврале 2008 года продал приватную базу своего бывшего работодателя немецким и британским спецслужбам, выручив за нее более $7 млн. Пример Кибера наглядно показал, насколько прибыльным может оказаться банковский инсайд. В "базе Кибера" содержались сведения о банковских счетах немецких предпринимателей, которые использовали банки Лихтенштейна для уклонения от налогов. Для немецких спецслужб покупка оказалась крайне выгодной - уже спустя неделю она окупилась практически в шесть раз. Однако банку LGT и всей финансовой системе Лихтенштейна Кибер нанес поистине невосполнимый ущерб.

Ко второму типу относятся те, кто крадёт информацию с возможностью использовать её в перспективе, однако, не имеющим полной уверенности и гарантии того, что это удастся. Примером второго типа могут служить стажеры и практиканты, которые, получив доступ к информации, постарались сохранить себе как можно большую (или как можно более важную на их взгляд) её часть, не имея конкретного плана по дальнейшему её использованию.

Примером сотрудников, самих использующих доступ и положение для получения материальных выгод могут служить работники банков, получившие доступ к прогнозам курсов валют на определённый промежуток времени.

Заключение

Зная цели, преследуемые инсайдерами компании можно предложить следующий комплекс мер по борьбе с возможными утечками информации:

- Контроль исходящего и входящего трафика
- Контроль входящей и исходящей электронной почты

- Ограничение использования подключаемых к компьютеру устройств
- Строгое и чёткое разграничение доступа к информации
- Совершенствование законодательной базы
- Проведение специализированных тренингов для персонала

Литература:

1. Дамир Равилов «Методы классификации внутренних нарушителей» http://infocom.uz/2009/12/16/metodyi-klassifikatsii-vnutrennih-narushiteley/
2. Алексей Комаров «Защита от инсайдера» http://www.osp.ru/text/print/302/5157097.html

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ ПРОТИВ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

(по законодательству Республики Молдова)

Светлана Грищук-Бучка,
Институт истории, государства и права АНМ
(Республика Молдова)

The paper is dedicated to the examination of the categories of crimes against computer safety. This article is based on the analysis of national criminal legislation of the Republic of Moldova.

Противоправные преступные деяния свойственны человечеству с древнейших времен. Однако с развитием цивилизации меняются не только предметы и методы преступного воздействия, но и сам объект преступного посягательства.

Одним из ярких примеров данной категории преступлений являются преступления в сфере компьютерной информации [1]. Активное развитие компьютерных технологий, доступность средств коммуникации, всеобщая информатизация населения стали с одной стороны, еще одной вехой развития цивилизации, а с другой стороны - серьезным испытанием для «права» и правового регулирования. «Наряду с очевидными преимуществами, которые получило человечество от развития информационных технологий, как

отмечает В.И. Волковский, налицо и новые проблемы, ранее нам неизвестные. Существующие сегодня в мире информационные сети позволяют не только обмениваться посланиями, но и проникать в информационные массивы, охраняемые государством» [2]. Соответственно возникает объективная необходимость в правовом регулировании данной сферы общественных отношений.

Законодатель Республики Молдова впервые закрепил уголовную ответственность за данную категорию преступлений в 2002 году в положениях отдельной главы XI Уголовного Кодекса Республики Молдова - «Преступления в сфере информатики». Данная глава содержала три статьи – ст.259-261. В настоящее время в Уголовном Кодексе Республики Молдова (далее УК РМ) данная глава получила новую редакцию и в настоящее время определена как «Информационные преступления и преступления в области электросвязи», и включает 9 статей [3]:

- несанкционированный доступ к компьютерный информации (ст.259 УК РМ);
- неправомерные производство, импорт, продажа или предоставление технических средств или программных продуктов (ст.260 УК РМ);
- неправомерный перехват передачи информационных данных (ст.260[1] УК РМ);
- нарушение целостности информационных данных, содержащихся в информационной системе (ст.260[2] УК РМ);
- воздействие на функционирование информационной системы (ст.260[3] УК РМ);
- неправомерные производство, импорт, продажа или предоставление паролей, кодов доступа или иных аналогичных данных (ст.260[4] УК РМ);
- подлог информационных данных (ст.260[5] УК РМ);
- информационное мошенничество (ст.260[6] УК РМ);
- нарушение правил безопасности информационных систем (ст.261 УК РМ);
- несанкционированный доступ к сетям и услугам электросвязи (ст.261[1] УК РМ).

Правовой анализ состава данных преступлений дает основание сделать следующие выводы, характеризующие их специфику:

Родовым объектом преступного посягательства данной категории преступлений выступают «общественные отношения, обеспечивающие права и законные интересы граждан и организаций, охраняемые законом интересы общества и государства в сфере создания и обращения компьютерной информации» [4; 5].

Объективная сторона компьютерных преступлений может характеризоваться деяниями как в форме действия (например, непра-

вомерный доступ к компьютерной информации – ст.259 УК РМ), так и путем бездействия (например, нарушение … правил защиты информационных систем – ст.261 УК РМ, в частности, виновный не включает систему защиты информации от несанкционированного доступа к ней, оставляет без присмотра свое рабочее место и т.д.) [5].

По конструкции объективной стороны все составы преступлений (за исключением состава, предусмотренного ст.260 УК РМ, 260[1] УК РМ) являются материальными, т.е., включающими в качестве обязательных признаков последствие и необходимую причинно-следственную связь между деянием и последствием. Это означает, что преступление считается оконченным с момента наступления указанных в уголовном законе последствий.

Субъективная сторона характеризуется, как правило, умышленной формой вины в виде прямого умысла.

Субъект компьютерных преступлений – общий – физическое вменяемое лицо, достигшее 16 лет. Согласно положениям ч.2 ст.21 субъектом преступления по ст.206 УК РМ «неправомерное производство, импорт, продажа или предоставление технических средств или программных продуктов» может выступать физическое вменяемое лицо, достигшее на момент совершения преступления 14 лет. Кроме того, положениями ст.261 УК РМ определен специальный субъект как лицо, имеющее в силу своего служебного положения доступ к компьютеру, информационной системе или сети. Следует отметить, что в качестве субъекта данной категории преступлений может выступать так же и юридическое лицо.

Базовые понятия в сфере информатики, такие термины как «компьютерная информация», «информация в компьютерах», «машинные носители», «информационная система», «сеть», «программные продукты», «информационные данные» определяют специфику данного рода преступлений, выступают непосредственными предметами преступного посягательства. «Компьютерная информация» как предмет преступления является обязательным признаком состава анализируемых преступлений [6].

А, соответственно, и подтверждает, тот факт, что данная категория преступлений должна определяться как «компьютерные преступления», «преступления против компьютерной безопасности», а не так как определена в действующем уголовном законодательстве Республики Молдова - «информационные преступления». На лицо подмена понятий, когда «информационная безопасность» рассматривается слишком узко, только лишь с позиции безопасности информации

содержащейся в компьютерах и информационных системах. Ошибочно отождествляются два совершенно разных по своей сущности понятия «защита информации» и «информационная безопасность», хотя на сегодняшний день это совершенно не одно и то же [7]. Кроме того, следует отметить, что и само понятие «информационная безопасность» - многогранно [7]. «Информационная безопасноть не сводится только лишь к компьютерной безопасности … «информационная безопасноть», включающая в себя компьютерную безопасноть в качестве необходимой составляющей распространяется на все социальные процессы современного общества[8]. Именно данное утверждение доктора философских наук Т.Н. Цырдя подчеркивает тот факт, что «в современном обществе информационная безопасность является составной и неотъемлемой частью государственной безопасности любого современного государства, обеспечивающей состояние защищенности личности, общества и государства от угроз в информационной сфере» [7].

Целесообразно, на наш взгляд, внести соответствующие изменения в положения Уголовного Кодекса Республики Молдова и изменить наименование данной главы с целью исключения возможности неверного истолкования категории «информационные преступления», так как в представленной форме это может привести к правовой коллизии и неправильной правовой трактовке и применению уголовно-правовых норм на практике. Более того, из положения самих статей УК РМ, четко явствует тот факт, что речь в данной главе идет именно о «преступлениях против компьютерной безопасности».

Литература:

1. Иван Бабенко. Расследование компьютерных преступлений в сети Internet/ „Securitatea informațională – 2009", conf. intern. (2009; Chişinău). Securitatea informațională – 2009: Conf. intern., 20-21 mai 2009, (ed. a 6-a) /com. org.: Grigore Belostecinic, Vadim Cojocaru, Tatiana Mişova [et al.]; coord. ed.: S. Ohrimenco. – Ch.: ASEM, 2009. – p. 14-18
2. Волковский В.И. Проблемы информационной безопасности //Журнал «Право и безопасность». – № 2-3 . – август, 2002. http://www.dpr.ru/pravo/pravo_3_26.htm
3. Уголовный кодекс Республики Молдова № 985-XV от 18 апреля 2002г.//. Повторно опубликован Monitorul Oficial al Republicii Moldova № 72-74, 2009.
4. Уголовное право. Особенная часть: Учебник/ Под ред.проф. Л.Д. Гаухмана и проф. С.В.Максимова. –2-е изд., перераб., доп. –М.: Изд-во Эксмо, 2005 – с.530-538

5. Лазарева Н. Проблемы квалификации преступлении в области информатики и электросвязи//Закон и жизнь. -2007. -№12. – С.49-56.
6. Лосев В. Преступления против информационной безопасности //Судовы весник. -2002. -№1. – С.40-46.
7. Рыженкова, О.Ю. Информационная безопасность: определение понятия, место в системе национальной безопасности//Закон и право. -2009. -№1. – С.50-51.
8. Теодор Н.Цырдя. Информационная безопасность в условиях информатизации общества http://security.ase.md/publ/ru/pubru06.html

ОРГАНИЗАЦИЯ ПРОГРАММНО- АППАРАТНОЙ ЗАШИТЫ ИНФОРМАЦИИ ОТ ИНСАЙДЕРОВ

Зинаида Гулка, Ольга Гешова,
Славянский университет (Республика Молдова)

In work the problem of distribution of insider trade is considered by the information. The set of software and tools for protection of the data with the short description of functionality of each utility is presented.

Важнейшей проблемой, стоящей перед руководством и службой безопасности любого предприятия, является проблема лояльности сотрудников, или, иными словами, проблема защиты информации от инсайдеров.[1] Существует множество ролей, приписываемых инсайдеру. Например, в финансовой деятельности незаконные инсайдерские торговые операции с ценными бумагами на основе внутренней информации о деятельности компании-эмитента. Обычно инсайдерами являются директора и старшие менеджеры, а также владельцы более 10 % голосов компании. Очевидно, что обиженный или недовольный сотрудник компании, имеющий легальный доступ к сетевым и информационным ресурсам и обладающий определенными знаниями о структуре корпоративной сети, может нанести своей компании гораздо больший ущерб, чем хакер, взламывающий корпоративную сеть через Интернет.

Более того, в результате ошибки или невнимательности инсайдером может оказаться и вполне лояльный сотрудник, который, например, может вынести из офиса диск с конфиденциальной информацией для того, чтобы поработать дома, и

потерять его или отправить письмо по электронной почте не тому адресату, для которого оно предназначено [2]. Серьезность проблемы инсайдеров подтверждается очередным ежегодным исследованием Института компьютерной безопасности CSI, Computer Security Institute. По результатам этого исследования, в 2007 году количество инцидентов с участием инсайдеров впервые вышло на первое место, обогнав таких традиционных лидеров в этой области как вирусы и кражи ноутбуков: 59% признали угрозой № 1 инсайдеров, 52% - вирусы и 50% - потерю мобильного носителя (ноутбука, флэш-накопителя).[9-11]

Проведенное исследование рынка ПО позволяет выделить следующий набор программных средств и инструментов для защиты данных:

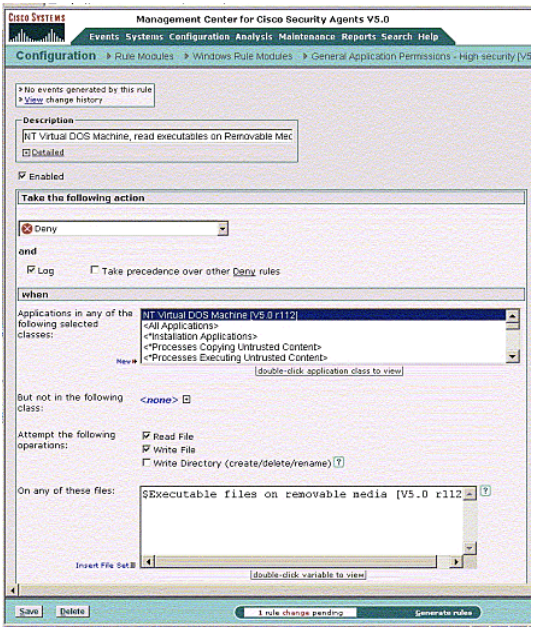


Рис. 1. **Окно программы CSA**

➘ **Cisco Security Agent (CSA)** – объединяет в одном решении различные защитные механизмы и функции по предотвращению атак, защиты от вредоносного кода, блокирования утечки информации через USB-порты и другие внешние устройства. CSA позволяет отражать широкий спектр нападений – сканирование портов, переполнение буфера, троянцев и червей и др. Это, в свою очередь, обеспечивает защиту компью-

тера от неизвестных атак, сигнатуры для которых пока не определены и отсутствуют в базах традиционных средств защиты [7].

➘ **Cryptic Disk** – приложение позволяет легко и надежно зашифровать диски и отдельные разделы на винчестере, защитив их от несанкционированного доступа паролем. При этом вся информация, находящаяся на защищённом диске или записываемая на него, будет автоматически шифроваться. При запуске операционной системы зашифрованный диск/раздел не виден до тех пор, пока он не будет активирован пользователем с помощью пароля доступа в программе Cryptic Disk [3].

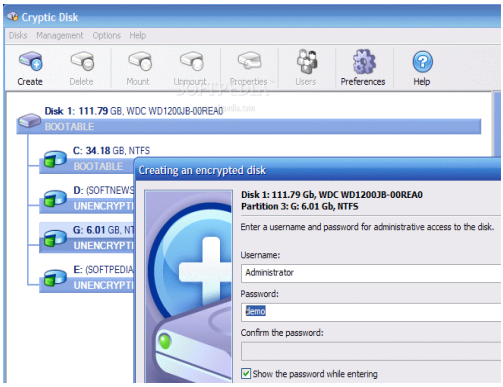


***Рис. 2.* Окно программы Cryptic Disk**

➘ **Safe'n'Sec** – программный модуль, выгодно отличается от большинства приложений, предназначенных для обеспечения безопасности. Следит за активностью разнообразных приложений, процессов, а также за атаками

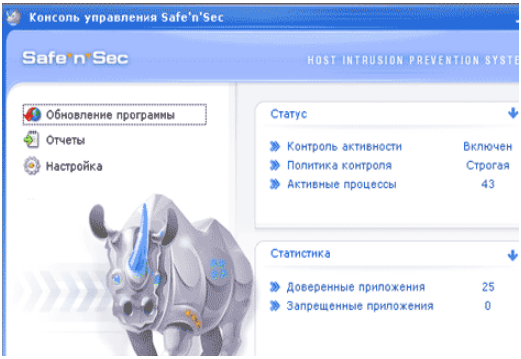


***Рис. 3.* Окно программы Safe'n'Sec**

извне и блокирует любые потенциально опасные действия, анализируя не код приложений, а их активность. Например, она пресекает попытки изменения системных файлов, добавления в реестр новых данных, открытия сетевого соединения для разнообразных приложений и т.д. Таким образом, Safe'n'Sec может защитить даже от самых новых вирусов, которые еще не были созданы на момент установки программы на компьютер [4].

➘ **Zlock** – утилита для защиты от копирования информации на мобильные накопители. Программа предназначена для разграничения доступа к устройствам и обеспечения реализации правил на разрешение или блокирование доступа в соответствии с заданными политиками доступа клиента и администратора. Например: разграничение/блокирование доступа к устройствам, запись событий и др. [5-6].

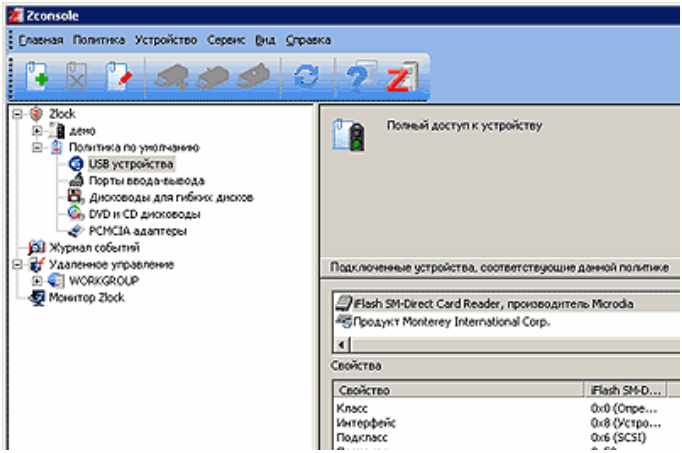


Рис. 4. **Окно программы Zlock**

Наряду с использованием готовых программных продуктов, описанных выше следует рекомендовать: для организации правильной системы разграничения доступа к информации - применение матричного разграничения доступом ко всем электронным файлам и документам предприятия; для защиты операционной системы каждой рабочей станции предприятия – использование всеми сотрудниками в обязательном порядке сложного, трудноподбираемого пароля от 8 символов для санкционированного входа в систему; для правильной работы ОС на всех рабочих станциях фирмы - отключение неиспользуемых служб для защиты компьютеров от внешних угроз [8].

Литература

1) Балина И.В., Гулка З.Н. Защита информации в экономических информационных системах Региональные и международные аспекты К.: Слав. ун-т., 2007. - 125 с.
2) Грушо А. А., Тимонина Е. Е. Теоретические основы защиты информации. М.: Яхтсмен, 2006, с. 192 – 199.
3) Козырев А.А. Информационные технологии в экономике и управлении: Учебник /А.А.Козырев. –СПб.: Изд-во Михайлова В.А., 2000. – 360 с.
4) Конев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с.
5) Мельников В. Защита информации в компьютерных системах. – М.: Электроинформ, 2005.- 102 с.
6) http://www.securit.ru/products/info/zlock/
7) http://www.lwcom.ru/solutions/doc.php?do=read&doc=72
8) http://www.surfcontrol.ru/products/email/

GESTIUNEA RESURSELOR INFORMAȚIONALE UNIVERSITARE

Constantin Sclifos,
Academia de Studii Economice din Moldova

The report presents and discusses the view according to which the information resources of the university need to design and operation of information security system is designed to ensure confidentiality, integrity and availability of information.

Scopul exploatării sistemelor informaționale în universități este de a optimiza consumul de resurse cheltuite necesare colectării, prelucrării, stocării și furnizării spre consumatori a informațiilor necesare.

Sistemul Informațional (SI) reprezintă prin sine un set de elemente componente interdependente, care colectează, procesează, stochează și difuzează informații pentru a sprijini activitățile organizației.

Sistemele informaționale moderne sunt caracterizate de un set de proprietăți-cheie, care afectează în mod semnificativ securitatea informațională și impun cerințe suplimentare față de sistemul de protecție a informației, printre care:

- sistem cu o structură complexă, format din mai multe sub-

sisteme, cu multiple ramificații multifuncționale interdependente între ele, aflându-se totodată într-o relație strânsă cu mediul extern;
- existența unor structuri ierarhice complexe organizatorice, de gestiune, și tehnologice;
- disponibilitatea de unități similare, care au aceleași funcții, cu o structură similară de organizare, și un circuit asemănător de documente;
- număr mare de utilizatori și o diversitate sporită de categorii de personal, care accesează simultan resursele informaționale;
- prezența în sistemul a informațiilor confidențiale, securitatea căreia este necesară a fi asigurată în conformitate cu legislația în vigoare. [1]

Utilizarea tehnologiilor informaționale în sistemul universitar poate fi separată în mai multe etape:

1. Prima etapă se caracterizează prin utilizarea calculatoarelor în scopul automatizării locurilor de lucru din cadrul Universității. Transmiterea de informații, la această etapă, se realizează prin intermediul unor medii de stocare externe.
2. Pentru a doua etapă este caracteristic schimbul de informații prin intermediul rețelelor locale, în limitele unor grupuri individuale variate, utilizarea unor medii de operare, a produselor software, cu acces la rețelele externe, inclusiv pe Internet (sau fără acces la rețelele externe și Internet).
3. În a treia etapă de extindere a SI a universității în mare este finalizată tranziția de la aplicații locale de software, menite să automatizeze procesele și activitățile individuale, care se bazează pe culegerea și exploatarea datelor la nivel local, către sisteme informaționale de tip client-server corporative, oferind astfel accesul utilizatorilor la bazele de date operative ale universității. A fost soluționată problema de integrare a datelor, generate în cadrul unei diversități de subsisteme informaționale, ceea ce permite perfecționarea business procese și prin aceasta îmbunătățirea procesului de gestiune și luare a deciziilor.
4. În stadiul actual sistemele informaționale sunt caracterizate printr-un grad avansat de integrare a aplicațiilor software existente, capabile să automatizeze procesele și activitățile susținute în cadrul instituției și unificarea formatelor utilizate pentru circuitul de documente etc.

În procesul de proiectare și exploatare a sistemului informațional utilizat în scopuri universitare premisele de bază sunt:

- Bază legislativă, normativă și cea științifică;

- Structura și sarcinile organelor (diversificată pe subdiviziuni) menite să asigure securitatea IT;
- Procedeele și metodele tehnico-organizatorice precum și măsurile de securitate (politica de securitate informațională);
- Modalitățile tehnice și mijloacele software de asigurare a securității informaționale [2].

Activitățile unei instituții de învățământ superior solicită prezența unei varietăți informaționale, sub aspectul reglementării accesului și utilizării acesteia, care poate fi deschis sau restricționat, și care intră sub incidența legilor privind secretele de stat, secretele comerciale, sau cele referitoare la datele personale etc.

Activitatea și dezvoltarea instituțiilor de învățământ superior este funcție de managementul instituției și de procesele decizionale. Deciziile pot fi eficiente numai în cazul în care informațiile, de colectare și analiză ulterioară, sunt relevante, complete, corecte și coerente.

În raportul de față este prezentat și pus în discuție punctul de vedere conform căruia resursele informaționale ale universității solicită proiectarea și funcționarea unui sistem de securitate informațională, conceput pentru să asigure confidențialitatea, integritatea și accesibilitatea informațiilor.

Bibliografie selectivă:

1. Демурчев Н. Г. «Проектирование системы разграничения доступа автоматизированной информационной системы на основе функционально-ролевой модели на примере высшего учебного заведения» автореферат на соискание ученой степени кандидата технических наук, Ставрополь, 2006
2. Домарев В. В. Безопасность информационных технологий. Системный подход - К.: ООО ТИД Диа Софт, 2004. — 992 с.
3. Крюков В.В., Шахгельдян К.И. Развитие информационной инфраструктуры вуза для решения задач управления - Университетское управление. 2004. № 4(32). С. 67-77
4. Гергенов А.С. Информационные технологии в управлении. Учебное пособие Издательство ВСГТУ, Улан-Удэ, 2005
5. Герасименко В. А. Защита информации в автоматизированных системах обработки данных — В 2-х кн.: М.: Энергоатомиздат. 1994

ПРАКТИЧЕСКИЕ АСПЕКТЫ РАЗРАБОТКИ И ВНЕДРЕНИЯ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Михаил Нищий,
зксперт (Республика Молдова)

The purpose of this article is to discuss practical aspects of the development and implementation of information security policy in an organization providing social services to the population

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

Под политикой информационной безопасности в данной работе понимается: разработанный в соответствии с требованиями международных стандартов нормативный документ, определяющий правила и требования информационной безопасности, систему мер, порядок действий. Документы, разработанные для внедрения политики ИБ, должны определить: зоны ответственности сотрудников организации за информационные ресурсы, за применение требований ИБ в своих зонах ответственности, регламентацию механизмов контроля в определенной области обеспечения безопасности.

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.

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 ин-

формационной 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.

Аудит ИБ представляет собой комплекс мероприятий получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности в компании, проводимый независимыми экспертами в соответствии с бизнес-процессами компании и международными стандартами. В соответствии с поставленными целями была определена область аудита и объекты аудита. Аудит ИБ позволил установить соответствие уровня информационной безопасности организации выдвигаемым внутренним требованиям, требованиям действующего законодательства и международных стандартов.

Проведенный аудит основывался на следующих принципах: 1) применение моделей нарушителей, как внутреннего нарушителя, так и внешнего нарушителя; 2) определение области проведения аудита; 3) анализ влияния выявленных уязвимостей на защищенность всей информационной системы в целом и отдельных ее компонент; 5) поиск новых уязвимостей; 6) наличие строгой системы классификации уязвимостей.

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

По результатам материалов детального отчета и анализа, проведенного аудита системы управления ИБ и в соответствии с согласованными требованиями в области ИБ, были разработаны основные документы по ИБ, в том числе, Концепция ИБ, Политика ИБ, основные Регламенты и другие организационные и распорядительные документы .

Для внедрения процессов управления ИТ-рисками в организации был разработан Регламент управления рисками, методика инвентаризации, категорирования и оценки рисков информационных ресурсов организации.

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.

Как показывает практика оценку ИТ-рисков желательно проводить не реже одного раза в год, чтобы можно было гарантировать, что не остались не выявленными новые опасности, а противодействие выявленным рискам осуществляется эффективно. Внутри организации работа по оценке рисков должна быть организована на основании разработанных и утвержденных Регламентов, процедур и инструкций и согласована с риск менеджментом бизнес процессов организации. В целях повышения эффективности и качества работ в данном направлении желательно автоматизировать процессы управления информационными рисками в организации.

Выводы:

1. Политика информационной безопасности – это организационно-правовой и технический документ одновременно. В этой связи при разработке мероприятий по внедрению и реализации политики ИБ необходимо опираться на принцип разумной достаточности и экономической целесообразности.

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. В качестве перспективного подхода, как показывает практика, является использование дистанционного обучения и E: Learning.

Список литературы:

1. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
2. ISO/IEC 17799:2005 Информационная технология. Практические правила управления информационной безопасностью.
3. ISO/IEC 27005:2008 Информационная технология – Методы Безопасности – Управление рисками информационной безопасности.
4. Н.Куканова. Практические аспекты применения международных стандартов безопасности информационных систем. ISO 27001: 2005. http://dsec.ru.

CYBERCRIME - A TREAT FOR SERBIAN ECONOMY

Goran Milovanovic, Nada Barac, Aleksandra Andjelkovic,
Faculty of Economics, Nis, Serbia

Cybercrime is a growing problem that negatively impacts Serbian economy. While a lot has been done to combat cybercrime over the then years, criminals still have the upper hand. Serbian IT experts are excited to be able to share their expertise with law enforcement around the world and join efforts in the fight against ccomputer crime.

***Keywords**: cybercrime, Mafiaboy, Russian Business Network, scope of cybercrimes in Serbia*

1. Cybercrime: Overview

Computer crime or cybercrime is a form of crime where the Internet used as a medium to commit a broad range of potentially illegal activities. Issues surrounding this type of crime have become high-profile, particularly those surrounding hacking, copyright infringement, and pornography.

Generally, computer crime may be divided into one of two types of categories: (1) crimes that target computer networks or devices directly (i.e. malware -malicious code, denial-of-service attacks, and computer viruses); (2) crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device (i.e. cyber stalking, fraud and identity theft, phishing scams, and information warfare). Unauthorized use of computers tends generally takes the following forms: Computer voyeur; Changing data; Deleting data, and Denying service to authorized users (DoS attack).

A few well-documented cases include the following:

-The Yahoo! website was pinged at the rate of one gigabyte/second by MafiaBoy at 10:30 PST on Monday, 7 February 2000. The attack lasted for three hours. On February 9, the same technique was extended to Amazon.com, eBay.com, Buy.com and CNN.com.[1] As a result of the attacks, a number of firms formed a consortium to fight DDoS attacks.[2] Investigation by the RCMP and the FBI located a 15 year old child in Montreal who used a modem to control zombies in his DDoS escapade.[3] On April 15, 2000, the RCMP arrested a Canadian juvenile known as Mafiaboy for the

1 Richtel, M. and S. Robinson (2000), Several Web Sites Are Attacked on Day After Assault Shut Yahoo, New York Times (February 9, 2000); http://www.nytimes.com/library/tech/00/02/biztech/articles/09hack.html

2 Messmer, E. (2000), Web sites unite to fight denial-of-service war, Network World (September 25, 2000).

3 http://www.mekabay.com/overviews/history.pdf

February 8th DDoS attack on CNN in Atlanta.

-Russian Business Network (RBN) was registered as an internet site in 2006. Initially, much of its activity was legal. The RBN, which is notorious for its hosting of illegal and dubious businesses, originated as an Internet service provider for child pornography, phishing, spam, and malware distribution physically based in St. Petersburg. By 2007, it developed partner and affiliate marketing techniques in many countries to provide a method for organized crime to target victims internationally. RBN has no official Web site of its own; those who want to buy its services must contact its operators via instant-messaging services or obscure, Russian-language online forums. It has been alleged that the RBN's leader and creator, a 24-year-old known as Flyman, is the cousin of a Russian politician. Because it is possible that recent cyberterrorism activities, such as the denial of service attacks on Georgia and Azerbaijan in August 2008, may have been coordinated by the RBN[4].

The global recession will lead to a rise of cybercrime worldwide. Security firm McAfee's annual Virtual Criminology report says approximately 1.5 million pieces of unique malware identified by the end of 2008, more than in the previous five years combined[5]. The United States has bypassed China as the biggest purveyor of malware as well as sends the most spam worldwide[6]. Not only is the United States relaying the most spam because too many of its computers have been compromised and are under the control of hackers, but it's also carrying the most malicious websites.

2. Cybercrime in Serbia

Organized cybercrime has taken root in Serbia. It doesn't have response mechanisms, laws, infrastructure and investigative support set up to respond to the threat quickly. It is evident that Serbia needs an organization that facilitates transnational law enforcement cooperation.

Serbia's Republic Agency for Telecommunications (RATEL) published on 21 July 2008 a document that contains the technical requirements for authorized monitoring of some telecom services and provides a list of obligations for the telecom operators. The Internet Service Providers (ISPs) are obligated to enable governmental bodies to access updated databases with personal data on users, contracts, maximum speed of data transfer, identification addresses as well as access to database about email users. Also, ISPs are obligated to provide hardware and software for passive monitoring in real time, collecting and analysing Internet activities, statistics, inter-

[4] http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare.html

[5] Matthew Harwood, Cybercrime Trends Will Worsen in 2009, According to Forecasts, Security Management, 12/10/2008.

[6] SOPHOS, Security Threat Report: 2009.

ception of email, attachments, web mail, IP video traffic, phone traffic, interception of IM traffic, peer-to-peer networks, service of email and forwarding the email content towards the centre of governmental bodies for supervision. ISPs will have to let the police access their databases, including users' e-mail content or browsing history[7]. This regulation seems to be the Serbian version of the data retention directive, since the scope is defined as fighting cyber crime and terrorism.

In Serbia cybercriminals are exploiting the global recession by luring in susceptible victims through the promise of easy money. While Serbian government and law enforcement have their attention diverted by the economy, the door is left open for cybercriminals to continue targeting bank balances and drop in consumer confidence, which is essential to Serbian economy recovery.

On 7 December 2009 an OSCE organized in Belgrade investigation training course for cybercrime experts in South-Eastern Europe on combating malicious software and worms. Fifteen computer crime experts from Serbia and neighboring countries took part in the course, which highlighted techniques used by computer criminals. The course marked the first time the OSCE's Strategic Police Matters Unit has partnered with the commercial sector to offer training for police officers[8].

In Serbia cybercriminals are increasingly focusing on Adobe PDF and Flash files, to infect victims with malware. In addition, they use rich content applications such as Flash files to distribute malicious code. Flash-based ads on the Web, because their binary file format, enable the cybercriminals to hide their malicious code and later exploit end-user browsers to install malware.

Three developments will influence the increase in cybercrime in Serbia. First, as more IT experts get laid off, some will shift into illegal activity to make money. Second, cybercriminals will be a main beneficiary of Serbian government's pledge to bring broadband Internet access to every Serbian citizen. Finally, cybercriminals will increasingly to exploit the best Web 2.0 technologies, such as Trojan technologies, to maximize their illicit gains.

Hackers have been breaking into Facebook and MySpace and implanting malware to distribute to a victim's social network. Serbian IT professionals are already aware of this risk.

The solution is increased coordination between national governments. Serbian government needs to commit to funding the resources

[7] Danica Radovanovic, Serbia: New Instructions and Law Regulations on Online Privacy, Global Voices, July 26th, 2008

[8] http://www.osce.org/spmu/item_1_41924.html

needed to combat cybercrime, and to involve in actions across national borders. Consequently, every government, business and individual must play their part in a global battle.

Conclusion

As Serbian economy begin to enter recession it will be more important for individuals and businesses to ensure that they are on guard against internet attack. The optimal way to prevent malicious files is real-time content inspection technologies that can inspect each and every piece of Web content in real-time which may be malicious.

Materialele Conferinței "Securitatea Informațională-2010"
sunt publicate în redacția autorilor.

Semnat pentru tipar 26.03.10.
Coli de tipar 6,94. Coli de autor 5,15.
Tiraj 25 ex.
Tipografia Departamentului Editorial-Poligrafic al ASEM