ACADEMIA DE STUDII ECONOMICE A MOLDOVEI
Laboratorul de Securitate Informațională al ASEM

SECURITATEA INFORMAȚIONALĂ 2018

CONFERINȚĂ INTERNAȚIONALĂ
(ediția a XIV-a)

20-21 martie 2018

Chișinău – 2018

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

COMITETUL DE ORGANIZARE:

Grigore Belostecinic, rector al Academiei de Studii Economice din Moldova, academician, doctor habilitat, profesor universitar (Republica Moldova)
Leszek Fryderyk Korzeniowski, prof. nadzw. dr hab., președintele Asociației Europene pentru Securitate (Polonia)
Tatiana Mișova, doctor, profesor, Academia de Studii Economice din Moldova (Republica Moldova)
Ion Bolun, dr. hab. în informatică, prof. univ., șef catedra Cibernetică și Informatică Economică, ASEM (Republica Moldova)
Anatol Godonoagă, doctor, conf. univ., decan Facultatea de Cibernetică, Statistică și Informatică Economică, ASEM
Veaceslav Perju, doctor habilitat, profesor, Vicepreședinte al Consiliului Național pentru Acreditare și Atestare al Republicii Moldova (Republica Moldova)
Serghei Ohrimenco, doctor habilitat, profesor, Academia de Studii Economice din Moldova (Republica Moldova)
Teodor Țîrdia, doctior habilitat, profesor, Universitatea de Stat de Medicină (Republica Moldova)
Tudor Leahu, doctor, Universitatea Cooperatist - Comercială (Republica Moldova)
Agop Sarkisian, doctor, Academia de Economie (Svistov, Bulgaria)
Vladimir Golubev, doctor, professor, Centrul de Cercetare a Crimelor de Computator (Zaporojie, Ucraina)
Igor Sofronescu, Locotenent-colonel Dr. Conf. Profesor al Academiei Militare a Forțelor Armate "Alexandru cel Bun" RM
Viktor Blagodstskih, doctor, profesor, Universitatea Tehnică de Stat din Moscova, de automobile si constructii rutiere (MADI) (Moscova, Rusia)
Veselin Dimitrov Popov, doctor, Academia Economică (Svistov, Bulgaria)
Olga Pugaceva, doctor, Francisk Skorina Gomel State University (Gomel, Belarus)
Anatol Prisacaru, doctor, conf.univ. șef catedră Tehnologii informaționale, ASEM (Republica Moldova)
Valerii Domarev, doctor, expert (Ucraina)
Andrzej Augustynek, doctor, AGH University of Science and Technology (Krakow, Polonia)
Vladimir Skvir, doctor, expert, Universitatea Politehnică Națională din Lvov (Lvov, Ucraina)
Serghei Kavun, dr. hab., Institul de banking din Harkov al Universității de Banking a Băncii Naționale din Ucraina (Harkov, Ucraina)
Constantin Sclifos, MCP, expert, Academia de Studii Economice din Moldova (Republica Moldova)
Vitalie Spînachi, LL.M., expert, primar s. Cărbuna (r-nul Ialoveni, Republica Moldova)
Tatiana Monasterska, dr., The President Stanisław Wojciechowski Higher Vocational State School in Kalisz (POLAND)
Ghenadie Ciobanu, PhD, cercetător principal, Institutul Național de Cercetare Științifică în Domeniul Muncii și protecției sociale (București, România)
Alexei Smirnov, doctor, profesor universitar, Universitatea Tehnică Națională Centrală din Ucraina (Kropivnitsky, Ucraina)
Altukhova Natalya, PhD, Universitatea financiară în Guvernul Federației Ruse (Moscova, Federația Rusă)
Zachosova Nataliia, Doctor of Economic Sciences, The Bohdan Khmelnytsky National University of Cherkassy (Cherkassy, Ukraine)
Serghei Portarescu, doctor, conf.univ. director MACIP-ASEM (Republica Moldova)
Tudor Bragaru, doctor, conferențiar universitar, Departamentul de Informatică, Facultatea de Matematică și Informatică, Universitatea de Stat din Moldova (Republica Moldova)
Mihail Butnari, Șef Direcția Tehnologii Informaționale, IS Posta Moldovei (Republica Moldova)
Dimitar Georgiev Velev, Prof., dr., University of National and World Economy (Sofia, Bulgaria)
Valeriu Cernei, expert, Moore Stephens Moldova, CISA, CRISC, ITIL (Republica Moldova)
Alexandru Donos, Co-președinte al organizației publice pentru protecția datelor cu caracter personal «ProDataLex», expert in domeniul cryptografiei, SRL "Compania Dekart"
Anatoly Krapivensky, Ph.D. in Sociology, Institute of Youth Policy & Social Work (Volgograd, Rusia)

Descrierea CIP a Camerei Naționale a Cărții
"Securitatea informațională 2018", conferință internațională (14 ; 2018 ; Chișinău). Securitatea informațională 2018 : conferință internațională, (ediția a 14-a), 20-21 martie 2018 / com. de org.: Grigore Belostecinic [et al.] ; coord. ed.: S. Ohrimenco. – Chișinău : ASEM, 2018. – 194 p. : fig., tab. Antetit.: Acad. de Studii Econ. a Moldovei, Lab. de Securitate Informațională al ASEM. – Texte : lb. rom., engl., rusă. – Rez.: lb. engl. – Referințe bibliogr. la sfârșitul art. 1 disc optic electronic (CD-ROM) : sd., col.; în conteiner, 15 x 15 cm.Cerințe de sistem: Windows 98/2000/XP, 64 Mb hard, PDF Reader.
ISBN 978-9975-75-910-6.
004.056(082)=135.1=111=161.1
S 40

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

ISBN 978-9975-75-910-6.

ORGANIZATORII CONFERINȚEI:

ACADEMIA DE STUDII ECONOMICE A MOLDOVEI
www.ase.md

LABORATORUL DE SECURITATE INFORMAȚIONALĂ
www.security.ase.md

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

SPONSORI:

Business
Solutions
Development

Consulting & Trainings

MAKE IT SECURE

Cuprins:

ПРОБЛЕМЫ, РИСКИ И ПЕРСПЕКТИВЫ БИТКОИН КАК МИРОВОЙ КРИПТОВАЛЮТЫ

Балина Ирина Витальевна, Славянский университет,
Директор Центра информационных технологий
и дистанционного обучения,
доктор экономики, конференциар университар
balina_i_v@mail.ru

The research of the phenomenon of crypto currency bitcoin was carried out. At the level of technology and economic feasibility, the main problems and risks are formulated. The prospects of development as a world reserve currency are determined.

Биткоин (Bitcoin, BTC) в настоящее время стал явлением, которое не замечать уже нельзя.

Являясь криптовалютой он обладает рядом особенностей, которые одновременно можно описывать и как **проблемные** с точки зрения технологической и экономической составляющих. Систематизация может выглядеть следующим образом:

- *Децентрализованность* – биткоин не контролирует ни одно учреждение в мире. Валюта заявлена создателем под псевдонимом Сатоши Накамото (Satoshi Nakamoto) для мгновенного обмена в электронном виде при минимальных издержках без любой центральной власти.
- *Относительная ограниченность производства* – согласно коду max можно создать 21 млн биткоинов, но как цифровая валюта он может быть разделен на сатоши (= 0,00000001 BTC).
- *Независимость валюты* - биткоин как чистая математика, не привязан в отличие от других валют ни к золоту, ни к другим эквивалентам.
- *Открытость кода* - исходный код скрипта опубликован в открытом виде и практически любой пользователь в любом месте мирового экономического пространства может просмотреть принципы его работы, запустить скрипт по производству (maining) биткоинов на ПК и выступить в функции мини-Центробанка.
- *Простота в использовании, анонимность и прозрачность в Bitcoin* – биткоин кошелёк полностью анонимен и одновременно полностью прозрачен, имеется возможность создавать бесконечное количество биткоин адресов без привязки к имени, адресу или любой другой информации. Для полной анонимности обычно используют один биткоин адрес для единственной транзакции. Комиссия за транзакции ничтожно мала.

Исторически время появления биткоин определяется как 31 октября 2008 года, когда Сатоши Накамото опубликовал статью «Bitcoin: A Peer-to-Peer Electronic Cash System»[1],[2] в списке рассылки о криптографии (*The Cryptography Mailing list*) metzdowd.com [3], в которой описал Биткойн как полностью децентрализованную систему электронной наличности, не требующую доверия третьим сторонам. В начале 2009 года он или группа лиц, скрывающихся за этим именем выпустили первую версию биткойн-кошелька и запустили сеть Биткойн.

При этом, не смотря на то, что реальность разработчика не подтверждена каким – либо физическим лицом, он, по данным журнала Forbes, в 44 редакции должен был занять 50 место в списке богатейших людей мира с оценкой состояния в $19,4 млрд. (при курсе биткоина $19771) непосредственно после со-основателя Microsoft Пола Аллен и вдовы Стива Джобса — Лорен Пауэлл Джобс, а также шведского предпринимателя и совладельца компании H&M Стефан Перссон. Для справки в октябре 2017 года Сатоши Накамото занимал 247 место в списке богатейших людей при оценке состояния в $5,9 млрд.

Сформулируем основные **риски**, наблюдаемые с криптовалютой биткоин.

1. Отсутствие централизованного контроля над биткоин как платежным средством со стороны государств и финансовых систем сторонники криптовалют считают плюсом биткоин и минусом современных платежных систем, выступая защитой от острых негативных тенденций.

Однако, опасность полной анонимности и бесконтрольности переводов денег, пусть и виртуальных, связана с тем, что такими свойствами "криптоденег" легко могут воспользоваться в криминальных целях такие преступники как финансовые махинаторы, наркодельцы. Что подтверждается неоднократными предупреждениями относиться к криптовалютам с чрезвычайной осторожностью.

2. Наличие у биткоина достаточно высокой степени волатильности, т.е. высокой амплитуды колебаний графика стоимости в эквиваленте к классическим валютам.

Высокая волатильность биткоина как ключевой параметр безопасности резервной валюты, показанная на рис.1., свидетельствует о неустойчивости или даже отсутствии фундаментальной базы стоимости криптовалюты.

У таких торговых инструментов как реальная (фиатная) валюта или акции, есть реальная материальная база. У акций это эквивалент рыночной стоимости действующего бизнеса, у классических валют – курс, который в немалой степени зависит от политики государства и политики центробанков, регулирующих денежное обращение и контролирующих риски для пользователей денежными средствами. У биткоина - же как стремительный рост его стоимости, так и стремительное падение зависит от баланса спроса и предложения, а также от классических психологических моделей поведения людей [4].

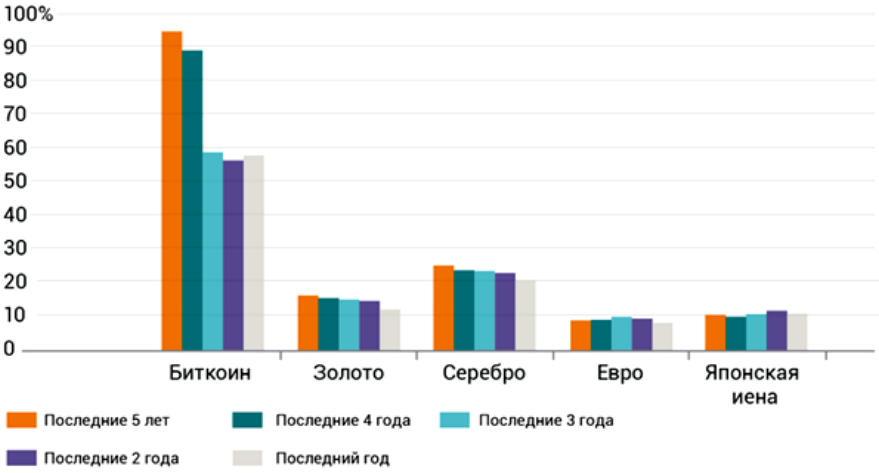


Рис. 1. **Стандартное отклонение дневной доходности в годовом исчислении**
Источник: Bloomberg, Bofa Merrill Lynch Global Reseach

Следует подчеркнуть, что рынок акций тоже достаточно волатильный. Но ключевое отличие акций от биткоина – это то, что у акций есть реальные, материальные активы, со своей реальной стоимостью, ниже которой стоимость акций вряд ли упадет. Предсказать на перспективу каким будет курс биткоина просто нереально. Примером может являться сравнение изменения курса биткоина в течение выборочных наблюдений по состоянию на 28.02.2018 г. и 01.03.2018 г., показанных на рис.2. и описанных ниже.

Рис. 2. **Курс биткоин по состоянию на 01.03.2018 г.**
Источник: https://www.fxclub.org/markets/crypto/bitcoin/

По итогам выборочных наблюдений 28.02.2018 г. на период времени 12^{07} курс составил $10 709,990, изменение за сутки 5,40%, на 12^{08} курс составил $10 702,400, изменение за сутки 5,33%, на 23^{16} - курс составил $10 669,990, изменение за сутки 5,01%. 01.03.2018 г. на период времени 12^{07} курс составил $10 620,990, изменение за сутки 2,90%. Таким образом, имеется неконтролируемость и непредсказуемость курса в течение рассмотренного периода.

В целом изменения курса биткоин за период своего существования приведены ниже: 2008 — (Запуск валюты) 2009 — (1000 BTC = 0.003 $) 2010 — (1 BTC = $0.50) 2011 — (1 BTC= $10) 2012 — (1 BTC =$10) 2013 — (1 BTC= $600) 2014 — (1 BTC= $310) 2015 — (1 BTC= $360) 2016 — (1 BTC= $940) 2017 — (1 BTC= $????) [5].

3. Одним из рисков использования биткоин является то, что на текущий момент можно констатировать, что порядка 4 млн. биткоинов уже утеряны навсегда – исследование
4. Использование on-line валюты и биткоин, в том числе, осуществляется на фоне спорности правовых вопросов существования данных валют в мировом пространстве, приводящих в целом к нерегулируемости глобальной экономики.

Цифровые деньги, популярность и спрос на которые растёт с момента создания биткоин в 2009 г., могут стать инструментами для анонимных Internet – преступников и угрозой нерегулируемости глобальной экономики.

Всего в мире в настоящее время насчитывается порядка 10 криптовалют. На рис. 3 показан список номинальной стоимости и изменения за сутки курсов основных мировых криптовалют.

Инструмент	Текущая цена	За сутки
Ethereum	862,920	1,00%
Bitcoin Cash	1 272,610	4,57%
Ripple	0,94660	8,06%
Litecoin	208,41000	3,27%
IOTA	1,96160	5,74%
DASH	601,080	1,99%
Monero	296,752	4,71%

***Рис. 3.* Курсы криптовалют по состоянию на 01.03.2018 г.**

Источник: https://www.fxclub.org/markets/crypto/bitcoin/

Транзакции, возникающие при использовании и обмене on-line валюты, способствуют возможности упрощения уклонения от уплаты налогов для

физических лиц, т.к. способ обмена сложно и в некоторых случаях невозможно отследить. Также принцип анонимности системы большинства могут служить более простым средством для отмывания денег. В отличие от отмывания денег через сложную сеть финансовых игроков и оффшорных банковских счетов, отмывание денег через цифровую валюту может быть достигнуто посредством анонимных транзакций [6].

5. Развернутая в сети Internet дискуссия о целесообразности выбора для проекта биткоин языков программирования позволила выявить у технологии Lightning Network (решения для масштабирования сети биткоина) ряд очевидных недостатков, одним из которых является использование языка программирования C из-за частых ошибок сегментации.

Об очевидных проблемах Lightning Network заявил разработчик Bitcoin Core Питер Тодд, отметив, что ошибки сегментации, возникающие при попытке обращения к недоступным для записи участкам памяти или при попытке изменения памяти запрещенным способом, приводят к провалу многих платежей [7]. Из чего следует однозначная рекомендация не полагаться на Android-кошелек Eclair, поскольку уже имеются случаи потери средств, используя данный сервис. Отбросив язык программирования C и Python, разработчик отдал предпочтение Rust, посчитав его самым подходящим для технологии Lightning.

В целом в нынешнем формате отмечается уязвимость к DoS-атакам как на P2P-уровне, так и на уровне блокчейна [8].

Исследуем основные **перспективы** использования биткоин как мировой валюты.

В качестве основных перспектив использования биткоин в качестве новой расчётной единицы является то, что данная криптовалюта воспринимается как альтернатива национальным валютам, в которой отсутствует порок монопольности эмиссии, находящейся в руках монетарных властей [9].

Этому будут способствовать анонимность тразакций, быстрота перевода средств и сложность кражи и подделки в отличие от реальных денег. Таким образом, продолжится рост стоимости биткоина, а транзакции в биткоинах всё больше будут замещать транзакции в национальных валютах. Что впоследствии может привести к тому, что биткоин станет одной из резервных мировых валют.

Не следует забывать о возможном противодействии централизованных властей ведущих мировых экономик, таких как Китай и др. В процессах применения биткоин придется преодолевать жесточайшее сопротивление центробанков и правительств, которым это угрожает утратой рычагов влияния на экономику [10].

Однако, сама технология блокчейн как огромной базы данных общего пользования, функционирующей без централизованного руководства, определяет потенциальную возможность создания будущей общемировой валюты. И именно здесь реальным становится преимущество криптографических методов и надёжность

способов эмиссии валюты без наличия единого эмиссионного центра. При этом сама эмиссия такой валюты должна быть неограниченной и привязанной не к мощности современных вычислительных средств и систем. Например, эмиссия может производиться в распределённой базе мировых экономик, и её новый объём может быть привязан к приросту каждой экономики. А саму эмиссию должны будут подтвердить другие участники этой распределённой базы.

В настоящее время американскими компаниями заявлено о проработке запуска специальных спутников, через которые будут проходить биткоин-транзакции по всему миру, даже без доступа к интернету.

В 2017 году начал развиваться новый сегмент криптовалютного рынка — лендинг. Он представляет собой частное кредитование с использованием криптовалют. Одной из главных предпосылок к развитию данного направления стало отсутствие возможности у обладателей больших криптовалютных капиталов использовать их для личного потребления иным путем, кроме продажи. Так, после достижения биткойном цены $17 тыс. общая капитализация данной криптовалюты достигла $300 млрд. При этом около 40% биткойнов принадлежат примерно одной тысяче владельцев, многие из которых не хотят продавать их немедленно [11]. Несколько стартапов предложили решение данной проблемы: они обеспечивают всем желающим возможность предоставления и взятия займов, номинированных в различных криптовалютах. В число наиболее известных лендинговых платформ по состоянию на конец 2017 года вошли Salt Lending, Nebeus, CoinLoan, EthLend, Unchained Capital, Othera, Everex. Одни из них привлекают криптовалютные средства путем продажи токенов, после чего выдают займы от своего лица, другие просто выступают в качестве посредников, помогая кредиторам и заемщикам заключить сделки друг с другом [12].

Выводы:

С точки зрения перспективности открытым остаётся принципиальный вопрос о том, стоит ли вообще вкладывать деньги в биткоин. Рассмотренные и кратко описанные особенности и риски биткоин не позволяют дать однозначно положительный ответ.

Не следует рассматривать биткоин как объект инвестиций, а как предмет кратковременной (возможно и спекулятивной) игры биткоин практически идеален.

Ограниченность законодательной трактовки биткоин и др. видов цифровой валюты не позволяют использовать их как расчетное средство (РМ, РФ и др.) и продолжается использование биткоин как средства хранения. Однако, финансовый рынок уже любезно приготовил для этого инструменты, нетребующие вхождения в сложные сетевые взаимоотношения владельцев биткоинов. Уже сейчас существуют или проходят стадию утверждения несколько биржевых фондов вложений в биткоин типа ETF в долларах, евро, франках и шведских кронах. Есть и ряд небиржевых инструментов, так или иначе привязанных к движению цены биткоина. И этот список, конечно, будет расти.

Таким образом, можно констатировать, что феномен биткоина как участника мирового валютного рынка представляет значительный интерес и является предметом дальнейшего изучения и прогнозирования.

Литература:

1. Satoshi's posts to Cryptography mailing list. Mail-archive.com. [Электронный ресурс]. Дата обращения: 25.02.2018 г.
2. Wallace, Benjamin The Rise and Fall of Bitcoin. Wired. — «It seemed doubtful that Nakamoto was even Japanese. His English had the flawless, idiomatic ring of a native speaker». [Электронный ресурс]. Дата обращения: 02.02.2018 г.
3. Мащенко П. Л., Пилипенко М. О. Технология Блокчейн и ее практическое применение // Наука, техника, образование. — Олимп, 2017. — № 32. — С. 61-64.
4. Хажиахметова Е. Ш. Криптовалюта - деньги XXI века // Новая наука: от идеи к результату. — Агентство международных исследований, 2016. — № 11-2. — С. 177-179.
5. Курс валют Bitcoin https://jantrish.com/bitcoin/ [Электронный ресурс]. Дата обращения: 01.03.2018 г.
6. Пещеров А. И. Понятие и место криптовалюты в системе денежных средств // Юридическая мысль. — 2016. — Т. 95, № 3. — С. 130-138.
7. Разработчик Bitcoin Core Питер Тодд рассказал о проблемах Lightning Network. [Электронный ресурс]. Дата обращения: 01.03.2018 г. https://forklog.com/razrabotchik-bitcoin-core-piter-todd-rasskazal-o-problemah-lighting-network/
8. Щербик Е. Е. Феномен криптовалют: опыт системного описания // Концепт. — 2017.
9. Рисс В. И. К вопросу о коллективных валютах или частных деньгах // Экономика, управление, и право: инновационное решение проблем. — 2017. — С. 21-23.
10. Алексей Лагутенков Криптовалюты. Правила применения // Наука и жизнь. — 2018. — № 2. — С. 22-26.
11. Options for Borrowing and Lending With Cryptocurrency Are on the Rise. *Bitcoin Magazine*. [Электронный ресурс]. Дата обращения: 14.01.2018 г.
12. These Guys Want to Lend You Money Against Your Bitcoin, Bloomberg, 14 декабря 2017 [Электронный ресурс]. Дата обращения: 15.01.2018 г.

СТЕГАНОГРАФИЯ ЧЕРНО - БЕЛЫХ ИЗОБРАЖЕНИЙ ПРИ ПОМОЩИ ПРЕОБРАЗОВАНИЯ АДАМАРА

Булат К. В.
Студентка группы SI-141
Academia de Studii Economice a Moldovei
Научный руководитель Згуряну А.

Keeping the secrecy of information is of great interest today. Steganography is the art and science of information hiding technique in an appropriate cover carrier like image, text, audio and video media. The major goals of effective steganography are High Embedding Capacity, Imperceptibility and Robustness. In this paper, will be considered a new method for steganography of images with domain transformation, where the Hadamard transform is performed on each 4x4 pixel block of which the image consists, and the secret data is built into the transformation coefficients.

***Keywords**: steganography, PMM (Pixel Mapping Method), Hadamard Transform.*

Введение

Стеганография - это искусство скрывать данные в данных, чтобы никто, кроме получателя, не мог обнаружить и получить скрытую информацию. Слово стеганография происходит от греческих слов «Steganos», что означает «скрытый» и «Graphei», что означает «писать». Именно искусство и наука скрывают данные в соответствующем носителе информации, таком как изображение, текст, аудио и видео. Среди различных типов стеганографии - стеганография изображений - самая популярная из-за ее высокой степени избыточности. В видео стеганографии тот же метод может быть использован для внедрения сообщения [1, 2]. Аудио стеганография вставляет сообщение в звуковой файл как шум на частоте, которая не входит в диапазон слуха человека [3]. Наиболее сложным видом стеганографии является текстовая стеганография или лингвистическая стеганография из-за отсутствия избыточной информации в тексте по сравнению с изображениями или аудио. Как определил Чапман, стеганография текста - это метод использования письменного естественного языка для сокрытия секретного сообщения [4]. Почти все цифровые форматы файлов могут использоваться для стеганографии, но изображения и аудиофайлы больше подходят из-за их высокой степени избыточности.

Сообщение встроено в цифровое изображение через алгоритм внедрения, с помощью секретного ключа. Полученное стего изображение передаётся по каналу в приёмник, где оно обрабатывается алгоритмом извлечения сообщения с использованием того же ключа. Во время передачи стего-изображения оно может контролироваться неавторизованными пользователями, которые будут видеть только передачу изображения без обнаружения существования скрытого сообщения.

Постановка задачи

В этой работе рассматривается специальный стеганографический метод для сокрытия информации в цифровых изображениях. Этот стеганографический метод основан на использовании преобразования Адамара и работает на изображениях с серой шкалой. Этот метод был тщательно протестирован на различных изображениях с различными текстурами и достаточно надёжен, чтобы избежать различных атак, например, добавление шума или сжатие. Результаты эксперимента показывают, что рассматриваемая система успешно сохраняет качество изображений и остаётся незамеченной известными методами стегоанализа.

Преобразование Адамара (также известное как преобразование Уолш-Адамара, преобразование Адамара-Радемахера-Уолша, преобразование Уолша или преобразование Уолша-Фурье) является примером обобщённого класса преобразований Фурье. Оно выполняет ортогональную, симметричную, линейную операцию над действительными числами (или комплексными числами, хотя сами матрицы Адамара чисто вещественны).

Преобразование Адамара обладает значительным вычислительным преимуществом над другими методами. Их унитарные матрицы и преобразования состоят из и вычисляются только с помощью прибавлений и вычитаний, но при этом не задействуют умножения. Следовательно, для процессоров, для которых умножение является трудоемкой операцией, достигается устойчивая экономия.

Алгоритм внедрения преобразование Адамара:

1. Выбирается изображение для роли контейнера и секретное сообщение для внедрения в контейнер;
2. Рассчитывается длина сообщения. Сообщение конвертируется в бинарную форму (каждый символ равен 8 бит);
3. Выбирается блок из стего-изображения размером 4x4 и применяется трансформация Адамара на выбранном блоке;
4. Используя Pixel Mapping Method, вставляется 2 бита сообщения в каждый пиксель выбранного блока, за исключением первой колонки;
5. Применяется обратная трансформация Адамара на выбранном блоке и он перезаписывается в обратно изображение-контейнер;
6. Повторяются шаги 3, 4 и 5 до тех пор, пока общее сообщение не будет внедрено полностью. (Блоки должны быть взяты смежным образом из исходных координат изображения.);
7. Наконец, получается стего изображение в пространственной области.

Алгоритм извлечения:

1. Выбирается стего изображение и длина вложенного в него сообщения.
2. Выбирается блок размером 4 x 4 и на нем применяется преобразование Адамара.
3. Используя метод сопоставления пикселей, извлекается два бита сообщения из каждого пикселя блока (кроме первого столбца).

4. Сохраняется часть сообщения, извлечённого из блока.
5. Повторяются шаги 2, 3 и 4 до тех пор, пока общее сообщение не будет извлечено. (Блоки должны быть взяты смежным образом из исходных координат изображения.)
6. Наконец, получается итоговое сообщение в символьном формате после его преобразования из двоичной формы.

Результаты эксперимента

Результаты эксперимента рассматриваемого метода основывались на двух критериях. Первый критерий - это способность скрывать данные, а второй - незаметность стего изображения, также называемая качеством стего изображения. Качество стего изображения, созданное предлагаемым методом, было исследовано на основе различных показателей сходства изображений и результаты этих исследований показывают эффективность и точность рассматриваемого метода с точки зрения безопасности скрытых данных и различных показателей сходства изображений. Объем скрываемых данных данного метода намного больше, по сравнению с некоторыми другими существующими методами в области преобразования. Кроме того, этот метод является надёжным методом, который позволяет избежать большинство атак, использующих добавление шумов или сжатие изображения. Скрытое сообщение также остаётся незамеченным при попытке обнаружить его при помощи известных методов стего-анализа.

Список источников

1. Н. Моримото В. Бендер, Д. Груль и А. Лу. Методы сокрытия данных. IBM Systems Journal, 35: 313-316, 1996.
2. Г. Доерр и Дж.Л. Дугелэй. Гид-экскурсия по применению водяных знаков на видео. Обработка сигналов: обмен изображениями, 18: 263-282, 2003.
3. К. Гопалан. Аудио стеганография с использованием битовой модификации. В работах Международной конференции IEEE по акустике, речи и обработке сигналов (ICASSP '03), том 2, страницы 421-424, 6-10 апреля 2003 года.
4. Г. Давида М. Чепмен и М. Ренхард. Практический и эффективный подход к крупномасштабной автоматизированной лингвистической стеганографии. В материалах конференции по информационной безопасности, страницы 156-165, октябрь 2001 года.

PROBLEMS OF INFORMATION SUPPLY OF FINANCIAL SECURITY OF THE STATE ESTIMATION

Cherevko Oleksander, Nataliia Zachosova,
Cherkasy National University named after Bogdan Khmelnytsky

The problems of information supply of the state financial security assessment are determined. Recommendations for upgrading the evaluation process and obtaining an assessment with a higher level of reliability have been made.

The quality of information that makes up the database for conducting the research, as well as the skills and abilities of the expert who will conduct the analysis, is extremely important for obtaining a reliable estimate of any calculation indicator.

According to the Methodological Recommendations for Calculating the Level of Economic Security of Ukraine (hereinafter - the Methodology) [1], which are a document recognized at the state level and contain methodological and informational and analytical support for the process of assessing the level of financial security of the country, financial security at the macro level should be assessed in a complex manner, taking into account the indicators of six components of its system: banking security, security of the non-bank financial market, debt, budgetary, currency, monetary security. In total, 32 indicators have been proposed for the assessment of such diverse elements of the financial system, which seems to us insufficient in the current, volatile economic conditions. However, such an amount could also provide an appropriate assessment of the level of financial security, provided that the information base for analytical manipulations is of sufficiently high quality, and in many cases it is not.

Some problems in assessing the level of the financial component of Ukraine's economic security were raised in [2]. It is regrettable to note the fact that in the three years since the previous study, nothing has changed. The composition of the indicators for evaluation has not been revised; at the state level, the evaluation was not carried out, the training of personnel with sufficient knowledge and skills to carry out such an assessment was not started. The first problem that any analyst encounters in an attempt to analyze and assess the level of financial security is data sources. Data for calculating a number of indicators suggested in the Methodology is not easy to obtain, especially given that they need to be and assessed in the dynamics. Despite the fact that the Methodology contains an indication of the source of data, where it is possible to obtain the necessary information, the proposed links to Internet resources are obsolete and not working, the printed publication is often impossible to obtain. Thus, the first problem in assessing the level of financial security of the country is the sources for obtaining data. In our opinion, since most of the necessary data are statistical indicators, the site of the State Statistics Service needs to allocate space for the placement of the necessary information. At the same time, it is not a secret that the statistics reveal a significant delay in time regarding

the moment they characterize. Thus, another problem is the timeliness of obtaining the necessary information. And of course, it raises doubts and concerns about the quality of statistical data, which, in the opinion of many experts, is nothing more than the "average temperature at the hospital".

At the same time, one more problem is that data of different organizations and institutions is needed for calculations. For example, in order to assess the level of banking security, data from the National Bank of Ukraine is needed, to assess the level of security of the non-bank financial sector - information held by the National Securities and Stock Market Commission and the National Commission that regulates financial services markets is needed. To obtain data on the size of the deficit of the state budget of Ukraine, it is necessary to look for and study legislative acts. Thus, the search, selection and preparation of data for the evaluation procedure is a very time consuming process, during which the analyst may not find all the information he needs. Taking this into account, it is advisable to recommend the creation of unified information resources that will contain a set of data necessary to assess the level of financial security of the state. Considering the important role of the three state regulators of financial markets in collecting the necessary data, it should be suggested that they themselves initiated the creation of such an information resource.

However, even with an indication of where to find the necessary data, in many cases it is still difficult to find them. Sites of many organizations and companies are not comfortable enough to use, have extremely complex internal infrastructure and low level of transparency. Therefore one should note another problem of the process of assessing the level of financial security - the complexity of access to the necessary data.

In our opinion, we also need to revise the weighting factors that determine the value of a particular indicator, both for the final level on the component of financial security that it contains, and for its overall level. Thus, the neglect of currency security and the allocation of its specific weight at the level of 0,1686 in the aggregate financial security index (a lower proportion has only the component of the non-bank financial market security - 0,1068) [1] proved to be unjustified when in 2014, precisely because of the sharp change of the hryvnia rate in relation to world currencies, the financial security of the country turned out to be at a record low level, and the economy of Ukraine has fallen into another financial crisis. Proceeding from this, it is necessary to review and once again weigh the importance of each component of financial security at the state level to ensure the process of realizing the financial interests of the country, business and citizens.

Speaking about the most methodological approach to assessing the level of financial security, it is worth noting that in the process of evaluation, experts do not take into account such an important indicator as the personal financial security of the country's residents. The study of foreign information resources related to economic and financial security allows us to conclude that in most developed countries, the understanding of the concept of "financial security" is reduced to a single person - a resident, a citizen, and at the macro level in such a definition is not considered. In the

process of scientific work we came across the results of studies on the financial security of citizens of the United States and of a number of European countries, according to which it was possible to determine whether there are free financial assets of the population, what level of financial literacy of citizens, whether they believe in the domestic banking system and are ready to trust financial institutions their savings. Such information would also be useful in the process of assessing the financial security of Ukraine, especially for analyzing the level of banking security and security of the non-bank financial market.

Thus, we arrive at the conclusion that in order to obtain a reliable assessment of the level of financial security of Ukraine at the current stage, it is necessary to review the methodology of evaluation itself, as well as to simplify the indicators for evaluation due to the lack of information for their calculation; to oblige government regulators of financial markets to publish the information necessary for analysis in a timely manner, without hindering access to the complex architecture of the sites and supplying the necessary data for at least a retrospective three years in order to determine the trends.

References:

1. Про затвердження Методичних рекомендацій щодо розрахунку рівня економічної безпеки України *[On Approval of Methodological Recommendations for Calculating the Level of Economic Security of Ukraine]* : наказ Міністерства економічного розвитку і торгівлі України від 29 жовтня 2013 року № 1277.
2. Зачосова Н.В. *[Zachosova N.V.]* (2015) Особливості аналізу рівня фінансової безпеки держави та значення оцінки стану економічної безпеки фінансових установ у цьому процесі *[Features of the analysis of the level of financial security of the state and the importance of assessing the state of economic security of financial institutions in this process]* // Науковий Вісник Міжнародного гуманітарного університету. Серія «Економіка і менеджмент» *[Scientific Herald of the International Humanitarian University. Series "Economics and Management"]*, №12, 191-194.

ВОПРОСЫ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Дмитрий Дорошев
ГГУ им.Ф.Скорины, г.Гомель, РБ

The digital signature is the integral element of e-economy which proves integrity, the invariance of information after signing. In world practice the legislation on the digital signature develops for the benefit of e-business.

Развитие и широкое применение информационных и коммуникационных технологий являются глобальной тенденцией современного мирового развития. Они имеют решающее значение для повышения конкурентоспособности экономики, расширения возможностей ее интеграции в мировую систему. Роль, которая раньше отводилась традиционным бумажным документам, взяла на себя электронная информация. Проблему установления подлинности электронной информации решает электронная цифровая подпись.

Понятие «электронная цифровая подпись» впервые было предложено Мартином Хеллманом и Уитфилдом Диффи в 1976 году. В то время исследователи всего лишь предположили, что схемы и алгоритмы электронной цифровой подписи могут существовать. Уже в 1977 году специалисты Ади Шамир, Рональд Ривест и Леонард Адлеман разработали первый криптографический алгоритм под названием RSA, который можно было использовать для создания электронной цифровой подписи. В основе RSA лежит задача факторизации произведения двух простых больших чисел.

В девяностых годах электронная цифровая подпись стала активно использоваться в информационных технологиях, прежде всего в банковской сфере.

На текущий момент электронная цифровая подпись получила достаточно широкое распространение и прошла длинный путь от непосредственно математической идеи до реализованной технологии. Эта технология включает в себя совокупность методов, процедур, программных и технических средств, которые относятся к современному практическому применению электронной цифровой подписи.

Постоянно совершенствуется законодательство в сфере регулирования электронной цифровой подписи. Так 12 июня 1996 года Комиссией Организации Объединенных Наций по праву международной торговли (UNCITRAL) был принят типовой Закон об электронной торговле. Целью закона была стандартизация законодательства мировых государств и он был призван облегчить применение средств связи и хранения информации. Закон об электронной цифровой подписи в Германии действует с 1997 года, в США и Австрии – с 2000 года, в Эстонии – с 2001 года.

В Российской Федерации в области электронной цифровой подписи актуален Закон №1-ФЗ «Об электронной цифровой подписи», принятый от 10 января 2002 года. В этом Законе электронная цифровая подпись определяется как информация в электронно-цифровой форме, использующаяся для идентификации физического или юридического лица. С 06 апреля 2011 года действует Федеральный закон «Об электронной подписи» № 63-ФЗ, где определяются два вида электронной подписи: простая электронная подпись и усиленная электронная подпись.

Правовые основы использования электронной цифровой подписи в Республике Беларусь заложены в пункте 2 статьи 161 Гражданского кодекса Республики Беларусь о письменной форме сделки. В данном пункте декларировано, что использование при совершении сделок факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронно-цифровой подписи либо иного аналога собственноручной подписи допускается в случаях и порядке, предусмотренных законодательством или соглашением сторон.

В декабре 2010 года вступил в силу Закон «Об электронном документе и электронной цифровой подписи», в котором определены условия, при исполнении которых электронный документ с электронной цифровой подписью приравнивается к документу на бумажном носителе и имеет одинаковую с ним юридическую силу.

В Республике Беларусь в соответствии с действующим законодательством осуществляется государственное регулирование в сфере технологий электронной цифровой подписи и включает в себя:

- формирование и проведение единой государственной политики в области применения электронной цифровой подписи, которая включает в себя решение концептуальных вопросов в данной сфере, определение принципов применения технологий электронной цифровой подписи, формулировку основных целей применения электронной цифровой подписи;
- утверждение и реализация государственных программ по развитию технологий электронной цифровой подписи в рамках которых ставятся задачи по применению криптографических средств для обеспечения подлинности электронных документов, обрабатываемых в автоматизированных информационных системах документационного обеспечения управления;
- разработка и развитие системы требований к элементам технологий электронной цифровой подписи;
- регулирование отношений в сфере функционирования Государственной системы управления открытыми ключами, работающей под эгидой Национального центра электронных услуг;
- регулирование деятельности субъектов хозяйствования в области технологий электронной цифровой подписи;

- контроль за деятельностью субъектов хозяйствования по использованию электронной цифровой подписи.

В соответствии с Законом «О техническом нормировании и стандартизации» осуществляется создание и развитие системы требований к элементам технологий электронной цифровой подписи. Основными объектами технического нормирования и стандартизации в сфере технологий электронной цифровой подписи являются:

- параметры алгоритмов и процедур создания и проверки электронной цифровой подписи;
- форматы используемых данных, таких как сертификаты открытых ключей, значения электронных цифровых подписей, списки отозванных сертификатов, процедуры хранения и защиты личных ключей и др.;
- средства управления ключами электронной цифровой подписи, программные и программно-технические средства автоматизации деятельности регистрационных и удостоверяющих центров, средства создания копий электронных документов на бумажном носителе и т.д.

В настоящее время в Республике Беларусь активно применяется электронная цифровая подпись при подписании электронных документов и обращений, подаваемых в Министерство по налогам и сборам, таможенные органы, фонды соцзащиты населения, «Белгосстрах», «Белстат» и др. Количество выданных ключей электронной цифровой подписи постоянно увеличивается и составляет в стране около 260 тыс. экземпляров.

Новым направлением использования электронной цифровой подписи является ее применение для доступа к единому порталу электронных услуг и, как следствие, простой и эффективный способ получения государственных услуг и административных процедур в электронном виде.

Литература

1. Комиссаренко, В. В. Регулирование технологий электронной цифровой подписи в Республике Беларусь / Научно-практическая конференция «Комплексная защита информации», 2011.
2. Юницын, А. И. Использование электронной цифровой подписи расширят в Беларуси в 2018 году. https://www.gb.by/novosti/ekonomika/ispolzovanie-elektronnoi-tsifrovoi-podpi [Электронный документ] Дата обращения: 12.12.2017.

СИСТЕМЫ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ: СОСТОЯНИЕ И РЕКОМЕНДАЦИИ ПО ВЫБОРУ

Станислав Голубов
Гомельский государственный университет имени Ф.Скорины

The article discusses the current state of the market of biometric authentication systems, provides recommendations for their choice.

Развитие информационно-коммуникационных технологий, локальных и глобальных сетей, спутниковых каналов связи, эффективных технической разведки и конфиденциальности существенно обострило проблему защиты информации, которая является одной из важнейших проблем современности.

К основным программным средствам защиты информации относятся: программы идентификации и аутентификации пользователей КС; программы разграничения доступа пользователе к ресурсам КС; программы защиты от несанкционированного доступа, копирования, изменения и использования и др. Под идентификацией пользователя, применительно к обеспечению безопасности КС, понимается однозначное распознание уникального имени субъекта КС. Аутентификация означает подтверждение того, что предъявленное имя соответствует именно данному субъекту.

Способы защиты информации и других ресурсов постоянно меняются, как меняется наше общество и технологии. Очень важно понять это, чтобы выработать правильный подход к обеспечению безопасности. Поэтому рассмотрим вопросы идентификации личности с помощью биометрических технологий – перспективного и развивающегося направления современных систем контроля доступа.

На данный момент более половины рынка занимают системы распознавания по отпечаткам пальцев. Множество белорусских и зарубежных компаний занимаются производством систем управления доступом, основанных на методе дактилоскопической идентификации. По причине того, что это направление является одним из самых давнишних, оно получило наибольшее распространение и является на сегодняшний день самым разработанным. Сканеры отпечатков пальцев прошли действительно длинный путь к улучшению. Современные системы оснащены различными датчиками (температуры, силы нажатия и т.п.), которые повышают степень защиты от подделок. С каждым днем системы становятся все более удобными и компактными. По сути, разработчики достигли уже некоего предела в данной области, и развивать метод дальше сложно. Кроме того, большинство компаний производят готовые системы, которые оснащены всем необходимым, включая программное обеспечение. Интеграторам в этой области просто нет необходимости собирать систему самостоятельно, так как это невыгодно и займет больше времени и сил, чем купить уже готовую и при этом недорогую систему, тем более выбор будет действительно широк.

Среди зарубежных компаний, занимающихся системами распознавания по отпечаткам пальцев, можно отметить SecuGeni, их USB-сканеры для PC, сканеры, которые можно устанавливать на предприятия или встраивать в замки, SDK и ПО для связи системы с компьютером, BayometricInc. (сканеры отпечатков пальцев, системы контроля доступа, SDK для разработки алгоритмов распознования отпечатков пальцев, встраиваемые модули распознавания отпечатков пальцев), DigitalPersona, Inc. (USB-сканеры, SDK). В СНГ в данной области работают такие компании: BioLink (дактилоскопические сканеры, биометрические устройства управления доступом, ПО), Сонда (дактилоскопические сканеры, биометрические устройства управления доступом, SDK), СмартЛок (дактилоскопические сканеры и модули) и другие.

Удельный вес технологий идентификации по радужной оболочке глаза на мировом биометрическом рынке составляет по разным подсчетам от 6 до 9 процентов [1]. Следует отметить, что с самого начала развития данного метода, его укрепление на рынке замедляла высокая стоимость оборудования и компонентов, необходимых, чтобы собрать систему идентификации. Однако по мере развития цифровых технологий, себестоимость отдельной системы стала снижаться. Лидером по разработке ПО в данной области является компания Iridian Technologies.

Вход на рынок большому количеству производителей был ограничен технической сложностью сканеров и, как следствие, их высокой стоимостью, а так же высокой ценой ПО из-за монопольного положения Iridian на рынке. Эти факторы позволяли развиться в области распознавания радужной оболочки только крупным компаниям, скорее всего уже занимающимся производством некоторых компонентов пригодных для системы идентификации (оптика высокого разрешения, миниатюрные камеры с инфракрасной подсветкой и т.п.). Примерами таких компаний могут быть LG Electronics, Panasonic, OKI. Они заключили договор с Iridian Technologies, и в результате совместной работы появились следующие системы идентификации: IrisAccess 2200, BM-ET500, OKI IrisPass. В дальнейшем возникли усовершенствованные модели систем, благодаря техническим возможностям данных компаний самостоятельно развиваться в этой области. Следует отметить, что вышеперечисленные компании разработали также собственное ПО, но в итоге в готовой системе отдают предпочтение программному обеспечению Iridian Technologies.

На рынке СНГ преобладает продукция зарубежных компаний. Длительное время фирма Папилон уверяла всех, что у них есть распознавание по радужной оболочке. Но даже представители РосАтома — их непосредственного покупателя, для которого они делали систему, утверждают, что это не соответствует действительности.

В последний год на мировой рынок вышло пара новых производителей в связи с истечением первичного патента на распознавание человека по радужной оболочке глаза: AOptix и SRI International.

Распознавание по геометрии лица причисляют к «трем большим биометрикам» вместе с распознаванием по отпечаткам пальцев и радужной оболочке. Надо сказать, что

данный метод довольно распространен, и ему пока отдают предпочтение перед распознаванием по радужке глаза. Удельный вес технологий распознавания по геометрии лица в общем объеме мирового биометрического рынка можно оценивать в пределах 13-18 процентов. В России к данной технологии также проявляется больший интерес, чем, например, к идентификации по радужной оболочке. Как уже упоминалось ранее, существует множество алгоритмов 3D распознавания. В большинстве своем компании предпочитают развивать готовые системы, включающие сканеры, сервера и ПО. Однако есть и те, кто предлагает потребителю только SDK. На сегодняшний день можно отметить следующие компании, занимающиеся развитием данной технологии: Geometrix, Inc. (3D сканеры лица, ПО), GenexTechnologies (3D сканеры лица, ПО) в США, CognitecSystemsGmbH (SDK, специальные вычислители, 2D камеры) в Германии, Bioscrypt (3D сканеры лица, ПО) – дочернее предприятие американской компании L-1 IdentitySolutions. В России в данном направлении работают компании ArtecGroup (3D сканеры лица и ПО) – компания, головной офис которой находится в Калифорнии, а разработки и производство ведутся в Москве. Также несколько российских компаний владеют технологией 2D распознавания лица – Vocord, ITV и др.

В области распознавания 2D лица основным предметом разработки является программное обеспечение, так как обычные камеры отлично справляются с захватом изображения лица. Решение задачи распознавания по изображению лица в какой-то степени зашло в тупик – уже на протяжении нескольких лет практически не происходит улучшения статистических показателей алгоритмов. В этой области происходит планомерная «работа над ошибками».

3D распознавание лица сейчас является куда более привлекательной областью для разработчиков. В нём трудится множество коллективов и регулярно слышно о новых открытиях. Множество работ находятся в конечной стадии разработки. Но пока что на рынке лишь старые предложения, за последние годы выбор не изменился.

Распознавание по рисунку вен руки является довольно новой технологией, и в связи с этим ее удельный вес на мировом рынке невелик и составляет около 3%. Однако к данному методу проявляется все больший интерес. Дело в том, что, являясь довольно точным, этот метод не требует столь дорогого оборудования, как, например, методы распознавания по геометрии лица или радужной оболочке. Сейчас многие компании ведут разработки в данной сфере. Так, например, по заказу английской компании TDSi было разработано ПО для биометрического считывателя вен ладони PalmVein, представленного компанией Fujitsu. Также в сфере идентификации по рисунку вен работают следующие компании VeidPte. Ltd., HitachiVeinID. В России развитие данной ветви биометрических технологий пока активно не осуществляется.

На данный момент выделяют две крупных компаний, занимающихся разработкой программного обеспечения для аутентификации по голосу. Одна из них была организована в 2004 году в Испании и получила название AGNITIO. Их продукт VoiceID в большей степени используется правительственными организациями для

предотвращения злодеяний, выявления преступников и предоставлений доказательств в суде, если такое потребуется. AGNITIO имеет обширную клиентскую базу, включающую полицию, разведку и другие государственные организации в более чем 35 странах. VoiceID также используется в контактных центрах, при совершении финансовых операций, телекоммуникациях и секторе безопасности предприятия. Компания предлагает два вида услуг голосового распознавания: текстонезависимый для решений реального времени и текстозависимый, основанный на произношении чисел для корпоративных работников. AGNITIO не разместила никаких данных о характеристиках FAR и FRR для своего продукта.

Другой компанией, которая добилась немалых результатов в данной области является «Центр речевых технологий» (ЦРТ) — российский производитель электронной техники и программного обеспечения в области записи, обработки и анализа звуковой информации. Основные направления деятельности ЦРТ — развитие мультимодальных биометрических систем и создание комплексных решений для контакт-центров различного уровня. Компания занимается внедрением технологий синтеза и распознавания речи в сфере ЖКХ, автомобильной промышленности и медицинских учреждениях. Также компания осуществляет консалтинговую и образовательную деятельность. Продукт ЦРТ под названием VoiceKey является биометрической платформой для подтверждения личности по голосу в телефонном канале, WEB-кабинете или мобильном приложении. Данное ПО активно используется с другими технологиями компании: системами многоканальной записи, речевой аналитики, шумоочистки и другими. Компания также не предоставила никакой информации и значениях FAR и FRR для VoiceKey.

Выбор какой-либо из систем биометрической аутентификации должен быть хорошо обдуман, проанализированы все преимущества и недостатки, с последующим выделением из них критических, то есть тех, которые обуславливают или, наоборот, препятствуют установке данной системы. Для тех, кто ищет оптимальное решение цены и качества, можно предложить системы распознавания отпечатков пальцев: она довольно распространена и не слишком дорога. Для тех же, кто ищут качественные системы с минимальным количеством ошибок, можно посоветовать системы аутентификации по радужной оболочке глаза, так как она является наиболее защищенной и имеет высокие характеристические показатели. Для энтузиастов и экспериментаторов отлично подойдут «новинки» в сфере биометрии: распознавание по венозному рисунку руки.

Литература

1. Технологии защиты [Электронный ресурс]. – 2017. – Режим доступа: http://www.tzmagazine.ru/ – Дата доступа: 07.02.2018.

ДИНАМИЧЕСКИЕ МЕТОДЫ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Сергей Говейко
Гомельский государственный университет имени Ф.Скорины

On the basis of the analysis of the current state of dynamic methods of biometric authentication, the possibilities of their use for the development of the digital economy in the Republic of Belarus are considered.

Главная тенденция развития современного общества тесно связана с ростом информационной составляющей (информационные ресурсы, информационные технологии и т.п.) и, как следствие, информационной безопасности. Вопросы информационной безопасности на современном этапе рассматриваются как приоритетные. Существующие на сегодняшний день методы и средства защиты информации в автоматизированных системах достаточно разнообразны, что, отражает многообразие способов и средств возможных несанкционированных действий.

Проблема аутентификации пользователя компьютерной системы со времени появления мультипользовательских систем стала весьма актуальной. Особое место в этой теме занимают биометрические методы, которые основываются на уникальности биометрической информации, носителем которой является человек.

Биометрический контроль доступа - это автоматизированный метод, с помощью которого путем проверки уникальных физиологических особенностей или поведенческих характеристик человека осуществляется аутентификации личности. Физиологические особенности, например такие, как капиллярный узор пальца, геометрия ладони или рисунок радужной оболочки глаза, являются постоянными физическими характеристиками человека. Поведенческие же характеристики, такие, как подпись, голос или клавиатурный почерк, находятся под влиянием, как управляемых действий так и психологических факторов, и называются динамическими. Рассмотрим подробнее динамические методы биометрической аутентификации.

Аутентификация по голосу. Биометрический метод аутентификации по голосу характеризуется простотой в применении. Данному методу не требуется дорогостоящая аппаратура, достаточно микрофона и звуковой платы. В настоящее время данная технология быстро развивается, так как этот метод аутентификации широко используется в современных бизнес-центрах. Выделяют три типа голосовой аутентификации:

- текстонезависимая: когда подтверждение личности происходит по спонтанной речи пользователя, т.е. нам не важно, что говорит человек. Это самый долгий метод подтверждения – чистой речи должно накопиться минимум 6-8 сек. Данный способ верификации можно применять скрытно от самого пользователя. Обычно этот способ применяется во время общения абонента с оператором контактного

центра, когда последнему нужно однозначно удостовериться, что абонент именно тот, за кого себя выдает;

- текстозависимая по статической парольной фразе: когда подтверждение личности происходит по парольной фразе, которую на момент регистрации придумал абонент. Парольная фраза всегда одинаковая. Длительность парольной фразы должна быть не менее 3 сек. Обычно предлагается говорить свои ФИО;
- текстозависимая по динамической парольной фразе: когда подтверждение личности происходит по парольной фразе, которую предлагает сама система в момент аутентификации, т.е. каждый раз парольная фраза разная. Обычно предлагается динамическая парольная фраза из последовательности цифр. Пользователь повторяет за системой числа до тех пор, пока она не примет однозначного решения «свой/чужой». Интересно то, то произнесение разных цифр дает разный объем информации: самая «полезная» цифра «восемь» – она больше всего содержит полезной речевой информации, самая бесполезная «два».

Основным и определяющим недостатком метода аутентификации по голосу - низкая точность метода. Например, человека с простудой система может не опознать. Важную проблему составляет многообразие проявлений голоса одного человека: голос способен изменяться в зависимости от состояния здоровья, возраста, настроения и т.д. Это многообразие представляет серьёзные трудности при выделении отличительных свойств голоса человека. Кроме того, учёт шумовой компоненты является ещё одной важной и не решенной проблемой в практическом использовании аутентификации по голосу. Так как вероятность ошибок второго рода при использовании данного метода велика (порядка одного процента), аутентификация по голосу применяется для управления доступом в помещениях среднего уровня безопасности, такие как компьютерные классы, лаборатории производственных компаний и т.д.

Аутентификация по рукописному почерку. Метод биометрической аутентификации по рукописному почерку основывается на специфическом движении человеческой руки во время подписания документов. Для сохранения подписи используют специальные ручки или восприимчивые к давлению поверхности. Шаблон создается в зависимости от необходимого уровня защиты.

Обычно выделяют два способа обработки данных о подписи:

- анализ самой росписи, то есть используется просто степень совпадения двух картинок;
- анализ динамических характеристик написания, то есть для аутентификации строится свертка, в которую входит информация по подписи, временными и статистическими характеристиками написания подписи.

Первый способ сильно подвержен ошибкам, так как является неточным, а также существует возможность подмены подписи злоумышленником. Из-за того, что

подпись не может быть всегда одинаковой, этот метод дает большой процент ошибок. В результате этот способ используется в местах, где точность результата не столь важна или процесс аутентификации контролируется.

Второй же способ очень популярен и развивается до сих пор. Передвижение пера может осуществляться вдоль одной прямой, относительно плоскости или в трехмерном пространстве, точность аутентификации возрастает с увеличением количества осей. В данном способе важна временная характеристика, указывающая на период, затраченный на ввод определенной части подписи. Большинство систем аутентификации по рукописному почерку останавливаются на зависимости перемещения пера от времени. Однако существуют характеристики, которые делают аутентификацию более точной: давление пера на поверхность и наклон пера к поверхности. Давление определяют с помощью специальных поверхностей, фиксирующих силу нажатия пера во время рукописного ввода. Обработка характерных значений наклона пера производится с помощью сложных подсчетов матрицы коэффициентов двумерного дискретного косинусного преобразования.

Метод аутентификации по рукописному подчерку нельзя использовать повсюду - в частности, этот метод не подходит для ограничения доступа в помещения или для доступа в компьютерные сети. Однако в некоторых областях, например в банковской сфере, а также всюду, где происходит оформление важных документов, проверка правильности подписи может стать наиболее эффективным, а главное - необременительным и незаметным способом. До сих пор финансовое сообщество не спешило принимать автоматизированные методы идентификации подписи для кредитных карточек и проверки заявления, потому что подписи все еще слишком легко подделать. Это препятствует внедрению идентификации личности по подписи в высокотехнологичные системы безопасности.

Аутентификация по клавиатурному почерку. Клавиатурный почерк, или ритм печатания, отражает способ печатания пользователем той или иной фразы. В качестве уникальной информации, присущей тому или иному пользователю, можно отметить наиболее очевидные признаки: количество ошибок при наборе, интервалы между нажатиями клавиш, время удержания клавиш, число перекрытий между клавишами, степень аритмичности при наборе, скорость набора. При этом временные интервалы между нажатием клавиш характеризуют темп работы, а время удержания клавиш характеризует стиль работы с клавиатурой - резкий удар или плавное нажатие. Именно анализ этих признаков лежит в основе существующих на сегодняшний день подходов изучения клавиатурного почерка.

Хотя современные исследования показывают, что клавиатурный почерк пользователя обладает некоторой стабильностью, что позволяет достаточно однозначно идентифицировать пользователя, работающего с клавиатурой, на практике часто возникают некоторые проблемы. Так, определено, что работоспособность существующих систем зависит от следующих факторов:

- устойчивости клавиатурного почерка пользователей;
- условий и времени работы;

- психического и физического состояния пользователя.

Особенные трудности выявления клавиатурного почерка могут возникнуть при вводе пользователем пароля, когда полученная информация не превышает десятка символов. Поэтому с целью повысить эффективность аутентификации предлагается искусственно добавить ритм. Пользователю предлагается набирать парольную фразу с заранее известным ритмом (например, под какую-нибудь мелодию). Таким образом, умышленно вносятся дополнительные биометрические характеристики в набор пароля. Возможно, мошеннику удастся получить логин и пароль для входа в систему, ритмику набора украсть представляется невозможным. Кроме того, оказалось, что введение ритма повышает и клавиатурную устойчивость набора пароля пользователем.

Для практического изучения данного метода аутентификации пользователя по паролю с использованием информации о ритме набора было проведено исследование, суть которого заключалось в сборе результатов аутентификации на основе различия ввода парольного слова: с заданным ритмом или без. Уже на начальном этапе изучения ритмики набора парольных фраз были получены хорошие результаты. Оказалось, что введение ритма в набор пароля положительно повлияло на устойчивость почерка пользователя. Даже при наборе коротких паролей отличие ритмограмм разных пользователей было очень заметно. А с удлинением парольной фразы влияние ритма увеличивалось на порядок. Так, корреляция данных нескольких ритмичных наборов одного пользователя колебалась в пределах 0,90-0,99, а для наборов без ритма составляла не более 0,1 [1] .

Следует заметить, что подобные системы не требуют дополнительного оборудования – необходимое программное обеспечение можно легко встраивать в уже готовые продукты. Однако аутентификация с использованием анализа ритмики клавиатурного набора является неисследованной и неприемлема в системах, требующих высокого уровня защиты.

Использование современных методов биометрической аутентификация будет способствовать реализации Декрета Президента Республики Беларусь № 8 "О развитии цифровой экономики" и Государственной программы развития цифровой экономики и информационного общества на 2016 – 2020 годы [2] .

Литература

1. Ивантер Э. В., Коросов А. В. Основы биометрии: Введение в статистический анализ биологических явлений и процессов / Ивантер Э. В., Коросов А. В. – Петрозаводск: ПетрГУ, 1992.
2. Развитие цифровой экономики и информационного общества на 2016-2020 гг. Национальный правовой интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: http://www.pravo.by/ – Дата доступа: 22.02.2018.

AUTENTICITATEA ÎN REȚELELE SOCIALE

Lilian Gudumac Nicolae
Studentul Departamentul: Informatică și Managementul Informației, ASEM

O rețea de socializare este un web site ce care permite utilizatorilor să se socializeze, să-și facă noi prieteni și cunoștințe, să se împartă cu imagini foto, video și de a promova o informație în interiorul ei.

Rețelele de socializare au luat un loc foarte important în viața cotidiană. Acum cu ajutorul unei rețele de socializare utilizatorii pot nu doar să transmită mesaje între ei sau să vadă fotografiile postate de către prietenii săi, acum rețeaua de socializare a devenit un un instrument de lucru în marketing, o platformă de amplasare a știrilor, un blog pentru un politician sau a unei vedete, un instrument de comunicare cu masele unde fiecare postare are o valoare foarte mare.

Deseori utilizatorii nu atrag atenția la ce scriu în public, ce fotografii plasează sau cu-i acordă încredere pe o rețea socială. Neglijența lor îi poate costa reputația sau pierdere financiară.

1. Definirea problemei de autenticitate în rețelele sociale

Un simplu cont care nu are fotografie, care în loc de nume și prenume are un șir de caractere aleatorii ne duce la gândul că acest profil este unul fals sau în engleză FAKE. Foarte des noi trecem pe alături aceste conturi fără a atrage o mare atenție uni asemenea cont. Atâta timp cât acest cont nu ne afectează pe noi avem impresia că totul este bine și nimic rău nu poate să se întâmple. Dar acest cont poate fi folosit ca un instrument de spionaj față de noi și de restul utilizatorilor din această rețea de socializare.

Iată ce pot să întreprindă utilizatorii unui cont inofensiv la prima vedere:

- Vizualizarea datelor personale de pe profilul accesat
- Utilizarea datelor colectate de pe profil în scopuri proprii fără a cere permisiune pentru utilizarea acestor date.
- Vizualizarea preferințelor și a postărilor de către utilizator.
- Posibilitate de a lăsa mesaje publice care pot ave un caracter pozitiv dar și negativ precum și cu caracter de dezorientate care să ducă în eroare pe utilizatori care poate provoca discuții furioase.
- Crearea unui dosar personal pe baza datelor acumulate pe pagina utilizatorului.

Sunt nenumeroase scenarii cu care un utilizator a unui cont FAKE poate utiliza informația utilizatorilor găsită pe paginile lor. Și consecințele pot avea urmări foarte grave pentru acest utilizator până la pierderea contului său și crearea unor situații de amenințare sănătății, vieții și chiar de stat.

2. Esența problemei.

Rețelele de socializare au un nivel foarte slab de verificare a noilor conturi care sunt create pe platforma lor necitând că în fiecare zi ele blochează mii de conturi false.

Utilizatorii plasează pe rețelele sociale foarte multă informație cu caracter personal care permite crearea unui portret de identificare a persoanei pe portalurile de internet iar rețeaua de socializare nu poate impudica răspândirea acestei informații din simplul motiv că utilizatorul o distribuie din lipsă de responsabilitate sau din neștiință că această informație poate fi publică. Astfel într-o rețea de socializare apar foarte multe conturi a utilizatorilor care î-și completează profilul cu o informație falsă cu scopul de salva anonimatul și navigarea pe rețea fără a se teme că numele lui real va fi divulgat, iar alți utilizatori creează conturi false pe rețelele de socializare unde fură identitatea unui om real și apoi acționează din numele lui.

Astfel cu un cont fals pe o rețea de socializare un potențial dușman poate deveni prieten cu un utilizator care nu știe cine se află în spatele acestui cont. Deseori în spatele unui asemenea cont sunt persoane care au menirea să scrie minorilor și î-și creează un cont unde se prezintă ca fiind unul din ei. Astfel el intră în zona de increare și scenariile care vor urma sunt de neștiut. Răufăcătorii pe o rețea de socializare nu se tem că vor fi găsiți, e sunt în siguranță și acțiunile sale pot avea un impact mare asupra unui om, sau a unui grup de oameni, sau chiar poate duce punerea în pericol a oamenilor prin organizare unor acte teroristice.

3. Cine este atras de datele noastre personale

Nu toți utilizatorii înțeleg care date sunt personale care nu, care date pot fi în acces liber și care nu.

Un exemplu clasic este de a posta pe rețelele sociale informația cu privință la o călătorie, un concediu îndelungat cu familia. Pentru noi această fotografie inofensivă, sau anunțarea prietinelor că ai ajuns într-un nou oraș de care ești foarte uimit este o informație inofensivă și pentru majoritatea din noi așa și este dar nu pentru toți. Această informație este foarte de folos pentru un hoț spre exemplu. El primind informația de pe profilul utilizatorului va avea încă un motiv de a face o vizită acestui utilizator. Iar dacă acest utilizatori în postările sale interioare a mai lăsat adresa de locuință a sa, se prea poate ca răufăcătorul să fie de la foarte mulți kilometri de la casa acestuia.

Deci cine este atras de informația noastră?

Atrași sunt în primul rând hoții de date personale care mai apoi le vând pe piața neagră, hoții de date bancare care mai apoi transferă bani pe conturile sale sau fac cumpărături online.

La fel sunt atrași fanii a persoanelor publice și a persoanelor celebre care cu orice preț vor să se manifeste în societate cu așa o cunoștință. Ne mai vorbind că la angajare noi suntem analizați prin prisma profilului nostru și ar fi bine să postă informație care nu ne-ar afecta viața reală în nici un caz.

Din acest motiv, la moment cea mai eficientă modalitate de a ne proteja pe o rețea socială este să limităm postările noastre, să ținem sub control datele cu caracter personal și să fim atenți cu cine vorbim și ce informație divulgăm prin intermediul serviciilor a rețelei sociale.

Concluzie:

Odată cu apariția rețelelor de socializare viața sociala sa schimbat radical, rețelele de socializare au devenit un instrument puternic pentru a ne socializa, ușurința de utilizare captivează tot mai mulți oameni în fiecare zi, iar utilizatorii bucuroși de acest instrument tare des neglijează normele de securitate pe aceste rețele, ei divulgă cu ușurință datele sale personale și creează un mediu favorabil pentru infractorii în spațiul cibernetic. Toate restricțiile și regulile create de către o rețea de socializare nu vor împiedica utilizatorii de a divulga datele personale pe unii, iar pe alții de a se folosi cu ușurință de acestea date utilizând instrumentele rețelei sociale.

Referințe:

1. http://www.kafedramk.ru/content/plyusy-i-minusy-sotsialnyh-setej
2. https://amnesty.org.ru/pdf/SocialmediaBriefingKazakhstanFEB2017RUS.pdf

ЛЕКСИКОГРАФИЧЕСКИЙ АНАЛИЗ ТЕРМИНА КАДРОВОЙ БЕЗОПАСНОСТИ

Царевская Виталия Витальевна

д.э.н., к.т.н., профессор
Кавун Сергей Витальевич

Харьковский учебно-научный институт
ГВУЗ «Университет банковского дела»

Одним из приоритетов в достижении стабильности и процветания предприятия является эффективное обеспечение кадровой безопасности. Такая безопасность является преобладающей, поскольку связана с персоналом, качество которого является основой. Важность кадровой составляющей обусловлена тем, что персонал играет главную роль в эффективной деятельности и конкурентоспособности фирмы.

Отдельные аспекты кадровой безопасности были предметом исследований А. Арефьевой, А. Джобава, З. Живко, А. Кибанова, А. Кириченко, А. Козаченко, А. Литовченко, Н. Логинова, Н. Петрова, Ю. Чаплыгиной, И. Чумарина, А. Шаваева, Н. Швец и др. Несмотря на то, что достаточно многие ученые занимаются изучением понятия «кадровая безопасность», до сих пор не существует единого определения [1].

Для того чтобы провести лингвистический анализ, было собрано популярные определение «кадровой безопасности» на русском и украинском языках; с помощью он-лайн ресурса [2] определены ключевые слова самого определения и статьи в целом, выявлены совпадения. Полученные данные приведены в табл. 1.

Таблица 1

Сводные данные по результатам поиска

№	Авторы	Определение	Ключевые слова; % в тексте		Совпадения ключевых слов
			определения	статьи	
1	А. Кибанов	Процесс предотвращения негативных воздействий на экономическую безопасность предприятия за счет рисков и угроз, связанных с персоналом, его интеллектуальным потенциалом и трудовыми отношениями в целом.	угроза, отношение, трудовой, потенциал, интеллектуальный, персонал, связанный, процесс, предотвращение, риск; 4,1%	безопасность, организация, персонал, обеспечение, система, охрана, средство, кадровый, мерить, деятельность; 1,3%	персонал
2	журнал «Деловой квадрат»	Обеспечение экономической безопасности предприятия за счет снижения рисков и угроз, связанных с недоброкачественной работой персонала, его интеллектуальным потенциалом и трудовыми отношениями в целом.	обеспечение, недоброкачественный, отношение, трудовой, потенциал, интеллектуальный, персонал, работа, экономический, связанный; 4,3%	безопасность, сотрудник, персонал, предприятие, компания, работа, отношение, угроза, кадровый, клиент; 1,1%	персонал, работа, отношение

3	Studme.org	Процесс предотвращения потенциальных и реальных угроз (рисков), связанных с персоналом (использованием трудового потенциала, развитием человеческого капитала, управлением человеческими ресурсами, совершенствованием трудовых отношений и т.д.).	трудовой, человеческий, потенциал, отношение, совершенствование, ресурс, управление, капитал, развитие, процесс; 4,8%	персонал, безопасность, кадровый, предприятие, компания, угроза, экономический, управление, риск, сотрудник; 1%	управление
…					
23	Чередниченко Н.В.	Комплекс дій та взаємовідношень персоналу, при якому відбувається ефективне економічне функціонування підприємства, його здатність протистояти внутрішнім і зовнішнім впливам і загрозам, пов'язаним з персоналом, діагностика та прогнозування впливу персоналу на показники роботи, його інтелектуальний потенціал і трудові відносини загалом.	персонал, комплекс, показник, діагностика, прогнозування, вплив, інтелектуальний, робота, пов'язаний, потенціал; 3%	безпека, персонал, підприємство, працівник, економічний, кадровий, створення, робота, пов'язаний, співробітник; 1,3%	персонал, робота, пов'язаний
24	С.В. Васильчак, І.Р. Мацюняк	Запобігання та попередження негативних впливів від персоналу, захист його самого, створення сприятливих умов для його роботи.	запобігання, попередження, вплив, персонал, захист, створення, сприятливий, умова, робота; 6,2%	безпека, персонал, кандидат, підприємство, служба, кадровий, робота, місце, відбір, менеджер; 1%	персонал, робота
25	К. Г. Гончарова	Процес моніторингу, мінімізації та превенції негативних впливів на економічну безпеку банку через ефективний ри-зик менеджмент загроз та небезпек, пов'язаних з персоналом.	процес, пов'язаний, небезпека, загроза, менеджмент, ризик, ефективний, банк, моніторинг, безпека; 4,7%	безпека, кадровий, персонал, економічний, система, загроза, банк, підприємство, фактор, стан; 1,9%	безпека, загроза, банк
26		Оптимальний стан захищеності персоналу банку від зовнішніх загроз та оптимальний стан економічної захищеності банку від внутрішніх загроз з боку персоналу.	оптимальний, стан, захищеність, персонал, банк, загроза, зовнішній, економічний, внутрішній, сторона; 8%		персонал, економічний, загроза, банк, стан
27	Н.С. Різник	Процес запобігання негативним впливам на безпеку банку через ри-зики, загрози та небезпеки, пов'язані з персоналом, його інтелекту-альним потенціалом і трудовими відносинами.	небезпека, трудова, потенціал, інтелектуальний, персонал, пов'язаний, процес, запобігання, загроза, ризик; 4,7%	безпека, кадровий, банку, персонал, працівник, політика, організація, забезпечення, менеджмент, соціальний; 1,6%	персонал
28	А.Мітрофанов	Становище організації як соціальної спільності й індивіда в ній, за якого вплив на них із боку природного, економічного й соціального середовищ, а також внутрішнього середовища самої людини не здатні заподіяти шкоди.	соціальний, середа, положення, природний, заподіяти, людина, внутрішній, економічний, сторона, організація; 3,8%	підприємство, кадровий, безпека, рішення, проблема, економічний, пов'язаний, персонал, управлінський, управління; 1,4%	економічний

Таким образом, по результатам лингвистического анализа выбранной категории «кадровой безопасности», авторами было определено множество ключевых тегов - персонал, работа, отношения, управления, угроза, трудовая, предприятие, предотвращения, потенциал, экономический, связанный, риски, обеспечения, состояние - которые отображении на рис. 1. Распределение рангов после сортировки по возрастанию значения ранга для всех определений приведены на рис. 2.

Рис. 1. **Облако тегов всех определений**

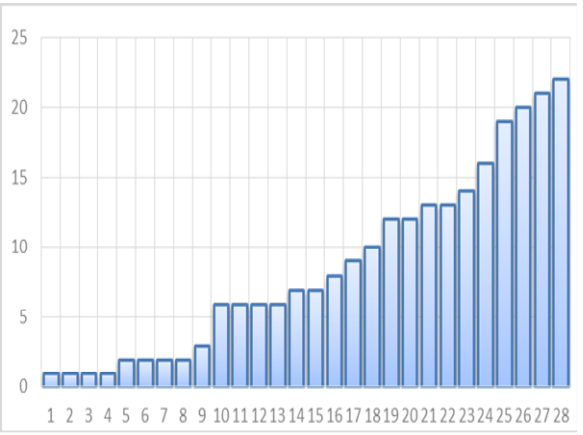


Рис. 2. **Распределение рангов**

Это позволило сформировать конечное определение термина «кадровой безопасности» с помощью лингвистического анализа [3], суть которого – **состояние работы и управления персоналом, связанное с предотвращением возникновения угроз и рисков и обеспечением роста экономического и трудового потенциала предприятия**. При этом средний процент применения ключевых слов в контексте составил 3,1%. Средний ранг ключевого слова в облаке тегов равна 9,2. Диапазон процента применения ключевых слов в контексте от 0,6 до 8.

Таким образом, авторами было доказано обоснованное определения тега «кадровой безопасности», которое, по их мнению, является более уместным и приятным для дальнейшего применения.

Список литературы

1. Кадрова безпека підприємства: поняття, структура та основні механізми її забезпечення [Электронный ресурс] – Режим доступа: http://naukajournal.org/index.php/naukajournal/article/view/96/133
2. Аналіз тексту он-лайн [Электронный ресурс] – Режим доступа: https://istio.com/rus/text/analyz/#top
3. Кочан І. М. Лінгвістичний аналіз тексту: Навч. посіб. — 2-ге вид., перероб. і доп. — К.: Знання, 2008. — 423 с.

ПРИМЕНЕНИЕ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ ДЛЯ ПОВЫШЕНИЯ НАДЕЖНОСТИ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ

Кешку А.А.
Студент SI-141
Экономическая Академия Республики Молдова
Научный руководитель Згуряну А.

Password authentication is no longer sufficient to protect valuable data. However, the decisive factor is the cost of the system. In any case, the technologies go forward and every year more and more systems and authorization models are introduced, which are obliged to protect us and our information from third parties.

Keywords: *Authorization, Multifactorial authorization, Security.*

Кража паролей пользователей – это одна из ключевых проблем информационной безопасности. Большинство сетевых атак были успешно реализованы злоумышленниками из-за ненадежных или украденных паролей пользователей или администраторов ИТ-систем.

В то же время пользователи продолжают создавать простые и слабые пароли, легко поддающиеся подбору. Без внедрения принудительных политик регулярного изменения пароля, пользователи изменяют его реже чем раз в год. С другой стороны, при использовании сложного пароля и частой смене пользователю трудно запомнить его. Это приводит к ошибкам при авторизации в ИТ-системах и в результате замедляет работу в целом. Пользователь может продублировать сложный и трудно запоминающийся пароль в личном блокноте или другом источнике. Таким образом снова возникает риск доступа к учетной записи посторонних лиц. Еще одна угроза, связанная с авторизацией — пользователь зачастую дублирует один и тот же пароль для подключения к различным корпоративным ИТ-системам. Это также снижает устойчивость пароля при попытке его подбора.

Для повышения безопасности при авторизации пользователей в корпоративных системах применяется технология многофакторной аутентификации. Это метод контроля доступа к ИТ-системам, при котором пользователю для входа и подключения к ресурсу необходимо предъявить более одного параметра аутентификации. Таким образом осуществляется дополнительная проверка подлинности пользователя и повышается безопасность при авторизации.

Многофакторная аутентификация представляет собой более защищенный механизм авторизации, в котором пользователю для получения доступа к информации необходимо предъявить более одного «доказательства механизма аутентификации» [1]. К категориям таких доказательств относят:

- **Знание** — информация, которую знает субъект. Например, пароль, пин-код.

- **Владение** — вещь, которой обладает субъект. Например, электронная или магнитная карта, токен, флеш-память, телефон.
- **Свойство, которым обладает субъект**. Например, биометрия, природные уникальные отличия: лицо, отпечатки пальцев, радужная оболочка глаз, капиллярные узоры, последовательность ДНК.

Выбирая для системы тот или иной фактор или способ аутентификации, необходимо, прежде всего, отталкиваться от требуемой степени защищенности, стоимости построения системы, обеспечения мобильности субъекта.

К преимуществам многофакторной аутентификации можно отнести её способность защитить информацию, как от внутренних угроз, так и от внешних вторжений. Определенной слабостью можно считать необходимость использования дополнительных программно-аппаратных комплексов, устройств хранения и считывания данных. В качестве примера может послужить процесс двухфакторной аутентификации пользователя, реализованный в молдавских банках: вход в личный кабинет пользователя посредством сети интернет возможен после ввода пароля на странице, после чего, следует передача одноразового пароля, в виде SMS, на мобильный телефон, ранее зарегистрированный пользователем. Первой проблемой многофакторной аутентификации является способ ее реализации. В настоящее время самым популярным вторым фактором, используемым поставщиками сервиса, является одноразовый пароль one time password — OTP. Применяя данный тип 2FA пользователь вводит на первом уровне аутентификации персональный пароль. На следующем этапе он должен ввести маркер OTP, обычно отправляемый с помощью SMS на его мобильное устройство. Идея способа понятна. OTP будет доступен только тому, кто, как предполагается в теории, ввел недоступный постороннему пароль [2]. Кроме того, многофакторная аутентификация не в состоянии предотвратить атаки класса MitM, которые часто используются в ходе фишинговых компаний с помощью электронной почты. В случае успеха атаки пользователь перейдет по мошеннической ссылке и попадет на сайт, похожий на онлайн-портал банка. Там пользователь введет информацию о входе в систему и другие конфиденциальные данные, которые будут использоваться злоумышленником чтобы получить доступ к реальному сайту.

Методика аутентификации при помощи SMS основана на использовании одноразового пароля: преимущество такого подхода, по сравнению с постоянным паролем в том, что этот пароль нельзя использовать повторно. Даже если предположить, что злоумышленнику удалось перехватить данные в процессе информационного обмена, он не сможет результативно использовать украденный пароль для получения доступа к системе. А вот пример, реализуемый с применением биометрических устройств и методов аутентификации: использование сканера отпечатка пальца, который имеется в ряде моделей ноутбуков. При входе в систему пользователь должен пройти процедуру сканирования пальца, а затем подтвердить свои полномочия паролем. Успешно завершенная аутентификация даст ему право на

использование локальных данных конкретного ПК. Тем не менее, регламентом работы в ИС может быть предусмотрена отдельная процедура аутентификации для доступа к сетевым ресурсам компании, которая помимо ввода другого пароля может включать в себя целый ряд требований к представлению аутентификаторов субъекта. Но даже при такой реализации, защищенность системы, несомненно, усиливается.

Многофакторная аутентификация имеет ряд недостатков, которые препятствуют её распространению. В частности человеку, который не разбирается в этой области, сложно следить за развитием аппаратных токенов или USB-штекеров [3]. Многие пользователи не могут самостоятельно установить сертифицированное клиентское программное обеспечение, так как не обладают соответствующими техническими навыками. В общем, многофакторные решения требуют дополнительных затрат на установку и оплату эксплуатационных расходов. Многие аппаратные комплексы, основанные на токенах, запатентованы, и некоторые разработчики взимают с пользователей ежегодную плату. С точки зрения логистики, разместить аппаратные токены трудно, так как они могут быть повреждены или потеряны. Выпуск токенов в таких крупных областях, как банки, или других крупных предприятиях должен быть отрегулирован.

Заключение

Аутентификации по паролю уже недостаточно для защиты ценных данных. Однако решающим фактором оказывается стоимость системы. Большинство из имеющихся на рынке решений слишком сложны и дороги в реализации и поддержке. Любая система, требующая наличия аппаратного ключа или отправки паролей на мобильный телефон, лишь делает процесс аутентификации более громоздким. В любом случае технологии идут вперед и с каждым годом внедряются все больше систем и моделей авторизации, которые обязаны защитить нас и нашу информацию от третьих лиц. В использовании двухфакторной аутентификации есть некоторые нюансы, но сложными они кажутся лишь на первый взгляд. Каким должно быть идеальное соотношение защиты и удобства, каждый решает для себя сам. Но в любом случае все это очень важно, когда дело заходит о безопасности платёжных данных или личной информации, не предназначенной для чужих глаз.

Литература

1. Блинов А. «*Информационная безопасность*». Издательство «СПбГУЭФ»: Санкт-Петербург, 2010 – 96 стр.
2. Ричард Э.Смит «*Аутентификация: От паролей до открытых ключей*». Издательство «Вильямс» 2002. — 432 стр.
3. Мельников В.П., Клейменов С.А. «*Информационная безопасность и защита информации*». Издательский центр «Академия» , 2013 – 336 стр.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КОНТЕКСТЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

Ольга Корнеенко, Наталья Нижевич
УО «Гомельский государственный университет имени Франциска Скорины»

In this article questions of information security from the point of view of the legislation of Republic of Belarus are considered. Objects, external and internal threats of national security in the information sphere are allocated.

Проблеме безопасности в информационной сфере в настоящее время уделяется много внимания на всех уровнях, как государственном, так и частном. Информационная безопасность приобретает особую актуальность в связи с проникновением технических средств сбора, обработки и передачи данных практически во все сферы деятельности.

Согласно Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь 9 ноября 2010 г. № 575, информационная безопасность – это состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [1].

Информационная безопасность государства предполагает такое состояние, при котором обеспечивается сохранность информационных ресурсов государства и защищенность законных прав личности и общества в информационной сфере.

Информационная безопасность является комплексным и многогранным понятием, имеющим два основных аспекта: содержательный (духовная сфера) и технический (материальная сфера). К первому относят содержание и направленность всей циркулирующей информации. Технический аспект – это совокупность информационно-телекоммуникационных средств, технологий, систем и ресурсов, предназначенных для создания, хранения, распространения, передачи и обработки информации [2, с. 207].

К объектам информационной безопасности относятся:

- информационные ресурсы, которые содержат конфиденциальную информацию (секретную, ограниченного доступа или же коммерческую тайну), а также общедоступную открытую информацию и научные знания;
- информационная инфраструктура общества (сети связи и информационных коммуникаций, центры анализа и обработки данных, системы и средства защиты информации);
- система формирования, распространения и использования информационных ресурсов в стране;

- система формирования общественного сознания, которая базируется на СМИ;
- права граждан, юридических лиц и государства на получение, распространение и использование информации, а также защиту конфиденциальной информации и интеллектуальной собственности.

Выделяют внутренние и внешние источники угроз национальной безопасности.

В информационной сфере внутренними источниками угроз национальной безопасности являются:

- распространение недостоверной или умышленно искаженной информации, которая способна причинить ущерб национальным интересам Республики Беларусь;
- зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, их неконтролируемое использование в системах, отказ или разрушение которых может причинить ущерб национальной безопасности;
- недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий;
- рост преступности с использованием информационно-коммуникационных технологий;
- недостаточная эффективность информационного обеспечения государственной политики;
- несовершенство системы обеспечения безопасности критически важных объектов информатизации.

В информационной сфере внешними источниками угроз национальной безопасности являются:

- открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия;
- доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами;
- информационная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, которая наносит ущерб национальным интересам Республики Беларусь, целенаправленное формирование информационных поводов для ее дискредитации;
- нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;
- развитие технологий манипулирования информацией;
- попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь, которые приводят к причинению ущерба ее национальным интересам.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы. Она представляет собой совокупность информации, информационной инфраструктуры, субъектов, которые осуществляют сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Информационная сфера выделяется как одна из сфер, где сосредоточены усилия и ресурсы по обеспечению национальной безопасности. Она активно влияет на состояние политической, экономической, оборонной и других составляющих национальной безопасности Республики Беларусь. Национальная безопасность страны существенно зависит от обеспечения информационной безопасности. В ходе дальнейшего технического прогресса данная зависимость будет постоянно возрастать.

Информационная безопасность входит в ограниченный перечень сфер, национальные интересы в которых определяют предмет национальной безопасности: политическая, экономическая, военная, экологическая, информационная, гуманитарная. Укрепление информационной безопасности выделено в Концепции национальной безопасности Беларуси в числе важнейших долгосрочных задач. Поэтому далее кратко рассмотрим основные аспекты государственной политики в сфере информационной безопасности.

Государственная политика обеспечения информационной безопасности неразрывно связана с обеспечением национальной безопасности Республики Беларусь в целом. Как отмечалось выше, в Республике Беларусь базовым документом в сфере обеспечения национальной безопасности является Концепция национальной безопасности Республики Беларусь.

Роль информационной безопасности и ее место в системе национальной безопасности страны определяются также тем, что государственная информационная политика тесно взаимодействует с государственной политикой обеспечения национальной безопасности страны через систему информационной безопасности, выступающую важным связующим звеном всех основных компонентов государственной политики в единое целое [3, с. 8].

Государственная политика обеспечения информационной безопасности Республики Беларусь определяет основные направления деятельности органов государственной власти и субъектов в этой области, порядок закрепления их обязанностей по защите интересов страны в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государство в процессе реализации своих функций по обеспечению информационной безопасности Республики Беларусь, в частности, в информационной сфере:

- проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности Республики Беларусь, разрабатывает меры по ее обеспечению;
- организует работу законодательных и исполнительных органов государственной власти Республики Беларусь по реализации комплекса

мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности Республики Беларусь;

- осуществляет контроль за разработкой, созданием, развитием, использованием средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;
- принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;
- способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;
- формулирует и реализует государственную информационную политику Беларуси;
- способствует интернационализации глобальных информационных сетей и систем, а также вхождению Беларуси в мировое информационное сообщество на условиях равноправного партнерства [4, с. 293].

Таким образом, государственная политика в области обеспечения информационной безопасности имеет важное значение. Данная политика должна быть закреплена на законодательном уровне. Именно государство в первую очередь должно определять основные направления деятельности субъектов в сфере информационной безопасности. Отсутствие данных направлений может привести к определению нечетко обозначенных прав и обязанностей каждого из субъектов, и, как следствие, к нарушению баланса интересов личности, общества и государства в информационной сфере. В случае нарушения такого баланса будет не соблюдаться понятие информационной безопасности, закрепленное в Концепции национальной безопасности Республики Беларусь. А, следовательно, и будет отсутствовать полное обеспечение безопасности в информационной сфере в нашей стране.

Список использованных источников:

1. Указ Президента Республики Беларусь, 9 ноября 2010 г., № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» [Электронный ресурс]. – Режим доступа: http://www.pravo.by. – Дата доступа: 25.02.2018.
2. Мясникович, М.В. Национальная безопасность Республики Беларусь / С. В. Зась [и др.]; под ред. М.В. Мясниковича и Л.С. Мальцева. – Минск: Беларус. навука, 2011. – 557 с.
3. Информационная безопасность как составляющая национальной безопасности государства: материалы Междунар. науч.-практ. конф., Минск, 11-13 июля 2013 года: в 3 т. / Ин-т нац. безопасности Респ. Беларусь; редкол.: С.Н. Князев (гл. ред.) [и др.]. – Минск, 2013. – 332 с.
4. Василевич, Г.А. Информационное право: учеб. пособие / Г.А. Василевич [и др.]. – Минск: Адукацыя і выхаванне, 2013. – 352 с.

ОРГАНИЗАЦИОННО-ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Ольга Корнеенко,
учреждение образования «Гомельский государственный университет имени Франциска Скорины»

In article organizational and psychological aspects of information security of the organization are considered. The main attention is paid to formation of the system directions of prevention of industrial espionage.

Информация является базовой составляющей знания. Знания накапливаются и передаются в форме интеллектуального продукта. Иначе говоря, знание в отличие от информации представляет собой постоянно увеличивающийся, в том числе и в результате информационных процессов, ресурс. Человеку как носителю и пользователю информации и знаний на всех стадиях информационного процесса принадлежит ведущая роль. От того, как в информационных процессах будут учтены интересы, психологические установки, свойства личности, зависит эффективность использования информации.

Если учесть главенствующую роль информации в системе ресурсного обеспечения бизнеса (кто владеет информацией тот владеет миром), то понятна необходимость и важность информационной безопасности для любой организации.

В качестве основных направлений обеспечения информационной безопасности бизнеса можно выделить следующие:

- экономическая безопасность – защита информации о состоянии и движении материальных активов;
- собственно информационная безопасность – защита информации о состоянии нематериальных активов и их носителях (персонале);
- защита средств хранения, обработки и передачи информации.

Для обеспечения безопасности бизнеса используются экономико-психологические методы, а для защиты информационных сетей – технико-технологические методы.

При этом, условия формирования системы экономической безопасности определяют:

- что делать. Необходимо четкое определение понятия «система экономической безопасности». Обеспечивать экономическую безопасность значит осуществлять постоянную деятельность по выявлению, предупреждению, локализации и нейтрализации угроз и сведению к минимуму ущерба от реализации угроз различного характера;

- для кого делать. Необходим учет мнений и позиций собственника, акционеров, менеджмента. Как показывает практика, их взгляды далеко не всегда совпадают;
- как это делать. Необходимо соблюдение принципов и алгоритма формирования системы экономической безопасности предприятия. В основу должно быть положено суждение, что любое действие, нарушающее нормальное функционирование организации, понимается как угроза ее экономической безопасности.

К сожалению, наиболее распространенной причиной утечки информации является небрежность первых лиц организации. Например, в частных фирмах более 75 % ответственных сотрудников при приеме посетителей не считают необходимым убирать конфиденциальные документы со стола или закрывать файл на компьютере. Это приводит к потере до 30 % оперативной информации. 75 % руководителей крупных организаций хорошо знают об увеличении возможности утечки информации при использовании современных технических средств. Однако, копирование материала в 53,6 % случаев происходит в режиме самообслуживания, в 32,7 % – оператором по устной просьбе служащего и только в 13,5 % случаев оператор делает копии под расписку или по письменному заказу. По данным проведенного итальянскими психологами исследования только 25 % служащих фирмы действительно являются надежными людьми. Еще 25 % ожидают удобного случая для разглашения известных им секретов, а 50 % будут действовать в зависимости от обстоятельств.

В США компьютерные преступления совершаются, как правило, допущенными к работе с информационными системами служащими. Чаще, чем профессиональные программисты, в нарушениях виновны клерки, администраторы и управляющие.

При этом зафиксированы случаи, когда программисты закладывали в информационную систему «логическую бомбу» на случай значимых для них обстоятельств, при наступлении которых она стирает весь массив информации и самоликвидируется.

Для создания атмосферы информационной безопасности наиболее эффективны меры, которые связаны с повышением информационной культуры сотрудников на предприятии.

Следует формировать четкую целевую установку на повышение надежности и ответственности по различным аспектам защиты информации. Так, во многих американских фирмах действует двухуровневая система защиты информации: 1) обеспечение информационной безопасности силами специальных служб, 2) культивирование атмосферы бдительности и ответственности с помощью так называемых координаторов, которые назначаются из состава служащих среднего звена.

Необходимо разбить технологический процесс на несколько самостоятельных этапов. Служащие будут знать лишь часть секретов, при том, что

цельные знания доступны только руководству или узкому кругу лиц. Целесообразен постоянный мониторинг отношений между людьми, владеющими информацией, учет их морального и психологического состояния. Причинами для беспокойства могут являться эмоциональная неуравновешенность, проявления недовольства, хитрости, разочарования сотрудников, идеи которых отвергнуты.

Весьма эффективны организационно-психологические меры защиты информации:

- дробление и распределение информации между сотрудниками;
- ведение учета ознакомления персонала с особо важной информацией;
- распространение информации исключительно через контролируемые каналы;
- назначение ответственных за контроль документации лиц;
- обязательное уничтожение неиспользованных копий документов и записей;
- четкое определение коммерческой тайны для сотрудников;
- составление, постоянная оценка и обновление перечня информации, которая составляет коммерческую тайну;
- включение пункта о неразглашении коммерческой тайны и ответственности за это в трудовой договор, правила внутреннего распорядка и должностные инструкции;
- включение положений по вопросам неразглашения конфиденциальной информации в партнерские соглашения, контракты и договоры.

Необходимо обратить особое внимание на меры по обеспечению информационной безопасности при увольнении сотрудника. Косвенно о намерении сотрудника уволиться свидетельствует посещение им соответствующих сайтов в Интернете, проявление активности по рассылке резюме. С этого момента вся переписка с использованием компьютера должна быть взята под негласный контроль. Целесообразно в отсутствие данного пользователя сделать резервную копию всех его файлов. Однако, нет необходимости сразу принимать явные меры безопасности, учитывая, что сотрудник может изменить свои намерения и остаться, а также допуская, что просмотр вакансий мог осуществляться по просьбе знакомых, ищущих работу.

Если сотрудник заявил об увольнении, необходимы следующие меры: информирование всех сотрудников о предстоящем увольнении и запрет передачи ему любой информации, имеющей отношение к работе; создание резервных копий файлов пользователя; организация передачи дел и постепенное сокращение прав доступа к информации; при необходимости организация сопровождения увольнения специалистом по информационной безопасности.

Если сотрудник уличен в шпионаже, то в срочном порядке следует лишить его всех прав доступа к информационным технологиям, скорректировать права доступа к общим информационным ресурсам (базам данных, принтерам, факсам). Все

сотрудники обязательно должны сменить личные пароли и до их сведения доводится информация о том, что данный специалист с установленной даты не работает, при любых попытках контакта с его стороны необходимо немедленно сообщать в службу безопасности. Определенное время контроль информационной система осуществляется в усиленном режиме.

Если сотрудник увольняется по иной причине, то названные меры не должны быть чрезмерно настойчивы, чтобы не оказывать негативного воздействия на психологическое состояние человека. Сотруднику необходимо внушить, что таков общий порядок на данном предприятии и он лично ни в чем не подозревается. Нецелесообразно портить отношения со всеми увольняющимися сотрудниками, ведь кто-то может вернуться, а кто-то – оказать в свое время посильную помощь. Кроме того, в коллективе может пострадать общий социально-психологический климат, если сотрудники увидят, что подобное увольнение неразрывно связано с моральным ущербом.

Если сотрудника увольняют, уличив в промышленном шпионаже, основная задача службы управления персоналом будет заключаться в том, что происходящее не должно нанести ущерб социально-психологическому климату в коллективе, а по возможности, напротив, консолидировать остальных сотрудников.

Меры по обеспечению информационной безопасности с позиций «человеческого фактора» можно рассматривать в качестве щита от воровства информации как специфического ресурса, имеющего значительную ценность. Воровство и мошенничество как психологическая проблема имеют и свою идеологию – «воруют все». С некоторыми вариациями это суждение существует уже столетия. Различают такие формы воровства, как: индивидуальное (в основе лежит генетический код и ощущение анонимности, самооправдание); коллективное (в основе – идеология восстановления социальной справедливости).

Эффективно противодействовать этому можно только учитывая такой фактор, как экономическое поведение работника. Это поведение, связанное с перебором экономических альтернатив с целью рационального выбора, то есть выбора, при котором минимизируются затраты и максимизируется выгода. В основе экономического поведения лежат ценностные ориентации людей (деньги, статус, роль, идеалы).

На экономическое поведение оказывают влияние различные факторы: технический уровень производства, организация, нормирование, оплата и условия труда, удовлетворенность трудом, морально-психологический климат в коллективе, образовательный и культурный уровень персонала, характер общественно-политической активности в обществе и в рабочей группе. Различают 4 стратегии экономического поведения: «минимум труда – минимум дохода», «минимум труда – максимум дохода», «максимум труда – гарантированный доход», «максимум труда – максимум дохода».

Исключительно мотивами регулируется поведение человека в рамках определенной стратегии. Переход от одной стратегии к другой регулируется

системой стимулов. Исключение составляет стратегия «максимум труда – максимум дохода», где поведение человека определяется стимулами. Стратегия «минимум труда – минимум дохода», возникая, как вынужденная реакция человека на ситуацию, формирует у работника чувство «внутреннего увольнения», подавленности, способствует становлению разрушительного поведения.

В качестве направлений по профилактике воровства в организации можно сформулировать следующие рекомендации:

- создать сильную корпоративную культуру организации (отношения, социальные приоритеты, мораль в организации). Если сформирована «критическая масса» работников, то новички попадают в систему самовоспроизводящегося общественного сознания;
- создать эффективную систему контроля, отвечающую требованиям регулярности и систематичности, а также персональной ответственности сотрудников. Основное условие –рассматривать контроль как помощь персоналу в борьбе с искушением украсть.
- сформулировать и использовать общие правила стимулирования, обеспечивающие безопасное поведение персонала: доступность («я тоже могу хорошо заработать»); ощутимость (премия не менее 20 % к окладу, оклад больше возможного ущерба); минимальный разрыв между результатами и оплатой по времени (недостаток материального стимулирования восполняется воровством); сочетание стимулов и мер наказания; сочетание материальных, социальных и психологических стимулов.
- разработать систему превентивных действий службы управления персоналом: гибкая организационная структура «под задачи» организации (лишние подразделения следует ликвидировать, перераспределив и частично уволив сотрудников); определение приоритетов в развитии персонала и реализация функций управления ими; ежегодная аттестация персонала; систематический пересмотр «Положений о подразделениях» и «Должностных инструкций» с целью их совершенствования в соответствии с изменениями в разделении и организации труда, а также в связи с изменениями уровня профессионализма самих работников; разработка компенсационных пакетов (размера, структуры, соотношения различных форм вознаграждения) с ориентацией на конечные результаты, значимые для организации (например, система сквозных показателей); разработка системы мер профилактики противоправного поведения сотрудников, в том числе и на случаи возникновения объективных причин к снижению уровня преданности фирме, например, при угрозе увольнения; постоянное информирование сотрудников о состоянии рынка товаров и услуг, на котором действует организация, формирование рыночного мышления, обеспечение причастности к проблемам организации.

Также могут быть приняты меры на случай снижения деловой активности организации и необходимости проводить сокращение численности персонала: заключения срочного трудового договора, заключение договора о сохранении коммерческой тайны, конфиденциальной информации, служебной тайны, о материальной ответственности, ознакомление под расписку с должностной инструкцией (а для руководителей подразделений и с Положением о подразделении), Правилами трудового распорядка, Положением об оплате и стимулировании труда, Коллективным договором, специальные меры в случае необходимости увольнения.

Таким образом, в организации следует создать систему внутрифирменной коммуникации, которая бы не допускала полной автономности отдельных работников. Психологическое обеспечение конфиденциальности и коммерческой тайны в процессе отбора, подготовки и движения кадров эффективнее и дешевле, чем простое засекречивание информации.

АНОНИМНОСТЬ В СЕТИ ИНТЕРНЕТ ПОСРЕДСТВОМ TOR (THE ONION ROUTER)

Косатая А.Ю.
Студентка SI-141
Academia de Studii Economice a Moldovei
Научный руководитель Згуряну А.

Tor was originally designed, implemented, and deployed for the primary purpose of protecting government communications. Nowadays, it is used for a wide variety of purposes by the military, journalists, law enforcement officers, activists, and many others.
***Keywords**: tor, tor privacy, protection, anonymity.*

В последнее время наметилась тенденция по ограничению приватности в сети Интернет. Это связано с ограничениями, которые воздействуют на пользователя государственное регулирование сети Интернет, которая действует во многих странах, например Китай, Россия, Беларусь. В то же время, целый ряд крупных он-лайн сервисов собирает информацию о пользователях для использования в коммерческих целях, таких как: показ Интернет-рекламы, предложения он-лайн покупок и т.д. Крупные специализированные службы собирают информацию о наиболее широком круге пользователей сети и хранят ее для использования в собственных целях. Хакерские группировки и компьютерные злоумышленники тоже собирают данные про пользователей сети, с целью получить доступ к информационным и финансовым активам. Такими предметами являются кредитные карты, системы он-лайн платежей, электронные кошельки и т.д. В сфере бизнеса сбор информации о субъекте предпринимательской деятельности ведется специалистами по конкурентной разведке.

Методы сокрытия активности интересны спецслужбам, которые занимаются изучением методов анонимизации, для чтобы добраться до злоумышленников, хакерам – для того, чтобы сокрыть следы вредоносных деяний, коммерческим предприятиям – для того чтобы сохранить свою коммерческую тайну, а также обычным пользователям – для личной приватности и безопасности.

Во время каждого входа в Интернет, человек оставляет, так называемые «следы», ими могут быть: пароли от аккаунтов, сообщения, личная информация о своих увлечениях и предпочтениях. Такие данные могут навредить, так как мошенники с целью выгоды используют против пользователей сети. Для того чтобы избежать таких проблем и дискомфорта, существуют целые системы, сети, приложения и браузеры, которые обеспечивают анонимное пребывание в сети. Однако анонимизация значительно усложняет работу по выявлению участников киберпреступлений, поскольку то, что находится в логе (IP-адрес) не является достоверной информацией.

Анонимная сеть [2] - это компьютерная сеть, которая создана для достижения приватности в Интернете и работающая поверх глобальной сети.

Специфика такой сети заключается в том, что разработчики вынуждены идти на компромисс между степенью защиты и лёгкостью использования системы, её «прозрачностью» для конечного пользователя. Также важен аспект сохранения анонимности и конфиденциальности при условии воздействия методов социальной инженерии или какого-либо давления на оператора сервера.

Многоуровневое шифрование и распределённый характер анонимных сетей, устраняя единую точку отказа и единый вектор атак, позволяют сделать перехват трафика или даже взлом части узлов сети не фатальным событием. За анонимность пользователь расплачивается увеличением времени отклика, снижением скорости, а также большими объёмами сетевого трафика.

Для осуществления анонимности в сети Интернет, существуют различные средства приватности, которые обеспечивают сокрытия трафика, личных данных и конфиденциальной информации, такие как на **рисунке 1**:

- прокси-серверы (анонимайзеры);
- децентрализованные анонимные сети (анонимная сеть I2P);
- гибридные анонимные сети (TOR, VPN).

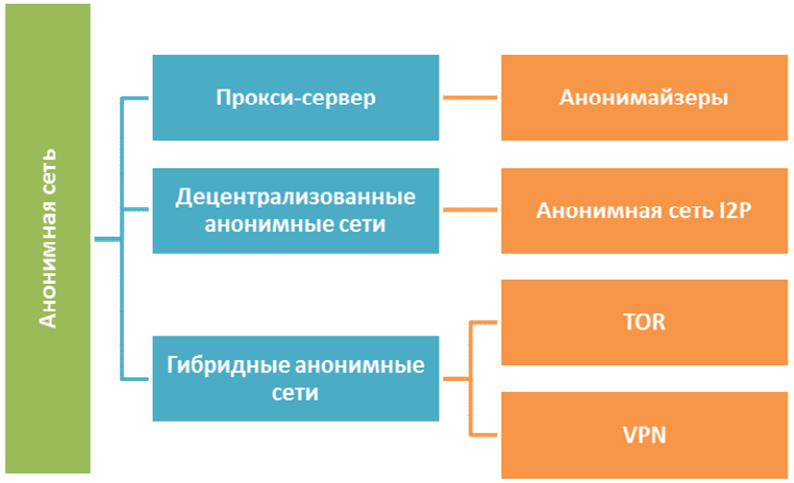


***Рис.1* Виды анонимных сетей.**

TOR (*The Onion Router*) [5] – это свободное и открытое программное обеспечение для реализации второго поколения луковой маршрутизации. Это технология анонимного обмена информацией через компьютерную сеть. Сообщения неоднократно шифруются и потом отсылаются через несколько сетевых узлов, называемых луковыми маршрутизаторами. Каждый маршрутизатор удаляет слой шифрования чтобы открыть трассировочные инструкции и отослать сообщения на следующий маршрутизатор, где все повторяется. Таким образом, промежуточные

узлы не знают источник, пункт назначения и содержание сообщения. Данная система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания.

TOR [1] обеспечивает надёжную и бесплатную анонимизацию, защищая пользователя от слежки, как за посетителями определённого сайта, так и за всей активностью самого пользователя. Когда пользователь передаёт данные, программа TOR скрывает и настоящий пункт их назначения и сами данные, перебрасывая данные в зашифрованном виде через цепочку промежуточных узлов сети. TOR случайным образом выбирает несколько серверов из всех доступных (список которых он периодически скачивает с центрального сервера-директории) и строит «тоннель», проходящий через эти промежуточные точки. Весь трафик будет пропускаться через этот тоннель; у него есть вход — приложение TOR на техническом средстве и выход - последний из случайно выбранных для этого тоннеля серверов сети TOR.

Ежедневно множество людей разных профессий, интересов используют TOR для обеспечения конфиденциальности данных и безопасности. Его использование защищает пользователя от частой формы интернет-наблюдения, известное как «анализ трафика». Анализ трафика [3] может быть использован для вывода, кто с кем общается по сети общего пользования. Знание источника и назначения Интернет-трафика позволяет другим отслеживать поведение и интересы. Это может повлиять на банковскую карту, если, например, сайт электронной коммерции использует ценовую дискриминацию, основанную в стране или учреждениях происхождения. Это может даже угрожать работе и физической безопасности, показывая, кем является человек и где находится. Например, если пользователь за границей и подключён к компьютерам работодателя, может непреднамеренно раскрыть свою страну и профессиональную принадлежность к любому наблюдателю сети, даже если соединение зашифровано.

TOR может быть с успехом использован с благими целями многими категориями людей [6]:

- Физическими лицами, чтобы предотвратить отслеживание, кражу личной информации, мошенничества и обеспечения безопасности пользователям сети Интернет. Скрытые сервисы TOR позволяют пользователям публиковать веб - сайты и пользоваться различными услугами без необходимости раскрывать местоположение сайта.
- Отдельными лицами, для социально-чувствительного общения: чаты и веб форумов для жертв насилия и оскорблений, или человек, который болен.
- Журналистами, чтобы безопасно общаться с осведомителями и диссидентами.
- Неправительственными организациями, чтобы позволить своим работникам подключаться к рабочим сайтам в то время как они

находятся в чужой стране, не распространяя информацию об организации.

- Корпорациями, для безопасного способа проведения конкурентного анализа и для защиты важных путей поставок от прослушивания.
- Правоохранительными органами, для посещения веб-сайтов, не выходя из правительственных IP-адресов в логах, и для безопасности во время операций.

Заключение

Все последние годы прошли в тренде все более усиливающегося контроля государства, Интернет-провайдера, шпионства мошенников за людьми. Особенно успешно этот процесс продвигается в сети Интернет.

В свете этих событий совершенно естественно желание людей, различных профессий обеспечить безопасность своих конфиденциальных данных и ослабление контроля за своей личной жизнью. Одной из мер для этого является противодействие своей идентификации в сети, то есть, обеспечение анонимности.

Обеспечение использования анонимизирующей сети Интернета сегодня является актуальной задачей. Текущие тенденции в области права, политики и технологии угрожают анонимности как никогда раньше, способствуя нарушить безопасное общение и приватность в сети. Эти тенденции также подрывают национальную безопасность и критическую инфраструктуру путём коммуникации между отдельными людьми, организациями, корпорациями и правительствами более уязвимых для анализа.

Список источников

1. T. Gneysu, F. Regazzoni, P. Sasdrich, and M. Wjcik, “Thor - the hardware onion router,” in 2014 24th International Conference on Field Programmable Logic and Applications (FPL), Sept 2014, pp. 1–4.
2. Junbeom Hur and Dong Kun Noh, “Efficient and Secure Identity-Based Onion Routing”, 2017, pp. 1-3
3. S. Nepal, S. Dahal, and S. Shin, “Deanonymizing schemes of hidden services in tor network: A survey,” in Information Networking (ICOIN), 2015 International Conference on, Jan 2015, pp. 468–473.
4. Daniele E. Asoni, Chen Chen, David Barrera, and Adrian Perrig. On Building Onion Routing into Future Internet Architectures, 2017, pp. 3-4
5. Анонимность при помощи TOR. http://www.securitylab.ru/analytics/474307.php
6. Кто использует TOR - https://www.torproject.org/about/torusers.html.en

ТЕСТИРОВАНИЕ УЯЗВИМОСТИ WEB-ПРИЛОЖЕНИЙ К АТАКЕ ВИДА МЕЖСАЙТОВЫЙ СКРИПТИНГ

А.В. Коваленко, А.С. Коваленко, А.А. Смирнов, С.А. Смирнов
Центральноукраинский национальный технический университет

Abstract: The paper presents research results and vulnerability testing algorithms for one of the most common types of attacks on Web-based applications - cross site scripting - DOM XSS. The approach of mathematical modeling based on GERT-networks is argued. Studies have shown that GERT (Graphical Evaluation and Review Technique) is a method of studying and analyzing stochastic networks used to describe the logical relationship between parts of a project or process steps.

В настоящее время большой спрос на Web-приложения и Web-услуги обуславливает большой интерес злоумышленников к их возможным уязвимостям. При этом основные угрозы в направлении серверных компонент трансформируется в атаки, направленные против обычных пользователей.

Проведенный анализ материалов Open Web Application Security Project (OWASP TOP-10) показал, что одним из наиболее опасных видов атак (уязвимостей) является межсайтовый скриптинг – XSS (Cross Site Scripting).

Межсайтовый скриптинг это ошибка валидации пользовательских данных, которая позволяет передать JavaScript код на исполнение в браузер пользователя. Атаки такого рода часто также называют HTML-инъекциями, ведь механизм их внедрения очень схож с SQL-инъекциями, но в отличие от последних, внедряемый код исполняется в браузере пользователя.

Под XSS обычно подразумевается моментальный и отложенный межсайтовый скриптинг. При моментальном XSS злонамеренный код (Javascript) возвращается атакуемым сервером немедленно в качестве ответа на HTTP запрос. Отложенный XSS означает, что злонамеренный код сохраняется на атакуемой системе и позднее может быть внедрен в HTML страницу уязвимой системы. Такая классификация предполагает, что фундаментальное свойство XSS состоит в том, что злонамеренный код отсылается из браузера на сервер и возвращается в этот же браузер (моментальный XSS) или любой другой браузер (отложенный XSS).

В ряде интернет-статей подробно описаны основные механизмы возникновения подобного рода угроз, а также пути возможного блокирования. Однако, чтобы идентифицировать эти угрозы и возможные последствия их распространения в процессе безопасного управления IT-проектами, а также предложить оптимальные пути решения этой проблемы, существует необходимость математической формализации процесса их инициализации и распространения.

Особенно актуальной задачей в этом направлении представляется моделирование DOM (Document Object Model) XSS уязвимости. Связано это с тем, что уязвимость DOM XSS представляет собой подвид XSS, в случае которой

результат атаки находится не в ответе сервера и, соответственно, не в HTML коде, а в DOM структуре HTML страницы.

Результаты атак посредством таких уязвимостей можно обнаружить только в процессе выполнения или анализе DOM структуры. Сам механизм атаки, а именно инъекция Javascript кода в уязвимый сегмент, остается неизменным.

Для математической формализации алгоритма анализа DOM XSS уязвимости воспользуемся основными положениями сетевого GERT-моделирования. Проведенные исследования показали, что GERT (*Graphical Evaluation and Review Technique*) – является методом изучения и анализа стохастических сетей, используемых для описания логической взаимосвязи между частями проекта или этапами процесса. Главной целью GERT является оценка логики сети и продолжительность активности и получения заключения о необходимости выполнения некоторых активностей.

Сети GERT состоят из узлов типа AND, INCLUSIVE-OR и EXCLUSIVE-OR, и веток с двумя и более параметрами. Ветка, имеет направление, имеет узел начала и узел конца. Параметры ветви содержат:

1) вероятность прохождения ветви (P_a) при условии, что узел, который является источником ветви, был реализован;
2) время (t_a) прохождения ветви, если она будет реализована.

Время t_a может быть случайной величиной. Если ветвь не является частью реализации сети, то есть во время выполнения процесса активность, связанная с ветвью, не происходит, то $t_a = 0$.

Узел в стохастической сети GERT состоит из функции входа (контрибутивной функции) и функции выхода (дистрибутивной функции). Каждая из функций описывается определенным логическим отношением относительно связанных ветвей.

В целом, проведенные исследования показали, что GERT-моделирование является эффективным способом определения заранее неизвестных законов и функций распределения случайных величин при известном алгоритме функционирования (процесса). Именно поэтому, в качестве инструмента математического моделирования нами было выбрано GERT-моделирование.

Построим, в соответствии с представленным описанием сетевую GERT-модель технологии тестирования DOM XSS уязвимости.

В представленной сети узлы графа интерпретируются состояниями компьютерной системы в процессе функционирования DOM структуры, а ветви графа – вероятностно-временными характеристиками переходов между состояниями. В частности:

- Ветвь (1,2) характеризует время получения и анализа содержимого тега.
- Ветвь (2,3) отображает временные характеристики выполнения атаки в случае наличия «source» структуры.
- Ветвь (2,4) задает случайное время обращения к содержимому удаленного файла (поиск «sink»).

- Ветвь (4,2) характеризует возврат на выполнение атаки.
- Ветвь (3,5) описывает продолжение атаки, в частности проверку содержимого DOM.
- Далее ветвь (5,6) характеризует время принятия решения об уязвимости, в то же время ветвь (5,1) отображает временные характеристики перехода к новому тегу.

Модель может быть использована для исследования процессов в компьютеризированных системах, при разработке новых средств и протоколов защиты данных.

Применение экспоненциальных стохастических моделей GERT даст возможность использования результатов, полученных в аналитическом виде (функции, плотности распределения) для проведения сравнительного анализа и исследований, более сложных компьютерных систем математическими методами.

Выводы

В работе разработан комплекс математических моделей технологии тестирования WEB-приложений. В основу математического моделирования положен подход GERT-сетевого синтеза. В результате разработаны математические модели технологии тестирования DOM XSS уязвимости.

Математическая модель технологии тестирования DOM XSS уязвимости отличается от известных, учетом выполнения или анализа DOM структуры, что дает возможность провести аналитическую оценку временных затрат тестирования указанной уязвимости в условиях реализации стратегии разработки безопасного программного обеспечения.

В ходе исследования представленных моделей было определено, что случайная величина времени выполнения рассматриваемых методов тестирования в целом соответствует гамма-распределению. Проверка этой гипотезы произведена по критерию χ^2 Пирсона.

АРХИТЕКТУРА ПРОГРАММНОГО ИНСТРУМЕНТАРИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ УЗЛА ЛВС

Кучеров Александр Иванович
Учреждение образования Гомельский государственный университет имени Франциска Скорины

The architecture of software Toolkit for secure LAN node by gathering and analyzing information about components of computers and the modes of its functioning article is discussed.

На данный момент современные вычислительные системы на уровне любого предприятия представляют собой сложный комплекс из автоматизированных рабочих мест (АРМ), взаимодействующих между собой, с серверами приложений и сетевыми устройствами. Взаимодействие обеспечивается через корпоративную сеть. Возникает сложная система, в которой правильная настройка и профилактические работы должны проводиться осознанно, т. е. перед выполнением регламентных работ обслуживающий персонал должен представлять, какие проблемы возникли в обслуживаемом оборудовании. На данный момент операционные системы компьютеров и серверов оснащены мощным диагностическим программным обеспечением. Это Windows Management Instrumentation (WMI-инструментарий) и счетчики производительности, которые собраны в оснастку Performance Logs and Alerts (Журналы и оповещения производительности). На основе этих двух компонент можно собирать информацию о конфигурации компьютеров, режимах работы памяти, процессора, жесткого диска, сетевого адаптера.

WMI, если говорить более развернуто, – это одна из базовых технологий для централизованного управления и слежения за работой различных частей компьютерной инфраструктуры под управлением платформы Windows.

С помощью оснастки Performance Logs and Alerts (Журналы и оповещения производительности) можно собирать данные о производительности с локальных или удаленных компьютеров. Собранные данные просматриваются в графическом виде с помощью системного монитора или экспортируются в электронные таблицы или базы данных для последующего анализа и создания отчетов.

На основе этих компонентов создано программное обеспечение, которое будет полезно обслуживающему персоналу для качественного выполнения профилактических и регламентных работ на узлах сети. При этом полученная информация в совокупности с информацией об интенсивности и характере использования клавиатуры и манипулятора «мышь», а также используемых программных продуктах тем или иным пользователем узла локальной вычислительной сети (ЛВС), позволит формировать идентификационный портрет пользователя ЛВС. В свою очередь, сравнивая идентификационный портрет пользователя ЛВС с текущими действиями пользователя на узле ЛВС, можно обеспечить безопасность узла ЛВС и тем самым увеличить его надежность.

Архитектура проекта представлена на рисунке 1. На нем указан перечень структурных элементов, входящих в проект и отношения между ними.

Программное обеспечение, обеспечивающее работу пользователя и разработанное в соответствии с требованиями проекта, состоит из трех приложений:

1. CompConfig.exe – обеспечивает пользователю выполнение ролей с первой по пятую.
2. Usertime.exe – участвует в выполнении четвертой роли «Время работы». Это приложение выполняет функции по записи в базу данных информации о времени работы компьютеров и пользователей.
3. WCounters.mdb – обеспечивает выполнение седьмой роли «Анализ производительности».

С инструментарием WMI работают два приложения CompConfig.exe и Usertime.exe. Чтобы получить информацию о конфигурации ЭВМ сегмента сети, они обращаются к инструментарию WMI, который интегрирован в операционную систему Windows и обеспечивает выполнение запросов к компьютерам через локальную сеть.

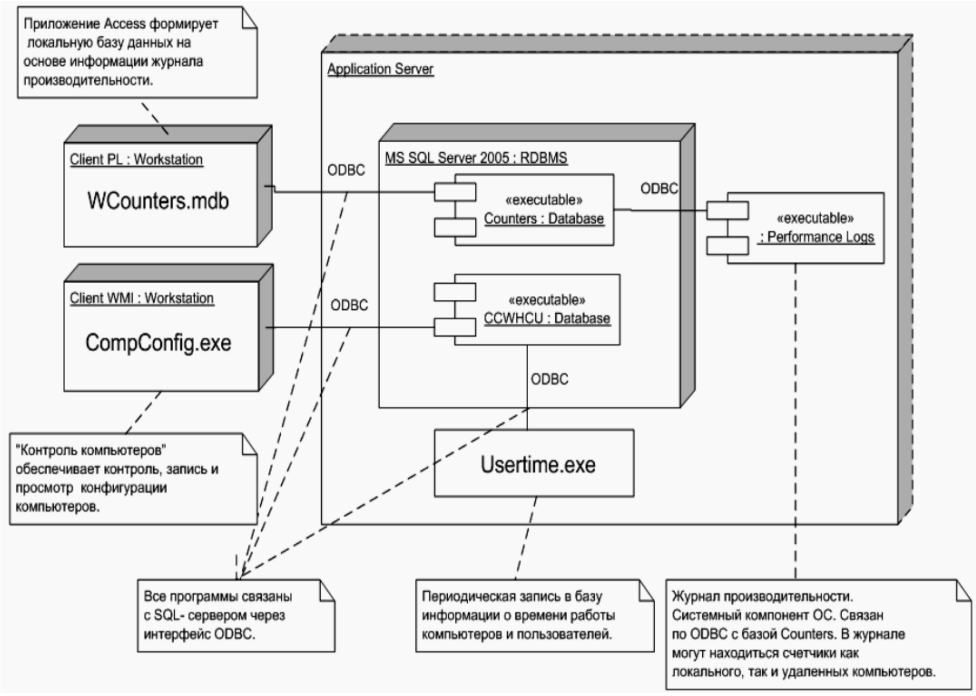


Рисунок 1 **– Диаграмма архитектуры связей ODBC**

Работа по сети нескольких экземпляров CompConfig.exe возможна и при рассмотрении работы этого приложения с компьютерами через инструментарий WMI. Если два экземпляра CompConfig.exe попытаются считать конфигурацию одного и того же компьютера, то этот компьютер выполнит сначала один запрос, а

затем второй. Поэтому у двух считанных конфигураций будет разное время регистрации и поэтому обе конфигурации могут быть записаны в базу данных (рисунок 2).

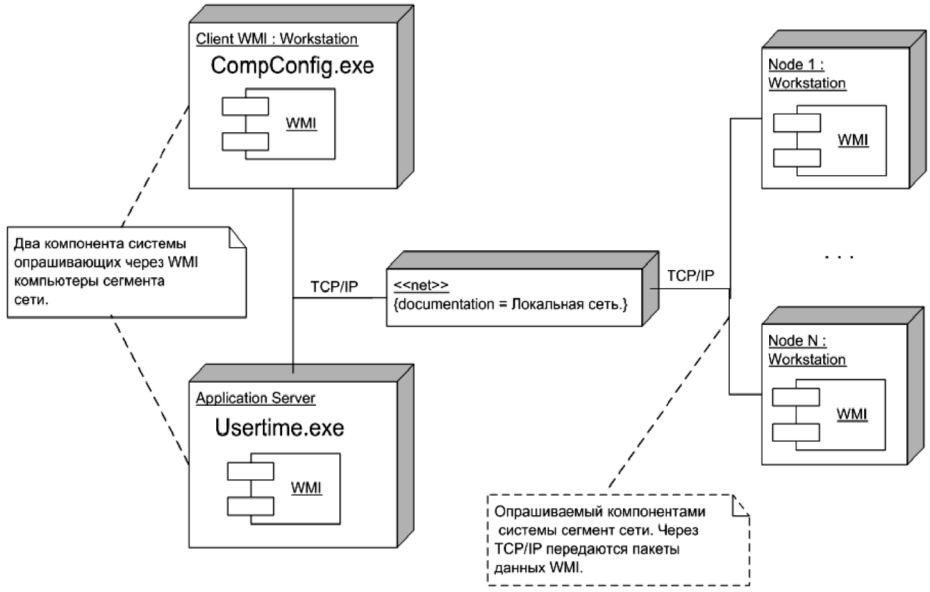


***Рисунок 2* – Диаграмма архитектуры связи по WMI**

На основании рассмотрения архитектуры проекта к реализации проекта можно выдвинуть следующее требование: реализация баз данных и компонент CompConfig.exe и WCounters.exe должна обеспечивать возможность работы с базой данных нескольких экземпляров этих программ.

Программный инструментарий может использоваться обслуживающим персоналом при планировании регламентных работ на узлах компьютерной сети. При этом формируется информация как для контроля действий обслуживающего персонала по выполнению графика профилактик и операций замены комплектующих, так и для анализа вычислительной нагрузки на узлы сети, рабочего времени компьютеров и пользователей.

Дальнейшее развитие программного комплекса может позволить создать качественный и полезный инструмент для обслуживающего персонала и в целом повысить защищенность и надежность узла локальной вычислительной сети.

Список используемой литературы

1. Кучеров, А.И. Методика повышения надежности вычислительных систем / А.И. Кучеров // Известия Гомельского государственного университета им. Ф.Скорины – 2012. – № 6 (75). – С. 120–123.
2. Кучеров, А.И. Получение информации об интенсивности использовании ЭВМ с целью дальнейшего повышения ее надежности / А.И. Кучеров // Известия

Гомельского государственного университета им. Ф. Скорины – 2013. – № 6 (81). – С. 125–129.

3. Кучеров, А.И. Инициализация начального состояния компьютера для реализации экспериментов по надежности узла локальной вычисли- тельной сети / А.И. Кучеров, А.В. Воруев, В.Д. Левчук // Известия Гомельского государственного университета им. Ф. Скорины – 2015. – № 6 (93). – С. 64–68.
4. Кучеров, А.И. Архитектура программного инструментария по обеспечению надежности узла ЛВС / А.И. Кучеров и др. // Проблемы физики, математики и техники – 2017. - № 4(33). – С. 100-103.

ВЫБОР ПРОТОКОЛОВ ДУБЛИРОВАНИЯ И АГРЕГИРОВАНИЯ КАНАЛОВ СВЯЗИ ДЛЯ ПОВЫШЕНИЯ НАДЕЖНОСТИ И ЗАЩИЩЕННОСТИ ПЕРЕДАЧИ ДАННЫХ В ГЕТЕРОГЕННОЙ СЕТИ

Кулинченко Владимир Николаевич
Учреждение образования Гомельский государственный университет имени Франциска Скорины

The choice of protocols for duplication and aggregation of communication channels is discussed to improve the reliability and security of data transmission in a heterogeneous network

Введение. В последнее время все чаще защищенность и достоверность доставки информации рассматриваются как равнозначные аспекты разработки и эксплуатации безопасных и высоконадежных систем передачи данных. Такой подход базируется на том, что актуальные информационные системы это в основном компьютерные системы на основе современных гетерогенных сетей передачи данных.

С точки зрения решения задачи коммутации в подобных Ethernet-сетях использование избыточности каналов связи является серьезной проблемой. В отличие от IP-пакетов, кадры Ethernet не содержат атрибут «время жизни» (TTL). Появление «петлевых линков» создает ситуацию, в которой кадры Ethernet бесконечно ретранслируются по созданному кольцу, накапливаются в очередях и замедляют передачу полезного трафика.

Избыточность каналов связи. Если в сети предприятия устройства коммутации предполагают использование единственного маршрута передачи данных – такая сеть надежной не является. Повреждение любого из каналов связи приведет к нарушению вычислительного процесса, связанного с сетевыми сервисами, одного или большего числа узлов сети. Аналогичная ситуация возникнет, если вместо канала связи будет повреждено любое из сетевых устройств. В зависимости от точки возникновения возможной аварийной ситуации структура сети делится на «домены возникновения сбоя». Если размер такого домена для канала связи стремится к 100% возникает необходимость внести избыточность в структуру каналов связи. Следствием пассивной избыточности каналов связи является возникновение петель коммутации. Из-за петель коммутации могут возникать: нестабильность базы данных MAC-адресов в привязке к порту устройства; многократная передача кадров одноадресной рассылки; многократная передача широковещательных кадров (широковещательный шторм). Во избежание возникновения петель коммутации требуется управление несколькими маршрутами со стороны самого устройства.

Для управления избыточностью каналов связи используются протоколы STP, PVST+, Rapid PVST+, MSTP (Multiple STP), SPB (Shortest Path Bridging). Метод

работы этих протоколов – заблокировать активность альтернативного канала во время передачи данных. В случае аварийной ситуации заблокированный канал связи может быть задействован и восстановление передачи данных не потребует немедленного вмешательства администратора. Длительность задержки, т.е. число пропущенных при передаче кадров данных, в этих протоколах различна. Администраторов сети интересует минимизация этого показателя, поэтому два из упомянутых протоколов получили коммерчески-ориентированную приставку к названию «Rapid», то есть «быстрый». На длительность задержки также оказывает влияние интервал времени, которое операционная система сетевого устройства затрачивает на определение роли порта. То есть следует упомянуть еще об одном протоколе – протоколе согласования режима порта DTP (Dynamic Trunking Protocol, динамический протокол транкинга). Надежность сети увеличивается, но скорость срабатывания механизма активации альтернативного канала различается в зависимости от типа протокола, режима его работы и особенностей реализации его конкретным производителем сетевого оборудования. Дополнительным фактором, который следует учитывать, является время подготовки устройства к работе. Оно увеличивается для сбора предварительной информации о топологии сети, распределения ролей между портами устройства и назначения их режимов. Эта задержка может сказаться на работоспособности ряда сетевых сервисов (например, DHCP распределения).

Согласно порядка действий инициализации протокола DTP портам коммутатора присваиваются следующие состояния:

- auto - порт находится в автоматическом режиме и будет переведён в состояние trunk, только если порт на другом конце находится в режиме on или desirable;
- desirable - порт находится в режиме «готов перейти в состояние trunk»; периодически передает DTP-кадры порту на другом конце, запрашивая удаленный порт перейти в состояние trunk;
- nonegotiate - порт готов перейти в режим trunk, но при этом не передает DTP-кадры порту на другом конце.

Порт согласовывает свое состояние с портом на соседнем устройстве. Возможные комбинации рабочих состояний представлены на рисунке 1.

Протокол MSTP (Multiple Spanning Tree Protocol) поддерживается операционными системами сетевых устройств компаний Cisco, HP, D-Link, Huawei и других. MSTP предполагает, что на всех коммутаторах, участвующие в MSTP, должны получить одинаково сконфигурированные группы VLAN (MST instances).

Резервирование интерфейса межсетевого перехода. В случае сбоя сетевого устройства или его интерфейса (IP-адрес которого используется в качестве шлюза по умолчанию), все узлы сети предприятия, для которых настроено использование этого шлюза по умолчанию, изолируются от внешних сетей. Наличие альтернативного маршрута обработать затруднительно из-за ограничений сетевого стека операционных

систем и механизмов согласования сетевых параметров протокола DHCP. Одним из способов для устранения единой точки отказа на шлюзе по умолчанию является реализация виртуального маршрутизатора. При совместном использовании IP-адреса и MAC-адреса два или более маршрутизаторов группы могут работать, как один виртуальный маршрутизатор. IP-адрес виртуального маршрутизатора настраивается в качестве шлюза по умолчанию для рабочих станций в отдельном сегменте IP.

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited Connectivity
Access	Access	Access	Limited Connectivity	Access

***Рисунок 1* – Режим порта коммутатора после обработки DTP**

Протоколы, обеспечивающие данный режим работы: HSRP (Cisco), GLBP (Cisco) и VRRP. Последние два предполагают распределение (балансировку) трафика через все маршрутизаторы группы.

Заключение. В результате анализа современных технологий по поддержке взаимодействия гетерогенных сетевых структур можно обозначить тенденцию о необходимости разработки конфигураций режимов сетевых устройств для использования протоколов MSTP, VRRP.

Список используемой литературы

1. Демиденко, О.М. Изучение влияния внешних помех на качество сигнала в сетях WI-FI. // О.М.Демиденко, В.Н. Кулинченко, / Проблемы физики, математики и техники. – 2015. – № 4 (25).– С. 96-99.
2. Кулинченко, В.Н. Диагностика беспроводных соединений локальных вычислительных сетей / Воруев, А.В. // Известия Гомельского государственного университета имени Ф. Скорины. – 2014.– № 6 (87).– С. 112-116.
3 Кулинченко, В.Н. Определение временных характеристик восстановления канала связи в различных модификациях протокола STP // Кулинченко, В.Н., Муха В.В. /Материалы XLV студенческой научно-практической конференции «Дни студенческой науки», 17–18 мая 2016 г.: в 2 ч. Ч. 1 – Гомель: ГГУ им. Ф. Скорины, 2016. – с.101-102

ABOUT THE ROLE OF CLOUD COMPUTING DATA PROCESSING AND BLOCKCHAIN TECHNOLOGY FOR ACCOUNTANTS AND AUDITORS

Leahovcenco Alexandru
Academy of Economic Studies of Moldova (ASEM),
str. Bănulescu-Bodoni 61, MD-2005, Chisinau, R. Moldova,
e-mail: alexandru.leahovcenco@yandex.com

Abstract. *In new era of technological revolution, it's become harder to organize and process data especially financial data, this paper describe the opportunities for auditors and accountants in the field of digital economy and help to understand the perspectives of their work in new technological environment such as could system and blockchain technologies.*

Keywords. *Cloud computing data processing, Blockchain, audit, digital economy*

1. Introduction

With the transition from an economy based on human force, to an economy based on information, automation of processes and technologies become unstoppable, the data becomes the main value by itself. As all known fact that the main tasks for any audit or consulting company is to attract new customers and earn a good reputation for themselves, but in our days enterprises and small business began to use more often cloud solutions to organize and storage of their data, as a result the prosses of automation of data processing can reduce the number of jobs in the financial sector, but how far as it is certain?

At the same time, last year's study by the International Association of Management Accounting Specialists (CIMA) revealed that companies are still very reluctant to resort to cloud computing, since, according to the majority (66%), data security has the highest priority. Only 25% of the companies out of a hundred implemented cloud technologies in their business systems, 19% apply them for financial reporting purposes, and 34% use it for Managerial Accounting [1].

The main prerogative of such companies is the ability to keep track of **client's business documents** at any time for better understanding of their financial situation, and it is good that day by day more enterprises are starting to organize their bookkeeping in cloud systems such as Xero, Pandle or 1C Cloud. In such approach all processes are automated, which greatly simplifies the case, in particular, with regard to the calculation of monthly wages of a staff.

The goal of this paper is to provide a possible vision on how can be realized an audit and account business in the next 10 years, and to show a perspective of developing of their workflow processing in the new technological areas such like could computing data process and blockchain technologies. The paper is organized as follows, section 2 reviews the key concepts of cloud computing data processing and blockchain

technology. Section 3 presents a business model of accountants and auditor's activities in the perspective of CCDP and block technology, Finally, Section 4 concludes this paper with the consequences of possible predictions of further development of business in these areas.

2. Definition of cloud computing data processing and blockchain technology

The main prerogative of every intelligent technology is an aptitude to organize and process data. Every year the data volumes are being processed and store by cloud systems but it is practically unreal for a human to process such massive data storage manually if it is necessary to make some analytical decisions so this dilemma result in two questions:

a) How can be organize the storage of data more effectively?
b) How this data can be processed more effectively?

As a solution can be used two technologies which, where actively evolving a few last years is a **blockchain technology** and **cloud computing data processing**.

The organization of data storage in a decentralized way can be developed in a several ways, as one of them is to storage data directly in Bitcoin blocks [2], this is the most ingenious way, in any case it solves the problem of decentralized storage, because the copy of every block of chains with data can be stored by anyone and cannot be changed.

Data can be encrypted, by using any cryptographic algorithm, so that anyone that supports storage can store a copy of encrypted data, but only a person with a private key would have access to it. But the chains of blocks (ex. Bitcoin) were not designed to handle large volumes of data. Their purpose is quite simple to storage transaction logs, even with such a small load, the bitcoin chain of blocks has reached over the last couple of years, the size of 38 GB [2]. Uploading data into a chain of blocks, force Bitcoin miners to store our data for free, depriving them of the incentive to maintain the network, because their costs start to exceed revenues. This solution looks already threatening, but the evolution of communication channels with light speed makes possible that tomorrow can be discovered a new era of data dissemination, in which data sets in a few petabytes will become commonplace. Storage data in the chain of blocks is not the best way to organize a reliable decentralized storage of data in the short term but it can be used as a start point for developing a new digital environment for data storing.

As a second one could be used a method to storage of data in a **distributed hash table (DHT)**. These tables distribute data copies and indexing functions that provide data retrieval and ensure reliability. The first truly effective implementation of DHT was the BitTorrent protocol. It is still used by more than 300 million users. Despite the decentralized storage of data (BitTorrent, Mainline DHT), it still depends on the performance of centralized trackers that are monitoring the network. As a second part in developing and scalability of decentralized data storage, can be used the new data transfer protocol know as **Interplanetary File System (IPFS)** [3].

Now when, there is a general idea of how data can be stored in a decentralized form it is time to comprehend how this data can be processed in a new way without a need to download and store it on a static machine for processing. If it can be assumed

that all data of enterprises is being store in cloud or block chains then it is logical to process this data ibidem.

The best solution for such task is a **cloud computing data processing** (CCDP) and here should be highlighted the difference between cloud computing data processing and **SaaS** (software as a service) which practically represents a software which can be rented and can be accessed remotely to execute practical need of a client. The CCDP can be represented as an algorithm that process **Big Data** in the publication of the journal of Science 2008, "Big Data" is defined as "Represents the progress of the human cognitive processes, usually includes data sets with sizes beyond the ability of current technology, method and theory to capture, manage, and process the data within a tolerable elapsed time" [4]. As well the definition of big data as also given by the Gartner: "Big Data are high-volume, high-velocity, and/or high-variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization" [5]. It's too much in volume to describe a new paradigm of a new global network based on blockchain technology but for better understanding could be presented **Blockchain-Based Decentralized Cloud Computing** known as iExec [6].

3. A business model of accountants and auditor's activities in the perspective of CCDP and block technology

Analyzing the state of the economy at current date, can be confidently confirmed that all operations of an economic and social nature are carried out exclusively in a virtual environment. Namely, searching for new partners for business, searching for goods in internet, their purchase, the taxes payments, dating in social networks, work activities. All important for the existence of humanity, economic relations are being produced in a virtual environment, for business this mean, most likely the next, that the former corporate structures will not work efficiently in the new digital economic environment, or even disappear. Considering this fact, can confidently assume that in the near future almost all current economic structures will be transferred in the virtual environment, and in our case, these will be enterprises that will be transformed into a new form of a digital enterprise.

The main features of a digital enterprise are as follows:

1. The enterprise exists exclusively in a virtual environment - this means that the enterprise is no longer legally bound to any country and is an independent structure in principle. "The term of virtual environment will be considered later".
2. Employees participating in the work of the enterprise and in its business processes can be located absolutely on any spot in the world.
3. Organization of work of employees and all relationships both in the enterprise itself and with other enterprises that are included in a virtual environment are carried out exclusively virtually with the exception of logistics.

Below is a schematic drawing that demonstrates exemplary relationships in a virtual environment. But first, for better understanding, must be explained the concept of virtual environment.

Virtual Environment - is a collection of network environment, network protocols and communication channels that establish interconnections of any unit that can access the virtual environment and here must be mentioned a fact what this environment can exist like under level of some sort of network like internet or blockchain based network or it can be developed like independent network that can be accessed throw internet or other communications channels.

As it shown in next figure, it's an example where users in our case accountants or auditors wish to make an analytical report based on data of several enterprises in classical case the data must be collected in particular from every enterprise but it is simple enough to admit that here can be applied a new concept where an account or audit make a request to a specific algorithm that's work in a virtual environment with a number of criteria that must be selected. The algorithm accesses the data that is based in cloud and analyze it when the requested criteria is found the algorithm send a result to user. To show the exclusivity of this method it is necessary to comprehend the idea that blockchain theology can be used more that just as data store it can be used like a tool to analyze data. The idea is to create a globe data storage based on blockchain theology which can include data of state structures. As a result of such adaptation of blockchain technology the relationship between economic agents will be in total different it means that decentralization and the absence of a hierarchical management structure will provide to a new aptitude for accountant business.

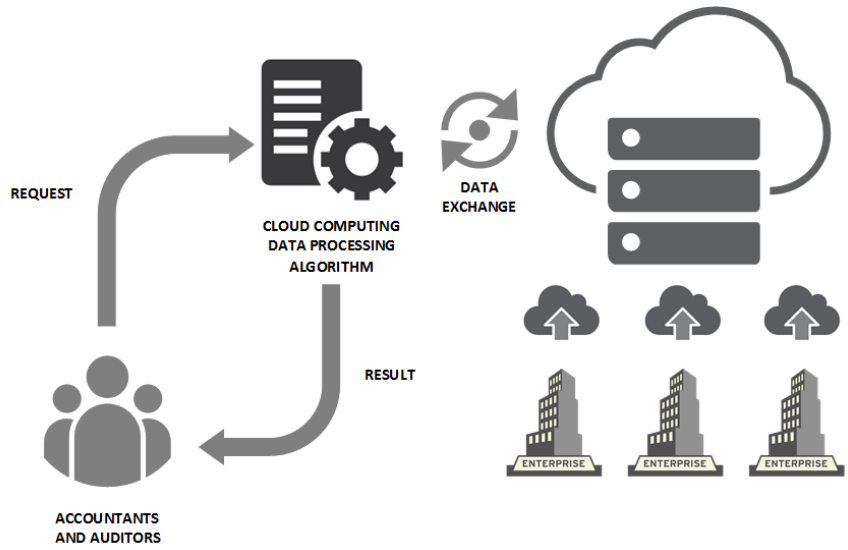


Figure 1. **Business model of CCDP and block technology**

In context of new economy, namely digital economy the role of CCDP and block technologies are vital and it appear to be what the role of the state as the main regulator in commercial transactions will be reduced, approaching to zero, although it will never reach it, since the exchange of goods, services and their payment occur outside the virtual

environment. In the case of economic relations in the digital economy, any agent is able to build strong contact with any other agent and begin to conduct economic activities with him without any border restrictions.

4. Conclusion

As a conclusion of this paper can be answered the question "How strong will be affected accountants and auditor?", as its clear from presented earlier information the time for changes has come, the fact that a new structure like digital economy is self-organize mechanism which adapts very quickly against aggressive external environment. This was made possible due to fast data transfer via the network channels that resulted in a quick response to a given request by any unit in the network. It will be very hard to manage such a fast-growing system but at least it can be directed in a right vector. Because in near future the meaning of accountant service will be critical changed. That means what accountant standards and methodologies must have a goal to develop mechanisms that can adapt to the virtual environment and make it safer to use instead to develop particular tools for every individual unit in the system like it is made in our days. It is necessary to develop a complex cloud storage based on block chain technology to unify all data flows in the global network what's why establishment of an international regime regulating developing of digital economy is important for the future of the international security environment and the security of all states that operate within.

Threats that will appear in virtual environment will affect every nation on earth therefore it's so important to presume and prevent their dissemination. The threats and challenges associated with the cyber domain will not dissipate on their instead they will continue to evolve. The process will certainly be complicated and time consuming. There will be disagreement between states regarding the specific nature of the problem, levels of state authority and responsibility, and the implications for state sovereignty.

The problem of establishing viable means of verification of compliance will be challenging. Multiple levels of coordination will need to be established, including interagency coordination within states, coordination between allies and partners, and global coordination and cooperation. Despite the difficulties associated with the formation of a global digital regime, makes to believe that such a regime will ultimately be achieved.

International cooperation will not be formed overnight, progress may be slow and incremental, but eventually the pieces will come together and the international community will unite in support of a mutually beneficial digital economy agreement.

References

1. The effects of cloud technology on management accounting and decision making, Volume 10 – Issue 6, https://www.cimaglobal.com/Research--Insight/The-effects-of-cloud-technology-on-management-accounting/.
2. Decentralized Applications - Harnessing Bitcoin's Blockchain Technology, by Siraj Raval : O'Reilly Media Release, July 2016 p 118, (44 - 56).

3. InterPlanetary File System, https://ipfs.io/.
4. "Big data: science in the petabyte era" Nature 455 (7209): 1, 2008.
5. Douglas and Laney, "The importance of 'big data': A definition," 2008.
6. Blockchain-Based Decentralized Cloud Computing https://iex.ec/.
7. Bradford De Long J., Froomkin A.M. The Next Economy. April 1997, http://www.law.miami.edu/~froomkin/articles/newecon.htm.
8. Barlow J. P. Selling Wine Without Bottles: The Economy of Mind on the Global Net: http://lib.ru/COPYRIGHT/barlou.txt.
9. Parinov S.I, Yakovleva T.I, Economy of the 21st century based on Internet technologies.
10. Big Data: Principles and Best Practices of Scalable Realtime Data Systems, by Nathan Marz, James Warren, p 328, 2015.
11. Computer Networking: A Top-Down Approach (6th Edition), by James F. Kurose, Keith W. Ross, p 880, 2012

ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ: «ЗА» И «ПРОТИВ»

Маклашевски А.С.
студентка SI-141
Экономическая академия Республики Молдова
Научный руководитель – Охрименко С.А.

The experience and practice of holding elections using electronic voting systems are considered. Special attention paid to the analysis of advantages and disadvantages of voting technologies using technologies and the Internet.

Ключевые слова: электронное голосование, выборы, внедрение, проблемы.

Разработка систем электронного голосования, начавшаяся в последние десятилетия XX века, была обусловлена стремительным развитием информационно – коммуникационных технологий, распространением доступа граждан к Интернету и сопровождалась ростом надежд на дальнейшее укрепление демократии.

Существующие системы электронного голосования предполагают, как непосредственное применение Интернет – технологий для учета волеизъявления граждан, так и использование специальных устройств. Интернет – голосование рассчитано на дистанционное участие избирателей в выборах и референдумах.

Против внедрения электронного голосования существует несколько причин: существующие системы передачи информации по каналам Всемирной сети весьма далеки от технического совершенства и слишком уязвимы с точки зрения потенциальным компьютерных сбоев и атак хакеров; серьезным доводом против введения Интернет – голосования служит «цифровое неравенство»; несоблюдение принципа тайны волеизъявления и фактическое превращение голосования в поименное: процедура электронной аутентификации избирателя посредством использования цифровой подписи, отпечатков пальцев, смарт – карты; несанкционированное вмешательство в избирательный процесс третьих лиц.

Принимая по внимание настоящий уровень развития информационных технологии, нельзя гарантировать, что программное обеспечение не будет подвержено манипуляциям, позволяющим хранить или распечатывать формы, отличные от тех, что отображаются на экране. Источник неполадок и сбоев оборудования вычислить и идентифицировать труднее, чем при использовании бумажных процедур. Не исключена возможность того, что в случае сбоя полностью автоматизированной системы и отсутствия резервной бумажной копии данных, пересчет голосов будет крайне проблематичным или вовсе неосуществимым.

Вероятно, самой крупной проблемой при дистанционном голосовании является обеспечение тайны голосования. Тем более что сценариев ее нарушения может быть достаточно много. Решением этой проблемы может стать действенная система идентификации на основе современных технологий, позволяющая гарантировать тайну голосования.

Из-за сложности протоколов электронного голосования, потенциальных компьютерных ошибок и хакерских атак избирательные комиссии возвращались к бумажным бюллетеням, урнам и ручному подсчету голосов.

Для электронного голосования, как и для современных средств коммуникаций посредством Интернета, существует еще одна значительная проблема – обучение. Несмотря на все старания разработчиков, дистанционное волеизъявление пока остается технически сложным.

Однако если говорить обо всех этих проблемах, нужно отметить, что они касаются не именно электронного голосования вообще, а технического воплощения электронного голосования, которое должно соответствовать всем предъявляемым в законе требованиям.

С другой стороны, технологии электронного голосования: могут предоставить возможность избирателям с ограниченными возможностями участвовать в голосовании без посторонней помощи и отдать свой голос в результате простой и тайной процедуры; привлекает большее число избирателей проголосовать в дистанционном режиме и таким образом увеличивает вероятность повышения явки «мобильного» электората; позволяет избирателям проголосовать вне пределов избирательного участка, в котором они зарегистрированы, и предлагает альтернативу избирателям, ранее голосовавшим по почте; снижают общие расходы по организации и проведению избирательного процесса с течением времени; позволяют осуществить подсчет голосов и объявить результаты выборов в более короткие сроки.

Кроме того, благодаря внедрению электронного голосования можно снизить вероятность искажения или подтасовки результатов за счет уменьшения влияния на весь процесс так называемого «человеческого фактора». Также пропагандируется снижение воздействия на избирателя местного административного ресурса.

Заключение:

Сторонники внедрения электронного голосования небезосновательно утверждают, что использование новейших технологий способствует повышению электоральной активности, вызывая у избирателей, прежде всего дополнительный интерес. В то же время, по справедливому мнению, критиков подобных проектов, использование электронных урн отнюдь не исключает возможности разного рода подтасовок и искажений результатов голосования вследствие вмешательства заинтересованных лиц в процесс разработки как самого оборудования, так и его программного обеспечения, подпадающих в целом ряде государств под действие законов о защите интеллектуальной собственности.

Литература:

1. Плюсы и минусы электронного голосования: https://www.golos-ameriki.ru/a/a-33-2007-11-04-voa4/631419.html
2. Выборы в интернете: за и против: https://cyberleninka.ru/article/n/elektronnoe-golosovanie-za-i-protiv
3. Значимость современных каналов коммуникации: http://elect-assist.ru/elektronnoe-pravitelstvo-elektronnoe-golosovanie-na-primere-estonii-i-ekvadora-znachimost-sovremennyx-kanalov-kommunikacii/

SEMNĂTURA ELECTRONICĂ CA MIJLOC DE AUTENTIFICARE

Viorel Malcoci
doctorand, Universitatea de stat a Moldovei

Abstract. *Lucrarea prezintă succint mecanismele de autentificare în baza funcțiilor criptografice realizate în semnătura electronică, considerată ca cel mai sigur instrument de autentificare și asigurare a confidențialității, integrității și non-repudierii informațiilor. Totodată, sunt prezentate câteva dintre utilizările semnăturii electronice pentru asigurarea schimbului de informații prin rețelele publice.*

Introducere

Dezvoltarea vertiginoasă a tehnologiilor și sistemelor informaționale, creșterea exponențială a volumului de date, informații și cunoștințe care circulă în societatea informațională, importanța acestora pentru dezvoltarea umană, creșterea simultană a numărului de atacuri asupra sistemelor și tehnologiilor informaționale, accesări nesancționate a informațiilor, impune noi preocupări de eficientizare a securității.

Majoritatea serviciilor informaționale contemporane, afaceri electronice (e-afaceri), e-comerț, e-plăți, e-educație etc. au la bază tehnologii informaționale (TI) moderne, rețele informatice, telefonia mobilă, Internet, Extranet etc. Pentru a profita de serviciile oferite prin aceste tehnologii, utilizatorul ar trebui, mai întâi, să-și demonstreze identitatea, că anume este persoana drept care se pretinde. Acest proces de stabilire a identității se numește ***autentificare.***

O altă problemă a comunicării moderne de date constă în asigurarea protecției informației care circulă în sistemele informaționale, precum și a păstrării/arhivării informaților în forma lor autentică, garantând respectarea următoarelor cerințe fundamentale de securitate informațională: *confidențialitatea* (asigurarea faptului ca informația este accesibilă doar persoanelor autorizate), *integritatea* (păstrarea acurateței și completitudinii informației și a metodelor de procesare), *disponibilitatea* (asigurarea faptului că utilizatorii autorizați au acces la informație și la resursele asociate atunci când este necesar) și *non-repudierea* (imposibilitatea negării, dezicerii de unele acțiuni săvârșite/efectuate)[1, cap. 1]. În acest scop pe lângă măsurile tehnico-organizatorice, cum ar fi elaborarea și implementarea politicilor, regulilor, instrucțiunilor, asigurarea protecției tehnice și logice a informației, este necesară implementarea *mecanismelor de autentificare,* bazate pe aplicarea metodelor criptografice de protecție și asigurare integrității informației și a sistemelor informaționale.

1. Particularități a mecanismelor de autentificare

Pentru asigurarea confidențialității și integrității informației sunt definite două tipuri de autentificare: *autentificarea entității* și *autentificarea emitentului de date* [6].

- *Autentificarea entității* este orientată spre verificarea în momentul inițierii conexiunii a identității unei entități de către alta printr-un mecanism de schimb reciproc de mesaje;
- *Autentificarea emitentului de date* asigură că sursa datelor expediate corespunde entității declarate. Acest mecanism asigură autenticitatea datelor, însă nu asigură protecția împotriva replicării sau modificării lor.

Autentificarea, în general, se realizează în urma schimbului de mesaje criptografice în care are loc partajarea unor informații secrete între entități. Prin urmare partajarea informațiilor secrete se bazate pe următorii factori:

- *Ceea ce cunoaște entitatea* – generic este un parametru secret, spre exemplu o parolă, un cod de acces etc. Dacă parametrul secret al entității corespunde cu cel prestabilit în sistem, atunci procedura de autentificare este reușită.
- *Ceea ce deține entitatea* – un dispozitiv material, care poate genera sau stoca sigur un parametru secret, ulterior acest dispozitiv fiind conectat într-un calculator gazdă, iar după verificarea datelor de autentificare stocate pe el se permite accesarea sistemului informațional. De regulă sunt utilizate carduri magnetice, tokene, smartphone-uri etc.
- *Ceea ce este propriu entității* – o caracteristică persistentă, permanentă, constantă și proprie naturii obiectului, fiind condiționată de acesta. De exemplu, autentificarea în baza unor dispozitive electronice care scanează datele biometrice ale entității, cum ar fi amprenta digitală, retina ochiului, irisul, vocea etc. și le compară cu cele stocate în sistem.

Metodele de autentificare bazate pe ceea ce cunoaște entitatea [1, p. 110-112], actualmente nu asigură o protecție suficientă a sistemelor și informațiilor. Pentru a avea un grad mai înalt de securitate a acestora este nevoie de implementarea mecanismelor mai avansate, bazate pe ceea ce deține entitatea cu utilizarea modelelor matematice moderne. Pentru acest scopul sunt utilizate protocoale criptografice, utilizând următoarele mecanisme de autentificare în baza funcțiilor criptografice:

- *mecanisme în baza codurilor de autentificare a mesajelor* MAC (Message Authentication Code) – $MAC_k(m)$ – cod de autentificare a mesajului m calculat cu cheia k, care permite o autentificare sigură a unui mesaj și se realizează în baza funcției hash, de exemplu, MD5 sau SHA1 prin utilizarea cheii secrete;
- *mecanisme în baza semnăturii electronice* ES (Electronic signature) – $ES_A(M)$ – aplicarea semnătura electronică a entității A asupra mesajului M, care se realizează în baza criptosistemelor cu cheii publice, astfel fiind asigurată autenticitatea informațiilor și determinată non-repudierea lor pentru entitatea emitentă.

În urma analizei comparative a funcțiilor criptografice $MAC_k(m)$ și $ES_A(M)$ se conturează avantajele oferite de către semnătura electronică prin faptul utilizării doar a unei chei publice pentru comunicarea cu mai multe entități, totodată rezolvându-se și problema schimbului de chei secrete.

Tabel 1

Analiza comparativă a sistemelor MAC și ES

$MAC_k(m)$		$ES_A(M)$	
avantaje	***dezavantaj***	***avantaje***	***dezavantaj***
Resurse mici pentru calcule aritmetice simple			Resurse mari pentru calcule aritmetice complexe
Lungime redusă a rezultatului funcției			Lungime mare a rezultatului funcției
	Se aplică chei secrete	Se aplică chei publice	
	Este necesar $n(n-1)/2$ chei secrete pentru a comunica cu n entități	Este suficienta o singura cheie publica pentru a comunica cu n entități	

2. Moduri de utilizare a semnăturii electronice

Prin sine, ***semnătura electronică*** reprezintă o consecutivitate de cifre de o lungime fixă care este calculată după anumite reguli cu ajutorul unor parametri cum ar fi mesajul destinat semnării, cheia privată a entității emitente pentru crearea semnăturii electronice și cheia publică pentru verificarea ei. Perechea de chei la rândul său, de asemenea este alcătuită din două consecutivități de cifre de lungime fixă care reprezintă elemente unice asociate fără de care nu poate fi creată și/sau verificată semnătura electronică a entității emitente.

Semnătura electronică poate fi utilizată în următoarele moduri:

- schimb protejat de mesaje;
- autentificarea mesajelor;
- combinat, schimb protejat de mesaje autentificate.

Schimbul protejat de mesaje, sau schimbul de mesaje criptate, presupune utilizarea de către entitatea emitentă (*Entitate A*) a cheii publice ($K_{Pub}{}^{B}$) a entității receptoare (*Entitate B*), care este utilizată pentru criptarea mesajului. Astfel decriptarea mesajului are loc doar cu ajutorul cheii private ($K_{Prv}{}^{B}$) corespunzătoare entității receptoare (*Entitatea B*) (figura. 1).

Figura 1. **Schimb de mesaje utilizând metoda asimetrică de criptare**

Autentificarea mesajelor presupune utilizarea de către entitatea emitentă (*Entitate A*) a cheii private proprii ($K_{Priv}{}^{A}$), care este utilizată pentru criptarea mesajului. Astfel decriptarea mesajului are loc doar cu ajutorul cheii publice ($K_{Pub}{}^{A}$) corespunzătoare entității emitente (*Entitatea A*) care este cunoscută de orișicine. În așa mod putem afirma

cu exactitate că semnatarul mesajului este entitatea căreia îi corespunde cheia K_{Priv}^{A}, adică *Entitatea A*.(figura. 2).

***Figura 2.* Autentificarea mesajelor utilizând metoda asimetrică de criptare**

Primul mod de utilizare ne permite să asigurăm confidențialitatea și integritatea mesajului expediat deoarece decriptarea poate fi efectuată doar de o singură entitatea care deține cheia privată, însă în acest caz nu este cunoscut nimic despre entitatea emițătoare.

Al doilea mod de utilizare ne permite să cunoaștem proveniența mesajelor ca rezultat al aplicării cheii private a entității emițătoare. Respectiv aplicând cheia publică a entității emițătoare, care este accesibilă și sunt cunoscute datele deținătorului, se asigură autenticitatea și non-repudierea mesajului expediat. În acest caz, cheia publică a emițătorului poate fi aplicată de orișicine care au obținut mesajul, legal sau ilegal, fiind pusă în pericol secretul corespondenței.

Pentru a obține o protecție sporită aceste două moduri pot fi combinate în așa fel în cât să se obțină un mod de schimb protejat de mesaje autentificate. În acest caz pentru expedierea unui mesaj mai întâi entitatea emitentă (*Entitate A*) aplică pentru criptare cheia privată proprie (K_{Priv}^{A}), iar apoi mai criptează încă odată rezultatul obținut cu cheia publică (K_{Pub}^{B}) a entității receptoare (*Entitate B*). Astfel, entitatea receptoare (*Entitatea B*) inițial va decripta mesajul cu cheia privată proprie (K_{Priv}^{B}), apoi va decripta repetat utilizând cheia publică a entității emitente (K_{Pub}^{A}). În acest mod fiind asigurată confidențialitatea, integritatea, autenticitatea și non-repudierea mesajului (figura. 3).

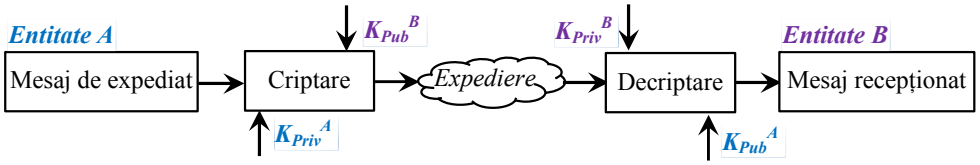


***Figura 3.* Schimbul protejat de mesaje autentificate utilizând metoda asimetrică de criptare**

Pentru rezolvarea problemelor de securitate a sistemelor informaționale și a accesului autorizat la date în practică semnătura electronică se utilizează mai des ca mijloc de autentificare a mesajelor sau schimb protejat de mesaje autentificate. Perechea de chei este generată de dispozitive sau aplicații specializate în așa fel încât cheia privată este păstrată în secret, iar cheia publică este supusă certificării.

2.1. Certificarea cheilor publice a semnăturii electronice

Certificarea cheilor publice reprezintă un proces organizațional de corelare între cheia publică generată pentru semnătura electronică și entitatea deținătoare de cheia publică respectivă în baza unor informații de identificare veridice ale entității deținătoare.

Certificarea cheilor publice are loc în cadrul unui centru de certificare. Rezultat al procedurii de certificare este certificatul cheii publice, cu ajutorul căruia poate fi garantată integritatea și autenticitatea datelor în procesul comunicării și care asigură o legătură strânsă între cheia publică și entitatea deținătoare a acestei chei publice.

Un *certificat al cheii publice* reprezintă un document electronic care conține cheia publică a entității și care este semnat de către centrul de certificare – emitentul certificatului. Suplimentar certificatul cheii publice conține și alte informații care identifică entitatea deținătoare. Odată ce a eliberat certificatul cheii publice, centrul de certificare garantează autenticitatea legăturii dintre cheia publică și entitatea deținătoare[4, p. 16].

Pentru certificatele cheilor publice formatul este prestabilit de standardul X.509, și include versiunea certificatului, numărul de înregistrare a certificatului, datele de identificare a prestatorului de servicii de certificare (organului de încredere), termenul de valabilitate a certificatului, datele de identificare a utilizatorului semnăturii electronice, cheia publică, algoritmul semnăturii emitentului certificatului, semnătura electronică a emitentului certificatului, termenul de valabilitate a cheii private, limitele de utilizare a cheilor, punctul de distribuție a listei certificatelor revocate și alte date [5].

Utilizarea autentificării prin certificate ale cheilor publice este pe larg utilizată pentru transmiterea protejată a datelor în rețeaua Internet. Cele mai răspândite protocoale care utilizează certificatele cheilor publice sunt:

- *protocol* TLS (*Transport Layer Security*), și SSL (*Secure Sockets Layer*). TLS permite aplicațiilor client-sever să comunice în rețea astfel încât este imposibil să fie recepționate pachetele și acces neautorizat;
- *protocolul* PPP (*Point-to-Point-Protocol*) – se utilizează pentru a stabili o conexiune directă între două noduri ale rețelei și asigură autentificarea conexiunii și criptarea;
- *protocolul* SSTP (*Secure Socket Tunneling Protocol*) – care se utilizează pentru crearea conexiunilor VPN (*Virtual Private Network*);
- *protocolul* SRTP (*Secure Real-time Transport Protocol*) – destinat pentru criptarea și stabilirea veridicității mesajelor, integrității, și protecției acestora.

2.2. Semnătura electronică ca mijloc de autentificare în Republica Moldova

Utilizarea semnăturii electronice în Republica Moldova este reglementată de Legea Nr. 91 din 29.05.2014 privind semnătura electronică și documentul electronic, prin care se stabilește regimul juridic al semnăturii electronice și al documentului electronic, inclusiv cerințele principale față de valabilitatea acestora și cerințele principale față de serviciile de certificare, iar semnătura electronică este definită ca date în formă electronică, care sunt atașate la sau logic asociate cu alte date în formă electronică și care sunt utilizate ca metodă de autentificare. [7, art. 1]. Prezenta lege stabilește următoarele tipuri de semnături electronice:

a) semnătura electronică simplă;

b) semnătura electronică avansată necalificată;
c) semnătura electronică avansată calificată.

Realizarea practică a mecanismelor semnăturii electronice în Republica Moldova este implementată prin serviciul electronic de autentificare și control al accesului (**MPass**) – un serviciu reutilizabil, găzduit pe platforma tehnologică guvernamentală comună, ce oferă un *mecanism integrator, securizat și flexibil de autentificare și control al accesului utilizatorilor în sistemele informaționale și serviciile electronice* [8, cap. I]. La moment, MPass oferă posibilitatea autentificării prin:

- Semnătura mobilă, eliberată de către operatorii naționali de telefonie mobilă Orange[1] și Moldcell[2];
- Semnătura electronică a Întreprinderii de Stat Centrul de telecomunicații speciale[3];
- Buletin de identitate electronic[4];
- Semnătura electronică a Întreprinderii de Stat Fiscservinform[5].

Printre servicii oferite de instituțiile statului cu autentificarea mediată de MPass se regăsesc:

- e-Raportare;
- e-Integritate;
- Registrul de Stat al Controalelor;
- e-Apostila;
- Depunerea petițiilor către Parlament;
- Portalul serviciilor electronice Registru;
- Servicii fiscale electronice.

În altă ordine de idei, pentru facilitarea schimbului de date dintre autorități precum și pentru creșterea eficienței și calității de prestare a serviciilor publice a fost creată platforma guvernamentală de interoperabilitate **MConnect**. Platforma de interoperabilitate este folosită în calitate de soluție tehnică ce asigură schimbul sigur de date dintre sistemele informaționale deținute de ministere și alte autorități ale administrației publice centrale subordonate Guvernului și structurile organizaționale din sfera lor de competentă, precum și de instituțiile publice autonome.

Pentru a asigura continuitatea schimbului de date sunt definite reguli de colectare, transmitere, conservare și restabilire a datelor. Aceste reguli includ măsuri și proceduri cum ar fi: identificarea unică a înregistrărilor, utilizarea obligatorie a metadatelor, *aplicarea semnăturii electronice*, mecanisme de restabilire, colectare, extragere, transportare garantată, conservarea și distrugerea datelor cu menținerea valorii probatorii a acestor [9, p.28].

[1] https://www.orange.md/?p=1&c=8&sc=87&s=872
[2] http://www.moldcell.md/rom/private/servicii/semnatura-mobila-0
[3] http://pki.cts.md/
[4] http://asp.gov.md/ro/buletin-de-indentitate-electronic
[5] https://pki.fsi.md

Prin intermediul cadrului de interoperabilitate autoritățile administrației publice, inclusiv și alte entități fac schimb de informații oficiale, ce pot implica accesul la registrele de stat. Dat fiind faptul că securitatea datelor este una dintre cele mai importante bariere pentru cadrul de interoperabilitate, acest schimb se realizează în mod sigur prin identificarea și autentificarea atât a entității emitente de date, cât și a entității receptoare utilizând certificatele cheii publice.

Concluzii

Actualmente semnătura electronică a devenit un instrument vital în procesul schimbului electronic de date și autentificării utilizatorilor. La moment aceasta reprezintă cel mai sigur mod de autentificare a persoanei în sistemele și serviciile electronice. Acest lucru se datorează modalității de creare a semnăturii electronice și utilizării mijloacelor tehnice dedicate în acest scop. În așa fel, pentru crearea și verificarea semnăturii electronice este necesară existența perechii de chei – cheia privată și cheia publică, un dispozitiv sau o aplicație specializată, care în baza documentului, unei funcției criptografice și cheii private creează și verifică semnătura electronică. În aceeași ordine de idei, este de atenționat că orice realizare a semnăturii electronice prevede limitarea accesului altor persoane la cheia privată prim măsurile tehnico-organizatorice, fapt care garantează siguranța acesteia și sporește nivelul de încredere față de semnătura electronică.

Un avantaj deosebit al semnăturii electronice constă în aceea, că ea conține mai multe informații despre semnatar decât cea olografă. Astfel, cheia privată și certificatul cheii publice conțin informație despre persoana care a aplicat semnătura electronică, cum ar fi numele, prenumele, numărul de identificare de stat (IDNP), numărul de telefon, locul de muncă, funcția deținută și alte date.

Ținând cont de dezvoltarea abundentă a tehnologiilor informaționale și utilizarea acestora pe scară largă în schimbul electronic de date, utilizarea semnăturii electronice în calitatea sa de mijloc de autentificare rezolvă o mare parte din problemele ce țin de asigurarea securității sistemelor informaționale, serviciilor electronice guvernamentale și a statului în întregime.

Comasarea opțiunilor de semnare și de autentificare în semnătura electronică asigură integritatea și autenticitatea datelor procesate/semnate, ca urmare mecanismul de semnătură electronică devine un mijloc comod și sigur pentru realizarea unui schimb sigur de date. Din aceste considerente mecanismul de semnătura electronică este promovat atât la nivel european, cât și la nivel național, prin crearea și dezvoltarea diverselor servicii de semnătură electronică, infrastructurii și cadrului normativ necesar.

Bibliografie

1. Bragaru Tudor, Malcoci Viorel, Galaicu Valeriu, Securitatea rețelelor informatice, Studia Universitatis Moldaviae, nr.8(98), 2017.
2. Gherman Teodora, Malcoci Viorel, Aspecte ale securității datelor în spațiul virtual, revista Administrarea Publică, nr. 2, 2014.

3. Simion Emil, Securitatea criptografică, suport de curs, 2011-2012.
4. Ротков Л. Ю., Зобнев А. В., Электронная цифровая подпись в электронном документообороте. Учебно-методические материалы. Нижний Новгород, 2006.
5. ITU-T Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC5280.
6. ISO 7498-2:1989(en). Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture.
7. Legea Nr. 91 din 29.05.2014 privind semnătura electronică și documentul electronic, publicată 04.07.2014 în Monitorul Oficial Nr. 174-177.
8. Hotărîrea Guvernului nr. 1090 din 31.12.2013, privind serviciul guvernamental de autentificare și control al accesului (MPass).
9. Hotărârea Guvernului nr.656 din 05.09.2012 cu privire la aprobarea Programului privind Cadrul de Interoperabilitate.

PROBLEMS OF THE NEUTRALIZATION OF THE INFORMATION THREATS OF THE FINANCIAL SECURITY OF THE STATE

Sergii Nazarenko, Nataliia Zachosova
Cherkasy National University named after Bogdan Khmelnytsky

Abstract. *The most popular and possible threats to the financial security of the country are given. Information threats, characteristic for financial institutions as the most active participants in the financial system of Ukraine, are identified.*

The importance of information threats for the national, economic, financial security of the country is recognized by the Government of Ukraine at the state level. So, in 2016 the Cybersecurity Strategy of Ukraine was adopted. In it, threats of informational nature for state security were cases of illegal collection, storage, use, destruction, distribution, personal data, illegal financial transactions, theft and fraud in the Internet. The document indicated that cybercrime becomes transnational and is capable of inflicting significant damage on the interests of the individual, society and the state. Increasingly, the information resources of financial institutions [1] become objects of cyberattacks and cybercrime, which we regard as a direct indication of the close connection between the level of cybercrime and the state of Ukraine's financial security. The government chose the National Bank of Ukraine as the subject of information threats neutralization in the financial environment, which was tasked with forming the requirements for cyber defense of critical information infrastructure in the banking sector [1]. However, it should not be forgotten that the country's financial security system has a complex structure, and is not limited to the security of the banking sector. Threats of information character are characteristic for other types of financial institutions, other than banks [2]. Thus, it is necessary to expand the list of subjects of ensuring cybersecurity of Ukraine with a view to organizing comprehensive protection of the financial sector and its participants.

As an attempt of state control of information threats for various subsystems of national security of the country became in 2017 the Doctrine of Information Security of Ukraine [3]. However, it did not pay attention to the problems of the financial sector; the emphasis was on the information war, which gained momentum in connection with the situation in the East. Therefore, this document can not be considered an information resource that can solve the problem of minimizing information threats to Ukraine's financial security.

Let us examine in more detail which types of information threats are typical for the country's financial security. The state of financial security at the macro level is based on the security of financial institutions and state regulators of the financial services markets. Therefore, the objects of information attacks for cybercriminals are financial institutions, their own assets and assets of their clients, information resources, databases. So,

information confidential for financial institutions (banks, insurance companies, investment funds, etc.) is included in the sphere of increased interest of competing financial companies. For unscrupulous competitors, corrupt officials and other intruders, information about the composition of bank management, their status and activities, especially if they have foreign investors, is of particular interest. Access to confidential information and its modification can significantly affect the financial position of the financial institution. At the same time, information leakage can be even partial. The reason for the leakage of information, if there is no proper provision of information security of the company, there may be various accidents caused by the inexperience of employees [4]. Employees were, are and will be the biggest problem for organizations of any kind of financial institutions. According to statistics, more than 60% of information leaks occur through the fault of the internal violator. Information often flows through electronic channels, so most financial institutions try to control all channels of information transfer: e-mail, Skype, ICQ, social networks.

As we mentioned earlier, special attention in the issue of ensuring the information and financial security of the state is given to the banking system. The banking system is a part of the critical infrastructure of the state, failures in the work of which can lead to disastrous consequences for the entire financial system. On October 4, 2017, the Resolution of the National Bank of Ukraine "On Approval of the Regulation on the Organization of Measures to Ensure Information Security in the Banking System of Ukraine" was published (hereinafter - Resolution No. 95). Ukrainian banks must until March 1, 2018 bring their own information security systems in line with the requirements, and in some cases - to build them from scratch. Thus, soon it will be possible to conclude how much new protection systems will be effective in comparison with the old ones.

In the context of Ukraine's integration into the European space, it is important for financial institutions to adhere to the standards of information protection adopted in the EU. The EU's requirements for the protection of confidential information are relevant to all organizations and institutions, including financial ones, without exception. They are documented in the form of the Regulation of the European Parliament and the Council of the European Union "On the Protection of Individuals in the Processing of Personal Data and on the Free Circulation of Such Data" No. 2016/679 of April 27, 2016. Thus, Ukraine needs to bring information security management systems in line with the requirements of the EU in the near future.

There are also a number of specific requirements applicable directly to Ukrainian banks. These are the requirements of the PCI DSS (Payment Card Industry Data Security Standard) to ensure the security of payment systems, as well as certain provisions of the standard 27001, etc. Resolution No 95 is more focused specifically on 27001, as well as a number of regulatory acts of the NBU aimed at ensuring the physical safety of banks.

The approach to the organization of information security is determined by three main factors. The first is the features of business processes in the organization. The second is the specifics of the information that is available and processed. And the third is

the circle of persons admitted to processing information. Regarding the last point - Resolution No. 95 provides the mandatory appointment of the person responsible for the information security of the bank - Chief Information Security Officer, CISO. That is, the functions of IT and information security will be delimited, as required by the standard 27001 [5].

The growth of IT-budgets becomes directly related to the practical component: financial organizations plan to increase security spending, facing a real threat. As an example, we can cite the cyber attack, which occurred in early summer of 2017 in Ukraine.

It is important that bank security specialists begin to prioritize the protection of business and reputation, and not just compliance with the requirements of the regulator. However, it must also be taken into account that, in addition to reputational losses, as additional risks may be rumors about a potential revocation of the license, when the problems with the information security of the bank raise the attention of the regulator. If the rumors are simultaneously associated with IS incidents, then the reputational threats grow extremely intensively, the outflow of clients, both private and corporate and public, starts, the credit rating suffers. The situation is growing like a snowball: the reputation suffers, the image of the company in the eyes of the public and the regulator is deteriorating, which in turn affects confidence and may entail the revocation of the license [6]. The withdrawal of banks from the market entails not fulfilling their obligations to clients, which undermines the confidence of the population and business in the financial system as a whole, and has a negative effect on the state of the country's financial security.

As before, DDoS attacks on financial sector organizations are arranged more often than on companies from other industries, for example, retail, media. However, now it is important not only that the attackers possess all the fullness of knowledge, where exactly the means of interest are stored, but also they understand by what methods this money can be obtained. By launching a DDoS attack as a distraction, attackers can use malware to capture a cashless payment management system and thus are able to transfer money between any accounts until they are discovered. It follows that the protection systems used in financial institutions are imperfect, and approaches to the development of the IT infrastructure need to be reviewed and updated [6].

Another significant threat to the financial security of the country is the popularization of crypto-currencies. Already now, the facts of obtaining crypto-currency on the servers of state information systems are known. Illegal activities were carried out by employees of information units of state structures that have access to powerful servers. In the mining of crypto-currencies, the servers of information systems of departments, their regional divisions, as well as the most productive office computers of employees were involved. To this end, special programs (miners) were secretly installed on servers and computers, which used computational resources, which reduced the processing speed of information and slowed down their work. These programs were installed in the form of system services and added to the list of programs that are used to exclude antivirus

programs. Thus, the resources were used for other purposes, which could have enormous consequences for national security.

Thus, it is necessary to create an Information Security Strategy at the state level, in which a separate paragraph would identify informational threats for the financial security of Ukraine, as well as strategic and tactical actions to minimize them.

References:

1. Стратегія кібербезпеки України *[Cybersecurity Strategy of Ukraine]* [Электронный ресурс] : Указ Президента України від 15 березня 2016 року № 96/2016 [*Decree of the President of Ukraine dated March 15, 2016 No. 96/2016].* – Режим доступа : http://zakon3.rada.gov.ua/laws/show/96/2016.
2. Фурман В.М., Зачосова Н.В. *[Furman V.M., Zachosova N.V.]* (2015) Сучасні загрози економічній безпеці вітчизняних фінансових установ (на прикладі банківських установ і страхових компаній) *[Modern threats to the economic security of domestic financial institutions (for example, banking institutions and insurance companies)]* // Журнал «Інвестиції: практика та досвід» *[The magazine "Investments: Practice and Experience"]*, №16, 7-11.
3. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» *[On the decision of the Council of National Security and Defense of Ukraine dated December 29, 2016 "On the Doctrine of Information Security of Ukraine"]* [Электронный ресурс]. – Режим доступа : http://www.president.gov.ua/documents/472017-21374.
4. Обеспечение информационной безопасности организации *[Ensuring information security of the organization]* [Электронный ресурс]. – Режим доступа : http://www.iccwbo.ru/blog/2016/obespechenie-informatsionnoy-bezopasnosti.
5. Информационная безопасность в украинских банках: инициативы НБУ глазами практика *[Information security in Ukrainian banks: NBU initiatives with eyes of practice]* [Электронный ресурс]. – Режим доступа : https://idev-hub.com/news/ynformatsyonnaya-bezopasnost-v-ukraynskyh-bankah-ynytsyatyvy-nbu-glazamy-praktyka/.
6. Информационная безопасность в финансовом секторе *[Information security in the financial sector]* [Электронный ресурс]. – Режим доступа : https://qrator.net/content/qrator_banks_2017.pdf

ROOTKITS УГРОЗА IT БЕЗОПАСНОСТИ

Откидач К.И.
студент SI-141 Экономическая академия Республики Молдова

Annotation: *A root kit is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that is not otherwise allowed (for example, to an unauthorized user) and often masks its existence or the existence of other software. The term rootkit is a concatenation of "root" (the traditional name of the privileged account on Unix-like operating systems) and the word "kit" (which refers to the software components that implement the tool). The term "rootkit" has negative connotations through its association with malware.*

Keywords: *DDoS attack, backdoor, masking of objects, data collection, Direct Kernel Object Manipulation.*

На сегодняшние дни компьютерные технологии развиваются стремительными темпами, но еще быстрее растут многочисленные угрозы информационной безопасности. В связи с этим наша информационная система постоянно подвергается как внутренним так и внешним угрозам со стороны нарушителей.

Одной из самых распространённых угроз , как для обычных пользователей и для корпоративных компаний, является Руткиты.

Представляется необходимым рассмотреть термин Руткит [**1**]**.** Руткиты существуют уже около 20 лет, помогая атакующим действовать на компьютерах своих жертв, подолгу оставаясь незамеченными. Термин нередко применяется к тем вредоносным программам, которые специально созданы так, чтобы действовать на зараженном компьютере скрытно и при этом позволять удаленно контролировать ПК. Поскольку руткиты относятся к наиболее неприятным разновидностям вредоносных приложений, я решил кратко объяснить, каков принцип действия руткита и как поступать, если вы подозреваете, что компьютер заражен подобной гадостью.

Содержание вредоносных инструментов в Рутките [**2**]**.** Руткит может содержать различные вредоносные инструменты, такие как:

- клавиатурный шпион;
- вор сохраненных паролей;
- сканер данных о банковских карточках;
- дистанционно управляемый бот для осуществления DDoS-атак;
- функции для отключения антивирусов.

Руткит обычно имеет также функции бэкдора, то есть он позволяет атакующему дистанционно подключаться к зараженному компьютеру, устанавливать или удалять дополнительные модули и таким образом делать с машиной все, что подскажет фантазия. Некоторые примеры актуальных сегодня руткитов для Windows это:

- TDSS;

- ZeroAccess;
- Alureon;
- Necurs.

Вариация Руткитов [3]**.** Руткиты делятся на две категории:

- уровня пользователя
- уровня ядра

Первые получают те же права, что обычное приложение, запущенное на компьютере. Они внедряются в другие запущенные процессы и используют их память. Это более распространенный вариант.

Что касается руткитов уровня ядра, то они работают на самом глубинном уровне ОС, получая максимальный уровень доступа на компьютере. После инсталляции такого руткита, возможности атакующего практически безграничны. Руткиты уровня ядра обычно более сложны в создании, поэтому встречаются реже. Также их гораздо сложней обнаружить и удалить.

Есть и еще более экзотические вариации, такие как буткиты (bootkit), которые модифицируют загрузчик компьютера и получают управление еще даже до запуска операционной системы. В последние годы появились также мобильные руткиты, атакующие смартфоны под управлением Android.

Метод инфицирования Руткита [4]**.** Первично руткиты попадают на компьютер так же, как другие вредоносные приложения. Обычно используется уязвимость в браузере или плагине, также популярный способ заражения – через USB-флешки. Атакующие иногда даже оставляют зараженные флешки в общественных местах, где их может подобрать подходящая жертва. Затем руткит использует уязвимости ОС чтобы получить привилегированное положение в системе и устанавливает дополнительные компоненты, обеспечивающие удаленный доступ к компьютеру и другую вредоносную функциональность.

Удаление Руткита [5]**.** Основная сложность борьбы с руткитами в том, что они активно противодействуют своему обнаружению, пряча свои файлы и ключи реестра от сканирующих программ, а также применяя другие методики. Существуют утилиты, специально созданные для поиска известных и неизвестных руткитов разными узкоспециальными методами, а также с помощью сигнатурного и поведенческого анализа. Удаление руткита – тоже сложный и многоэтапный процесс, который редко сводится к удалению пары файлов. Обычно приходится применять специальную программу, такую как TDSSkiller, созданную для борьбы с руткитом TDSS. В некоторых случаях жертве даже приходится переустанавливать операционную систему, если в результате заражения компьютерные файлы повреждены слишком глубоко. Для менее сложных и вредоносных руткитов удаление может быть осуществлено с помощью обычной функции лечения в антивирусной программе.

Заключение: В заключение хотелось бы упомянуть, что мы не должны не обращать внимание на угрозы применяемые при помощи использования руткитов.

Необходимо осознать угрозы и принять меры по их минимизации. В первую очередь корпоративным компания следует:

- Разработать политику безопасности предприятия;
- Использовать программные обеспечения защиты ОС;
- Проводить мониторинг системы, как внутренней, так и внешней;
- Проводить тренинги в рамках IT безопасности.

Литература:

1. Тема: Классификация руткитов[1], http://qoo.by/3WOx
2. Тема: Вариации и удаление руткитов [2], http://qoo.by/3WOB
3. Тема: анализ риска руткита[3], http://qoo.by/3WOS

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПРОБЛЕМЫ ЕЕ ОБЕСПЕЧЕНИЯ В РЕСПУБЛИКЕ БЕЛАРУСЬ

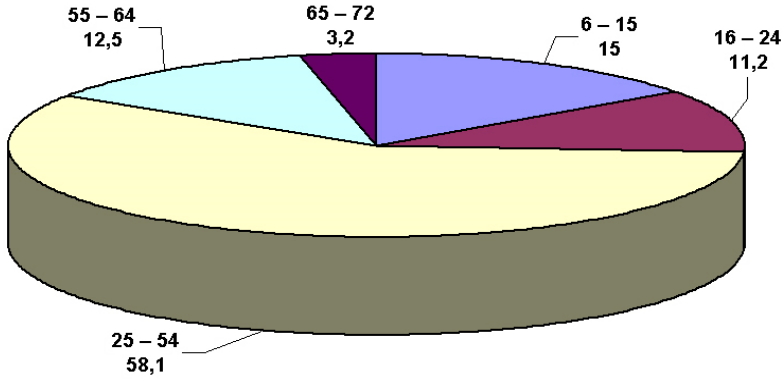
Ольга Пугачева
Гомельский государственный университет имени Ф.Скорины

The issues of the necessity to form an information security policy, as well as the main problems of its ensuring of the Republic of Belarus

Цифровая трансформация экономики является одним из приоритетов социально-экономического развития Беларуси. Определенных успехов в этой сфере уже удалось добиться. По ряду показателей страна выглядит вполне прогрессивно, хотя еще уступает развитым странам Евросоюза.

На конец 2016 г. в республике числилось 11083 тыс. абонентов всех видов передачи данных с выходом в Интернет – почти вдвое больше, чем в 2010 г. Такие сведения приведены в статистическом сборнике «Социальное положение и уровень жизни населения Республики Беларусь» [1]. При этом удельный вес домохозяйств, имеющих доступ к Интернету с домашнего компьютера, тоже удвоился за этот период: с 31,2 до 62,5%. Возрастная структура интернет-пользователей в 2016 г. представлена на рисунке 1.

Рис. 1. Возрастная структура интернет-пользователей в Беларуси в 2016 г. (лет/%)

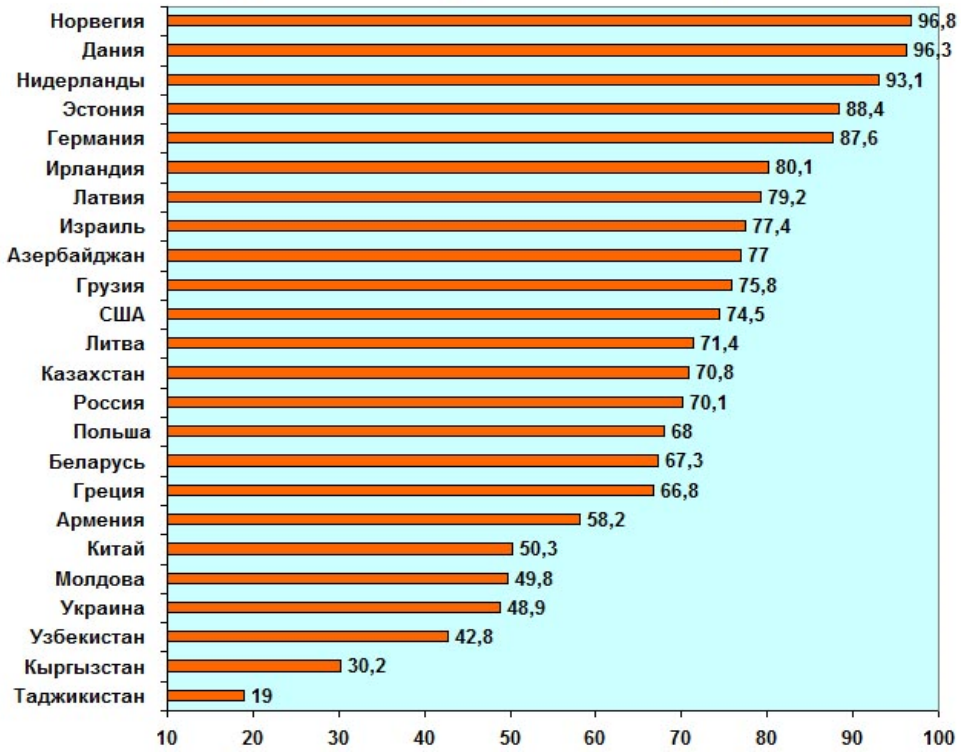


В рейтинге ИКТ, составляемом Международным союзом электросвязи, Республика Беларусь занимает 31-е место из 175, опережая остальные страны СНГ [1]. Но по охвату Интернетом Беларусь выглядит вполне средне: он выше, чем в большинстве стран СНГ (кроме России), Китае и Турции, но ниже, чем в странах Балтии и развитых странах ЕС (рисунок 2).

Такое положение обостряет проблемы в области сетевой безопасности в Беларуси и требует анализа новых вызовов и практики борьбы с преступлениями в сфере высоких технологий, а также развития международного сотрудничества, юридических и технических средств защиты от киберугроз.

Республика Беларусь заняла 39-е место из 165 в Глобальном рейтинге кибербезопасности (Global Cybersecurity Index 2017), составленном Международным союзом электросвязи и ABI Research.

Рис. 2. Удельный вес интернет-пользователей (в % за 2015 г.)



Глобальный индекс кибербезопасности (GCI) отражает уровень киберзащищенности государств и усилия, которые прилагает страна для его улучшения. При составлении GCI учитывается уровень обязательств в 5 сферах – правовые, технические меры, организационные, развитие потенциала и международное сотрудничество.

Лидерами рейтинга кибербезопасности являются Сингапур, США, Малайзия. Китай занял 32-е место, Польша – 33-е. Республика Беларусь с индексом 0,59 заняла 39-е место в общем рейтинге (таблица 1) и 3-е среди стран СНГ.

Среди постсоветских стран наилучших результатов добились Эстония, занявшая 5-е место, Грузия – 8-е и Россия – 10-е (0,78). Латвия заняла 22-е место, Литва – 57-е, Азербайджан – 48-е, Украина – 59-е, Молдова – 73-е, Казахстан – 83-е, Таджикистан – 91-е, Узбекистан – 93-е, Армения – 111-е, Туркменистан – 132-е. Замыкают список в Глобальном рейтинге кибербезопасности Экваториальная Гвинея, Йемен и ЦАР [2].

Таблица 1

Место Республики Беларусь в Глобальном рейтинге кибербезопасности в 2017 году

Страна	Законода-тельство	Технические меры	Организацион-ные меры	Потенциал	Междуна-родное сотрудни-чество	Итого
Сингапур	0,95	0,96	0,88	0,97	0,87	0,92
США	1,00	0,96	0,92	1,00	0,73	0,91
Малайзия	0,87	0,96	0,77	1,00	0,87	0,89
Эстония	0,99	0,82	0,85	0,94	0,64	0,84
…						
Грузия	0,91	0,77	0,82	0,90	0,70	0,81
Россия	0,82	0,67	0,85	0,91	0,70	0,78
Беларусь	0,85	0,63	0,33	0,68	0,47	0,59

Республика Беларусь традиционно занимает высокие позиции по уровню риска заражения через интернет, которому подвергаются компьютеры пользователей в разных странах мира. По данным Kaspersky Security Network, 27% белорусских пользователей столкнулись со срабатыванием веб-антивируса. Таким образом, страна оказалась на 8-м месте в рейтинге стран с наибольшим риском заражения через интернет [3].

Является очевидным, что в отдельно взятой стране невозможно построить безопасный интернет, поскольку современные угрозы транснациональны. Поэтому в Беларуси выстраивается система работы в этой области на основе международных практик, внедряются правовые акты, которые определяют, как на рынке действуют те или иные компании.

Так, в 2010 г. в Беларуси появился институт уполномоченных поставщиков интернет-услуг – провайдеров, которые оказывают услуги для госорганов (хостинга и передачи данных). Они должны выполнять ряд требований по безопасности, которые корректируются в зависимости от существующих угроз. Эта система позволяет каждому из них создать базовую модель безопасности и предоставлять через нее безопасные услуги.

В Беларуси создана команда реагирования на компьютерные инциденты – Cert.by, через которую ведется взаимодействие с аналогичными командами во всем мире. Происходит обмен информацией о текущих угрозах, взаимодействие в части предупреждения. На территории Европы нет проблем при взаимодействии в юридическом или техническом плане. Но когда поддержка нужна специалистам другой страны, тех же США, Австралии, Беларуси, то возникают проблемы юридического характера. Сегодня важный международный документ в этой сфере – Будапештская конвенция киберпреступности, и, несмотря на то, что некоторые страны не хотят ее ратифицировать, это реально работающий правовой инструмент. Белорусское уголовное законодательство практически полностью повторяет Будапештскую конвенцию.

С целью обеспечения кибербезопасности Нацбанк Республики Беларусь объявил о создании центра мониторинга и противодействия компьютерным атакам в кредитно-финансовой сфере (FinCERT) по примеру российских и прочих зарубежных коллег. Опыт работы в белорусской банковской сфере, в т.ч. по вопросам информационной безопасности, подсказывает, что при создании подобной структуры придется столкнуться с рядом проблем.

Любой банк крайне зависим от своих информационных систем и информационной инфраструктуры. Если одновременно будут атакованы все серверы какого-нибудь крупного банка, это будет коллапс с огромными потерями. Поэтому естественно желание регулятора как-то стандартизировать работу информационных систем и, главное, – отслеживать любые инциденты, влияющие на их работу. В целом процедура мониторинга описана в ТКП 288-2010 (07040) «Банковские технологии. Управление рисками в сфере информационных технологий» и содержит перечень типовых источников (причин) рисков в сфере информационных технологий, по которым каждый банк отчитывается перед регулятором. На деле отдел рисков банка отсылает профильным руководителям (IT и информационная безопасность чаще всего) формы таблиц, которые те с определенной периодичностью заполняют. Отдел рисков консолидирует эту информацию и отсылает регулятору.

На этом этапе обеспечения кибербезопасности возникают следующие проблемы [4]. Во-первых, это связано с самой процедурой мониторинга событий, будь то шпионаж, хищение активов, утечка информации и т.п. Их отслеживание требует серьезных и дорогостоящих систем. Например, DLP (Data Leak Prevention) системы, SIEM (security information and event management), организованы SOC (Security Operation Center) и другие. Любая из них стоит сотни тысяч долларов. Далеко не у всех белорусских банков они есть. Но без них нельзя эффективно собирать данные о проблемах в информационных системах и предоставлять регулятору полные и точные сведения.

Во-вторых, кадровая проблема. Обучить специалиста пользованию сложными SIEM- системами стоит около 4 тыс. у.е. Соответственно, таких людей на рынке крайне мало и стоят они дорого. Даже если банк оплатит учебу для своего сотрудника, это не значит, что он станет платить ему зарплату в соответствии с ее рыночным уровнем.

Третья и наиболее важная проблема в том, что банки не хотят делиться информацией об инцидентах и проблемах, опасаясь внеплановых проверок регулятора или иных неприятностей.

Работа создаваемого центра должна быть направлена по четырем типам инцидентов:

- DDoS-атаки;
- несанкционированный доступ к конфиденциальной информации;
- мошеннические SMS и звонки;
- вредоносное программное обеспечение (ПО).

Направлений может быть больше, вплоть до поиска уязвимостей в инфраструктуре отдельных банков [5].

Предполагается, что специалисты FinCERT будут проводить мониторинг ситуации в интернете, СМИ, по любым открытым и закрытым источникам, оперативно получать информацию от профильных силовых структур, получать информацию от банков, которые подверглись атакам. На основании собранной информации должны формироваться рекомендации по борьбе с этими атаками и инцидентами, а также оперативно рассылаться по всем, кто будет подключен к системе.

Однако по-прежнему сохраняются все те же проблемы.

Во-первых, непонятно, как эффективно консолидировать информацию, поскольку нет уверенности, что в этом согласятся участвовать специалисты по расследованию преступлений против информационной безопасности и интеллектуальной собственности главного следственного управления СК Республики Беларусь или Оперативно-аналитического центра при Президенте (ОАЦ), да и банки будут крайне неохотно предоставлять информацию об инцидентах.

Во-вторых, кадровый вопрос. Хороший специалист по кибербезопасности стоит на рынке 2–3 тыс. у.е., профильный руководитель – около 5 тыс. у.е. Даже если найдутся молодые талантливые кадры или эти места займут представители спецслужб, то их придется обучать и мотивировать. Но нельзя исключать того, что через некоторое время эти кадры начнут уезжать в западном или восточном направлении, туда, где спрос на таких специалистов и их заработки выше.

Таким образом, кибербезопасность – понятие комплексное. Для ее обеспечения, по мнению экспертов, необходима специальная работа, в том числе через законодательство, через реализацию политики безопасности.

Литература

1 Социальное положение и уровень жизни населения Республики Беларусь. Национальный статистический комитет Республики Беларусь [Электронный ресурс]. – Режим доступа: http://www.belstat.gov.by/ - Дата доступа: 15.02.18

2 Measuring the Information Society ICT Opportunity Index and World Telecommunication/ICT Indicators – 2017 - Сайт Международного союза электросвязи [Электронный ресурс] – Режим доступа: http://www.itu.int/en/publications/Pages/default.aspx - Дата доступа: 10.02.18

3. Информационная безопасность бизнеса [Электронный ресурс]. – Режим доступа: http://media.kaspersky.com/pdf/it_risk_report_russia_2014.pdf - Дата доступа: 5.02.18

4 «Безопасность в Интернете» Форум по управлению интернетом (Belarus IGF-2017) - [Электронный ресурс] – Режим доступа: https://igf.by/BelarusIGF-2017.pdf- Дата доступа: 14.02.18

5 XIV Международный форум по банковским информационным технологиям "БанкИТ'2017") - [Электронный ресурс] – Режим доступа: http://bankit.it-event.pro/ - Дата доступа: 4.02.18

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И БОРЬБА С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Ольга Пугачева
Гомельский государственный университет имени Ф.Скорины

Based on the analysis of users of the Internet and the information technology market, the main threats and recommendations on combating them of the Republic of Belarus

Важнейшими факторами повышения конкурентоспособности базовых отраслей и успешного развития новых секторов экономики Республики Беларусь являются комплексная цифровая трансформация экономики (информатизация), широкое внедрение информационно-коммуникационных технологий.

Ускоренное развитие информационно-коммуникационных технологий как ключевой составляющей инновационной стратегии предусматривается осуществлять за счет: дальнейшего развития мультисервисной системы электросвязи, широкополосного доступа в сеть Интернет, цифрового телевизионного вещания, сотовой связи следующего поколения; информатизации всех сфер социально-экономического развития; расширения внутреннего рынка путем стимулирования внедрения информационно-коммуникационных технологий в реальном секторе экономики, социальной сфере, государственном управлении, в том числе для предоставления государственных услуг и осуществления административных процедур в электронном виде.

На основе сведений, приведенных в статистическом сборнике «Социальное положение и уровень жизни населения Республики Беларусь», можно сделать следующий интернет-портрет белорусских пользователей всемирной сети [1].

Распределение интернет-пользователей по частоте выхода в Интернет в 2016 г. представлено в таблице 1 (здесь и далее – по данным выборочного обследования домашних хозяйств по уровню жизни, в % к итогу).

Таблица 1

Распределение интернет-пользователей по частоте выхода в Интернет в 2016 г.

	ежедневно	**не менее 1 раза в неделю**	**от случая к случаю**
Всего	68,3	16,2	15,5
города и поселки городского типа	70,6	15,5	13,9
сельские населенные пункты	59,2	19,3	21,5

Распределение интернет-пользователей по месту выхода в сеть Интернет в 2016 г. (в % от общего числа интернет-пользователей соответствующей группы) представлено в таблице 2.

Таблица 2

Распределение интернет-пользователей по месту выхода в сеть Интернет в 2016 г.

	через проводную сеть или Wi-Fi					в любом месте через сеть сотовой подвижной электросвязи
	дома	по месту работы	по месту учебы	у родствен-ников, знакомых	в компьютерном клубе, интернет-кафе и т.д.	
Всего	93,5	19,1	4,4	27,7	9,8	56,5
по месту проживания:						
города и поселки городского типа	94,3	20,5	4,5	29,0	11,5	60,3
сельские населенные пункты	90,3	13,8	4,2	22,9	3,2	41,9

Распределение интернет-пользователей по целям выхода в сеть Интернет в 2016 г. представлено в таблице 3 (в % от общего числа интернет-пользователей соответствующей группы).

Таблица 3

Распределение интернет-пользователей по целям выхода в сеть Интернет в 2016 г.

	Всего	в т.ч.	
		города и поселки городского типа	сельские населенные пункты
поиск информации	92,6	94,3	86,0
просмотр и скачивание фильмов, прослушивание и скачивание музыки и т.д.	79,8	80,1	78,8
общения в социальных сетях	74,7	76,0	69,6
отправки, получения электронной почты, переговоров	52,8	56,9	36,9
компьютерные игры	46,9	46,4	49,1
осуществления финансовых операций	29,8	32,9	17,7
покупки товаров, получения услуг	28,6	31,6	17,1
образование	23,2	23,2	23,1
взаимодействие с органами госуправления	13,0	15,2	4,6

Уровень удовлетворенности белорусских интернет-пользователей качеством услуг сети Интернет в 2016 г. представлен в таблице 4. При этом отношение в регионах существенно отличается. Например, в Гомельской области все устраивает 47,8% пользователей, Могилевской – 48,3%, Брестской – 43,1%, Минской – 45%, а в столице – только 38%. Больше всего скорее недовольных и совершенно недовольных

качеством интернет-услуг в Витебской области (8,5% и 1,7% соответственно), тогда как в Минске их всего 3,4% и 0,6%.

Таблица 4

Уровень удовлетворенности белорусских интернет-пользователей качеством услуг сети Интернет в 2016 г.

	Всего	в т.ч.	
		города и поселки городского типа	сельские населенные пункты
полностью удовлетворены	43,8	42,3	49,6
скорее удовлетворены	42,4	43,4	38,6
и да, и нет	8,0	8,3	6,8
скорее не удовлетворены	5,1	5,4	4,0
совершенно не удовлетворены	0,7	0,6	1,0

В 2016–2020 гг. белорусские власти намерены добиваться существенных сдвигов в сфере информатизации. Для этого в Программе социально-экономического развития сформулировано 12 ключевых задач [2]. Среди них – создание современной инфраструктуры телекоммуникаций в Восточной Европе. За 5 лет планируется построить около 10 тыс. км волоконно-оптических линий связи для всей многоэтажной жилой и общественной застройки. Прогнозируется, что к концу 2020 г. около 35% населения страны будет пользоваться данными услугами, 90% населения станет пользователями услуг беспроводного широкополосного доступа к сети Интернет, а уровень проникновения Интернета к 2020 г. должен составить минимум 82% домохозяйств.

Предполагается создание полноценного электронного правительства и перевод в электронный формат к концу 2020 г. 75% административных процедур. При этом 40% населения должны стать пользователями Общегосударственной автоматизированной информационной системы, а все граждане страны к 2018 г. смогут использовать цифровую подпись.

Также запланировано создание сектора информационных услуг для населения и бизнеса, широкомасштабное использование электронных документов в коммерческой деятельности, включая разрешительную, фискальную, контрактную, платежную и товарно-сопроводительную функции, создание единой системы электронного здравоохранения, расширение ИТ-технологий в торговле, банковской сфере, государственном управлении, нотариате, образовании и других сферах.

Анализ рынка высоких технологий в Беларуси в 2017 году показал, что криминогенная обстановка на нем остается напряженной. На основе материалов конференции, посвященной информационной безопасности, с представителями Следственного комитета, управления «К» МВД и Национального центра законодательства и правовых исследований (НЦЗПИ) можно сформулировать основные угрозы и рекомендации по борьбе с ними [3].

Самыми распространенными угрозами являются вредоносное программное обеспечение (ПО) и неправильное использование корпоративных ИТ-ресурсов.

Количество «виртуальных» преступлений в Беларуси за год выросло на четверть (с 2471 до 3099), и в основном это хищения.

Почти три четверти злодеяний в киберпространстве связаны с хищениями путем использования компьютерной техники (ст. 212 УК Беларуси). Кроме того, на 20% (с 651 до 781) увеличилось количество выявленных преступлений против информационной безопасности (ст.ст. 349-355 УК). В первую очередь это обусловлено ростом числа фактов неправомерного завладения компьютерной информацией (с 13 до 29), а также случаев модификации компьютерной информации (с 13 до 25) и несанкционированного доступа к компьютерной информации (с 258 до 462). Сумма ущерба от противоправных действий в виртуальном пространстве в 2017 году составила Br3,2 млн. Эти данные можно смело умножать в несколько раз, уверены сотрудники силовых ведомств, потому что о киберпреступлениях в милицию заявляют не так часто. Потерпевшие, да и преступники все еще убеждены, что раскрыть «виртуальные» преступления случаи отечественной милиции не под силу, но это не так. В 2017 году сотрудники подразделений по раскрытию преступлений в сфере высоких технологий криминальной милиции Министерства внутренних дел Беларуси установили 1052 причастных к киберзлодеяниям граждан, что на 86 человек больше, чем в 2016 году. К уголовной ответственности привлечено 956 лиц, в том числе 294 имеющих судимость, 683 нигде не работающих и не учащихся, 34 несовершеннолетних.

По оценкам экспертов, хакеры все успешнее справляются с довольно сложными задачами. При этом киберпреступники продолжают «молодеть», – судя по суммам, указанным в запросах, и грамматическим ошибкам в текстах сообщений, – большинству из них не больше 17 лет, максимум – 22 года. Под угрозой – частный бизнес и простые обыватели. Государственный сектор и банки, по мнению сотрудников ведомств, защищены достаточно хорошо [3].

Часто жертвами программ-шифровальщиков становятся мелкие предприятия в силу личных ошибок. Например, если компьютер подключен к локальной сети и менеджер, открывая личную почту, запускает прикрепленный к письму с незнакомого адреса файл.

Все еще остается серьезной проблема блокирования бухгалтерских баз данных «1-С». Чтобы избежать таких ситуаций необходимо работу по созданию бэкапов (резервных копий) держать на контроле руководством предприятий. Если бэкап делается раз в неделю, то восстановить бухгалтерскую отчетность не составляет труда. Но если бэкап отсутствует как таковой в течение полугода, то блокирование баз данных вызывает серьезную проблему.

В 2017 году появилось несколько заявлений по поводу краж криптовалют. По мнению специалистов управления по раскрытию преступлений в сфере технологий криминальной милиции МВД, сложность таких дел не столько в хищении, а в

определении, является ли криптовалюта деньгами: люди не могли подтвердить, законным ли путем они получили токены.

Эксперты отмечают, что растет количество хищений с использованием новых интернет-услуг, оказываемых операторами. Например, используется мобильное приложение v-banking, которое позволяет переводить деньги. Часто мошенники под предлогом совершения звонка просят телефон и через приложения берут микрозаймы по 100 BYN.

По-прежнему увеличивается количество мошенничеств и вымогательств в сети. Часто звонят по объявлениям о продаже недвижимости или другого имущества и под предлогом перевода аванса просят данные карты, а потом похищают с нее деньги. Растет количество хищений с использованием социальной сети «ВКонтакте». Совет по защите от таких нападений простой: чтобы не стать жертвой, нужно сомневаться в бескорыстности предлагающего много и быстро заработать или что-то подарить. Следует знать, что силовые структуры и контролирующие органы никогда не блокируют компьютеры пользователей, и, если есть сообщение о блокировке системы якобы от лица МВД, – это мошенники.

В последнее время мошенники стали использовать вредоносное ПО для скрытого майнинга криптовалют. В силу того, что курс биткоина растет, сейчас появился такой вид преступления, когда посредством внедрения вредоносного кода в компьютер он используется как часть бот-сети для постоянной работы – для майнинга криптовалют. Поэтому надо контролировать включенность ноутбуков, работу всех девайсов, чтобы не становиться жертвами таких киберпреступлений. Представители Следственного комитета рекомендуют хотя бы раз в сутки выключать модем, поскольку в основном бот-сети строятся на конкретном IP-адресе. А, если выключить модем и обнулить его, IP-адрес будет другой, и получить доступ к компьютеру будет сложнее. В любом случае надо следить за своими устройствами, и при некорректной работе переустанавливать операционную систему.

Кстати, недавно белорусскими силовиками совместно с ФБР была проведена нашумевшая операция по задержанию группировки «Андромеда», распространявшей вредоносное ПО в основном на территории США. При этом главный виновник находился и был задержан в Беларуси. По подсчетам ФБР, общая сумма нанесенного ущерба превысила 10 млн. USD.

WannaCry, Petya и Petya-2, BadRabbit и CobaltStrik— эти и ряд других вредоносных вирусов взламывали компьютеры и целые системы в 2017 году, причинив миллиардный вред во многих странах.

Как полагают эксперты, в 2018 году останутся неконтролируемыми риски, связанные с Интернетом вещей, будет расти криминальный сервис и т.д. Объектами кибератак станут не только личные данные, под угрозой конфиденциальная информация компаний и критически важная инфраструктура.

По оценкам «Лаборатории Касперского», всего сейчас в мире насчитывается 500 миллионов вирусов, в новом 2018 году появится более 90 миллионов новых вредоносных программ. То есть за год их количество вырастет почти на 20%.

Эксперты поясняют, почему за 2017 год в мире резко возросло количество кибератак, и чем это грозит в ближайшем будущем. После того, как Wikileaks опубликовал более 150-ти вредоносных программ из арсенала АНБ, ЦРУ и ФБР, они попали в руки хакерского сообщества и превратились в кибероружие. Кроме того, в мире появились и конструкторы вирусов, часть которых распространяется бесплатно. Таким образом, стало возможным создавать вирусы, даже не будучи хакером-профессионалом. Соответственно, число троянов будет только возрастать, считают эксперты. Они также полагают, что кибероружие постепенно выйдет на стадию промышленного применения, то есть следующая война будет базироваться не столько на бомбах, сколько на выведении из строя компонентов инфраструктур — транспортной, коммуникационной, финансовой, медицинской и так далее

Повысить информационную безопасность Беларуси поможет Закон о персональных данных, который сейчас прорабатывается специалистами. Он позволит контролировать деятельность граждан в интернете. Законом будут защищены права и обязанности госорганов при работе с персональными данными. Конституцией Беларуси закреплено право каждого на защиту от незаконного вмешательства в его личную жизнь. Вместе с этим в Беларуси отсутствует комплексное правовое регулирование порядка работы с персональными данными физических лиц. Это нередко приводит к нарушению указанного права и вызывает затруднения в практической деятельности.

Принятие закона с учетом общеевропейских подходов к защите персональных данных позволит устранить препятствия для развития бизнеса, связанного с информационными технологиями. Основная идея законопроекта - поиск разумного баланса между защитой персональных данных, развитием информационных технологий и необходимостью выполнения государственных функций. В законопроекте планируется закрепить порядок трансграничной передачи персональных данных и случаи, когда обработка персональных данных может осуществляться без согласия граждан. Устанавливается определение категорий общедоступных персональных данных, которые не подлежат защите, и специальных персональных данных, подлежащих дополнительной защите. Предполагается регулирование вопросов контроля и общих положений об ответственности в сфере обращения с персональными данными, компетенции уполномоченного органа по защите прав субъектов персональных данных. Кроме того, сейчас в Палате представителей на рассмотрении находятся два законопроекта. Один из них предусматривает внесение изменений и дополнений в закон о регистре населения и второй, который будет корректировать закон об электронном документе и электронной цифровой подписи.

Представители ведомств согласились с тем, что в стране назрела необходимость страхования в сфере высоких технологий. Нужен инструмент для компенсации финансовых и репутационных потерь. Но пока страховщики не стремятся в этот сегмент. У них нет методики оценки подобных рисков, и они не могут объективно подойти к ценообразованию.

Таким образом, в концепции национальной безопасности Республики Беларусь информационная безопасность является одним из приоритетных направлений деятельности по обеспечению безопасности белорусского общества.

Литература

1 Социальное положение и уровень жизни населения Республики Беларусь. Национальный статистический комитет Республики Беларусь [Электронный ресурс]. – Режим доступа: http://www.belstat.gov.by/ - Дата доступа: 15.02.18

2 Программа социально-экономического развития Республики Беларусь на 2016 – 2020 годы. Сайт Совета Министров Республики Беларусь. [Электронный ресурс]. – Режим доступа: - http://www.government.by/upload/docs/program_ek2016-2020.pdf - Дата доступа: 20.02.18

3 Информационная безопасность и борьба с преступлениями в сфере высоких технологий [Электронный ресурс]. – Режим доступа: http://www.belta.by/pressconference/view/informatsionnaja-bezopasnost-i-borba-s-prestuplenijami-v-sfere-vysokih-tehnologij-1012/ - Дата доступа: 20.02.18

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ НА ПРИМЕРЕ УЧЕБНОГО ЗАВЕДЕНИЯ

Ротару А.В.
Студент SI-141
Экономическая Академия Республики Молдова
Научный руководитель Охрименко С.

The widespread use of information has created a new type of risk - information risks, which can pose a serious threat to the development and functioning of the school. Therefore, information risks require immediate detection, analysis and evaluation for subsequent reduction, disposal or transfer. Work to ensure information security should be comprehensive and include many systems and techniques for the calculation and analysis of possible information risks.
Keywords: *Information risks, Information security, Comprehensive system, Analysis.*

Одной из важнейших составляющих успешного развития общества является защищенность его информационных ресурсов. Информация в современном информационном обществе становится одним из ключевых элементов бизнеса, она становится предметом купли-продажи, обладающим стоимостными характеристиками. Любые процессы в финансово-промышленной, политической или социальной сфере сегодня напрямую связаны с информационными ресурсами и использованием информационных технологий.

Современные информационные технологии предлагают неограниченные возможности для развития бизнеса, предоставляя необходимую для принятия решений информацию нужного качества и в нужное время. Информация, критичная для бизнеса, должна быть доступной, целостной и конфиденциальной. В то же время, в связи с возрастающей сложностью информационных систем и используемых в них информационных технологий, возрастает и количество уязвимостей и потенциальных угроз этим системам.

Очевидно, что вопросы информационной безопасности сегодня актуальны не только для правительственных и коммерческих структур. В последнее время все чаще и чаще стоит вопрос об обеспечении устойчивого функционирования и повышении конкурентоспособности образовательных учреждений.

В связи с этим задачи обеспечения защиты информационных ресурсов образовательного учреждения и связанные с ними вопросы анализа информационных рисков и управления ими приобретают особую актуальность.

Под риском понимается возможная опасность потерь, вытекающая из специфики тех или иных явлений природы и видов деятельности человеческого общества.

Риск – это историческая и экономическая категория. Как историческая категория, риск представляет собой осознанную человеком возможную опасность.

Она свидетельствует о том, что риск исторически связан со всем ходом общественного развития. Как экономическая категория риск представляет собой событие, которое может произойти или не произойти.

В случае совершения такого события возможны три экономических результата: отрицательный (проигрыш, ущерб, убыток); нулевой; положительный (выигрыш, выгода, прибыль).

Риском можно управлять, то есть использовать различные меры, позволяющие в определенной степени прогнозировать наступление рискового события и принимать меры к снижению степени риска. Любой субъект экономики на любом ее уровне неизбежно сталкивается с неординарными ситуациями, незапланированными или непредвиденными событиями, на которые необходимо адекватно реагировать, чтобы не понести убытки.

Для повышение эффективности управления информационной безопасностью учебного заведения и управления информационными рисками требуется решить следующие задачи:

1. Провести системный анализ бизнес-процессов учебного заведения как объекта защиты и определить требования к обеспечению информационной безопасности учебного заведения.
2. Разработать комплекс моделей, определяющих основные компоненты информационных рисков учебного заведения (модели угроз, злоумышленников, уязвимостей, ущерба).
3. Разработать инструментальные программные средства для оценки уровня информационных рисков учебного заведения и выбора необходимых контрмер для управления информационной безопасностью.

Заключение

С переходом к рыночной экономике и ростом значения прогнозирования экономического развития существенно возросла роль информации. Широкое использование информации породило новый вид рисков – информационные риски, которые могут составлять серьезную угрозу развитию и функционированию учебного заведения. Поэтому информационные риски требуют незамедлительного выявления, анализа и оценки в целях последующего сокращения, утилизации или передачи. Необходимо помнить, что формулирование и осуществление политики безопасности по устранению подобных рисков не будет эффективной, если существующие шаблоны и правила используются не так, как должны, что происходит из-за необученности сотрудников или их неосведомленности о важности проблемы. Именно поэтому работы по обеспечению информационной безопасности должны быть комплексными и включать в себя множество систем и методик по расчету и анализу возможных информационных рисков.

Данная тема актуальна, так как в стремительно развивающихся рыночных условиях образовательное учреждение в целях нормальной работы должно просчитывать существующие риски и уметь их предотвратить.

Литература

1. В.И. Борисов. «*Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем*». Издательство «Научная книга» 2016.
2. А.А. Варфоломеев «*Управление информационными рисками*». Учебное пособие, Москва, 2008.
3. Алексей Лукацкий. «*Эффективность информационной безопасности*». Cisco Systems, 2006.

ЗАЩИТА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ ОТ КИБЕРСКВОТТИНГА

Ирина Шнып
УО «Гомельский государственный университет имени Ф. Скорины»

The article deals with the current system of legislation in the field of protection of rights to intellectual property, types of cybersquatting and measures of protection against it

Совершенствование нормативной правовой базы является основой защиты интеллектуальной собственности. Действующая система законодательства в области охраны прав на объекты интеллектуальной собственности сформирована с учетом норм международных договоров, участником которых является Республика Беларусь.

Для обеспечения эффективной защиты интеллектуальной собственности были разработаны:

- Государственной программе защиты интеллектуальной собственности в Республике Беларусь на 2004-2006 годы (утверждена постановлением Совета Министров Республики Беларусь от 12.07.2004 г. № 843);
- Государственной программе по охране и управлению интеллектуальной собственностью Республики Беларусь на 2008-2010 годы (утверждена постановлением Совета Министров Республики Беларусь от 21.11.2007 г. № 1555).

Стратегия Республики Беларусь в сфере интеллектуальной собственности на 2012-2020 годы, утвержденная постановлением Совета Министров Республики Беларусь от 02.03.2012 г. № 205, является продолжением работы по развитию национальной системы интеллектуальной собственности, которая осуществлялась в соответствии с Государственной программой по охране интеллектуальной собственности на 2008-2010 годы [1].

Законодательство Республики Беларусь в области авторского права и смежных прав основывается на Конституции Республики Беларусь. К нормативным правовым актам в этой области относятся:

- Гражданский кодекс Республики Беларусь;
- Закон Республики Беларусь от 17 мая 2011 года № 262-З «Об авторском праве и смежных правах»;
- Закон Республики Беларусь от 5 февраля 1993 года № 2181-XII «О товарных знаках и знаках обслуживания»;
- нормативные правовые акты Президента Республики Беларусь;
- постановления Совета Министров Республики Беларусь;
- постановления Государственного комитета по науке и технологиям Республики Беларусь.

Кибersквоттинг – регистрация доменных имен, содержащих торговую марку, принадлежащую другому лицу с целью их дальнейшей перепродажи или недобросовестного использования.

Название произошло от английского слова «cybersquatting», которое означает «захват некой территории, самовольное поселение незаконным способом».

Кибersквоттинг появился в США в начале 90-х годов. Тогда доменное имя можно было зарегистрировать бесплатно у регистратора Network Solutions. Сообразительные американские пользователи сети Интернет предвидели развитие всемирной паутины и предположили, что количество коротких и запоминающихся доменных имен достаточно ограничено и будет пользоваться большим спросом. Они начали регистрировать на себя потенциально перспективные доменные имена, затем продавать домены заинтересованным лицам. Первые крупные сделки, принесшие доход в несколько десятков тысяч долларов, стали примером для последователей и начал активно развиваться, в том числе и у белорусских пользователей сети Интернет.

В зависимости от целей и тактики выбора доменного имени кибersквоттинг подразделяется на несколько видов:

1 Отраслевой кибersквоттинг – регистрация доменных имён, содержащих общеупотребительные слова из разных сфер жизнедеятельности человека: коммерческая деятельность, отрасли промышленности, организации, товары и т.д. Такие домены самые дорогие на рынке кибersквоттинга, так как содержат в своем названии, легко запоминающиеся слова. Например, домен business.com был продан на аукционе почти за 7,5 млн. долларов.

Отраслевой кибersквоттинг считается вполне легальным бизнесом в Интернете, где используется схема рыночных отношений «купил дешевле – продал дороже», не посягая на права собственника.

2 Брендовый кибersквоттинг – регистрация доменных имён, содержащих товарные знаки, фирменные наименования, популярные собственные имена, то есть средства индивидуализации, охраняемые законом, а также регистрация «на перспективу», например, регистрируется домен «А» в надежде, что будет создано предприятие или товарный знак с таким именем. У кибersквоттера существует риск лишиться домена. Например, белорусские граждане зарегистрировали домен google.by и сделали сайт, который использовал технологию Google для поиска, размещали там рекламу, извлекая прибыль. Заметив это, компания обратилась в суд, и после достаточно долгого судебного процесса Google получил этот домен в пользование. Аналогичный процесс у компании Google был в отношении доменного имени Google.ua.

Законные владельцы товарных знаков предпочитают не судиться из-за длительности процесс судебного разбирательства, и не редко выкупают захваченные домены.

Брендовый кибersквоттинг относят к числу не законных методов получения прибыли.

3 Именной киберсквоттинг – регистрация доменных имен, идентичных именам, фамилиям известных людей. Даже если такой домен (например, Lukashenko.by) не удастся продать потенциально привлекательному покупателю, его владелец может рассчитывать на большую посещаемость такого сайта. Также на таких сайтах может распространяться конфиденциальная или недостоверная информация об известных людях.

В отличие от брендового киберсквоттинга очень сложно отсудить такой домен. Например, Ирине Дорофеевой очень трудно будет доказать в суде, что сайт с доменом dorofeeva.by должен принадлежать именно ей. Для решения этой проблемы нужно зарегистрировать свое имя как товарный знак. Например, Мадонна зарегистрировала свое имя как торговую марку и отсудила себе доменное имя Madonna.com. Патрисия Каас избежала скандала и отвоевала сайт с доменом patriciaKaas.com, где злоумышленники разместили порноресурс.

4 Тайпсквоттинг – регистрация доменных имен, схожих по написанию с доменами известных сайтов, марок, брендов, в расчёте на ошибку части пользователей. На этом можно заработать за счет показа рекламы на своем сайте, который посещают невнимательные посетители. Например, был зарегистрирован домен jandex.ru, на котором была размещена реклама. Позже компания Яндекс отсудила этот домен себе. Также на таком сайте могут размещать компромат на оригинал или продавать поддельную продукцию, но сейчас это редко применяется из-за повышенного риска уголовного преследования.

В связи с этим крупным сайтам рекомендуется регистрировать наряду со своим доменом так же предположительно похожие домены.

Редко владельцы сайтов покупают схожие доменные имена, чтобы исключить нанесение ущерба имиджу компании. Например, ложные двойники Downlaod.com, Donwload.com и Dawnload.com были проданы за 80 тыс. долларов.

5 Защитный киберсквоттинг – некоммерческий вид киберсквоттинга. Легальный владелец сайта регистрирует доменные имена, созвучные, похожие, связанные по смыслу с его собственным доменным именем для защиты от киберсквоттеров.

Сама по себе регистрация доменов не противоречит закону. Национальными домена верхнего уровня в Республике Беларусь являются домен .BY и домен .БЕЛ. Согласно «Инструкции о порядке регистрации доменных имен в пространстве иерархических имен национального сегмента сети интернет» регистрация доменов .BY и .БЕЛ может осуществляться юридическими лицами, аккредитованными техническим администратором национальной доменной зоны. В настоящее время аккредитованными регистраторами являются пять компаний, их адреса можно найти на официальном сайте доменных зон .BY и .БЕЛ http://cctld.by.

В 2017 году зарегистрировано более 31 000 новых доменов .BY и .БЕЛ, аннулировано 29 947. Всего в обеих национальных зонах на начало 2018 зарегистрировано 137 319 имен, из которых домены .BY составляют 89 % [2].

На сайте http://cctld.by есть сервис «Whois», от английского «Who Is?» («Кто есть?»). Сервис предоставляет информацию о доменных именах. При помощи данного сервиса можно определить:

- свободно ли доменное имя;
- администратора (владельца) доменного имени и его контактные данные;
- с какими DNS-серверами делегировано доменное имя;
- дату регистрации и дату окончания срока регистрации доменного имени [2].

Развитие информационных технологий и бизнеса в Республике Беларусь способствовало развитию киберсквоттинга и обусловило появление в национальном сегменте сети Интернет доменных имен, схожих до степени смешения с охраняемыми в стране товарными знаками и знаками обслуживания, исключительные права на которые принадлежат другим лицам.

Согласно пункту 1 статьи 20 Закона Республики Беларусь от 5 февраля 1993 года «О товарных знаках и знаках обслуживания» использованием товарного знака и знака обслуживания признается, помимо прочего, его использование путем применения в глобальной компьютерной сети Интернет (например, в доменном имени) [3].

В соответствии с пунктом 3 статьи 3 закона нарушением прав владельца товарного знака признается несанкционированное введение в гражданский оборот товарного знака или товара, обозначенного этим знаком, или обозначения, сходного с ним до степени смешения, в отношении однородных товаров, а также неоднородных товаров, обозначенных товарным знаком, признанным общеизвестным в Республике Беларусь.

В Республике Беларусь сложилась практика, что почти со стопроцентной вероятностью можно отсудить домен, если существует зарегистрированная с тем же названием латиницей торговая марка. Даже если домен зарегистрирован раньше, чем одноименная торговая марка.

За защитой принадлежащих им личных неимущественных и имущественных прав авторы и иные правообладатели могут обращаться в установленном порядке в судебные и другие органы в соответствии с их компетенцией [4].

Авторы или иные правообладатели, исходя из содержания нарушенного права и характера правонарушения в результате киберсквоттинга, вправе требовать:

- признания права;
- восстановления положения, существовавшего до нарушения права;
- пресечения действий, нарушающих право или создающих угрозу его нарушения;
- возмещения убытков либо выплаты компенсации в размере от десяти до пятидесяти тысяч базовых величин, определяемом судом;
- компенсации морального вреда;

- обязательной публикации о допущенном нарушении с включением в нее сведений о том, кому принадлежит нарушенное право.

Меры защиты от киберсквоттинга:

1 Не разглашать названий будущих товаров, услуг, проектов. Сначала надо зарегистрировать домен, а затем объявлять о запуске продукта. Также можно подбирать название для продукта, исходя из наличия свободных доменных имен.
2 Выбирать оригинальные названия, что позволяет снизить вероятность совпадения с уже занятыми доменными именами.
3 При регистрации товарного знака регистрировать схожее с ним доменное имя в целях повышения уровня охраны товарных знаков и предотвращения ситуаций, связанных с необходимостью защиты исключительных прав на них в судебном порядке.
4 Регистрировать при покупке основного домена сразу несколько похожих имен.
5 Продлевать вовремя регистрацию доменного имени.
6 Участвовать в аукционах доменных имен, где можете подобрать подходящий домен без доплат сквоттерам. Аукционы проводятся на сайтах регистраторов доменных имен.

Литература

1 Стратегия Республики Беларусь в сфере интеллектуальной собственности на 2012-2020 годы, утв. постановлением Совета Министров Республики Беларусь от 02.03.2012, № 205 [Электронный ресурс] / Национальный правовой Интернет-портал Республики Беларусь. - Режим доступа: http://www.pravo.by. - Дата доступа: 01.03.2018.
2 Официальный сайт доменных зон .BY и .БЕЛ [Электронный ресурс]. - Режим доступа: http://cctld.by. - Дата доступа: 01.03.2018.
3 Закон Республики Беларусь от 5 февраля 1993 года № 2181-XII «О товарных знаках и знаках обслуживания» [Электронный ресурс] / Национальный правовой Интернет-портал Республики Беларусь. - Режим доступа: http://www.pravo.by. - Дата доступа: 01.03.2018.
4 Официальный сайт национального цента интеллектуальной собственности [Электронный ресурс]. - Режим доступа: http:// http://belgospatent.by. - Дата доступа: 01.03.2018.

REȚELELE NEURONALE- UN ASALT TEHNOLOGIC ÎN DOMENIULUI IT

Sîrbu Cristina, Sîrbu Corina
student anul III, specialitatea transmisiuni,
Academia Militară a Forțelor Armate „Alexandru cel Bun, Republica Moldova

The field of neural networks is very active nowadays, which is somewhat surprising, considering that some ideas are over 60 years old. Only in recent years has this field really become attractive, thanks to the GPU cards that allowed a much higher drive speed. Neural networks are part of the broad spectrum of artificial intelligence, but as you will see, much of the concepts presented here are found in other classes of algorithms.

Rețelele neurale (RN, în engleză: ANN de la *artificial neural network*) sunt o ramură din știința inteligenței artificiale, și constituie totodată, principial, un obiect de cercetare și pentru neuroinformatică. Rețelele neurale artificiale caracterizează ansambluri de elemente de procesare simple, puternic interconectate și operând în paralel, care urmăresc să interacționeze cu mediul înconjurător într-un mod asemănător creierelor biologice și care prezintă capacitatea de a învăța. Ele sunt compuse din neuroni artificiali, sunt parte a inteligenței artificiale și își au, conceptional, originea ca și neuronii artificiali, în biologie. Nu există pentru RNA o definiție general acceptată a acestor tipuri de sisteme, dar majoritatea cercetătorilor sunt de acord cu definirea rețelelor neurale artificiale ca rețele de elemente simple puternic interconectate prin intermediul unor legături numite interconexiuni prin care se propagă informație numerică.

Din punct de vedere *functional* o retea neuronala este un sistem ce primeste date de intrare (corespunzator datelor initiale ale unei probleme) si produce date de iesire (ce pot fi interpretate ca raspunsuri ale problemei analizate). O caracteristica esentiala a retelelor neuronale este capacitatea de a se adapta la mediul informational corespunzator unei probleme concrete printr-un process de invatare. In felul acesta reteaua extrage modelul problemei pornind de la exemple. Se poate spune ca o retea neuronala construieste singura algoritmul pentru rezolvarea unei probleme, daca ii furnizam o multime reprezentativa de cazuri particulare (exemple de instruire).

Din punct de vedere *structural* o retea neuronala este un ansamblu de unitati interconectate, fiecare fiind caracterizata de o functionare simpla. Functionarea unitatilor este influentata de o serie de parametri adaptabili. Astfel o retea neuronala este un sistem extrem de flexibil. Structura unitatilor functionale, prezenta conexiunilor si a parametrilor adaptivi precum si modul de functionare sunt inspirate de creierul uman. Fiecare unitate functionala primeste cateva semnale de intrare pe care le prelucreaza si produce un semnal de iesire. Un astfel de sistem invata prin modificarea intensitatii de conexiune dintre elemente, adica schimband ponderile asociate acestor conexiuni. Cunoasterea initiala ce este furnizata sistemului este reprezentata de caracteristicile obiectelor

considerate si de o configuratie initiala a retelei.Sistemul invata construind o reprezentare simbolica a unei multimi date de concepte prin analiza conceptelor si contraexemplelor acestor concepte.O retea neuronala artificiala este un ansamblu de unitati functionale amplasate in nodurile unui graf orientat si intre care circula semnale de-a lungul arcelor grafului. Retelele neuronale artificiale sunt retele de modele de neuroni conectati prin intermediul unor sinapse ajustabile. Toate modelele de retele neuronale se bazeaza pe interconectarea unor elemente simple de calcul dintr-o retea densa de conexiuni.

Elementele definitorii ale unei retele neuronale sunt :

1. *Arhitectura*: specifica modul prin care sunt amplasate si interconectate unitatile functionale. Arhitectura determina si fluxul informational in cadrul retelei.
2. *Functionarea*: specifica modul in care fiecare unitate in parte si reteaua in ansamblul ei transforma semnalele de intrare in semnale de iesire. Functionarea e influentata de arhitectura, in special de modul de interconectare a unitatilor.
3. *Adaptarea (invatarea)*: specifica modul de stabilire a parametrilor ajustabili astfel incat reteua sa poata rezolva anumite probleme. In functie de natura informatiei de care se dispune, invatarea poate fi *supervizata* sau *nesupervizata*.

Invatarea supervizata este un tip de invatare inductiva ce pleaca de la un set de exemple de instante ale problemei si formeaza o functie de evaluare (sablon) care sa permita clasificarea (rezolvarea) unor instante noi. Invatarea este supervizata in sensul ca setul de exemple este dat impreuna cu clasificarea lor corecta. Aceste instante rezolvate se numesc instante de antrenament. Formal, setul de instante de antrenament este o multime de perechi atribut-valoare $(x,f(x))$, unde x este instanta iar $f(x)$ clasa careia ii apartine instanta respectiva. Scopul invatarii este construirea unei functii-sablon care sa clasifice corect instantele-exemplu, iar pentru un x pentru care nu se cunoaste $f(x)$ sa propuna o aproximare cat mai corecta a valorii $f(x)$.

Invatarea nesupervizata elimina complet necesitatea unor instante de antrenament, deci si problemele legate de acestea. Scopul invatarii nesupervizate nu este definit anterior ca un concept tinta, algoritmul fiind lasat singur sa identifice concepte posibile. In general, invatarea nesupervizata presupune existenta unor instante neclasificate, un set de reguli euristice pentru crearea de noi instante si evaluarea unor concepte deduse, eventual un model general al spatiului de cunostinte in care se gasesc aceste instante. Un algoritm de invatare nesupervizata construieste concepte pentru a clasifica instantele, le evalueaza si le dezvolta pe cele considerate interesante de regulile euristice. In general, concepte interesante sunt considerate cele care acopera o parte din instante, dar nu pe toate. Invatarea nesupervizata permite identificarea unor concepte complet noi plecand de la date cunoscute

Parti componente:

- set de unitati de procesare – neuronii-celulele
- o stare de activare y_k pt fiecare unitate – echivaland cu rezultatele iesirii din neuroni
- conexiuni intre unitati – in general fiecare conexiune e definita de o pondere w_{jk} care determina efectul pe care-l va avea semnalul j asupra unitatii k

- o regula de propagare care determina inputul efectiv s_k a unei unitati de la inputul extern
- o functie de activare F_k care determina noul nivel de activare bazat pe inputul efectiv $s_k(t)$ si activarea curenta $y_k(t)$
- un input extern (offset) θ_k pt fiecare unitate
- o metoda pentru adunarea de informatii (regula de invatare)
- un mediu in care sistemul sa opereze avand semnale de input si daca e necesar semnale de eroare

Unitatile de procesare:

- fiecare unitate de procesare parcurge urmatorii pasi :
  - primeste inputurile de la vecini sau din surse externe
  - foloseste acest input pentru a calcula un semnal de output
  - propaga acest semnal de output spre alte unitati
  - uneori ajusteaza ponderile
- sistemul poate fi vazut ca paralel datorita faptului ca mai multe unitati isi fac calculele in acelasi timp
- se pot distinge 3 tipuri de unitati :
  - de input (se vor nota cu indexul *i*) – primesc informatii din afara RNA
  - de output (se vor nota cu indexul *o*) – trimit informtii in afara RNA
  - ascuns (se vor nota cu indexul *h*) – semnalele lor de I/O raman in RNA
- in timpul operatiilor unitatile pot fi updatate *sincron* sau *asincron*
- sincron : toate unitatile updateaza activare simultan
- asincron : fiecare unitate are o probabilitate (de obicei fixata) de a-si updata activarea intr-un moment dat – de obicei o singura unitate fiind capabila de a face asta la un moment dat (exista avantaje)

Conexiunile dintre unitati: In majoritatea cazutilor se presupune ca fiecare unitate aduce o contributie inputului unitatii cu care e conectata. Acest input al unitatii k este suma ponderala a outputurilor din toate celulele conectate plus un offset .

$$s_k(t)=\Sigma w_{jk}(t)y_j(t) + \theta_k(t).$$

Unitatile cu regula de propagare s.n. unitati sigma.O regula diferita de propagare a fost introdusa de Feldman si Ballard (1982) – propagarea pentru unitatea sigma-pi :

$$s_k(t) =\Sigma w_{jk}(t)\Pi y_{jm}(t) + \theta_k(t).$$

Desi aceste unitati nu sunt frecvent folosite au valoare pentru implementarea tabelelor de look-up si gating al inputului.Activarea si regulile de output:Este necesara o regula care da efectul a inputului total asupra unitatii de activare – F_k – functie care preia inputul total $s_k(t)$ si activarea curenta $y_k(t)$ si produce o noua valoare de activare a unitatii k:

$$y_k(t+1)=F_k(y_k(t), s_k(t)).$$

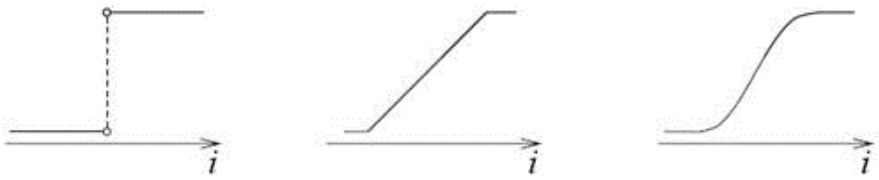
De obicei functia de activare este o functie nedescrescatoare a totalului inputului unei unitati.

$$y_k(t+1)=F_k(s_k(t))=F_k(\Sigma w_{jk}(t)y_j(t)+\theta_k(t)).$$

Cu toate ca functiile de activare nu sunt restrictionate la funtii nedescrescatoare. In general un fel de functie de prag este folosita: o functie de prag puternic limitatoare (o functie sgn - signum) sau o functie liniara sau semiliniara, sau o functie de prag usor limitatoare – functii sigmoide.

Ex . $y_k=F(s_k)=1/(1+e^{-sk})$ (functie sigmoidala)

Functii hiperboidale tangente cu valori intre [-1,1].



a) functia sgn b) functia semi-lineara c) functia sigmoida

***Fig. 1.* Diferite functii de activare pentru o unitate**

In anumite cazuri output-ul unei unitati poate fi o functie stohastica a totalului inputului corespunzator unitatii. In acest caz activarea nu e de determinata deterministic de neuronul de input, ci neuronul de input determina probabilitatea *p* a a unui neuron de a primi o valoare mare de activare:

$$p(y_k \leftarrow 1) = \frac{1}{1 + e^{-s_k/T}},$$

T- este parametrul care determina curba functiei de probabilitate.

Retele neuronale feedforward uninivel

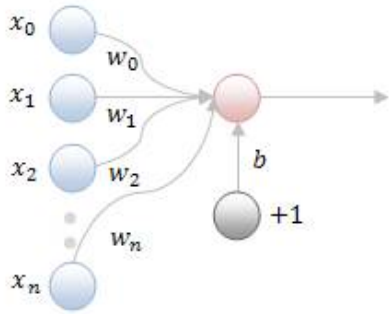


***Fig.2.* Diagrama schematica a unei retele neuronale feedforward uninivel, x-valorile de intrare, w-ponderile si unitatea fictiva**

Aceste retele realizeaza o propagare inainte a intrarilor, intr-un singur pas. Unitatile de prelucrare din cadrul unei retele feedforward uninivel sunt in general neuroni treapta, cu domeniu real al valorilor de intrare si cu domeniu binar (0,1) sau bipolar (-1,1) al valorilor de output.

Conditia de activare a unei unitati de output Uj (de fixare a unitatii Uj pe valoarea 1) este:

$\sum_i w_{ji} x_i \geq T_j$, unde i desemneaza o unitate de input

Valoarea de activare 1 a unei unitati de output Uj poate primi semnificatia incadrarii vectorului de intrare intr-o clasa, sa spunem A, in timp ce valoarea de activare - 1/0 poate avea semnificatia clasificarii vectorului de intrare intr-o alta clasa, sa spunem B.

Ecuatia: $\sum_i w_{ji} x_i = T_j$ formeaza un hiperplan in spatiul n-dimensional, ce separa acest spatiu in doua regiuni. Cand spatiul este bidimensional, hiperplanul devine o linie.

Datorita restrictiilor de configuratie, retelele feedforward uninivel nu sunt capabile sa realizeze decat o clasificare pe clase liniar separabile. Separabilitatea liniara se refera la existenta unui hiperplan liniar, ce permite izolarea instantelor unei clase intr-o regiune distincta de cea in care sunt plasate instantele celeilalte clase. Una dintre cele mai mari provocari ale erei informatice este gasirea de pattern-uri, tendinte si anomalii in seturile de date ce devin din ce in ce mai mari si consistente.

In cazul oamenilor in spatele unui proces de identificare considerat obisnuit, cum ar fi recunoasterea unei fete sau citirea caracterelor scrise de mana, sau identificarea prin simt a unor obiecte, etc. , se ascunde de fapt un proces complex. Aceste activitati apartin vietii de zi cu zi, fiind necesare in interactiunea cu mediul. Eficienta cu care oamenii desfasoara aceasta activitate este remarcabila.O provocare continua pentru sistemle automate inteligente o reprezinta dezvoltarea metodelor capabile de a simula cele mai variate forme ale recunoasterii obiectelor. In aceste sisteme obiectele sunt reprezentate intr-un mod convenabil pentru tipul de procesare pentru care sunt destinate. Aceste reprezentari se numesc pattern-uri.Recunoasterea pattern-urilor poate fi definita ca asignarea unui obiect fizic sau unui eveniment unei categorii prespecificate. Aceasta presupune implementarea de metode atat pentru descrierea obiecteleor cat si pentru clasificarea lor. Urmareste proiectarea si implementarea algoritmilor care sa simuleze abilitatea umana de a descrie si clasifica obiecte. Este un domeniu de cercetare care are multiple legaturi cu alte discipline.

In medicina, in mod caracteristic avem de a face cu cantitati enorme de date, fie ele sub forma de imagini, numerice sau nominale.Recunoasterea pattern-urilor depinde de perceperea inter-relatiilor dintre observatii separate. Ea are un rol central in stiinta medicala. Exista tehnici statistice ce pot defini pattern-urile structurale din cadrul unui set de observatii, si pot asigna ponderile potrivite importantei contributiei fiecarei variabile la pattern.In ceea ce priveste data mining, acest proces presupune extragerea din date a informatiei in prealabil necunoscuta si potentia folositoare. Ideea centrala in data mining este construirea de programe care analizeaza baze de date in mod automat, cautand regularitati sau pattern-uri. Pattern-urile “puternice” identificate vor fi folosite pentru predictii precise asupra unor date viitoare.Problemele potentiale care pot aparea sunt datorate existentei de pattern-urilor superficiale, a coincidentelor accidentale din setul de

date, denaturarea datelor disponibile (date inexacte, date lipsa, etc). Algoritmii folositi trebuie sa fie destul de stabili pentru a depasi si trata seturile de date imperfecte, si a fi capabili de a extrage pattern-uri folositoare. Procesul de data mining automatizeaza descoperirea unor relatii si combinatii in cadrul datelor brute, rezultatele obtinute putand fi mai apoi incadrate intr-un sistem automat de suport a deciziei.

Fundamentul tehnic al procesului de data mining este invatarea automata. Prin invatare automata se presupune achizitionarea de descrieri structurale din exemple. Rezultatele invatarii poti fi folosite fie pentru predictii (asupra ce se va intampla in situatii noi pornind de la exemple ce descriu situatii din trecut) sau acestea pot construi o descriere actuala a unei structuri ce poate fi folosita pentru clasificarea altor exemple decat cele folosite in procesul invatarii. In cadrul domeniului medical data miningul este util la prelucrarea bazelor de date ce contin dosarele computerizate ale pacientilor, sau la prezicerea evolutiei unei boli, la definirea modelelor de comportare ale pacientilor de risc,etc.Metodele data mining provin din calculul statistic clasic, din administrarea bazelor de date si din inteligenta artificiala. Ele nu inlocuiesc metodele traditionale ale statisticii, ci sunt considerate a fi extinderi ale tehnicilor grafice si statistice. Deoarece softului ii lipseste intuitia umana (pentru a face recunoasterea a ceea ce este relevant de ceea ce nu este), rezultatele metodelor data mining vor trebui supuse in mod sistematic unei supravegheri umane.Structura tipica de date potrivita pentru data mining contine observatiile (cazurile, de exemplu referitoare la pacienti) plasate pe linii iar variabilele plasate pe coloane.Modelele identificate de o metoda de data mining vor putea fi transformate in cunostinte doar dupa o validare corespunzatoare.

Bibliografie

1. Anders L. Madsen, *Probabilistic Networks - An Introduction toBayesian Networks and Influence Diagrams*, Uffe B. Kjærulff Department of Computer Science Aalborg University, 10 May 2005
2. Batchelor, B.G., *Practical Approach To Pattern Recognition*, Plenum Press, New York, 1974.
3. Bigus, J. P. 1996. *Data mining with neural networks.* New York: McGraw Hill.
4. Duda, R. O., P. E. Hart, *Pattern classification and scene analysis*, John Wiley, New York, 1973
5. J.P. Marques de Sa, *Pattern Recognition - Concepts, Methods and Applications*, Springer-Verlag, 2002.
6. O. L. Mangasarian and W. H. Wolberg, *Cancer diagnosis via linear Programming*, SIAM News, Volume 23, Number 5, September 1990, pp 1 & 18.
7. Wasserman P.D., *Advanced Methods in Neural Computing*, Van Nostrand Reinhold, New York, 1993.

DEVELOPMENT OF THE COMMON ENERGY POLICY IN THE EU

Taranic Igor
Senior Research Manager - Valdani Vicari & Associati Economics and Policy, Brussels
PhD Candidate - Academy of Economic Studies of Moldova (ASEM)
E-mail: tsaranik@gmail.com

The aim of this paper is to present the development of the Energy Policy framework of the European Union, from late 1940s till nowadays. The integration of the European energy markets and development of common elements of the energy policies has been a very long process. What looks today like a natural state of play, when EU member states (almost) fully cooperate on the energy issues was a result of long term process, navigated through changing geopolitical, economic and social conditions within and outside the EU.

Key words: *energy policy, energy security, security of supply, European Union*

Historical Development—Six Periods of the European Energy Policy

The notion of cooperation in the energy field and especially creating common energy policies between different countries is relatively new and quite rare phenomenon. One of the main reasons to that is well expressed by Dehousse (2007): *"The stability of energy provision is a fundamental strategic objective for all States, since energy is the basis of most economic activity"*. [1] Therefore, the way to cooperation between the Member States of the European Union in the area of energy policy has taken several decades, reaching the establishment of the Energy Union in 2015, with partly integrated energy markets and nearly common approach in the external energy policy.

In their article from 2010, Bozhilova and Hashimoto indicate five periods in the European Energy security, affected by both the internal European and external developments. [2]

1945–1957 – Energy to prevent a military conflict

European Coal and Steel Community (ECSC) is considered to be the beginning of the modern European Integration that led to the establishment of the European Union on a later stage. Often presented as the beginning of the integration of the energy policy on European level, the role of the ECSC was different, namely to prevent the possibility of another war in Europe by providing supranational management of steel and coal extraction (logistical prerequisites for military operations at that time). Common or coordinated energy policy was not an interest for the ECSC Member States.

1957–1972 - Cheap oil

That was the era of cheap oil, supplied from Arab countries, when Europe (amongst others) enjoyed abundant and cheap energy. Energy security was not Europe's concern and did not seem to require a policy, especially a coordinated one on the European level.

1973–1985 – National champions

The oil embargo, imposed by the Gulf states after the October 1973 war, followed by the quadrupled oil and gas prices, have raised the importance of the energy security concept. In fact, since 1973, energy security became one of the most important political and economic topics, causing political and at times military (e.g. Iraq's invasion in Kuwait) conflicts on one hand, and strengthening cooperation in the European Union, on the other hand.

Belkin and Morelli highlight three main immediate effects of that oil shock on the energy policy in Europe:

- It emphasized the need for crisis management mechanisms for possible future energy disruptions.
- It exposed the need for cooperation between members of the Community and between the EC and producers regarding energy policies.
- Europe understood that it needs to prepare strategies to prevent future usage of energy as an economic and political weapon. One of the immediate results was the creation of the International Energy Agency (IEA) in 1974, whose aim was to "help countries co-ordinate a collective response to major disruptions in oil supply through the release of emergency oil stocks to the markets" (International Energy Agency, 1974). [3]

Despite that, European Community's Member States preferred mainly national solutions [4], creating National energy "champions" companies.

1985–2000 – Liberalization

Soviet Union has been a reliable supplier of oil and gas to some of the European countries, but was considered as a security threat during the Cold War. It was one of the reasons that prevented European Community's Member States to establish a common energy policy.

With the collapse of the USSR, the opposition towards a common energy policy in Europe has slightly reduced. It was also the beginning of another process concerning energy policies – the beginning of the liberalization of the National energy markets and first attempts to create a common European energy market.

2000-2015 – Integration

The development of the European energy policy was impacted by both external and internal developments. Externally, rapid economic growth in the developing world was associated with increasing demand for energy, causing a sharp and significant increase in the oil prices, from about USD 20 per barrel of oil in 2001 to almost USD 100 in 2013, until the prices significantly dropped in 2014 and stabilized in the price range of USD 40-50 from 2015 onwards. [5]

Internally, the Lisbon Treaty was adopted, the first Treaty to include an energy provision. For the first time, the treaty gives the Union authority in the energy field, while each Member State still determines its own energy mix. What does it mean in practice? A good and illustrative (although somewhat extreme example) is the comparison of the

power (electricity) mix in France and Germany. France is a leader in nuclear electricity production in Europe and Germany is phasing out its production of nuclear power. As to coal, Germany's share of coal in electricity production is above 40% (2014), while in France the coal is hardly used. [6]

The main EU energy policy objectives are often presented as relationships between the competitiveness (also referred to as internal market), climate (also referred to as sustainability) and security of supply.[7]

The pillar of Climate/Sustainability

The EU has started the process of transition to a low carbon economy by 2050, aiming at limiting the global warming to less than two degrees Celsius, by reducing greenhouse gas emissions by 80% compared to the 1990 level. The plans for 2020 and 2030 are derived from the 2050 vision. In 2009 the EU decided on the so-called 20-20-20 targets by 2020 - 20-20-20 targets by 2020: 20% less Greenhouse Gas Emissions; 20% of renewable energy sources of the European Energy Mix and 20% more energy efficiency. In 2014 the 2030 targets of 40-27-27 % reduction were set - 40% less Greenhouse Gas Emissions; 27% of renewable energy sources of the European Energy Mix and 27% more energy efficiency.

Competitiveness/Internal Energy Market

Integration of national energy markets into the internal energy market began in 1990 with attempts to integrate gas and electricity markets. In 1996-98 the EU has legislated its first gas and electricity directives aiming at liberalizing the national energy markets. In 2003 a Second Energy Package opened the national borders of the EU Member States to gas and electricity trade.

The purpose of the current gas and electricity framework (Third Energy Package, which entered into force in 2009) is to further open gas and electricity markets in the EU.

Another instrument for achieving the internal energy market comes in the form of physical interconnections between Member States. For instance, the target for interconnecting electricity by 2020 is 10% and 15% for 2030 [8].

Energy Security

Since the 1990s the EU has been addressing the security of supply in different ways. The first way was building institutions of international cooperation.

1994—Energy Charter Treaty (ECT)

The main aim of the treaty was to integrate energy sectors of NIS and East European countries with Western Europe, which could enhance political and economic stability. [9] Russia signed but did not ratify the ECT.

Since 2000—EU-Russia Energy Dialogue

The EU-Russia Energy Dialogue was launched on 30 October 2000 at the sixth Summit between Russia and the EU in Paris. According to Cleutinx and Piper, "the underlying objective was to construct an effective energy community between the EU and the Russian Federation." [10] Aalto and Westphal argue that the dialogue was initiated because Russia did not ratify the ECT; the Commission needed a working energy

framework with Russia. [11] The dialogue was helpful for resolving technical issues of cooperation, but did not address political aspects and was "*largely put on hold*" as a result of the Russia-Ukraine crisis in 2013. [12]

2005—Energy Community Treaty

Given the limited scope of the Energy Charter Treaty, the EU and a number of third countries established a new energy community, the main purpose of which was to export the EU's energy *acquis communautaire* to neighboring countries (for example, adoption of the Third Energy package, described in the previous section). Like the Energy Charter Treaty, the Energy Community has limited scope, since Russia is not a part of it (Taranic 2016).

In the last ten years the notion of diversification became the leading component of European energy security strategy, in order to reduce energy dependence on Russia, the main exporter of energy sources to the EU. Russia's reputation as a reliable energy supplier to Europe was damaged twice - in 2006 and 2009 due to Russia's disputes over gas transit to Europe with Ukraine. It resulted in gas supply shortages to (especially) eastern European countries during the winter time. [13]

The 3Ds of European energy security are: diversification of energy sources, diversification of routes of supply, and diversification of suppliers.

In 2014 the EU commission has published the European Energy Security strategy, aiming at reducing its dependency on Russia and further improve interconnectedness between the Member States.

To summarize, an analysis of the EU's energy security initiatives shows that from the mid-1990s to mid-2000s the approach focused on strengthening international markets and institutions of energy, with the objective of facilitating cooperation with energy suppliers, especially Russia. In the mid-2000s the approach gradually shifted to geopolitics, with a strong quest to diversify from Russia (Taranic 2016). To date, when EU-Russia relations have reached their lowest point, "the quest for diversification is more relevant than ever." [14]

2015 - ongoing - Energy Union

Taranic (2016) claims that the EU has entered its sixth energy policy era – the creation of the Energy Union. In 2014 appointed European Commission has created a post of Commissioner for Energy Union, aiming at sending a message regarding the importance of this policy area clarifying what the Energy Union should be in its Energy Union package. It includes five main areas:

- Security of supply via diversification of energy sources and solidarity and cooperation between EU member states
- Fully integrated energy market
- Improved energy efficiency
- Low carbon economy
- Supporting research, innovation and competitiveness

In principle, the policy areas covered under the Energy Union were previously covered by various EU policies and strategies and is in the framework of the EU energy policy triangle. But addressing all those policy areas at once under one administrative supervision (and leadership) of a dedicated Commissioner could potentially make the Energy Union bigger than the sum of its parts.

The Energy Union project seems to be a wide consensus in the EU. In the past three years it has been delivering some positive results. Internally, the Commission has put forward two big legislative packages – "Clean energy for all Europeans" and "Clean mobility". Externally, EU's Commissioner for the Energy Union has been involved in the high politics, mediating talks between Russia and Ukraine on gas supplies.

Conclusions

This paper provides an overview of the development of the EU energy policy, starting from 1945 until nowadays. Since 1945, energy policies in the European Union have taken different shapes. Those policies were influenced by internal and external developments and slowly but surely were leading the EU towards a common energy policy approach.

The European energy debate started with attempts to monitor and control the production of coal to prevent another military conflict after WWII. Cheap oil of the 1950s-beginning 1970s did not require a coordinated energy policy. 1970s-1980s were dominated by national energy policies. 1990s was a decade of national energy markets liberalization and the beginning of the European integration in the energy field; in addition, EU has tried to create international market oriented institutions, such as Energy Charter, to create a level playing field for international energy trade. This approach has reversed in the 2000s, when the geopolitical approach of the security of supply started dominating the energy debate. 2000s was also a decade of unprecedented cooperation in the energy field between the EU member states, reaching its peak and resulting in the creation of the Energy Union in 2015.

References

1. Dehousse F. (2007): Towards a Real New Energy Policy for the European Union? The 2007 Challenge. In *Studia Diplomatica* 60 (2), pp. 11–23.
2. Bozhilova D. and Hashimoto T. (2010): EU - Russia Energy Negotiations: a Choice between Rational Self - Interest and Collective Action. In *European Security* 19 (4), pp. 627–642.
3. P. Belkin P. and V. L. Morelli (2007): *The European Union's Energy Security Challenges*, Washington D.C.: Library of Congress.
4. S. Andoura. (2007): "Security of Supply and the External Dimension of a European Energy Policy," *Studia Diplomatica* 60 (2): 27–109.
5. US Energy Information Administration (2017): US Crude oil first purchase price, https://www.eia.gov/dnav/pet/hist/LeafHandler.ashx?n=PET&s=F000000__3&f=A

6. Taranic I. (2016): EU energy policies and their relevance to the Eastern Mediterranean. In Gianacopulos A. (Ed.): Energy Cooperation and Security in the Eastern Mediterranean: A Seismic Shift towards Peace or Conflict? Tel Aviv University
7. Triple E (2015): EU energy governance for the future, Study requested by the European Parliament's Committee on Industry, Research and Energy
8. European Commission (2015): "Energy Union Package Communication: Achieving the 10% Electricity Interconnection Target. Making Europe's Electricity Grid Fit for 2020," COM(2015) 82 final, http://ec.europa.eu/priorities/energy-union/docs/interconnectors_en.pdf.
9. R.S. Axelrod (1996): "The European Energy Charter Treaty: Reality or Illusion?" *Energy Policy* 24 (6): 497–505.
10. C. Cleutinx and J. Piper J. (2008): "The EU-Russia Energy Dialogue." In K. Barysch (ed.), *Pipelines, Politics and Power: The Future of EU-Russia Energy Relations*, London: Centre for European Reform, pp. 25–34.
11. P. Aalto and K. Westphal (2008): "Introduction." In Aalto, op. cit., pp. 1–22.
12. European Commission (2015): The state of play of EU-Russia energy relations, Speech of Vice President of the European Commission for the Energy Union http://europa.eu/rapid/press-release_SPEECH-15-4709_en.htm
13. Taranic I. (2012): The Common European Energy Policy and the projects of Nord Stream and South Stream, Master Thesis, Dusseldorf University
14. S. Matalucci (2015): "European Funds for Mediterranean Gas Psychologically Important," *Natural Gas Europe*, 2/7/2015, http://www.naturalgaseurope.com/european-funds-for-middle-east-gas-psychologically-important-says-taranic-24448.

БЕЗОПАСНОСТЬ МОБИЛЬНЫХ УСТРОЙСТВ ANDROID

Татарова К.В.
Студентка SI-141
Экономическая Академия Республики Молдова
Научный руководитель- Охрименко.С.А.

Today, Android is the most widespread and leading mobile system. But, unfortunately, the platform can not be completely safe. And the popularity of the platform attracts more and more intruders. The main tasks of this document are to consider the problems and threats to the security of the Android mobile OS and determine the protection mechanisms.

Рынок мобильных устройств пережил большой рост. Поскольку все больше людей используют смартфоны и планшеты для просмотра веб-страниц, общения в социальных сетях, совершения покупок и банковских операций в интернете, киберпреступники все чаще атакуют мобильные устройства, используя при этом новые угрозы для смартфонов и мобильных устройств. Устройства создаются десятками производителей, работают под управлением разных платформ, под них написано огромное количество приложений, каждое из которых может нести риск. Зачастую на мобильном устройстве обрабатывается информация, относящаяся к персональным данным и, составляющая коммерческую тайну.

В 2012 году 99% всех вредоносных программ для мобильных устройств, обнаруженных «Лабораторией Касперского», были нацелены на платформу Android. За год эксперты «Лаборатории Касперского» обнаружили более 35 000 вредоносных программ для Android-устройств [1].

Существует несколько причин появления угроз Android. Во-первых, платформа Android стала наиболее распространенной ОС. Во-вторых, это открытость системы. Она заключается в доступности кода, простоты создания приложения, возможности устанавливать приложения не только из официального каталога приложений, общедоступности создания приложений. В-третьих, фрагментация платформы привела к сложности оптимизации приложений и отсутствию использования функциональности новых версий на устаревших моделях устройств. Производители устройств самостоятельно развивают кодовую базу с целью достижения большей функциональности и производительности. Побочным результатом такой деятельности становятся уязвимости и слабости в системе. Вредоносное ПО использует эти уязвимости для повышения прав и преодоления защитных механизмов. Некоторые вредоносные программы не используют эксплойты сами, напрямую, а вводят пользователя в заблуждение и побуждают его самого выполнить необходимые действия, тем самым дав вредоносной программе требуемые ей возможности.

Соответственно, одна из главных проблем, с которыми могут столкнуться пользователи, — уязвимости системы, позволяющие получить права root.

Существуют специальные приложения и программные модули, выполняющие эту задачу. Другое дело, что эти же уязвимости взяли на вооружение создатели вредоносных приложений. Используя те самые программные модули и скрипты для повышения своих прав до уровня root, они получают возможность, например, беспрепятственно устанавливать другие программы без разрешения пользователя. Некоторые вредоносные программы не используют эксплойты сами, напрямую, а вводят пользователя в заблуждение и побуждают его самого выполнить необходимые действия, тем самым дав вредоносной программе требуемые ей возможности. ОС имеет защиту от модификации, но, возможно получение полного доступа к системе. После получения root возможна запись в системные области и даже подмена системных приложений.

Так же, угрозу представляют: СМС-троянцы, коммерческие программы-шпионы, рекламные модули, использование неофициальных или сторонних прошивок.

Сегодня безопасность мобильной операционной системы Android обеспечивается с помощью трехуровневой системы: на уровне безопасности данных, на уровне безопасности приложений, на уровне безопасности устройств. Архитектура Android построена таким образом, что все приложения работают с ограниченными правами и не имеют доступа к защищенным данным других приложений. В системе по умолчанию включен режим SELinux, который предусматривает принудительный контроль прав доступа на уровне ядра ОС. Так же, одним из ключевых элементов безопасности Android является система разрешений. В системе поддерживается протокол Exchange Activesync.

Однако, популярность платформы Android привлекает все больше злоумышленников. Для того, чтобы обезопасить физический доступ устройства следует использовать блокировки (PIN, пароль, биометрия, росчерк), шифровать память устройства и внешней SD-карты, дополнительно устанавливать антивирус. При необходимости использовать возможность удаленной очистки данных, а также проводить анализ защищенности приложений.

Заключение

Основными проблемами безопасности мобильной ОС Android являются несвоевременность или невозможность получения обновлений, обход защиты самим пользователем, отсутствие корпоративной политики безопасности для мобильных устройств. Если разработчики прикладного ПО не уделяют достаточное внимание безопасности при работе с данными пользователей, эти данные могут быть скомпрометированы.

В условиях текущей ситуации, когда количество угроз растет, атаки становятся все более сложными. Необходимо внедрять новые технологии, проводить дополнительные исследования в области безопасности. Чтобы достойно справиться со сложностью атак и угроз, пользователям необходимо иметь инструменты и решения безопасности, которые способны анализировать и классифицировать поведение всех файлов и процессов.

Единственный эффективный путь решения проблемы – это построение комплексной многоуровневой системы безопасности, позволяющей существенно снизить риски утечки конфиденциальных данных, опции расширенной защиты для предотвращения и противодействия новым угрозам безопасности.

Литература

1. Угрозы безопасности мобильных устройств Android [Электронный ресурс]. URL: https://www.kaspersky.ru/resource-center/threats/android-mobile-threats
2. Пискунов И., Безопасность Android: взгляд внутрь [Электронный ресурс]. URL: https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/325122.php , 2016
3. Мишин А., Пылаева Е., Казуров А., Шоханова О., Android и мобильная безопасность [Электронный ресурс]. URL: http://bit.samag.ru/archive/article/1865 , 2017

REPORTING OF PUBLIC PROCUREMENT AUDIT RESULTS IN THE REPUBLIC OF BULGARIA

Lyubomir Rosenov Terziev, PhD Student
D. A. Tsenov Academy of Economics, Svishtov, Bulgaria
Department of Control and Analysis of Economic Activity

Abstract: *This paper aims to investigate the reporting of results from public procurement audits. This stage is essential as the publicity of auditors' reports informs all stakeholders about the findings of the auditors from the National Audit Office of the Republic of Bulgaria. These reports determine whether public procurement spending complies with the requirements for eligibility and appropriateness. Where material errors and infringements have been identified, control bodies shall modify their conclusion and take action to impose administrative and criminal liability on the contracting authority. The results of the survey show that these reports focus mainly on negative findings and do not include information about good practices established by contracting authorities.*

Keywords: *public procurement, audit report, conclusions, findings, Audit Office*

***

Reporting the findings is one of the last stages[1] of public procurement[2] auditing. At this stage the findings of the Audit Office control bodies are summarized in an audit report, which contains certain recommendations. The reports ensure the transparency of and inform the public about public spending. The content of the report should be consistent with the fact that the general public does not have direct access to the audit information.

Audit reports inform the general public and all stakeholders whether public procurement spending complies with the legislative provisions for eligibility and appropriateness. According to data published by the Public Procurement Agency, a total of ***90,792*** public procurement contracts were concluded in the country in the period 2012-2016. ***The total amount of public funds spent on these contracts is over BGN 34,68 bln.***[3] These facts show that there is a need for establishing a competitive, transparent, and well-regulated public procurement market that ensures optimal use of the European funds.[4]

***

[1] The stage of public procurement audit is preceded by the stages of planning and auditing.

[2] In Art. 1 (2) of the Public Procurement Act, public procurement is defined as "*acquiring by one, or several awarding authorities through a public procurement contract of public works, supply or services by selected by them contractors, and in sector awarding authorities – for fulfilment of sector activities.*"

[3] Data retrieved from the site of the Public Procurement Agency (http://rop3-app1.aop.bg:7778/portal/page?_pageid=93,1590259&_dad=portal&_schema=PORTAL) on 07 Feb. 2018.

[4] **Pavlova**, M. Novoto zakonodatelstvo po obshtestvenite porachki v Bulgaria – predisvikatelstvo I vazmozhnosti // *Normativna uredba, 2016, N2, p. 3.*

Reporting the results of public procurement audits can be considered in ***two aspects:***

1. ***Audit report preparation,*** including drafting and final reporting. This stage includes ***a series of procedures***: ***drafting*** the audit report; ***control over the quality*** of the draft and the audit itself; ***submitting*** the draft for approval or rejection of the draft for completion and/or elimination of omissions; ***communicating*** the audit report draft to the manager of the audited organization; ***considering the objections*** of the manager of the audited organization regarding the audit report draft[1]; ***preparation of final conclusion and review*** of the audit report by the National Audit Office; approval of ***the final audit report*** and decision; ***submitting*** the final audit report to the contracting authority subject to audit and/or to the competent authorities (where the audit report contains information about violations of the current legislation) as well as its publication on the website of the National Audit Office.

These procedures ***aim*** to ensure that all disputes are settled in accordance with the existing regulations and professional standards and by competent authorities. They are ***essential for the stage of reporting and administrative conclusion of the audit.***

2. ***Control over the implementation of audit recommendations.*** The control over the implementation of audit recommendations is carried out through follow-up checks, for which the control bodies draw up reports. ***The aim*** of this procedure is do determine ***the degree of implementation of the recommendations provided by the National Audit Office.*** The control over the implementation of audit recommendations is the ***final stage*** of the overall audit process.

According to the provisions of the current legislation, the audit report shall comprise the following parts: abstract, introduction, audit scope and approach, findings, conclusion, and recommendations. The first ***three*** parts are descriptive and provide information about the contracting authority subject to the audit.[2] This information is not subject to processing by the auditor. These three parts account for the ***smallest part*** of the bulk of the report.[3] The other parts (findings, conclusion, and recommendations)

---

[1] Note that when the contracting authority has objections regarding the findings in the audit report, it shall send them in writing to the Head of Department of the NAO. The Head of Department shall consider the objections and submit them to the National Audit Office for a final justified decision, which is sent in writing to the contracting authority.

[2] The term "contracting authority" has two meanings in the Public Procurement Act. The ***first*** meaning refers to public and sector authorities liable for planning and awarding of public procurement. These authorities are listed in Art. 5 of the Act. The ***second*** meaning refers to private entities and/or their unifications that are contracting authorities for concrete cases. The common feature of these two categories is that the conclude public procurement contracts with private entities.

[3] See **Audit** reports of the National Audit Office of the Republic of Bulgaria http://www.bulnao.government.bg/bg/articles/dokladi-128 [Last retrieved on 07 Feb. 2018].

constitute the ***main*** part of the audit report. They are not descriptive but analytical and justify the conclusions made by the auditors during the audit. Therefore, they can be defined as the ***material and important*** part of the audit report.

The findings part is the main section of the report, in which the collected evidence is analysed and evaluated. They follow the logical structure of the assessment criteria set during the audit planning stage. Audit findings are used as evidence for the control bodies to impose ***administrative and/or criminal liability on the contracting authorities and/or other persons involved in the process of awarding and execution of public procurement contracts.*** Note that the administrative and/or criminal punishment ***is not*** a typical function of the audits performed by the National Audit Office. This is due to the following ***two*** facts:

- ***The first one*** is based on the fact that the sanctioning function attributed to the National Audit Office control bodies ***is not*** typical for audit. This is supported by the opinion that "*The National Audit Office Act provides for a stark sanctioning derogation from the typical functions of a parliamentary Audit Office. In addition to the rights associated with its compliance auditing functions, its Chairperson is attributed administrative sanctioning competence as well.*"[1]
- ***The second one*** is based on the difference between the evidence collected under the Administrative Violations and Sanctions Act and the evidence collected in the course of the audit. The evidence in the administrative proceedings are related to facts and circumstances, significant for the rights or the obligations or the legitimate interests of the interested citizens or organisations. The aim is to establish all facts and circumstances related to the administrative proceeding.[2] They are established by the order provided by the Administrative Procedure Code.[3] Whereas the Administrative Procedure Code provides for the order for establishing evidence, the International Auditing Standards do not provide for the type of evidence to be established by the control bodies of the National Audit Office. Auditors gather a combination of the following types of evidence: accounting system information; documentary evidence; third-party representations; physical evidence; data interrelations, etc.[4]

Audit conclusion is the final ***essential component*** of the audit report. It ***summarizes*** the independent auditor's judgement whether the procedures were conducted by the contracting authority in accordance with the ***legislative provisions and all material aspects***. Audit conclusion accurately reflects the content of the report and

---

[1] **Dimitrov**, V. Auditat v Bulgaria, Fosia, 2012, p. 71.

[2] **Tsankov**, P. Dokazatelstva I dokazatelstveni sredstva v administrativnoto proizvodstvo po DOPK, Danatsite v Republika Bulgaria, I5-6, 2016, p. 13.

[3] See **Administrative Procedure Code**, prom. SG No. 30 / 2006, Art. 37.

[4] **Whittington**, O., **Pany**, K. Principles of Auditing and Other Assurance Services. New York, McGraw-Hill/ Irwin, 2012, pp. 142 – 148.

provides information about the significance of all irregularities found. The purpose of the conclusion is to provide information on the results achieved in terms of control guidelines - ***whether the contracting authority conducted the procedures in compliance with the law and what was/is the performance of its financial management and control system***.

Audi report conclusions are statements based on audit procedures, evidence, and findings. They must be based on significant findings, assessments, and evidence that are tied to the level of materiality.[1] Conclusions should be formulated objectively, rationally and according to set evaluation criteria. Audit report ***conclusions*** fall into ***two*** main categories:[2] ***conclusion for compliance in all material aspects and conclusion for non-compliance.***

a) ***Conclusion for compliance is drawn in all cases*** where the audit findings prove adherence to all regulations and regularity in ***all material aspects*** of the public procurement procedures subjected to auditing. These ***material aspects include all regulatory requirements and the clauses of the contracts concluded between the contracting authority and the contractor***. In order to form an opinion on the compliance in all material respects, auditors assess whether the audit evidence obtained proves material misstatements due to ***intent***.

The conclusion for compliance is based on findings which prove that the contracting authority has systematically observed all requirements regarding public procurement procedures. The review of the audit reports published on the website of the National Audit Office[3] shows that they focus mainly on ***findings related to non-compliance and misstatements and do not describe good practices***, which does not mean that non-compliances were found for all contracting authorities. ***In this respect, audit reports should present in a balanced manner both the negative and the positive findings regarding the contracting authority's activities***. This can be facilitated by the digitalization of public procurement, for which some legislative motions have already been made. ***The expected effect from dissemination of best practices will optimize the management processes of the contracting authorities and improve the efficiency of public spending. Our legislation does not explicitly provide for content restrictions or require that audit reports should include only the negative findings***.

b) ***Conclusion for non-compliance is drawn*** depending on ***the degree and scope of non-compliances*** found during the audit. Such conclusion is drawn for one or more aspects of non-compliance the audited authority and ***is not comprehensive*** for the entire process of awarding and execution of the public procurement contract. All conclusions for non-compliance must be justified by

---

[1] According to the Compliance Audit section of the Manual on International Audit Standards and Auditing, *"materiality is defined by the significance and importance of the audited activity, function, programme, process, revenue, expenditure, transaction, etc."*

[2] See **Manual** on International Audit Standards and Auditing, Compliance Audit section, Sofia, 2014, p. 223.

[3] See **Audit** reports of the National Audit Office of the Republic of Bulgaria http://www.bulnao.government.bg/bg/articles/dokladi-128 [Last retrieved on 07 Feb. 2018].

describing in the report the concrete ***findings*** of material non-compliance. In such cases the auditor shall inform the management of the audited entity about the findings that provide grounds for such a conclusion.

Where the obtained evidence is ***insufficient and/or circumstantial*** due to ***scope limitations*** but proves non-compliances that are both ***material and comprehensive*** to the organization, the auditor may ***refuse to draw a conclusion.***[1] In such cases, as in all other cases where non-compliance is found, the auditors give recommendations related to the findings that prove the non-compliance.[2]

Recommendations aim to improve the contracting authority's performance in the public procurement process. This is why they must be justified with specific reasons, add value, and address the identified problems and violations. Recommendations should include measures to be undertaken by the audited contracting authority in order to overcome the identified shortcomings and improve the process of public procurement.

Recommendations should include measures that are relevant the rights of the audited entity's management. They are more effective when they include reference to specific findings. The survey of actual audit reports shows that their recommendations only refer to provisions of the Public Procurement Act and ***do not state the causes*** of the non-compliance. In cases of ***non-compliance with internal regulations,***[3] ***the recommendations refer to:*** procedures and periods of public procurement planning; officials responsible for analyzing, summarizing and prioritizing the need for procurement of goods, services and building construction for preparation of annual plans; procedures for control over contract execution; procedures for preparation, filing, communication and archiving of the public procurement files. Recommendations are important in terms of their content, but also in terms of the control of their implementation, i.e. the ***follow-up control*** over the corrective measures taken and the effect thereof.

---

[1] **Kostova**, S. Mezhdunarodni standarti za vanshen odit, AI Tsenov, Svishtov, 2014, p. 175.

[2] **Donchev**, T. PhD Thesis: Control over the efficient spending of EU funds under extended de-centralization of their management, p. 148.

[3] The Public Procurement Act provides that "public contracting authorities shall adopt internal rules for management of the cycle of the public procurements, where they spend the annual budget, including with the funds, provided through various European funds and programmes, equal, or larger than BGN 5 mln. According to the requirements of Art. 140 of the Rules for the Implementation of the Public Procurement Law the internal rules shall provide at least for the procedure for: forecasting the needs of awarding, including for establishing the dates on which public procurement contracts in force must be present; planning conducting the procedures, by accounting the time for preparation, conducting of the procedures and signing the contracts; assigning the officials, responsible for the preparation of the procedures and the procedure for performing control over their work; receiving and storage of participation applications, offers and project and the procedure for assigning the staff and way of operation of the commission for performing selection of the applicants and participants, for consideration and assessment of the offers and or conducting negotiations and dialogue, as well as of the jury; signing the contracts; tracing the fulfilment of the signed contracts and for accepting the results from them; the actions in appealing the procedures; conducting of introductory and maintaining training of the persons, engaged with management of the public procurement cycle; documentation of each stage of the public procurement cycle and maintenance of the buyer's profile.

Therefore, we may conclude that audit reports aim to inform all stakeholders about the efficiency of public spending. Reports from public procurement audits supports the fair competition mechanism by preventing price speculations and ensuring the procurement of quality goods and services. They are important because public procurement is associated with a significant amount of public funds in the implementation of key projects for our economy.

References

1. Whittington, O., Pany, K. Principles of Auditing and Other Assurance Services. New York, McGraw-Hill/Irwin, 2012.
2. Administrative Procedure Code, prom. SG, No. 30 / 2006.
3. Dimitrov, V. Auditat v Bulgaria, Fosia, 2012.
4. Donchev, T. PhD Thesis: Control over the efficient spending of EU funds under extended de-centralization of their management.
5. Kostova, S. Mezhdunarodni standarti za vanshen odit, AI Tsenov, Svishtov, 2014.
6. Manual on International Audit Standards and Auditing, Compliance Audit section, Sofia, 2014.
7. Audit reports of the National Audit Office of the Republic of Bulgaria, http://www.bulnao.government.bg/bg/articles/dokladi-128[Last retrieved on 07 Feb. 2018].
8. Pavlova, M. Novoto zakonodatelstvo po obshtestvenite porachki v Bulgaria – predisvikatelstvo I vazmozhnosti // Normativna uredba, 2016, N2.
9. Tsankov, P. Dokazatelstva I dokazatelstveni sredstva v administrativnoto proizvodstvo po DOPK, Danatsite v Republika Bulgaria, I5-6, 2016.

ANALIZA FRAUDELOR INFORMAȚIONALE ȘI A MIJLOACELOR DE PROTECȚIE

Veronica Topala Anatolie - CIB studenta
Departmentul Informatică și Managementul Informației ASEM

Datorită dezvoltării tehnologiei, sistemul informatic a devenit un instrument de comunicare indispensabil. Lumea în care trăim este într-o permanentă schimbare şi se complică pe zi ce trece.

Evoluția din secolul anterior a mijloacelor de comunicare în masă și apariția noilor tehnologii de comunicare au spart barierele dintre state, în acest context informația a devenit, uneori, mult mai periculoasă şi distructivă decât armele de foc.

Domeniul securității informatice caută soluții tehnice pentru rezolvarea acestei contradicții aparente.

Însă utilizarea serviciilor de poştă electronică, web, transfer de fonduri, etc., se bazează pe un sentiment, adeseori fals de securitate a comunicațiilor, care poate transforma potențialele câştiguri generate de accesul rapid la informații, în pierderi majore, cauzate de furtul de date sau de inserarea de date false.

Toată lumea foloseşte sisteme informatice, dar foarte puțini sunt, care cunosc riscurile şi vulnerabilitățile acestora şi mai puțini sunt cei care ştiu să se protejeze.

Toate aspectele vietii noastre, depend de tehnologiile informaționale.

1. Definire fraudelor informaționale

Programele distructive în natura lor poartă efecte cu caracter distructiv iar consecințele activării și utilizării acestora, pot conduce la daune în acele domenii ale activității umane în care utilizarea sistemelor informatice este vitală.

Aceste programe îndeplinesc urmatoarele functii:

- pot ascunde semnele prezenței lor în sistemul informatic;
- posibilitatea de auto-dublicare, inclusiv crearea copiilor modificate;
- pot distruge codul altor programe în memoria internă RAM;
- pot transfera fragmente de informații din memoria RAM în anumite zone ale memoriei externe accesibile unui atacator;
- pot distruge și modifica datele sau componentele sistemului;
- pot crea canale de transmisie de date ascunse;
- pot monitoriza procesele de procesare a informațiilor și a datelor, principiile funcționării echipamentului de protecție;

Programele distructive sunt împărțite în următoarele clase:

1. **Viruși informatici** sunt programe care se instalează singure, fără voia utilizatorului, și poate provoca pagube atît în sistemul de operare cît și în elementele hardware (fizice) ale computerului.
2. **"Viermi"** sunt programe a căror funcție principală este auto-dublicarea prin distribuție în rețele, după principiul „caută şi distruge" (Search and Distroy), utilizând vulnerabilitățile sistemelor de aplicații și ale serviciilor de rețea.

3. **"Cai troieni"** sunt programe a căror funcție principală constă, de obicei, de a fura informații, cum ar fi numere de card de credit, aceștea pot fi descărcați cu ușurință și în necunoștință de cauză.
4. **Programele spion (Spyware)**, sunt programe atașate de obicei la programe gratuite, care captează pe ascuns date de marketing (prin analiza siturilor pe care le vizitează utilizatorul) și le folosește apoi pentru a transmite utilizatorului reclame corespunzătoare dar nesolicitate.

Vulnerabilitatea rețelelor se manifestă pe două planuri:

- **posibilitatea modificării sau distrugerii informației, adică atacul la integritatea ei fizică;**
- **posibilitatea folosirii neautorizate a informațiilor, adică scurgerea lor din cercul de utilizatori stabilit.**

Câteva studii de securitate a calculatoarelor estimează că jumătate din costurile implicate de incidente sunt datorate acțiunilor voit distructive, un sfert dezastrelor naturale sau accidentale şi un sfert greşelilor uname.

Atacurile presupun, în general, fie citirea informațiilor neautorizate, fie distrugerea parțială sau totală a datelor sau a calculatoarelor.

Se disting două categorii principale de atacuri: **pasive** şi **active.**

Atacurile pasive sunt acelea în cadrul cărora intrusul observă informația că trece prin "canal" fără să interfereze cu fluxul sau conținutul mesajelor.

Acestea au următoarele caracteristici:

1. nu cauzează pagube (nu şterg sau se modifică datele);
2. încalcă regulile de confidențialitate;
3. obiectivul este de a monitoriza datele;

Atacuri active – sunt acelea în care intrusul se angajează fie în furtul mesajelor, fie în modificarea, reluarea sau inserarea de mesaje false.

Aceasta înseamnă că el poate şterge, întârzia sau modifica mesaje, inserarea unor mesaje false sau vechi, poate schimba ordinea mesajelor, fie pe o anumită direcție, fie pe ambele direcții ale unui canal logic.Aceste atacuri sunt serioase deoarece modifică starea sistemelor de calcul, a datelor sau a sistemelor de comunicații.

John D. Howard propune următoarele şapte categorii de autori ai atacurilor informatice:

- **Hackeri** – persoane, mai ales tineri, care pătrund în sistemele informatice din motivații legate mai ales de provocare intelectuală sau de obținerea şi menținerea unui anumit statut în comunitatea prietenilor.
- **Crackeri** reprezintă un stil anumit de hacker, care sunt specializați în „spargerea" programelor shareware sau care necesită un anumit cod serial.
- **Spioni** – persoane ce pătrund în sistemele informatice pentru a obține informații care să le permită câştiguri de natură politică.
- **Teroriști** – persoane ce pătrund în sistemele informatice cu scopul de a produce teamă, în scopuri politice.

- **Atacatori cu scop economic** – pătrund în sistemele informatice ale concurenței, cu scopul obținerii de câştiguri financiare.
- **Criminali de profesie** – pătrund în sistemele informatice ale întreprinderilor pentru a obține câştig financiar, în interes personal.
- **Vandali** – persoane ce pătrund în sistemele informatice cu scopul de a produce pagube**.**

2. Cum interacționează programele distructive

Pentru a obține rezultatele pe care le doreşte, un atacator poate folosi mai multe metode de a patrunde spre informații, atît software cît şi harware, printre care putem enumera urmatoarele cîteva metode :

1. Furtul de parole – metode de a obține parolele altor utilizatori.
2. Inginerie socială – convingerea persoanelor să divulge informații confidențiale.
3. Greşeli de programare şi portițe lăsate special în programe – obținerea de avantaje de la sistemele care nu respectă specificațiile sau înlocuire de software cu versiuni compromise.
4. Defecte ale autentificării – înfrângerea mecanismelor utilizate pentru autentificare.
5. Defecte ale protocoalelor – protocoalele sunt impropriu proiectate sau implementate.
6. Scurgere de informații – utilizarea de sisteme ca DNS pentru a obține informații care sunt necesare administratorilor şi bunei funcționări a rețelei, dar care pot fi folosite şi de atacatori.
7. Transmiterea prin intermediul USB flash drive – încercarea fizica a programului distructiv.

3. Combaterea cu fraudele informaționale

În zilele noastre informația înseamnă puterea, drept pentru care tot mai multe persoane încearcă să obțină informații pe toate căile posibile. Important să ştim cum să protejăm informațiile.

Iată cîteva metode de protecție:

- **Antivirus software** - instalarea programelor de protecție
- **Controlul accesului la system** - asigură că utilizatorii neautorizați nu pot pătrunde în sistem şi încurajează (uneori chiar forțează) utilizatorii autorizați să fie conştienți de necesitatea securizării computerelor.
- **Criptarea** - este o altă metodă importantă de protejare a informațiilor sensibile stocate în sistemele de calcul, dar şi a celor care sunt transmise pe liniile de comunicație.
- **Implimentarea legislatiei RM - LEGE** Nr. 20 din 03.02.2009, privind prevenirea şi combaterea criminalității informatice.

Concluzie:

Odată cu evoluția tehnologică din ultimii ani şi datorită mediului electronic de transmitere, stocare şi gestionare a informațiilor din secolul prezent, un secol al vitezei şi al globalizării, se pune tot mai des problema securității informatice. Utilizînd la maxim metodele de combatere cu fraudele informaționale, reușim totuși sa evităm unele de problem, însă în multe cazuri nici acestea nu sunt deajuns.

Referințe:

1. Dr. Maxim Dobrinoiu (2006). INFRACȚIUNI ÎN DOMENIUL INFORMATIC.
2. М.А. Иванова (2011). РАЗРУШАЮЩИЕ ПРОГРАММНЫЕ ВОЗДЕЙСТВИЯ3.
3. https://www.juridice.ro/412111/vulnerabilitati-ale-sistemelor-informatice.html
4. http://www.cosmin-mihai.com/wp-content/uploads/PhD-Resume.pdf

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ КОМПАНИИ СОГЛАСНО МЕЖДУНАРОДНЫМ СТАНДАРТАМ

Тулуб Е.М.
Черкасский национальный университет имени Богдана Хмельницкого

Abstract. *The issue of information risk management is considered on the basis of international standards of risk management in the information security system.*

Усовершенствование технологий передачи и обработки данных, резкий рост количества и качества кибератак, необходимость обеспечения нового уровня информационной безопасности является причиной повышенного внимания к проблеме оценки информационных рисков и усовершенствованию систем управления ними.

Для процесса управления множеством информационных рисков в системе экономической безопасности мировым сообществом был создан ряд стандартов по обеспечению информационной безопасности и управлению рисками в бизнесе. К таким нормативным документам следует отнести:

- Международный стандарт ISO/IEC 17799:2005 (BS 7799–1:2000) «Управление информационной безопасностью - Информационные технологии. - Information technology- Information security management» [1].
- Группа стандартов ISO 27000, разработанная ISO/IEC JTC 1/SC, представляет собой требования к системам управления информационной безопасностью, метрики, изменения, управление рисками, а также руководство по внедрению.
- ГСТУ ISO/IEC 27001:2015 Информационные технологии. Методы защиты системы управления информационной безопасностью. Требования (ISO/IEC 27001:2013; Cor 1:2014, IDT). Данный национальный стандарт полностью соответствует международному стандарту ISO/IEC 27001:2013; Cor 1:2014, IDT) [2].

Согласно стандартам основополагающими этапами оценки рисков для системы управления информационной безопасностью можно считать:

- определение методики оценки рисков (использование различных методик, возможность повторной оценки и сравнения с результатами по другим методикам);
- идентификация рисков (дестабилизующих факторов, опасностей, угроз, уязвимых мест);
- анализ и оценка информационных рисков;

- анализ и оценка возможности снижения степени риска, его минимизации или локализации.

Преимуществами использования в работе с системой управления информационной безопасностью а основе международных стандартов являются: обеспечение беспрерывности работы информационных сервисов; минимизация рисков, связанных с кражами, неправильным и нецелевым применением оборудования, повреждениями и т.д.; снижение затрат на реализацию средств защиты информационных ресурсов, благодаря использованию новейших технологий и средств защиты информационных ресурсов; обеспечение целостности, конфиденциальности, а также комплексного подхода в системе защиты информации.

Для эффективного уровня функционирования компании необходимо одновременно управлять многими процессами. Управление информационными рисками позволяет компании достигать высокого уровня эффективности при приемлемом уровне риска, при этом руководство компании имеет доступный метод организации ресурсами. Стратегия реализации управления рисками позволяет компании своевременно снижать степень риска до приемлемого уровня. В зависимости структуры определенной информационной системы определяется уровень приемлемого риска и подход к управлению ним.

В начале процесса управления информационными рисками на основе международных стандартов необходимо провести анализ структуры, функций информационного объекта, далее проводится выявление и ранжирование угроз информационных ресурсов. После построения неформальной модели субъекта проводится анализ и оценка самого риска. Разработка предложений и рекомендаций строится на основе усовершенствования существующих, а также внедрения новых методов, методик, техник и инструментария.

Процесс менеджмента рисков в системе безопасности сочетает элементы количественного (более детального) и качественного (более простого) методов анализа, что делает его эффективным, удобным в использовании и понятным на каждом шагу оценивания для всех стейкхолдеров. Качественный подход уменьшает противодействие персонала на этапах анализа риска и принятия решений, дает возможность найти удовлетворительное решение и организовать его поддержку на протяжении всего управленческого процесса. Качественный подход используется, в первую очередь, в компаниях с наименьшим уровнем зрелости.

В процессе оценки информационных рисков качественный подход применяют для оперативного составления списка всех рисков, а количественный подход дает возможность в дальнейшем выполнить детальный анализ относительно небольшого количества наиболее вероятных рисков, обнаруженных на этом этапе. Анализ рисков может производиться с различной степенью детализации в зависимости от критичности ресурсов информационного объекта, уже известных слабых звеньев и предыдущих инцидентов информационной безопасности.

Анализ информационных рисков - основа для создания подсистемы управления информационной безопасностью субъекта хозяйствования. В ходе

процедур анализа степени информационных рисков следует придерживаться следующих шагов: идентификация информационных ресурсов (активов) компании, которые могут быть объектом риска, вероятных угроз актива и определения степени угроз безопасности информационной системы компании; оценивания уровня действенности средств контроля безопасности корпоративной системы; оценивания уязвимости корпоративной системы, рассматривается как результат влияния факторов возможного уровня силы угрозы и уровня действенности средств контроля; оценивания частоты событий потерь от информационных рисков как результата влияния факторов частоты возникновения угрозы и уязвимости корпоративной системы; оценивания величины возможных убытков от информационных рисков в корпоративной системы; оценивания уровня рисков в корпоративной системы как результирующей двух факторов: частоты событий потерь и величины возможных потерь от информационных рисков.

Литература:

1. ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management.
2. Національний стандарт України, Інформаційні технології, методи захисту системи управління інформаційною безпекою, вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT) ДСТУ ISO/IEC Cor 27001:2015

PROTEJAREA PROPRIETAȚII INTELECTUALE ȘI A DREPTULUI DE AUTOR

Ulinici Maxim
Elev al Colegiului Național de comerț al ASEM

Rezume: In this presentation will try to show you the importance of protection of the intellectual property and the copyright.Also all the laws and protections that the state gives us for our intellectual property and moral rights.

1.Drepturile morale

Drepturile morale de autor reprezintă expresia juridică a legăturii existente între operă şi creatorul ei. Astfel drepturile morale de autor influențează dreptul de autor in asa mod, încât înlătură aplicarea regulilor de drept comun.Chiar şi după ce autorul unei opere a cedat drepturile sale patrimoniale, el îşi păstrează drepturile morale de autor ca o consecință caracterului acestora. În doctrina română se utilizează expresia„drepturi personale nepatrimoniale" prin care se desemnează sfera drepturilormorale în general, în care se include şi drepturile morale de autor. Temeiul drepturilor morale de autor rezidă în asigurarea protecției personalității autorului

Cu toate acestea, drepturile morale de autor nu se suprapun, sub toate aspectele,cu drepturile personalității. Aria lor este mai largă întrucât protejează autorul împotriva oricărei atingeri aduse operei şi nu numai împotriva acelora îndreptatecontra onoarei sau reputației autorului.

Caracterele juridice ale drepturilor morale de autor

Legea nu enunță în mod expres caracterele juridice ale drepturilor moralede autor, dar acestea se degajă implicit din unele dispoziții ale legii.Dreptul moral de autor are următoarele caractere juridice:

a) caracterul perpetuu
b) caracterul legăturii strict personale în sensul că este ataşat de persoana autorului operei;
c) caracterul inalienabil şi insesizabil
d) caracterul imprescriptibil
e) caracterul absolut, opozabil erga-omnes
f) caracterul netransmisibil (cu excepția dreptului la paternitatea şi la inviolabilitatea operei)

2. Obiectul dreptului de autor

Obiectul dreptului de autor il constituie operele literare, artistice si stiintifice, indiferent de forma lor de exprimare, de valoarea sau destinatia lor.

Analiza dispozitiilor legale a permis doctrinei sa desprinda trei conditii esentiale de care depinde vocatia la protectie in cadrul dreptului de autor si anume:

- opera trebuie sa fie rezultatul unei activitati creatoare a autorului;

- sa imbrace o forma concreta de exprimare, perceptibila simturilor;
- sa fie susceptibila de aducere la cunostinta publicului.

In cele ce urmeaza vom vedea la ce se refera aceste trei conditii:

a) Opera trebuie sa fie rezultatul unei activitati creatoare a autorului.

Pentru a fi considerata indeplinita aceasta conditie, autorul nu trebuie sa se limiteze la o reproducere mecanica a operei, fara o contributie proprie in ceea ce priveste substanta de idei a operei in discutie.

In doctrina aceasta conditie poarta si numele de originalitate. Astfel, pentru a fi protejata, opera trebuie sa poarte amprenta personalitatii, a individualitatii individului.

b) Pentru a forma obiectul unui drept de autor, opera trebuie sa imbrace o forma concreta de exprimare, perceptibila simturilor.

Aceasta conditie, inseamna ca dreptul de autor se naste din momentul in care opera imbraca forma de manuscris, schita, tema, tablou ori alta forma concreta.

c) Cea de a treia conditie pentru ca o opera sa aiba vocatie de protectie este aceea de a fi susceptibila de aducere la cunostinta publicului, prin reproducere, executare, expunere sau orice alt mijloc. Aceasta cerinta fiind strans legata de cea precedenta, unii autori nu mentioneaza decat doua conditii ale protectiei, in cadrul dreptului de autor.

Conform legii dreptului de autor constituie obiect al acestui drept urmatoarele:

- scrierile literare si publicistice, conferintele, predicile, pledoariile, prelegerile si orice alte opere scrise sau orale, precum si programele pentru calculator;
- operele stiintifice, scrise sau orale, cum ar fi: comunicarile, studiile, cursurile universitare, manualele scolare, proiectele si documentatiile stiintifice;
- compozitiile muzicale cu sau fara text;
- operele dramatice, dramatico-muzicale, operele coregrafice si pantomimele;
- operele cinematografice, precum si orice alte opere audiovizuale;
- operele fotografice, precum si orice alte opere exprimate printr-un procedeu analog fotografiei;
- operele de arta grafica sau plastica, cum ar fi: operele de sculptura, pictura, gravura, litografie, arta monumentala, scenografie, tapiserie, ceramica, plastica sticlei si a metalului, desene, design, precum si alte opere de arta aplicata produselor destinate unei utilizari practice;
- operele de arhitectura, inclusiv plansele, machetele si lucrarile grafice ce formeaza proiectele de arhitectura;
- lucrarile plastice, hartile si desenele din domeniul topografiei, geografiei si stiintei in general;
- operele de arta digitala.

3.Protejarea proprietatii intelectuale

In legea nr 114 din 03.07.2014 al Republicii Moldova sunt clar evidentiate urmatoarele:

„Articolul 3. Proprietatea intelectuală

(1) Proprietatea intelectuală este proprietate privată, care aparţine persoanelor fizice sau juridice cu drept de posesiune, folosinţă şi dispoziţie.
(2) Proprietatea intelectuală cuprinde obiectele ce rezultă din activitatea intelectuală în domeniile industrial, economic, comercial, ştiinţific, informaţional, literar şi/sau artistic, precum şi în alte domenii.
(3) Proprietatea intelectuală se constituie din următoarele componente:
a) proprietatea industrială;
b) dreptul de autor şi drepturile conexe.''

În concluzie statul garantează dreptul cetăţenilor la proprietate intelectuală, libertatea creaţiei artistice şi ştiinţifice, precum şi apărarea, în baza legii, a intereselor lor economice şi personale ce apar în legătură cu practicarea diverselor genuri de creaţii intelectuale.

Bibliografie:

https://ru.scribd.com/doc/48549162/Referat-Dr-Proprietatii-Intelectuale

http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=354811http://www.qreferat.com/referate/drept/DREPTUL-DE-AUTOR448.php

НЕКОТОРЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ ФИНАНСОВОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

Василенко В.Э.
Черкасский национальный университет имени Богдана Хмельницкого

Для осознания важности эффективного обеспечения финансовой безопасности государства необходима разработка, а также реализация определенного механизма, который являлся бы системным образованием организационных и институционально-правовых основ и мероприятий для своевременной идентификации, предупреждения, нейтрализации и ликвидации угроз финансовой безопасности государства. Механизм обеспечения финансовой безопасности необходимо реализовывать на основе создания определенных научных теорий, концепций, стратегий и тактик финансовой политики, систематизации угроз, применения средств, способов и методов обеспечения безопасности при условии высокого уровня информационных рисков.

Сейчас в информационной сфере можно определить определенные потенциальные угрозы национальной безопасности страны, а именно: несбалансированность государственной политики и отсутствие необходимой инфраструктуры в информационной сфере; медленное вхождение Украины в мировой информационный рынок, отсутствие у международного сообщества объективного представления об Украине как информационно развитого государства; информационная экспансия со стороны других стран; отток информации, содержащей государственную тайну, а также конфиденциальной информации, являющейся собственностью государства [1].

В современных условиях развития мировых глобальных информационно-телекоммуникационных систем и глобализации экономических отношений проблема обеспечения экономической безопасности социальных систем, обладающих государственным суверенитетом, приобретает новое содержание и новое значение: система обеспечения экономической безопасности по своей сути призвана служить гарантом суверенитета и независимости страны, ее стабильного и устойчивого социально-экономического развития, поскольку национальная безопасность и обороноспособность страны тесно связаны с состоянием экономики.

Так как компьютерные системы прямо интегрированы в информационные структуры современной финансовой системы страны, средства защиты должны учитывать соответствующие формы представления информации, обеспечивать безопасность на уровне информационных ресурсов, а не отдельных документов, файлов или сообщений. Вопросами информационной безопасности государства в Украине занимаются более 20 государственных органов власти, однако до сих пор не

существует эффективного межведомственного взаимодействия, нет специального уполномоченного органа, который занимался бы комплексным решением проблем.

Высокий уровень угроз в киберпространстве подтверждается данными Государственного агентства по вопросам науки, инноваций и информатизации, приведенным в докладе о состоянии информатизации и развитии информационного общества в Украине за 2014 год. [2]. фактически количество преступлений, совершенных в результате несанкционированного доступа к информации достигла с семьдесят четвёртой 2012 году до четыреста сорок второго 2014 году, несанкционированного изменения данных количество преступлений увеличилось в 7 раз, нарушение правил пользования информацией - в 9 раз [3].

Ситуация, которая сложилась, говорит о неэффективности существующего механизма оценки защищенности информационных систем, особенно в финансовой сфере. Субъективные характеристики к сожалению не работают, а потому актуальной задачей является объективная оценка уровня защищенности информационных ресурсов и состояния уровня финансовой безопасности государства.

В современных условиях работы финансовых структур, в условиях обострения проблемы взаимосвязи информационной и финансовой безопасности государства, необходимо вовремя идентифицировать и оценить возникающие угрозы финансовой и информационной безопасности, и на этой основе применять необходимые меры по предотвращению угроз, по защите информационных и финансовых интересов от потенциальных угроз. Угрозы финансовой и информационной безопасности, касаются не только отдельных компонентов государственной системы, а также регионов, крупных компаний и территориальных образований. Они создают информационное воздействие на финансовую систему государства. Информационные системы, которые включают телекоммуникации, аналитическую и прогнозируемую информацию воздействуют не только на состояние рынка ценных бумаг, но и на состояние финансовой системы страны в целом. В процессе таких влияний происходят изменения курсов национальных валют, колебания цен и снижение конкурентоспособности товаров и услуг, возникают угрозы экономической безопасности субъектов рынка государства, а вследствие этого и финансовой безопасности государства.

Решение проблемы обеспечения безопасности борьбы в информационной сфере необходимо свести не только к защите каналов и средств передачи информации, охране государственной тайны, правительственной связи и информации и другим вопросам, которые принято рассматривать при анализе совокупности угроз и системы мер по обеспечению информационной безопасности. К задачам информационной безопасности в финансовой сфере также следует отнести безопасность информационных систем управления промышленностью, отраслями, предприятиями, банками. Финансовые и информационные угрозы могут возникать касательно любого компонента финансовой системы страны или же связей между ними, в том числе, относительно потоков товаров и услуг, потоков

денежных средств, информационных потоков. Кроме этого, угрозы безопасности могут возникать относительно тех элементов экономической системы или их связей, которые могут появиться в будущем, но определить содержание их в данных условиях достаточно сложно.

Таким образом, новые опасности и угрозы, такие как международный кибертерроризм, информационный шпионаж, организованная преступность в информационной сфере, опасность распространения вирусных компьютерных атак на информационно-управляющие системы в экономике и, прежде всего, в финансовой сфере и др. имеют глобальный характер и требуют серьёзных мер предотвращения, минимизации и т.д.

Литература:

1. Марєєв С. В. Інформаційна безпека як складова національної безпеки України / Марєєв С. В., Перевезій С. С., Степова С. В. // [Електронний ресурс]. – Режим доступу: http://www.rusnauka.com/16_ADEN_2010/Informatica/68028.doc.htm
2. Доповідь про стан інформатизації та розвиток інформаційного суспільства в Україні за 2014 рік. – [Електронний ресурс]. – Режим доступу : http://dknii.gov.ua/content/shchorichnadopovid-pro-rozvytok-informaciynogo-suspilstva
3. Янчев А. В. Організаційно-методологічні положення електронного документування в системі бухгалтерського обліку. – Автореферат дис. на здобуття наук. ступеня докт. екон. наук за спеціальністю 08.00.09 – бухгалтерський облік, аналіз та аудит (за видами економічної діяльності). – Житомир. Держ. технолог. універ., 2015. – С. 1.

GOOD PRACTICES AND MODELS FOR INFORMATION SECURITY IN BUSINESS ORGANIZATIONS

Vladislav Vladimirov Vassilev - PhD student
Department of Business Informatics
SA "Tsenov" – Svishtov

This report aims to justify the need to make the decision to invest in information security,to analyze the steps of this solution, describing them as clearly as possible from the point of view of business organization management. For this purpose, four models for investment in information security are considered and analyzed, and based on the analysis criteria for choosing such a model will be formulated.

In today's world, information systems of business organizations face the challenge of providing information security for their digital assets, protecting them from various types of threats. Practice shows that business executives do not pay attention to these requirements, mainly due to their efforts towards the end result, which are profit and additional dividends.

1. The need to protect information assets

With the advent of new information technologies, there have been significant changes in the various spheres of human activity. These changes not only affect the organizational structure, but also support the way in which different activities are carried out in entire sectors. An important role in this change is the digital information and its transformation into a strategic resource used in different spheres. Each business organization strives to use its information system to effectively process and store the collected data. At the same time, however, threats to information security are increasing.

Threats to information security are constantly evolving and require a timely response to reduce the risk of security penetration. Describing good risk management practices and frameworks for its assessment, analyzing different models for investment in information security, we are attempting to define the steps needed to build effective information protection.

2. Risk management for security of the information system

Good risk management practices are an important part of building an effective information security system. They help balance the cost-effectiveness of protecting business information assets. Various options are available, the most common ones being based on ISO27001 and certified by this standard. The use of ISO / IEC 27002: 2013 is recommended to apply in cases where certification under this standard is required. Other methods may also be used based on the needs of the business organization.

Risk management and its assessment are important guidelines for the decision to invest in information security, but as part of this decision, it is important to clarify the financial parameters of this process. Even when there are serious threats to information

security, it is difficult to decide on investments to secure it. Typically, management departments do not prioritize investment in information security even when assessing such risk due to the abstract nature of this issue. Their expectations are that an investment is expected to return to the resource input, and this is not the case for information security.

To support the decision to invest in information security, specially defined models for assessing the necessary investments can be used. They present different approaches for optimal investment in information security.

Below, we will take a look at information security investment models of Gordon-Loeb's model - for mitigation; of Sonnaric - oriented towards determining the risk of a breakthrough; of Kremorini and Martini - risk-oriented based on annual reports; of Bodjan, Blazis and Tekakjak - a model for risk assessment.

Model of Gordon and Loeb

This model was developed by Gordon and Loeb. Their idea is to make investments to provide information security to mitigate damage from an already existing vulnerability. This means that it should not focus on the potential loss or vulnerability of the business organization's information system, but to address the medium-risk vulnerabilities.

The model is based on the following assumptions:

- If the information is completely detached, there is regulated access to it, it will remain fully protected and there will be no need for investment in information security;
- If there is no investment in information security and there is external access to information, the probability of a security breach depends on the value of the information stored;
- As security investments increase, information becomes safer, but with a decreasing value in the long term;
- By investing sufficiently in security, the probability of a security breach is reduced to practically zero.

Gordon and Loeb estimate that no more than 37% of the expected loss should be invested based on an actual or hypothetical penetration.

Sonnaric's model

According to Sonnaric, Albanese, and Stout, return on investment is determined on the basis of the risk of a penetration, mitigation of potential loss and costs. The authors point out that risk assessment and mitigation is extremely difficult because there is no single model or approach that gives accurate results. As additional parameters to reduce these difficulties, they offer the following criteria:

- Risk measurement - in-depth research on the relationship risk assessment with the organization's performance;
- To mitigate the loss - use of different algorithms and comparing their results;
- Cost - the impact of the resources used on the performance of the organization must be determined.

Model of Cremorini and Martini

In their model, Cremonini & Martini calculate the return on investment in information security based on annual loss forecasts. They present the argument that based on only one index for assessing information security, only partial characterization can be given. Cremorini and Martini define and add as an additional index the return on investment after a successful attack related to the type of malicious attack and how to counter it.

This includes:

- the persistence of attempts to break into information security
- opposing these attempts
- implemented security controls.

The model of Bojanc, Jerman-Blazic, Tekavcic

Bojanc, Jerzy-Blazic and Tekavcic highlight the introduction of a mathematical model for optimal investment in information security and investment decision-making based on in-depth risk research for business information assets organization. In their view, attention should be paid to the types of information security measures and their impact on the functionality of the organization. At the same time, they also present the need to define a clear and accurate risk control methodology. Their model is formed by:

- Evaluation of information assets;
- The degree of vulnerability of the system;
- Probability of breakthrough;
- Loss after breakthrough.

In trying to find potential losses through a financial framework, Bodjan, Blazis and Tekakik also offer a simplified risk-based system based on the following rules:

- Reducing risk;
- Transmitting the risk;
- Acceptance of risk.

They also offer simplified rules for building information security:

- Preventive measures - reducing the possibility of breakthrough;
- Correction / Reducing Measures - Reducing Loss;
- Identification measures - ways of timely reporting of irregularities.

Criteria for selecting an investment model from a business organization perspective

After presenting the selected investment models to provide information security, we will define criteria for their applicability from the point of view of business organizations. Our suggestion is:

- Financial framework - use of financial resources;
- Way of investment;
- Benefits;
- Negatives.

Table 1

Comparison of investment patterns to provide information security

Criteria	Model of Gordon and Loeb	Sonnaric's model	Model of Cremorini and Martini	The model of Bojanc, Jerman-Blazic, Tekavcic
Financial framework	An optimal investment of 37% of net revenue is presented.	It presents a financial framework that is based on the value of the information and can not be accurately determined.	It presents a framework based on an annual financial plan, anticipating potential losses, changing on the basis of the attacks.	A financial framework based on the value of the information and the vulnerability of the system is presented.
Way to invest	Fixed investment method with precise and clearly defined parameters.	A fixed way to invest, which is determined at the early stage of building information security.	A fixed way to invest, based on annual loss expectations and return on investment after a successful attack.	Fixed, offering the possibility of a continuous investment, based on the risk analysis of the information assets.
Benefits	Benefits consist of protecting assets with a higher risk of causing damage and building protection for them with a fixed amount of investment.	The model offers benefits focusing on mitigating losses and highlighting the link between productivity and business organization security.	The model offers an analysis of the attacks that constantly threaten the security of the information.	Benefits derive from risk definition and assessment and proposed information security policies based on good practice.
Negatives	No attention is paid to the probability of a breakthrough that the attackers use.	Constantly evolving threats are not taken into account. In so doing, mitigating losses may not be effective.	Permanent exposure to breakthrough risks may be unprofitable and potentially dangerous.	The ability to undergo changes in defining financial parameters based on risk analysis and assessment.

On the basis of this analysis, we propose to use the positive aspects of the Gordon and Loeb model – the fixed investment values and the benefits of identifying while assessing the risks proposed by the Bodjan, Blazis and Tekacik model. This would help in building an effective information security system.

Conclusion

On the basis of the above, we come to the conclusion that risk control and its analysis is an extremely important part of the decision to build information security. It is a fundamental step that business organizations must take.

The considered models for investments in information security have different specifications, meeting the different requirements of management. They take into account available information assets and offer different approaches to ensure their protection.

The criteria we propose cover the main points to be addressed when applying the listed protection models. Based on them, our proposal to use the utility of the models provides flexibility and helps in the selection of such a model and will undoubtedly assist management in choosing a solution to protect the information assets of the business organization.

References:

1. Bojanc, R., Jerman-Blazic, & Tekavcic, M. (2012). Managing the investment in information security technology by use of a quantitative modeling. Information Processing & Management.
2. Cremonini, M., & Martini, P. (2005). Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA). 4th Workshop on the Economics on Information Security 2005.
3. Lawrence, G., & Loeb, M. (2002). ACM Transactions on Information and System Security (TISSEC) - The Economics of Information Security Investment, 438-457.
4. Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return On Security Investment - A Practical Quantitative Model. Journal of Research and Practice in Information Technology.

РОЛЬ ВНУТРЕННЕГО ИТ КОНТРОЛЯ В ПРОЦЕССЕ УПРАВЛЕНИЯ ИЗМЕНЕНИЯМИ

Водопьянова Е.А., Комогорова Е.Ю.
Студенты 2 курса направления подготовки магистров «Бизнес-информатика»
Научные руководители: Алтухова Н.Ф., к.э.н., зав. кафедрой;
Зараменских Е.П., к.т.н., доц.
Финансовый университет при Правительстве РФ, Москва, Россия

В век инноваций контроль над изменениями в организации становится основой ее конкурентоспособности. Компании, для которых степень удовлетворенности клиента напрямую зависит от уровня развития ИТ, вынуждены внедрять процессы управления изменениями для своевременного реагирования и использования улучшений. Кроме того, процесс управления изменениями дает возможность оценивать потенциальные риски изменения ИТ инфраструктуры и минимизировать их.

Грамотная модель процесса управления изменениями должна охватывать все стадии обработки изменений: от осознания потребности бизнеса до реализации изменений в функционале информационных системах компании. Так как все подразделения компании взаимодействуют друг с другом, то очевидно, что изменение в функционале одного подразделения неизменно повлияют на работу другого функции. Поэтому при внедрении изменений в работу одного подразделения необходимо оценить степень влияния на деятельность других подразделений и, в случае необходимости, проинформировать и согласовать с ключевыми пользователями данные изменения. В противном случае, несогласованность и отсутствие информирования других подразделений может привести к невозможности использования изменений, связанной с неготовностью перестраивать свои процессы под внедренные изменения. Непродуманное внедрение изменений на предприятии ведет к простоям в работе, а как следствие, к убыткам компании.

Как следствие, неотъемлемой частью подобной модели является внутренний контроль, который позволяет оценивать и формировать методы по снижению или устранению рисков. В связи с тем, что в современных компаниях именно ИТ является основой для реализации бизнес-процессов, т.к. информационные системы настраиваются и дорабатываются под нужды компании, то анализ изменений в информационных системах позволяет управлять не только рисками информационной безопасности, но и выстраивать корректные автоматические контроли бизнес процесса и разграничение полномочий и зоны ответственности сотрудников.

Целью исследования было проанализировать лучшие практики и стандарты по управления изменениями, а также предложить вариант эффективного контроля за данным процессом.

Цель процесса управления изменениями — обеспечение внесения изменений в IT-инфраструктуру в соответствии со стандартизованными процедурами, для эффективного проведения изменений и минимизации рисков внесения изменений на функционирование инфраструктуры[4]. В процесс управления изменениями входят следующие виды деятельности: регистрация и фильтрация запросов на изменение, классификация запросов на изменение, оценка влияния и ресурсов (приоритет и степень воздействия), согласование и одобрение процесса управления изменениями, планирование изменений, построение, тестирование и реализация изменений, оценка выполненных изменений (подтверждение итогов). Благодаря проведению данных работ улучшается согласованность услуг и бизнеса, изменения своевременно доводятся до сведений всех заинтересованных лиц от бизнеса, что снижает риск внедрения некачественных изменений, а также повышается продуктивность работы ключевых пользователей[3]. В связи необходимость эффективного внедрения и использования процесса управления изменениями становится очевидной для всех конкурентоспособных компаний.

Под управлением изменениями понимают процесс, который позволяет организации модифицировать любую часть ее структуры, чтобы эффективно функционировать в постоянно меняющейся среде. Целью этого организационного процесса является расширение прав и возможностей сотрудников принять и поддержать изменения в их текущем бизнес-окружении [5].

Исходя из того, что изменения в бизнесе происходят постоянно, то эффективное управление изменениями является ключевой особенностью успешного бизнеса. Система «управления постоянными изменениями» это глубоко интегрированный в бизнес функциональный модуль, который необходимо грамотно спроектировать и интегрировать с другими бизнес-процессами компании.

Для организации процесса, в первую очередь, необходимо оценить ИТ-цели, на которые он направлен, его активности, метрики для измерения этого процесса. Ключевые атрибуты процесса возможно определить, обратившись к соответствующим стандартам, которые можно использовать в качестве референтных моделей по организации процесса управления изменениями. Далее будут рассмотрены международные практики и стандартны по управлению изменениями: ITIL, Cobit и BABOK.

В BABOK (Business Analyst Body of Knowledge) процесс управления изменениями рассматривается как процесс осознания бизнес потребности и формирование требований к изменению функциональности системы. Свод знаний BABOK описывает процесс анализа бизнес потребностей, а также методы, которыми возможно пользоваться при проведении данного анализа. Однако BABOK не затрагивает технических аспектов внедрения изменений [3].

Согласно ITIL процесс управления изменениями включает в себя следующие виды деятельности: регистрация и фильтрация запросов на изменение, классификация запросов на изменение, оценка влияния и ресурсов (приоритет и степень воздействия), согласование и одобрение процесса управления изменениями, планирование изменений, построение, тестирование и реализация изменений,

оценка выполненных изменений (подтверждение итогов)[2]. В библиотеке ITIL выделены входы и выходы процесса. Входами процесса считаются: RFC (Request for Comments), CMDB (Configuration management database), FSC (Forward Schedule of Change). Выходами: RFC (Request for Comments), FSC (Forward Schedule of Change), Отчеты, Протоколы изменений [2].

Согласно Cobit 4.1 процесс управления внесением изменений сосредоточен на оценке последствий, авторизации и внедрении всех изменений в ИТ инфраструктуру, приложения и технические решения; минимизации ошибок, возникающих по причине неполных спецификаций; предотвращении реализации неавторизованных изменений [1].

Процесс управления изменениями направлен на достижение следующих ИТ-целей:

- обеспечить соответствие изменений бизнес-требованиям;
- внести авторизованные изменения в ИТ-инфраструктуру и приложения;
- оценить последствия изменений для ИТ-инфраструктуры, приложений и технических решений;
- отслеживать и отчитываться о статусе изменений перед основными заинтересованными сторонами;
- минимизировать ошибки, вызванные неполными спецификациями при запросах на изменения.

Управление внесением изменений достигается с помощью:

- определения и информирования о процедурах внесения изменений включая аварийные изменения;
- оценки, расстановки приоритетов и авторизации изменений;
- мониторинга статуса и отчетность об изменениях.

Результаты управления внесением изменений оцениваются с помощью следующих показателей:

- число сбоев и ошибок в данных, вызванных неточными спецификациями или неполной оценкой последствий;
- количество переделок в приложениях или инфраструктуре, вызванных неверными спецификациями изменений;
- доля изменений, которые производятся согласно формализованным процессам контроля.

Однако данные стандарты не учитывают участие контрольных функций в процессе, которое необходимо для управления рисками организации. Современные изменения бизнес-процессов часто инициируют изменения в информационных системах, а следовательно контроль над ИТ-изменениями является основой для построения эффективной системы внутреннего контроля в целом.

Компании приходят к практике создания направлений по управлению общими ИТ-контролям, к функционалу которых относится:

- проверка корректности разграничения полномочий;

- проверка отсутствия уязвимостей в коде программы, разработанной под новые бизнес-функции;
- отслеживание запросов на изменение в информационных системах определение влияния изменений в ИС на процесс для предоставления информации подразделениям, осуществляющих контроль на уровне бизнеса.

Сотрудников общих ИТ контролей целесообразно привлекать к управлению изменениями на различных этапах. Например, при разработке нового функционала эффективно провести согласование как на этапе формирования бизнес-требований к новой ИТ разработке, так и на этапе тестирования нового функционала. Это позволит сотрудникам внутреннего контроля проанализировать степень влияния новой разработки на связанный функционал, выявить и проинформировать заинтересованных бизнес-пользователей (возможно, провести дополнительно согласование), среагировать на попытку реализации критичных изменений, которые могут привести к остановке бизнеса, а также выявить уязвимости в коде программы (например, отсутствие необходимого разграничения полномочий) при проверке последующей реализации. Именно такое выстраивание процесса является, на наш взгляд, наиболее эффективным с точки зрения соблюдения практик внутреннего контроля

Однако данный подход влияет на скорость внесения изменений, т.к. сотрудники ИТ подразделений вынуждены закладывать время на дополнительное согласование. Это может оказаться критичным для инновационных компаний, в которых изменения внедряются на постоянной основе. Такие компании могут построить модель, согласно которой сотрудники внутреннего контроля будут участвовать в проектах по внедрению изменений на постоянной основе и корректировать бизнес-требования и технические задания на изменения.

Вне зависимости от того, в каком статусе сотрудники внутреннего контроля включены в процесс управления изменениями, их роль в процессе невозможно игнорировать. В случае отсутствия контроля над изменениями в информационных системах, сотрудники внутреннего контроля не смогут полноценно настраивать контроли в бизнес-среде, что в дальнейшем может привести к низкой эффективности контрольных процедур и реализации рисков компании, что в свою очередь влияет на ее финансовые показатели и положение на рынке в целом.

Список использованной литературы

1. Стандарт CoBit5 // ISAACA, 2013
2. Библиотека ITIL v3, 2007
3. BABOK v3, 2008.
4. Глушаков В.Е. Управление изменениями в бизнесе. – М.: Дикта, 2011. – 212 с.
5. Hiat, Jeff. The definition and history of change management, 2008.

СТЕГАНОГРАФИЯ ВИДЕО ПРИ ПОМОЩИ ДИСКРЕТНОГО КОСИНУСНОГО ПРЕОБРАЗОВАНИЯ НА ОСНОВЕ КОДОВ КОРРЕКЦИИ ОШИБОК ДЛЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ДАННЫХ

Врančану Е. С.
Студент группы SI-141
Academia de Studii Economice a Moldovei
Научный руководитель Згуряну А.

At present, the science of hiding information has gained immense importance due to advances in information and communication technologies. The performance of any steganographic algorithm depends on the effectiveness of the implementation, the introduction of payload and reliability for the attackers. Low hidden ratio, less security and poor quality of video are the main problems of many existing steganographic methods. In this article, reviewed a new method for video steganography in the discrete cosine transform (DCT) domain based on error correction codes (ECC).

***Keywords**: video, steganography, ECC, DCT.*

Введение

Общая задача как стеганографии, так и криптографии заключается в обеспечении конфиденциальности и защиты данных. Стеганография, что в переводе «защищенная письменность», устанавливает скрытый канал связи между законными сторонами; в то время как криптография, в переводе «секретная запись», создает открытый канал связи [1]. В криптографии само наличие секретных данных известно; однако его содержимое является неизвестным для неавторизованных пользователей. Чтобы повысить уровень безопасности, стеганографии и криптографии следует работать вместе в одной системе [2].

Видео стеганография

Благодаря продвижению интернет-технологий и мультимедийных технологий, цифровые видеоролики стали популярным выбором для сокрытия данных. Видео содержат огромное количество избыточных данных, которые могут быть использованы для встраивания секретной информации. В последнее время существует множество полезных применений методов видео стеганографии, в таких областях как: исправление ошибок видео [3], военные службы, экономия трафика сети, видеонаблюдение и защита медицинской видеоинформации [4]. Методы видео -стеганографии классифицируются в сжатые и несжатые домены [5].

Стандарт H.264 повысил эффективность сжатия видео по сравнению с предыдущими версиями. Некоторые новые возможности видеокодека H.264 включают в себя гибкое упорядочение макроблоков, интерполяцию в четверть пикселя, внутреннее предсказание во внутрикадровом режиме, пост-обработку

фильтрации деблокирования и возможность задания опорных кадров [6]. Обычно кодек H.264 содержит несколько групп изображений. Каждая группа включает в себя три типа кадров: внутренний кадр, предсказанный кадр и двунаправленный кадр. Во время сжатия видео процессы оценки и компенсации движения минимизируют временную избыточность. Поскольку видеопоток представляет собой количество коррелированных неподвижных изображений, кадр может быть предсказан с использованием одного или нескольких опорных кадров на основе методов оценки и компенсации движения.

В отличие от сжатого видео, стеганографические методы необработанного видео работают с ним, как с последовательностью кадров с одинаковым форматом. Во-первых, цифровое видео преобразуется в кадры, статические изображения, а затем каждый кадр индивидуально используется в качестве контейнера для встраивания скрытой информации. После процесса внедрения все кадры объединяются вместе для создания стего видео. Стеганографические методы необработанных видео состоят из пространственных методов и методов преобразования домена [7].

Дискретное косинусное преобразование

DCT - хорошо известный метод, который используется во многих приложениях, таких как сжатие изображений и видео. DCT разделяет сигнал на низкие, средние и высокочастотные области. DCT тесно связан с DFT. Это сепарабельное линейное преобразование. Для входного видеокадра A разрешения M × N частотные коэффициенты DCT для преобразованного кадра, B и обратные DCT коэффициенты восстановленного кадра вычисляются в соответствии со следующими уравнениями соответственно:

$$B_{pq} = \propto p \propto q \sum_{1}^{m} = \theta M-1 \sum_{1}^{n} = \theta N-1 A_{mn} * \cos\pi(2m+1)p_2 M \cos\pi(2n+1)q2N \quad (1)$$

$$A_{mn} = \sum_{1}^{p} = \theta M-1 \sum_{1}^{q} = \theta N-1 \propto p \propto q B_{pq} * \cos\pi(2m+1)p_2 M \cos\pi(2n+1)q2N, \quad (2)$$

где

$$\propto p = \{ 1M,\ p = \theta 2M,\ 1 \le p \le M-1$$

и

$$\propto q = \{1N,\ q = \theta 2N,\ 1 \le q \le N-1$$

а (m, n) - значение пикселя в строке m и столбце у кадра A, а B (p, q) - коэффициент в строке p и столбце q матрицы 2D-DCT. Каждый из низких, средних и высокочастотных коэффициентов использовался в качестве контейнера для встраивания закодированного секретного сообщения.

Коды Хэмминга и BCH для исправления ошибок

В этой работе используются коды Хэмминга $(7, 4)$ (n = 7, k = 4 и p = 3), которые могут исправить идентификацию ошибки одного бита. Сообщение размера M $(m_1, m_2, ..., m_k)$ кодируется путем добавления дополнительных битов p (p_1, p_2, p_3) в качестве четности, чтобы стать кодовым словом 7-битовой длины. Кодовое слово

готово для передачи по каналу связи к концу приемника. Общая комбинация данных сообщения и четности с использованием этих типов кодов заключается в размещении битов четности в положении $2i$ ($i = 0, 1, ..., n\text{-}k$), таких как $p_1, p_2, m_1, p_3, m_2, m_3, m_4$. Логическая диаграмма кодов Хэмминга $(7, 4)$ показана на рисунке 1.

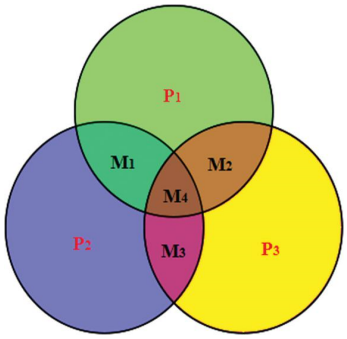


***Рисунок 1:* Логическая диаграмма кодов Хэмминга (4, 7).**

В этом разделе был рассмотрен новый алгоритм видео стеганографии в области DCT на основе кодов Хэмминга и BCH (1, 4, 7). Вначале видеопоследовательность разделяется на кадры; каждый кадр преобразуется в цветовое пространство YCbCr. Причиной преобразования в цветовое пространство YCbCr является устранение корреляции между красными, зелеными и синими цветами. Методология предложения состоит из этапа внедрения данных и этапа извлечения данных.

Этап внедрения данных. Для целей безопасности скрытое сообщение зашифровывается с помощью секретного ключа, а затем к нему будут применяться коды Хэмминга и BCH (1, 4, 7), которые генерируют закодированное сообщение. Все закодированное сообщение преобразуется из двоичных чисел в восьмеричные. С другой стороны, каждая видеопоследовательность преобразуется в несколько кадров. Каждый кадр разделяется на цветовое пространство YUV. Затем 2D-DCT применяется индивидуально на каждой плоскости. Впоследствии процесс встраивания достигается путем сокрытия каждой восьмеричной цифры кодированного сообщения в частотные коэффициенты DCT, за исключением DC-коэффициентов каждой из плоскостей *Y, U* и *V*. После этого обратное к 2D-DCT применяется к трем стего компонентам каждого кадра, создавая стего кадр. Наконец, стего видео построено из этих стего кадров. Секретное сообщение скрывается в каждом из DCT коэффициентов *Yij, Uij* и *Vij* следующим образом:

$$Y^{ij} = \{ Embedding(\left|Y_{ij}\right|, D_k)\ Embedding\ (Y_{ij}, D_k);\ Y_{ij} < 0;\ Y_{ij} \geq 0 \qquad (3)$$

$$U^{ij} = \{ Embedding(\left|U_{ij}\right|, D_k)\ Embedding\ (U_{ij}, D_k);\ U_{ij} < 0;\ U_{ij} \geq 0 \qquad (4)$$

$$V^{ij} = \{ Embedding(\left|V_{ij}\right|, D_k)\ Embedding\ (V_{ij}, D_k);\ V_{ij} < 0;\ V_{ij} \geq 0, \qquad (5)$$

где Y^{ij}, U^{ij} и V^{ij} - DCT коэффициенты стего *Y, U* и *V* плоскостей соответственно, а D_k - закодированные цифры $D_k = \{000, ..., 111\}$.

Этап экстракции данных. Каждый кадр делится на *Y, U* и *V*. Затем 2D-DCT применяется отдельно на каждой плоскости. Процесс извлечения закодированного сообщения выполняется путем приема D_k цифр из каждого из коэффициентов *Y, U* и *V* DCT, соответственно, за исключением DC-коэффициентов. Данные результатов декодируются декодером Хэмминга и BCH (1, 4, 7), за которым следует процесс дешифрования для извлечения действительного встроенного сообщения. Цель использования методов шифрования и кодирования перед процессом внедрения заключается в повышении безопасности и надежности предлагаемого алгоритма. Более того, секретный ключ делится только между отправителем и получателем и используется как в процессах внедрения так и извлечения данных. Скрытое сообщение может быть получено следующим образом:

$$D^k = \{\ Extracting(\left|Y^{ij}\right|)\ Extracting\ (Y^{ij});\ Y^{ij} < 0;\ Y^{ij} \geq 0 \quad (6)$$

$$D^k = \{\ Extracting(\left|U^{ij}\right|)\ Extracting\ (U^{ij});\ U^{ij} < 0;\ U^{ij} \geq 0 \quad (7)$$

$$D^k = \{\ Extracting(\left|V^{ij}\right|)\ Extracting\ (V^{ij});\ V^{ij} < 0;\ V^{ij} \geq 0, \quad (8)$$

где Y^{ij}, U^{ij} и V^{ij} - DCT коэффициенты для стего YUV плоскостей, а D^k - полученное секретное сообщение.

Заключение

Стеганографический алгоритм преобразует видео в кадры; он делит каждый кадр на *Y, U* и *V* компоненты. До процесса внедрения секретное сообщение шифруется и кодируется с использованием кодов Хэмминга и BCH. 2D-DCT применяется к каждому компоненту YUV. Коэффициенты DCT, исключая коэффициенты DC, выбираются для встраивания секретных данных.

Предлагаемый алгоритм имеет высокую полезную нагрузку для встраивания, также высокое качество стего видео. Более того, экспериментальные результаты показали, что предложенный алгоритм устойчив к нескольким атакам. Кроме того, безопасность этого метода улучшается за счет процессов шифрования и кодирования до процесса внедрения.

Список источников

1) Abu-Marie, W., Gutub, A. and Abu-Mansour, H. (2010). Image based steganography using truth table based and determinate array on RGB indicator. *Int. J. Signal Image Process.* 1, 196–204.
2) Das, R. and Tuithung, T. (2012). "A novel steganography method for image based on Huffman Encoding," in *Proceedings of the 2012 3rd National Conference on Emerging Trends and Applications in Computer Science*, (Piscataway, NJ: IEEE), 14–18.
3) Mstafa, R. J. and Elleithy, K. M. (2016). "A novel video steganography algorithm in DCT domain based on hamming and BCH codes," in *Proceedings of the 2016 IEEE 37th Sarnoff Symposium*, (Newark, NJ: IEEE), 208–213.

4) Muhammad, K., Sajjad, M., Lee, M. Y., and Baik, S. W. (2017). Efficient visual attention driven framework for key frames extraction from hysteroscopy videos. *Biomed. Signal Process. Control* 33, 161–168.
5) Sajjad, M., Muhammad, K., Baik, S. W., Rho, S., Jan, Z., Yeo, S.-S., et al. (2016). Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices. *Multimed. Tools Appl.* 1–18.
6) Shanableh, T. (2012). Data hiding in MPEG video files using multivariate regression and flexible macroblock ordering. *Inform. For. Secur. IEEE Trans.* 7, 455–464.
7) Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., and Baik, S. (2015). A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. *Multimed. Tools Appl.* 1–27.

О НЕКОТОРЫХ ПРОБЛЕМАХ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ

Забияко Д.
Студент SI-141
Academia de Studii Economice a Moldovei
Научный руководитель Згуряну А.

Nowadays, every company uses web applications in different forms, which help companies to develop their businesses. Vulnerabilities of these web applications can lead to serious problems. So every employer should take care of security of web applications, which are used in his business.
***Keywords**: testing, intruders, web application, breaking.*

Веб-приложение - это любое приложение, которое использует веб-браузер, как клиент. Это может быть простым форумом или сложной электронной таблицей. Веб-приложение - это наиболее широко используемый тип приложения в любой организации. Они являются стандартом для большинства приложений, которые взаимодействуют с интернетом. Если вы смотрите на планшет или смартфон, то можно обнаружить, что большинство приложений также являются веб-приложениями. Это создало большую аудиторию для тестеров, так и для хакеров, которые взламывают системы.

Сегодня веб-приложения получают все большую и большую популярность. eBay позволяет продавать и покупать все что угодно, предоставляя торговую площадку в сети, YouTube дает возможность загружать и показывать пользователям Интернета различные видеоролики. Gmail предлагает функционал, едва ли не превосходящий функционал традиционных почтовых клиентов.

Таким образом, веб-приложения сегодня прочно вошли в нашу жизнь, и многими из них мы пользуемся даже, не задумываясь – тем же поиском Google или почтовым сервисом Gmail. Инновации в технологиях навсегда изменили способ ведения бизнеса. Сегодня, веб-приложение – это не только "визитная карточка", а логическое продолжение бренда, которое может решить множество бизнес-процессов, привлекать новых клиентов и повышать прибыли. В мире существует огромное количество веб-приложений, но мало кто заботится о безопасности веб-приложений. С уверенностью можно сказать, что в каждом веб-приложении существуют уязвимости, каждая из которых может быть критичной.

Злоумышленники. Злоумышленников можно разделить на следующие типы:

Этичные хакеры (white hat). Занимаются исследованием систем на предмет безопасности.

Script kiddies – их характеристики (беспорядочные хаотичные действия, например сканирование системы, непродуманные действия, хулиганские действия - которые ведут к блокировке сайта).

Профессионалы - чётко знают чего они хотят, чётко знают как сломать систему, не будут делать хулиганских действий, стараются быть более незаметными, оставаться в тени, и будут стараться получить с ресурса то, за чем они пришли.

Боты – автоматические системы, которые созданы злоумышленниками для использования известных уязвимостей и реализации каких-то заранее определённых действий. В основном боты пытаются проанализировать систему жертвы на уязвимости.

У каждого злоумышленника есть свои причины для взлома веб-приложения. Например, если есть возможность заработать на ресурсе, то управлять системой они будут тихо и незаметно, и будут стараться сохранить контроль как можно больше. Могут так же ради интереса проникнуть в систему или же использовать ресурс для атаки на другие системы.

Причины взлома. Большинство начинающих хакеров и антихакеров задаются вопросом: «А для чего же нужно взламывать веб-сайты?». Этот вопрос возникает просто из-за недопонимания устройства сайтов. Многие наивно полагают, что, взломав сайт, можно найти лишь веб-странички и больше ничего интересного. Однако веб-сайты работают не только с веб-страницами, но зачастую и с базами данных. Например, сайт электронного магазина может взаимодействовать с базой данных, в которой содержится огромное количество номеров кредиток, а сайт, который предоставляет услуги электронной почты, — с базой, содержащей логины и пароли пользователей. Веб-сайты размещаются на сервере, поэтому, взломав сайт, хакер может получить доступ к командной строке этого сервера, и довольно часто это заканчивается получением прав суперпользователя (то есть полным контролем над сервером) [3].

Само проникновение через веб-сайт можно осуществить без особых проблем, так как чаще всего сайты общедоступны. Следовательно, взломщик, получив контроль над веб-сайтом, сможет через него проводить различные действия с атакуемым компьютером.

Существуют множество людей, которые получают прибыль от взлома, но этих людей можно поделить на две категории. Первая категория – это этичные хакеры (white hat), а вторая категория - это злоумышленники (black hat). Исходя из этой классификации можно способы заработка на взломах существенно различаются [4].

Для этичных хакеров различаются следующие способы взлома:

- Исследования в области ИБ - поиск уязвимостей, исследование продуктов, изучение работы вредоносного ПО.
- Участие в reward-программах, bounty hunting.
- Проведение аудитов, проведение тестирования на проникновения, проведение консультаций в рамках определённой компании.

Если говорить о второй категории, то у них возможностей заработка на взломах больше:

- Исследования в области ИБ.

- Reward-программы, bounty-hunting.
- Разработка и продажа эксплойтов.
- Продажа аккаунтов.
- Ботнет.
- Инфрейм-траффик - траффик на систему партнёрской программы, которая предназначена для рекламы. Эти системы обычно предлагают услуги сомнительного характера и платят злоумышленникам, чтобы они направляли на них траффик. Злоумышленник может направить траффик при помощи создания своего сайта, раскручивая его, делая его популярным и размещением баннера этой партнёрской программы. С другой стороны, злоумышленник может взломать сайт и разместить там инфрейм. С появлением социальных сетей, появилась возможность проведения социального спама.
- Кардинг - работа с кредитными картами (перехват кредитных карт пользователей и попытка их реализации например в интернет-магазинах). В основном злоумышленнику нужен номер кредитной карты, защитный код и имя, фамилия на кого зарегистрирована карточка и дата эксплуатации. Далее он берёт эти данные и использует для покупки чего-нибудь и потом как-то выводит эти деньги, либо через покупку или напрямую переводя финансы на другие депозиты или карты. Это одна из самых популярных схем, которая может обеспечить заработок злоумышленнику.
- «Конкурентная разведка».
- Кража виртуальных артефактов – «донат» в играх. В основном это взлом игровых аккаунтов, с целью продажи артефактов из игры. Если артефакт достаточно редкий, то можно получить довольно небольшую сумму. Или как вариант он взламывает игру, создаёт свой артефакт и потом продаёт его за большие деньги.

Тесты на проникновение - это поиск и оценивание уязвимостей, чтобы проверить реальна ли эта уязвимость или нет. Например, проводя аудит можно использовать сканнеры, которые найдут несколько сотен возможных уязвимостей в разных системах. А в своё время, проводя тесты на проникновение, нужно попробовать атаковать эти уязвимости, как это сделал бы злоумышленник, чтобы посмотреть какие из этих уязвимостей правдивы, с целью уменьшить этот список [2]. Целенаправленное нападение на систему показывает больше о системе безопасности, чем простое сканирование уязвимостей. Хороший тестер на проникновение может определить всю инфраструктуру безопасности и связанные риски с этой жертвой. Тестирование на проникновение оценивает эффективность существующей безопасности. Если у клиента нет сильной системы безопасности, то он получит мало пользы от услуг на проникновение.

Методологии тестирования. Наиболее распространённая классификация тестирования - это Black Box тестирование, White Box тестирование, Grey Box тестирование (которое является комбинацией первых двух) [1].

Black Box - подразумевает собой ситуацию, когда у тестера нет достаточно знаний о цели. Эта методология требует большого количества разведки и как правило занимает больше времени. Это означает, что у взломщика потребуется много времени для того чтобы осуществить атаку. Клиенты не готовы, в большинстве случаев, заплатить за неограниченное время разведки, однако если не провести достаточно времени на разведку, то тест на проникновение провалится не успев начаться.

White Box- это тот случай, когда у тестера есть достаточно знаний о системе. Цели тестирования явно определены и ожидается отчёт о проделанной работе. Тестеру предоставляется информация о цели: сетевая информация, типы систем, бизнес процессы компании и услуги. White Box может уменьшить ресурсы на сбор информации, на разведку и стоит меньше, чем Black Box.

Grey Box- это среднее между White Box и Black Box. Это такая ситуация, когда владелец соглашается, что некоторая секретная информация в конечном счёте будет известна в фазе разведки. Тестер снабжён основной подробной информацией о цели, однако внутренние работы и некоторая другая секретная информация всё ещё сохранены от тестера. Настоящие нападающие склонны иметь информацию о цели до нападения. Большинство нападающих (за исключением script kiddies) не выбирают случайных целей. Они мотивированы и обычно взаимодействовали с целью до нападения. Grey Box - привлекательный подход для многих тестеров, потому что это похоже на реальные подходы, которые используют нападающие и фокусируются на слабые места, а не на разведку.

Выводы

Современный мир несет в себе тысячи угроз и потенциальных опасностей буквально на каждом шагу и в каждый момент времени. Всемирная сеть, ставшая неотъемлемой частью нашей жизни, не является исключением. Киберпреступность сейчас развита как никогда – ведь почти каждая компания имеет свой сайт в интернете, а злоумышленник в сети может легко оставаться анонимным. При этом все компании, имеющие сайт в интернете, делятся на три типа:

- Те, чей сайт уже сломали.
- Те, чей сайт еще не ломали.
- Те, кто знаком с основными векторами атак и защитил приложения.

Количество угроз растет пропорционально росту бизнеса, однако как показала многолетняя практика, 99% атак происходят через десяток стандартных ошибок валидации входящих данных, либо обнаруженные уязвимости в установленных компонентах программного обеспечения сторонних производителей, либо банально, по халатности системных администраторов, использующих настройки и пароли, установленные по умолчанию. Поэтому следует, заботится о безопасности веб-приложений, так как последствия могут быть критичными, вплоть до разрушения бизнеса.

Список источников

1. Joseph Muniz, Aamir Lakhani, “Web Penetration Testing with Kali Linux”, Packt Publishing Ltd., 2013.
2. Georgia Weidman, “Penetration Testing”, no starch press, 2014.
3. Kimberly Graves, “Certified Ethical Hacker Study Guide”, Sybex, 2010
4. David Kennedy, Jim O’Gorman, Devon Kearns, “Metasploit, The Penetration Tester’s Guide”, no starch press, 2011.

INFORMATIONAL THREATS OF THE FINANCIAL SECURITY OF THE STATE AND THE STEPS OF THE EUROPEAN UNION ON COMBATING IT

Nataliia Zachosova
Cherkasy National University named after Bogdan Khmelnytsky

Abstract. *The possibility of damage to financial security of the country through the implementation of information threats has been determined. EU measures concerning counteraction to cybercrime are considered. Cases of influence of information threats on the state of financial security of Ukraine are mentioned.*

The consequences of the implementation of information threats in recent years were most noticeable in the financial system of the state, and had a negative impact on the level of financial security of many countries. Financial globalization has led to the fact that interference with the functioning of elements of the financial architecture of one state, leads to violations of financial mechanisms of other participants in the world financial space. Distortion of information flows, violation of the quality of information resources, unauthorized access to data and interference with the mechanism of work of information channels paralyze or ineffective the work of economic structures and authorities and cause great damage, which affects the financial and, consequently, national security of the country. The awareness of this fact by the European community was the beginning of the development of information and analytical security of members of the Union.

The European Security Strategy was adopted in December 2003 and marked a milestone on the path to the development of EU security policy. Modern economies rely heavily on critical infrastructure, including transport, communications, energy supplies, and, moreover, the Internet. The European Strategy for a Secure Information Society, adopted in 2006, was aimed at combating Internet crime. However, separate actions against private and state-owned IT systems in the EU member states brought a new tint to the problem, demonstrating that Internet crime has become a potential new economic, political and military weapon [1].

More often than not, the purpose of attacks on the information segment of the security system at both the micro and macro levels is to cause damage to the object of attack or to receive profit. Even without having such a goal during implementation, information threats always have a negative financial effect. In order to violate the state of financial security of the state, objects of information attacks can be four main types of targets: financial institutions, financial regulators, software developers for financial traders and those whose business is related to crypto currency.

In June 2016, hackers entered several Ukrainian financial institutions, from one of which they stole $ 10 million through the SWIFT system. At the end of 2016, hacking attacks blocked the work of the sites of the Ministry of Finance and the State Treasury

Service in order to hurt the planned progress of the budget process, which substantially weakened the state of budgetary security. Subsequently, an attack on the Pension Fund website was launched.

Such cases have ceased to be a rarity in the states of Europe. In 2016, the European Central Bank announced its intention to create a database for recording cases of cybercrime in commercial banks in the euro area. However, the constant and open exchange of information between the country's leadership in regard to cyber incidents is still an odd prospect, since recognizing the success of cyberattacks is still the recognition of the inability to organize a highly effective security system at the state level.

On June 27, 2017, at 11.00, a massive cyberattack was launched against Ukraine, using the version of the "wannacry" virus - "cryptolocker" modified for Ukraine. The virus simultaneously captured banks, post offices, train stations, energy companies, state-owned Internet resources and local networks, as well as a number of media. Nothing revolutionary - an ordinary computer pest infects thousands of servers and blocked the work of the financial system of the country. Private companies are beginning to function normally the next day, however, the process of filing tax reporting that poses a threat to tax security has been violated. State enterprises, authorities for three days were trying to recover lost information. Cybersecurity experts estimated that losses for the country's financial security system were at least UAH 10 billion.

Thus, the events of 2017 became a catalyst for the emergence of a new term - cyber hygiene. In order not to encounter a virus in cyberspace, one must adhere to the elementary rules of information security [2].

What information threats are waiting for participants in the financial market in 2018? According to analytical studies, 92.6% of Ukrainian companies are already faced with a leakage of information. In Europe and the US, the situation is also not quite optimistic: around 90% of organizations lost important information over the past 12 months.

Gartner company says that worldwide security costs for information security will reach $ 86.4 billion by the end of 2017, while the cybercrime report said that the damage would cost the world 6 trillion dollars a year by 2021.

According to the Accenture Security report, the most noticeable threats to information security faced by financial sector companies in 2017 were:

- Reverse Deception Tactics - tools such as code that prevents malware from being analyzed, steganography (sending information in encrypted form with the secret of the transfer), and botnets, as well as control and monitoring servers used for concealing stolen data.
- Sophisticated fishing campaigns. Fishing messages often used to deliver malware are becoming increasingly complex, with specific company information, such as invoicing, etc.
- Cyberattacks and cybercrime are tools that are increasingly used by states and other actors to achieve economic and political goals.

- Alternative cryptographic - the popularity of bitcoins makes cybercriminals improve money laundering techniques or even use different crypto-converters [3].

As a response to current information threats, a framework document with a list of diplomatic responses to cybercrime actions will soon be set up in Brussels. It is also proposed to create a cybernetic force for the rapid reaction in the European Union. In the framework of the European Commission's project called Horizon 2020, € 450 million will be earmarked for cyber security this year. The total investment in the industry is expected to reach € 1.8 billion by 2020. Now, in 2018, the European Commission's initiatives are aimed primarily at protecting against cyberattacks and increasing the competitiveness of the IT security sector [4].

Thus, in order to stabilize the state of financial security by timely counteracting information threats, Ukraine should be involved in European cybercrime protection practices, develop adequate documentary supply of information security and oblige professional financial institutions to create or upgrade information security departments in accordance with existing threats of the present day.

References:

1. Украину ждут масштабные кибератаки: как уберечь компании и гаджеты *[Large-scale cyberattacks are waiting for Ukraine: how to save companies and gadgets]* [Электронный ресурс]. – Режим доступа: https://ru.tsn.ua/nauka_it/ukrainu-zhdut-masshtabnye-kiberataki-kak-uberech-kompanii-i-gadzhety-1078085.html.
2. Исследование: угрозы информационной безопасности. Часть 2: тренды и прогнозы 2018 *[Investigation: threats to information security. Part 2: Trends and Forecasts 2018]* [Электронный ресурс]. – Режим доступа: https://stakhanovets.ru/blog/issledovanie-ugrozy-informacionnoj-bezopasnosti-chast-2-trendy-i-prognozy-2018/.
3. Кибератаки прошлого и будущего: чего ждать в 2018-м? *[Cyber Attacks of the Past and the Future: What to Expect in 2018?]* [Электронный ресурс]. – Режим доступа : https://delo.ua/special/kiberataki-proshlogo-i-buduschego-chego-zhdat-v-2018-m-339201/.
4. Европейская стратегия безопасности. Безопасная Европа в лучшем мире *[European Security Strategy. Safe Europe is in the best world]* [Электронный ресурс]. – Режим доступа : https://www.consilium.europa.eu/media/30825/qc7809568ruc.pdf.

RANSOMWARE – A GROWING THREAT TO THE INFORMATION SECURITY OF BUSINESS ORGANIZATIONS

Asen Bozhikov,
D. A. Tsenov Academy of Economics, Svishtov, Bulgaria
a.bozhikov@uni-svishtov.bg

Abstract: *The rapid evolution of information technologies unlocks new opportunities for business organizations to achieve competitive advantages and economies of scale. But at the same time that technological advancement is used by the cybercrime to develop new attack types. The present paper gives a brief overview of the ransomware and the reasons behind its massive adoption by the cybercriminals.*

Ransomware became one of the key cyber threats targeting business organizations. It uses different vectors to disseminate and attacks data availability. The McAfee CEO, Christopher D. Young, recently told that ransomware is today's modern-day extortion, and it's something that criminals are going to continue to drive because they can make money of it.

Ransomware is a piece of sophisticated malicious software that is used to digitally extort the victims to pay a specific amount of money, usually in cryptocurrency, so that they regain access to their devices or files. We use the term device because ransomware targets not only computers (with Windows, Linux, Mac OS) but also mobile devices (with Android, iOS), IoT devices and even industrial control systems. There are two main types of ransomware [12]:

- *Locker ransomware* –locks the victim's device and use a pop-up or browser window to show the ransom message. As the name imply the device is unusable until the ransom is paid.
- *Crypto ransomware* – use encryption to encrypt the victim's files on the device and then shows a pop-up or browser window to display the ransom message. In this case the device itself can be used, only the victim's files are encrypted.

The idea behind the ransomware is not a new one. It dates back to 1989 when the AIDS Trojan (PC Cyborg) was created and propagated on a 5,25'' floppy disk to 20 000 people [8]. In 1996 Young and Yung proposed a method for using public key cryptography in ransomware and in a later publication they indicate that combining strong cryptographic algorithms and malware will pose a new threat for the security of the information systems [13, 14].

It wasn't until 2014 when cybercriminals started to use crypto ransomware as a main malware tool for cyber extortion. Since then every year there is a rise in the number of ransomware attacks. Hampton et al. in their study of the evolution of malware over a period of 26 years state that to be a successful, ransomware needs to align three core technologies:

strong, reversible encryption; a system to anonymously communicate keys and decryption tools; untraceable way of payment [3]. The first ransomware which combined these three characteristics appeared in the middle of 2014 – CTB-Locker. CTB states for Curve (using Elliptic-curve cryptography), TOR (using The Onion Router as an anonymous communication channel) and Bitcoin (using cryptocurrency as a payment method).

In 2016 the number of attacks grew 167 times compared to 2015, from 4 million to 638 million [9]. 2017 unveiled another concerning statistic as Malwarebytes products indicated that consumer and business ransomware detections have increased 90% and 93% respectively [6]. In addition to that statement a research conducted by the security company Carbon Black found that from 2016 to 2017, there has been a 2502% increase in the sale of ransomware on the dark web [1].

There are some notable examples of companies that have been infected with ransomware and paid the demanded ransom - web hosting company Nayana ($1 million), University of Calgary ($20 000) and Hollywood Presbyterian Medical Center ($17 000). In 2017 the infamous WannaCry ransomware infected many high-profile business organizations as most notable of them were: UK National Health Service, Spanish telephone giant Telephonica, French automobile giant Renault, German train operator Deutsche Bahn and logistic company Fed-Ex [4].

As we can see the target of the ransomware attacks is not a single industry. A research by security company Sophos shows that the most attacked sector is Healthcare, followed by Energy and utilities, Business and professional services and Retail and distribution [10]. The impact of the ransomware attacks for the business organizations could be summarized in a three points: financial losses, damaged reputation and disruption of operations.

The reasons behind the massive growth of ransomware attacks could be defined in the following directions:

- *Increased availability of strong cryptography;*
- *Increased reliance on the IT and Internet connectivity for everyday business operations;*
- *Rise of the Bring Your Own Device workplace;*
- *Emergence of Ransomware as a service (RaaS);*
- *Cryptocurrencies as a ransom payment method.*

Cybercriminals adopted the subscription based model which is used by businesses to get the necessary resources on demand (as a service) and started to use it for their evil purposes. The birth of the ransomware as a service is one of the main factors for the rapid spread of this type of malware. RaaS is a way for criminals without the adequate technical competency and knowledge to organize massive ransomware campaigns thus making money from extorting companies or individuals. There are different RaaS models but the most common of them relies on the proven affiliate model in the business. There is a supervisor, usually the creator of the ransomware, and affiliates that get access to a copy of that malware or a command interface with many customization options, which they could

use to infect multiple targets. When an infected victim pays the ransom, part of the sum, which is between 5% and 40% is going to the supervisor as a commission and the rest is for the affiliate [5]. Examples of widely distributed ransomware packages through RaaS are Cerber, Satan, Atom and MacRansom. Modern RaaS offers a thorough user guide how to launch a successful ransomware campaign, sometimes live chat support and is advertised not only on the forums in the dark web but also on the sites for video sharing like YouTube.

2017 was a year in which the cryptocurrency market saw a big movement upward. Cryptocurrencies are the primary mean of payment for getting the key to decrypt infected files, which the ransomware encrypted. Bitcoin is the most famous cryptocurrency and it has become the de facto standard for currency used as a mean of payment for the ransom. Bitcoin allows the ransom money to move to the cybercriminals without identifying their bank account, although that system is not perfectly anonymous [7]. To make it really hard for the law enforcement to trace the money cybercriminals use additional laundering services or transfer the money in other cryptocurrencies. In 2018 security experts expect a shift in the main currency for ransomware because of the high volatility of Bitcoin and the loss of anonymity it affords [15]. The possible variants for replacement are: Monero, Dash or Z-Cash.

Another important factor for the rising trend of ransomware cyberattacks is the increasing number of the Internet of Things (IoT) devices that are used worldwide. Usually their security is at poor level and that was proofed by the Mirai botnet network which included more than 600 000 infected IoT devices like home routers, air-quality monitors and personal surveillance cameras [2]. With this in mind we could expect that smart devices would be used not only for a denial of service attacks but also they would be point of infection with ransomware in the next few years. According to IBM Security's vice president of threat intelligence Caleb Barlow, large business organizations with deployments of IoT security cameras, digital video recorders, and sensors will be especially impacted by ransomware [11].

We could summarize than ransomware is not a new cyber threat as it exists on the scene for more than 25 years but last two years it become a main method for cyber extortion of individuals and businesses of all types and industries. Experts' expectations unanimously suggest that ransomware attacks will continue, targeting even more devices, searching for specific file types to encrypt and trying to exfiltrate the data before the encryption process starts. To be prepared for that new wave of ransomware business organizations need a proactive security approach, proper backup policy and regular employees' training about the cyber threats.

References

1. Carbon Black. The Ransomware Economy (2017). Available [Online] https://cdn.www.carbonblack.com/wp-content/uploads/2017/10/Carbon-Black-Ransomware-Economy-Report-101117.pdf [Accessed 1st March, 2018]
2. CloudFlare. Inside the infamous Mirai IoT Botnet: A Retrospective Analysis (2017). Available [Online] https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/ [Accessed 1st March, 2018]

3. Hampton, M. Ransomware: Emergence of the cyber-extortion menace. Proceedings of 13th Australian Information Security Management Conference, pp. 47-56, 2015
4. International Business Times. WannaCry: List of major companies and networks hit by ransomware around the globe (2017). Available [Online] http://www.ibtimes.co.uk/wannacry-list-major-companies-networks-hit-by-deadly-ransomware-around-globe-1621587 [Accessed 1st March, 2018]
5. Liska, A & Gallo, T. Ransomware: Defending Against Digital Extortion. O'Reilly, 2017
6. Malwarebytes Labs. Cybercrime tactics and techniques: 2017 state of malware (2017). Available [Online] https://www.malwarebytes.com/pdf/white-papers/CTNT-Q4-17.pdf [Accessed 1st March, 2018]
7. Orman, H. Evil Offspring-Ransomware and Crypto Technology. IEEE Internet Computing 20, no. 5 (2016), pp.89-94
8. Pope, J. Ransomware: Minimizing the risk, Innovation in Clinical Neuroscience, 2016, vol. 13(11–12), pp. 37–40
9. SonicWall. 2017 SonicWall Annual Threat Report (2017). Available [Online] https://www.sonicwall.com/en-us/resources/white-papers/2017-sonicwall-annual-threat-report [Accessed 1st March, 2018]
10. Sophos. The State of Endpoint Security Today (2017). Available [Online] https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/endpoint-survey-report.pdf?la=en [Accessed 1st March, 2018]
11. TechRepublic. Ransomware attacks will target more IoT devices in 2018 (2018). Available [Online] https://www.techrepublic.com/article/ransomware-attacks-will-target-more-iot-devices-in-2018/ [Accessed 1st March, 2018]
12. Thakkar, D. Preventing Digital Extortion, Packt Publishing, Birmingham,2017
13. Young, A. & Yung, M. Cryptovirology: Extortion-Based Security Threats and Countermeasures, Proc. IEEE Symp. Security and Privacy, 1996, pp. 129–140.
14. Young, A. & Yung, M. Malicious Cryptography: Exposing Cryptovirology, 2004, pp. 416, Wiley Publication.
15. ZDNet. Ransomware: Why the crooks are ditching bitcoin and where they are going next (2018). Available [Online] http://www.zdnet.com/article/ransomware-why-the-crooks-are-ditching-bitcoin-and-where-they-are-going-next/ [Accessed 1st March, 2018]

THE MODEL OF BOTNET PROFITABILITY

Borta Grigorii,
PhD student, ASEM

In the modern times, the goals of the malefactors moved from dealing direct damage and self-affirmation towards maximizing their income and profit. Thus, in order to be able to counteract their actions in an efficient manner an economic approach is required. The approach should be based on analyzing the sources of their income and creation of conditions that would be unfavorable enough to reduce all possible incomes to zero. If an opportunity of profiteering in the domain of shadow information economics is open, there will always be people willing to use it.

Bot-master aims to increase their income by means of infecting as many devices as possible using as few resources as possible. The used resources include but are not limited to Pay-per-Install services, control channels. The malefactor will be able to either rent the botnet or use its computing power and networking capabilities to their own gain.

The following model is proposed:

From the bot-master perspective:

$$y_1 = P * b - k - a(B) - i(B) \quad (1)$$

From the renter perspective:

$$y_2 = M(b) - O - P * b \quad (2)$$

Where:

- P – the cost of renting an infected computer;
- b – the number of rented infected machines;
- k – payment for command and control channels, schematically represented on figure 1.

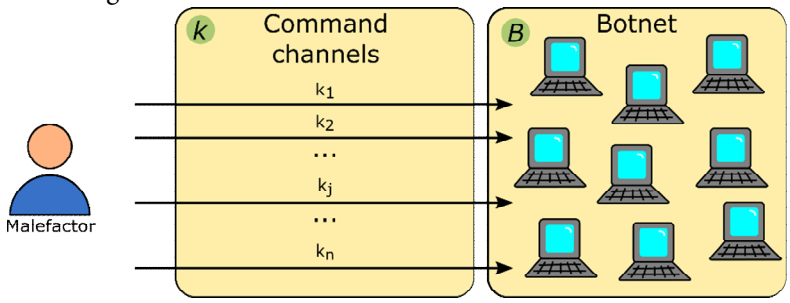


Figure 1. **Command and control channels used by the malefactor.**

- B – botnet size;
- a(B) – penalty function, damage suffered by the malefactor in case of botnet being seized;
- i(B) – cost of infecting computers;
- M(b) – total income of the renter for the time of botnet rent;
- O – cost of infrastructure upkeep by the renter.

All the above mentioned parameters are represented on figure 2.

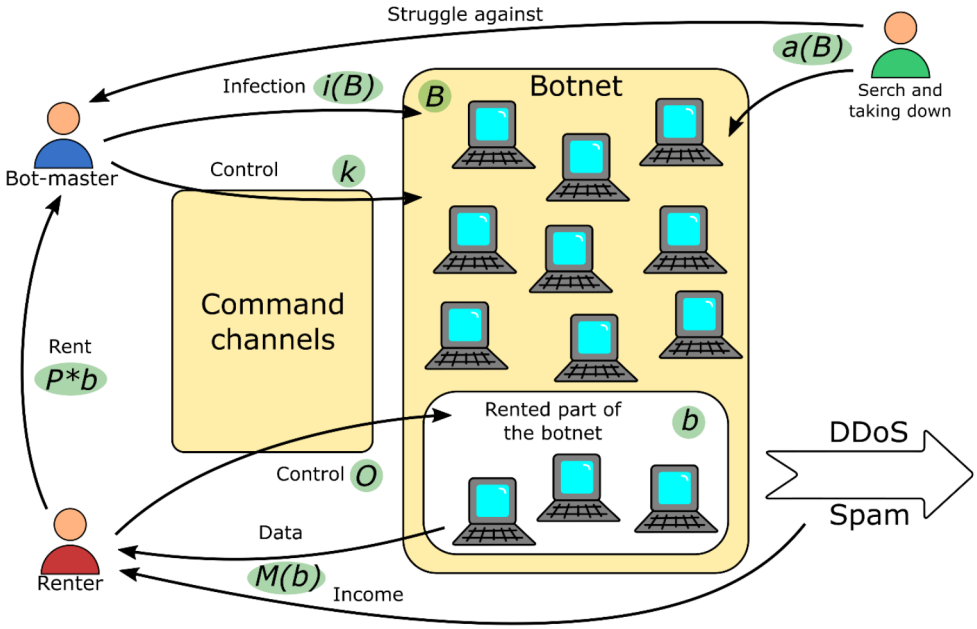


***Figure 2.* Botnet profitability model representation.**

Thus, the proposed model allows for the following possible vectors of botnet profitability counteraction:

1. Maximization of penalty function a(B) by means of legal actions, law enforcement, etc.;
2. Maximization of infection cost, i(B);
3. Minimizing the effectiveness of renting infected zombie devices;
4. Developing technical and technological hindrances on the way of botnet creation;
5. Creating hindrance on the way of communication between possible service renters and bot-masters.

Bibliography

1. **Li Z., Liao Q., Blaich A., Striegel A.** Fighting botnets with economic uncertainty. Albion College, University of Notre Dame, 15 07 2010 r., http://onlinelibrary.wiley.com/doi/10.1002/sec.235/abstract.
2. **Li Z., Liao Q., Striegel A.** Botnet Economics: Uncertainty Matters. Albion College, University of Notre Dame, 22 12 2008 r., http://www.econinfosec.org/archive/weis2008/papers/Liao.pdf.

PRIORITATILE UNEI ECONOMII DIGITALE PENTRU REPUBLICA MOLDOVA REIESIND DIN EXPERIENTA ECONOMIEI DIGITALE ROMANESTI ?

Ghenadie Ciobanu
Institutul National de cercetare ştiinţifică în domeniul muncii şi protecţiei sociale , Bucureşti

Economia digitală se caracterizează prin următoarele trăsături caracteristice:

Infrastructura economiei digitale. TIC a crescut rapid în ultima perioadă atât în economie cât şi în societate în general.

Pieţele electronice. Principalele trăsături ale pieţelor electronice sunt: noi agenţi, noi tipuri de produse şi servicii, noi relaţii de afaceri, noi modele de comunicaţie şi organizare.

Produse bazate pe informaţii şi cunoştinţe. Cele mai multe produse existente pe pieţele electronice sunt produsele intangibile.

Agenţii prezenţi pe pieţe: consumatori, oameni de afaceri, intermediari. În economia digitală consumatorii beneficiază de informaţie 24 de ore din 24, au acces la informaţie pe piaţă indiferent de distanţă.

Transformări macroeconomice şi procese de globalizare. Din punct de vedere macroeconomic schimbările apărute în economie afectează variabilele macroeconomice. Internetul înlătură graniţele fizice favorizând evoluţia procesului de globalizare.

Penetrarea progresivă şi agresivă a economiei digitale în viaţa economico-socială a societăţii moderne din secolul XXI.

Noţiunea de economie digitală nu implică în nici un caz o alternativă sau un substitut al economiei clasice.

Astfel încât Uniunea Europeană să dezvolte o economie inteligentă, durabilă şi favorabilă incluziunii.

Primul şi probabil cel mai important obiectiv dintr-un set de cinci strategii socio-economice majore constă în creşterea ratei de ocupare a forţei de muncă la 75% în rândul populaţiei cu vârste cuprinse între 20 şi 64 de ani.

Al doilea obiectiv - provocări comune la nivel internaţional induse de criza economică şi financiară prelungită.

Al treilea obiectiv - evoluţii şi structuri pe piaţa muncii la nivelul U.E. 28, zonei Euro şi României, în corelaţie cu cerinţele flexicurităţii pieţei muncii şi implicaţiile crizei economice

Al patrulea obiectiv - paradoxul crizei de personal de valoare şi mare talent într-o lume sufocată de lipsa acută de locuri de muncă

Al cincilea obiectiv - arta managementului resurselor umane-probabil cel mai puternic factor responsabil de creşterea şi productivitatea companiilor în viitorul apropiat

Al şaselea obiectiv - penetrarea progresivă şi agresivă a economiei digitale în viaţa economico-socială a societăţii moderne din secolul XXI.

Al şaptelea obiectiv - deziderat major al economiei digitale în perspectiva viitorului imediat al României: guvernarea electronică.

Activitatea digitală în contextul strategiei 2020

În conformitate cu documentul fundamental în acest domeniu "Strategia 2020", lansat la 3 martie 2010 de Comisia Europeană cu titlul Europa 2020 – O strategie europeană pentru creştere inteligentă, durabilă şi favorabilă incluziunii, scopul general al strategiei este de a ghida economia UE în următorul deceniu, prin abordarea tematică unitară a reformelor în plan economic şi social, concentrate pe cele trei priorităţi ale strategiei Europa 2020 care definesc viziunea UE asupra economiei sociale de piaţă

Comerțul electronic efectuat de către mediul de afaceri, în 2013 doar 9% dintre IMM-urile din România au vândut bunuri şi servicii online, iar întreprinderile mari au atins un procent de 13% pentru acelaşi an.

Conform Raportului concurentei pe anul 2017 rezultatele finale ale anchetei sectoriale evidentiaza tendintele pietei (1) În ultimii zece ani , mulți producători au decis să își vândă produsele prin magazinele online proprii, intrand în concurență cu distribuitorii proprii. (2) Utilizarea tot mai largă a restricțiilor contractule, prin care producătorii încearcă să-şi sporească controlul asupra distribuției.

Conform Raportului pentru anul 2017 , rezultatele preliminare ale analiyei sectoriale a CC indică faptul că sectorul comerţului electronic prezintă caracteristicile unei piețe de tip oligopol, fiind alcătuită dintr+un nucleu al jucătorilor relevanți, şi o categorie a comercianţilor ce dețin cote de piață nesemnificativă.

Conform GPeC , doar de Black Fridaz 2016, românii au cumpărat produse în valoare de circa 130 mil. euro (ce reprezintă peste 7 % din valoarea întregului segment de comerț electronic din 2016) , fiind în crestere fata de anii anteriori.

Tabel 1

	2012	2013	2014	2015	2016
Evoluția Comerțului online	0,6 mld. Euro	0,6 mld. Euro	1,1 mld. Euro	1,4 mld. Euro	1,8 ml. Euro
Vanyari online			75 mil. euro	1,4 mld. Euro	1,8 mld. Euro

Sursa: Raportului Evoluția concurenței în sectoarele cheie 2017

Momente importante sunt:

1. **Creşterea nivelului de informare al furnizorilor de servicii online şi al utilizatorilor de e-comerț.** O barieră importantă în fața dezvoltării e-comerțului o constituie absența informației la nivelul operatorilor de servicii online şi de internet.
2. **Capacitatea de cunoaştere şi inovare a regiunilor depinde de mulți factori** - cultură antreprenorială, competențele forței de muncă, instituțiile de educație

şi de formare, serviciile pentru susținerea inovației, mecanismele de transfer tehnologic, infrastructura pentru inovația în TIC, mobilitatea cercetătorilor, incubatoarele de afaceri, noile surse de finanțare şi potențialul creator local.

În conformitate cu lucrarea „Accesul populației la tehnologia informațiilor şi comunicațiilor[1]" lucrări elaborate anual de INS în anii 2010-2014 Studiul prezintă informații privind accesul populației la diferite tehnologii de comunicație (calculatoare personale, telefoane mobile, şi accesul la internet. Se urmăreşte evidențierea frecvenței şi scopurilor utilizării tehnologiei informaționale, locul desfăşurării, utilizarea computerului şi a internetului de acasă).

Am considerat că nu doar datele statistice şi informațiile statistice oficiale sau preluate din diverse alte surse pot folosi argumentărilor noastre ci cu atât mai mult o anchetă realizată cât mai recent va fi utilă studiului nostru.

În activitatea curentă 7 din 10 firme care utilizează computerul şi au conexiune la internet au şi o pagină web/de internet, iar cele mai multe dintre acestea între 66%-80% oferă pe pagina web *„datele de contact ale companiei"*, *„conținut media"*, *„acces direct către pagina de pe rețele de socializare"* şi o pagină unde îşi prezintă produsele sau/şi serviciile. Datele arată, pe de altă parte, că mai sunt multe de făcut pentru a putea vorbi de digitalizare de înaltă performanță în companiile româneşti, atât timp cât numai 2 din 10 companii care au o *„pagină web au versiune optimizată pentru telefon mobil"* şi mai puțin de 4 din 10 „conexiune securizată".

Concluzia acestei anchete, în urma prelucrării răspunsurilor respondenților adică a reprezentanților (managerii companiilor) este aceea că orice tip de competențe digitale sunt utile şi necesare în orice domeniu de activitate. Dincolo de asta, există resurse nelimitate de dezvoltare a acestei piețe a muncii digitale, există oportunități de creştere a acestui segment în ocupare. Ocuparea în munca digitală poate fi foarte avantajoasă ,mai ales prin faptul că se poate adapta oricăror categorii de vârstă, mai tineri sau mai vârstnici, oricăror domenii dar chiar şi oricăror categorii adică şi celor cu dizabilități fizice.

Această deschidere spre orice persoană activă care poate învăța sau se poate instrui în munca digitală oferă şanse mai mari de a ocupa mai rapid un loc de muncă pe piața muncii. De asemenea, competențele digitale pot oferi o mobilitate şi posibilitatea de adaptabilitate de la un domeniu la altul sau pot oferi şanse de angajare mai bune şi mai mari. Digitalizarea muncii oferă perspective numeroase din toate punctele de vedere. **Sunt din ce în ce mai mulți cei care lucrează în munca digitală şi din ce în ce mai multe locuri de muncă se pot crea pe acest segment al muncii.**

Concluzii

- Structura pieței digitale , influențează comportamentul firmelor, care influențează performanța de piață.
- Firmele digitale se concurează în dezvoltarea unor noi modele de afaceri, limitele pieței relevante se modifică continuu sa sunt create noi piețe.

[1] Studiul privind Accesul populației la tehnologia informațiilor şi comunicațiilor,

- Abordarea prospectivă şi implicarea în interacțiuni regulate cu părțile interesate şi experții sectoriali , dar şi o sincroniyare

Bibliografie

1. Banca Mondială, Programul de Dezvoltare a Țării, p. 7; URL: http://siteresources.worldbank.org/ROMANIAEXTN/Resources/2751531253883114942/CPS0913_Country_Development_Program.pdf World Bank, The Country's Development Program
2. Strategia Națională privind Agenda Digitală pentru România Iulie 2014 The National Strategy for the Digital Agenda for Romania, July 2014
3. Agenda Digitală pentru Europa 2014 – 2020, http://europa.eu/ legislation_ summaries/ information_society/strategies/si0016_ro.htmThe Digital Agenda for Europe 2014-2020
4. "Competențe digitale pentru locuri de muncă în Europa" Măsurarea progresului şi avansarea, Comisia Europeană, 2014 Digital competences for work placed in Europe. "Measuring progress an d advancement, European Commission 2014
5. Report prepared by the research Directorate and approved in the

ОРГАНИЗАЦИОННО – ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ РАЗРАБОТКИ БЕЗОПАСНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА УЧЕБНОГО ЗАВЕДЕНИЯ

Герасимов Владимир Анатольевич, Славянский университет,
магистрант, 1 курс, специальность «Информатика»
lanceman_92@mail.ru

In work the main advantages of implementation of the adaptive platform of the information portal of the educational website, organizational security measures are investigated. Stages are described. Conclusions are formulated.

Вопросы репутации и безопасности электронного портала – понятия взаимосвязанные и интерес к ним возрастает по мере роста мировой киберпреступности. Это касается всех видов web- ресурсов, как связанных коммерческими обязательствами со своими пользователями, клиентами, посетителями, так и других категорий. Представленное исследование описывает практику разработки нового функционала и технологической платформы официального сайта учебного заведения. Отдельным блоком выделены предлагаемые и потенциальные рекомендации системы администрирования безопасности портала.

Целью работы является исследование современных адаптивных технологий и проектирование на этой основе безопасного электронного образовательного портала.

Практическая значимость самой темы обусловлена тем, что проведенное исследование позволило на практике обеспечить доступ к информационному пространству электронного портала Славянского университета с учётом индивидуальной программно – аппаратной оснащённости пользователя вне зависимости от ограничений мультимедийных данных (рисунки, таблицы, видео и др.)

Практическая значимость выполненной работы заключается в том, что разработанный проект фактически готов к эксплуатации и работает в настоящее время тестовом режиме по адресу: http://k95185st.beget.tech/ [1]. По мере наполнения контентом динамических станиц может быть использован как информационное поле для учебно – методической, научной и профориентационной работы Славянского университета в Республике Молдова.

При создании проекта электронного портала Славянского университета использовались следующие этапы:

- первый этап начался с постановки задачи. Прежде всего, был определен перечень задач, которые необходимо решить, подготовлены необходимые материалы, фото и видео информация. Данный этап занял от 10 до 15-ти дней;
- второй этап заключался в разработке и утверждении дизайна сайта а также разработке структуры сайта (меню) (Рис 1.). Для выполнения

этого этапа были определены цветовые предпочтения главной страницы, дизайна динамических страниц, кнопок, фона. Данный этап занял две-три недели.

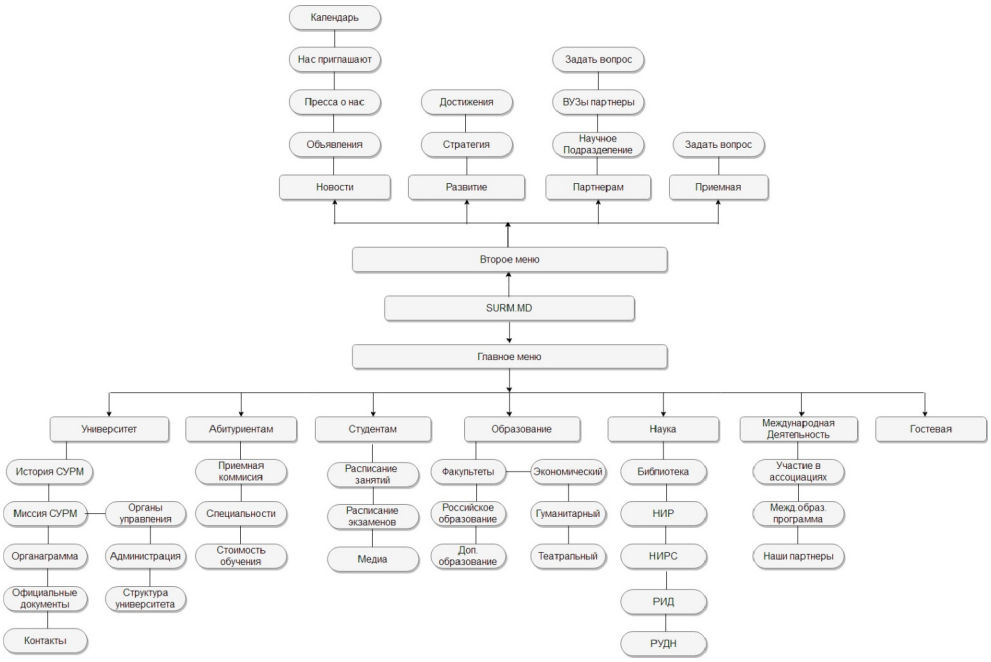


***Рис. 1.* Структура меню**

Источник: *разработка автора*

- на третьем этапе выполнена интеграция дизайна электронного портала с системой управления. Этапы создания веб портала не могут обойтись без данной процедуры, особенно, если основной целью создания портала будет продвижение образовательных услуг, в частности - Славянского университета в Республике Молдова и в Российском образовательном пространстве. На данный этап уходит примерно пять-шесть дней;
- четвертый этап – это процедура публикации портала в сети Интернет;
- пятый и шестой этапы создания веб портала – это процесс заполнения его необходимой информацией и дальнейшая его поддержка.
- Седьмой этап – анализ системы безопасности сайта и разработка мер по ее усилению. Работа в режиме постоянного обновления и поддержки.

Проект адаптивного портала Славянского университета разработан на системе управления Joomla! Версия 3.7. Joomla! - это система управления содержимым (CMS), которая создана для визуального управления контентом. Система проста и бесплатна в использовании, что и делает ее такой популярной и доступной. В настоящее время данная система является второй по популярности в мире, что делает ее одновременно и второй по наличию кибератак и уязвимости.

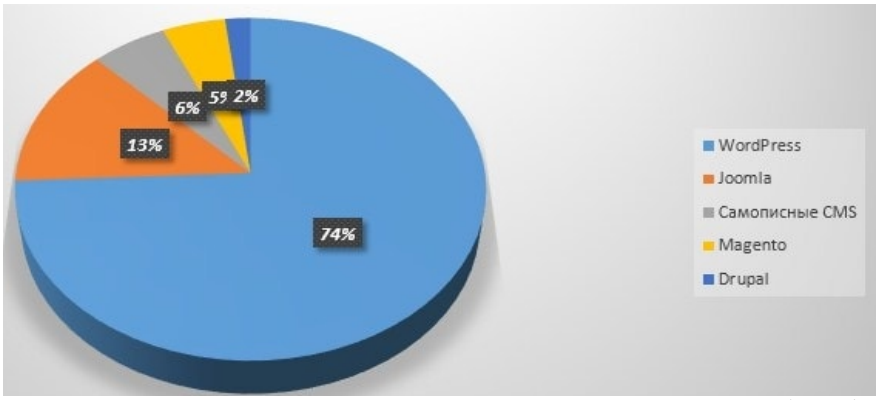


Рис. 2. **Статистика взломов сайтов на популярных платформах (CMS)**
Источник: https://www.site2b.com.ua/web-blog/zachem-nuzhna-povyshennaya-bezopasnost-sajta.html [2]

Согласно приведенным на рис.2 данным, сайты, разработанные на Joomla! входят в тройку наиболее подверженных взломам (13%) после WordPress (74%). Это связанно с тем, что данные системы доступны широкому кругу лиц для изучения их структуры и логики работы.

Необходимость перехода на новый портал обоснована тем, что имеющийся в настоящее время действующий сайт устарел как морально, так и физически, перегружен функциональными меню, информационно невразумителен, небезопасен в использовании, имеются проблемы с администрированием и доступом (просмотром) на современных устройствах (планшетах, смартфонах и др.) Сайт также был написан на Joomla! [3].

Выбор системы Joomla! версии 3.7. позволил реализовать при создании нового сайта СУРМ следующие преимущества:

1. Расширенный функционал, который увеличивается с использованием компонентов, плагинов. В сети интернет существует много платных и бесплатных расширений для Joomla посредством которых можно создать полноценный сайт или настоящий интернет - магазин с нуля.
2. Использованы средства безопасности для пользователей и администратора. Безопасность в Joomla совершенствуется с каждой версией. Следует понимать, что любой сайт можно взломать, от этого никто не застрахован, но разработчики Joomla 3 постарались максимально уменьшить уязвимость сайта и обеспечить максимальную безопасность от взлома.

В качестве средств безопасности предусмотрены:

3. Система шаблонов, которая позволяет достаточно просто менять внешний вид сайта. В Joomla предусмотрена система визуальных шаблонов.

При создании портала реализованы:

4. Позиции модулей. Посредством самих модулей и позиций для них, легко можно как в конструкторе создавать и менять расположение различных форм нашего сайта. Например, слева у нас находится форма авторизации

для пользователя, а нам нужно ее переместить в шапку сайта или на правую сторону: в админ панели Joomla это решается в два клика мышки.

5. Легкость в редактировании кода шаблона. Если нам необходимо изменить или отредактировать его, достаточно открыть Менеджер шаблонов и найти соответствующий файл для редактирования.

Использованы следующие возможности административной панели:

- Возможность установить начало и конец публикации определенной страницы по календарю и времени. Например, нам необходимо чтобы определенная статья опубликована была в заданное время, для этого просто в редакторе статьи настраиваем данную функцию.

Также можно поступить и с завершением публикации.

- Ограничение доступа к определенным разделам для незарегистрированных пользователей. Можно настроить, чтобы на конкретную статью или на все материалы был ограничен доступ для незарегистрированных пользователей, то есть для просмотра этой страницы им нужно будет пройти регистрацию.
- Установить и настроить мультиязычность. В Joomla предусмотрена система языков, посредством которых весь наш портал будет отображаться, например, как это сделано у нас: на русском, румынском и на английском языке.
- Удобство в настройке блога. С ее помощью можно просто и без проблем настроить вывод материалов в виде блога.
- Удобство в установке модулей и компонентов. Установка полезных расширений происходит в два клика, нужно просто выбрать архив и нажать кнопку установить.

В качестве примеров установленных компонентов предложены:

- Установка ЧПУ (человеко-понятных урлов) например site.com/novosti. Это полезная функция, так как ЧПУ урлы играют значительную роль в продвижении нашего портала.
- Создание форм обратной связи. Как правило, такая форма создается на странице контактов, чтобы любой пользователь мог написать сообщение администратору.

Основными составляющими Joomla является ядро и система шаблонов, компонентов, модулей и плагинов. Ниже представлены некоторые примеры их реализации.

1.Шаблон. Это оболочка сайта, видимая ее часть, которая легко настраивается в админ-панели и имеет достаточно много настроек. С помощью их, мы легко настраиваем работу портала.

- Шапка сайта, в левом углу расположен логотип университета, адрес, где расположен университет, меню с переходами на другие страницы, а также слайдер.

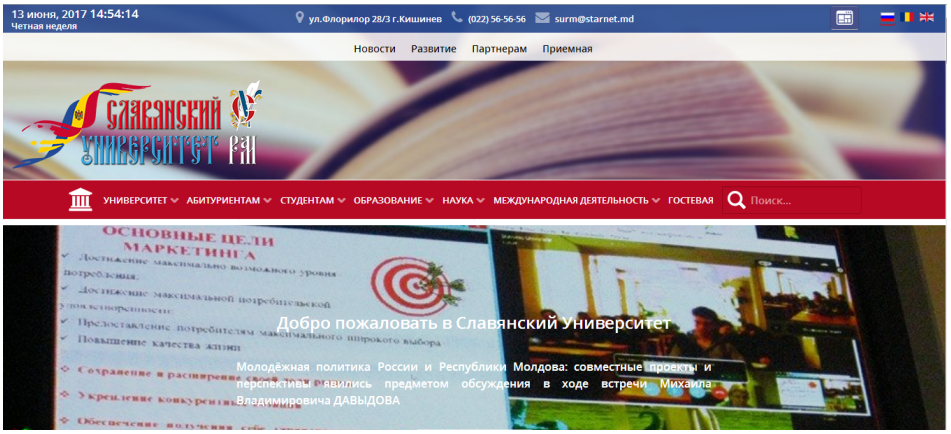


***Рис.3.* Скриншот Главного меню проекта (фрагмент)**

Источник: *разработка автора*

2.Плагины. Это элементы, которые дополняют функциональность нашего сайта.

На сайте используются следующие компоненты: Widgekit, Rocket Gallery. Rocket Spocket, Cagenda.

3.Модули. Элементы, которые выводятся на сайте в виде различных блоков, например, может быть блок регистрации или авторизации (у нас он пока в режиме разработки).

Блок «Новости» показывает 3 последние новости - рис. 4.

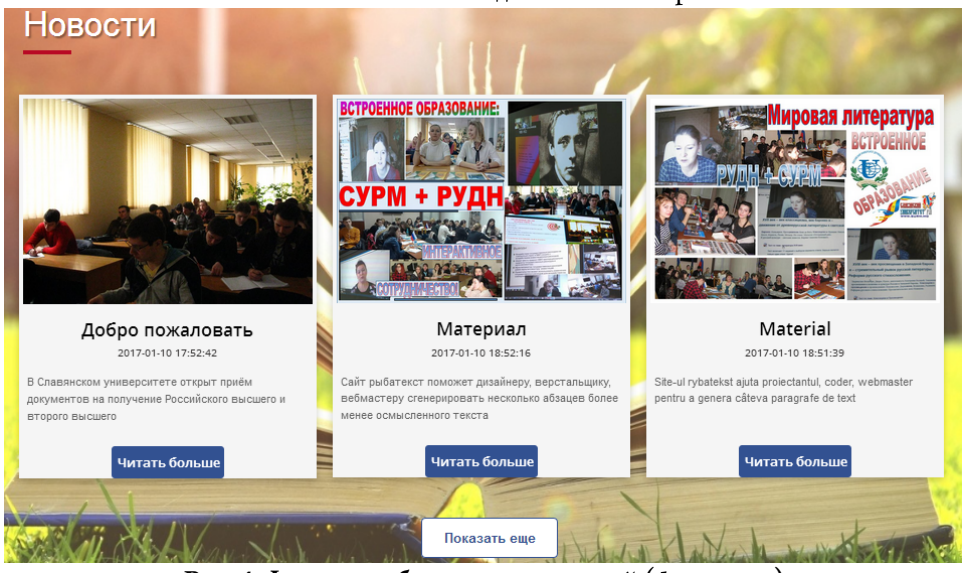


***Рис. 4.* Форма отображения новостей (фрагмент)**

Источник: *разработка автора*

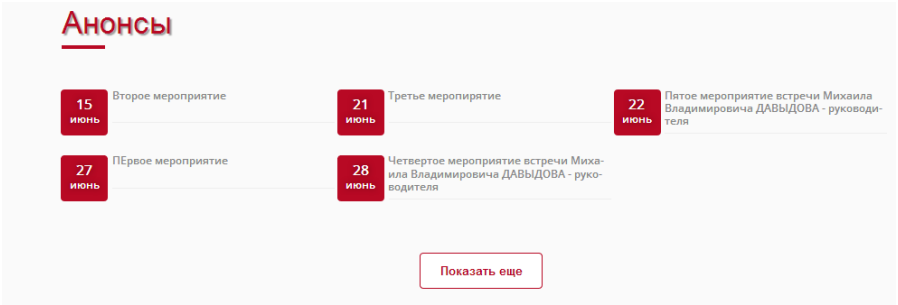


Рис.5. **Скриншот блока вывода анонсов предстоящих событий в Славянском университете**

Источник: *разработка автора*

Блок отображения в социальных сетях Facebook и Twitter показан на рис. 6.

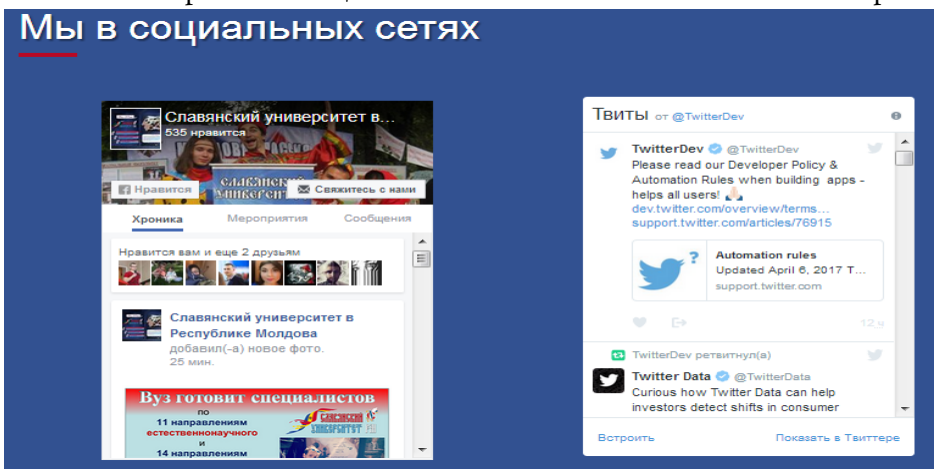


Рис.6. **Отображение информации в социальных сетях**

Источник: *разработка автора*

Анализ существующих атак на сайты позволяет выявить среди наиболее часто встречающиеся в последнее время атаки, связанные с перебором паролей на админ-панель сайта, которые носят характер DDoSa, т.к. осуществляются многопоточно и с разных IP адресов.

В связи с этим, для безопасности и стабилизации работы сервера следует использовать следующие дополнительные меры безопасности:

1) Как один из наиболее простых и эффективных вариантов, можно рекомендовать установить http авторизацию на админку Joomla. - создать файл с названием ".htpasswd" в корне сайта и при помощи сайта http://www.htaccesstools.com/htpasswd-generator/ сгенерировать его содержание, указав желаемый логин и пароль [4].

В файл ".htaccess" в папке /administrator/ необходимо добавить добавить следующие строки:

Код

```
AuthName "Access Denied"
AuthType Basic
AuthUserFile полный_путь_до_корня_сайта/.htpasswd
require valid-user
```

2) Вторым рекомендуемым способом защиты CMS Joomla может стать ограничение или разрешение доступа по определенному IP к административной части сайта.

Для этого в файл ".htaccess" в папке /administrator/ необходимо прописать следующие строки:

Код

```
Order deny,allow
  Deny from All  (закрыть доступ ко всем IP)
  Allow from 00.00.00.00
```

Это и будет IP, которому разрешается доступ к админчасти.

На основании проведенного исследования можно сформулировать следующие **выводы:**

1. Проект адаптивного портала Славянского университета, разработанный на системе управления содержимым (CMS) Joomla! Версия 3.7. Joomla! позволил реализовать при создании сайта СУРМ преимущества адаптивного дизайна и расширенного функционала.
2. Использованные средства безопасности для пользователей и администратора проекта позволяют уменьшить уязвимость сайта и обеспечить максимальную безопасность от взлома.

Таким образом, спроектированный, разработанный и готовый к внедрению электронный образовательный портал можно рассматривать как основу для создания нового открытого безопасного информационного пространства Славянского университета Республики Молдова в сети Internet.

Литература:

1. Информационный портал Славянского университета. Тестовый режим. Режим доступа: http://k95185st.beget.tech/ [Электронный ресурс]. Дата обращения: 20.02.2018 г.
2. Веб-студия Business Site. Режим доступа: https://www.site2b.com.ua/web-blog/zachem-nuzhna-povyshennaya-bezopasnost-sajta.html [Электронный ресурс]. Дата обращения: 25.02.2018 г.
3. Официальный сайт Славянского университета. Режим доступа: http://surm.md/ [Электронный ресурс]. Дата обращения: 07.02.2018 г.
4. Генератор паролей on-line Htpasswd Generator – Create htpasswd. Режим доступа: http://www.htaccesstools.com/htpasswd-generator/ [Электронный ресурс]. Дата обращения: 11.01.2018 г.

ОСНОВНЫЕ ПОДХОДЫ К РЕШЕНИЮ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ[1]

Никольская К. Ю., Асяев Г.Д.

Федеральное государственное автономное образовательное учреждение высшего образования «Южно-Уральский государственный университет (национальный исследовательский университет)»

Аннотация: В статье рассматриваются понятия аппаратной и программной защиты информации. Рассмотрены средства защиты информации компьютерных сетей. Описаны свойства и функции, которыми должна обладать система обеспечения безопасности компьютерных сетей.

Ключевые слова: компьютерные сети, защита информации, защита компьютерных сетей.

К аппаратным средствам защиты информации относятся: брандмауэры, сетевые экраны, сетевые фильтры, антивирусные программы, устройства шифрования протокола и др.

К программным защиты относятся: мониторинг сети, средства архивации данных, антивирусные программы, криптографические средства, средства аутентификации и аутентификации, средства управления доступом, протоколирование и аудит.

Как примеры комбинаций вышеперечисленных мер можно привести:

- - защиту баз данных;
- - защиту информации при работе в компьютерных сетях.

При создание крупномасштабных (локальных, корпоративных и т.д.) компьютерных сетей возникает проблема обеспечения взаимодействия большого числа компьютеров, серверов, подсетей и сетей т.е. проблема поиска и выбора оптимальной топологий становится главной задачей.

Важнейшим компонентом локальных и корпоративных сетей является их системная топология, которая определяется архитектурой межкомпьютерных связей. Известно, что в компьютерных сетях для обеспечения безопасности информации и сети подлежит обработке критическая информация. Термином «критическая информация» это: определенные факты относительно намерений, способностей и действий, жизненно необходимых для эффективного управления и деятельности критически важных структур, эффективного выполнения стоящих стратегических

[1] Статья выполнена при поддержке Правительства РФ (Постановление № 211 от 16.03.2013 г.), соглашение № 02.A03.21.0011 и при поддержке Совета по грантам Президента Российской Федерации (Соглашение № СП-5430.2018.5)

задач с различными грифами секретности; информация для служебного пользования; информация, составляющая коммерческую тайну или тайну фирмы; информация, являющаяся собственностью некоторой организации или частного лица.

В компьютерных сетях должны быть, предусмотрены аутентификация и шифрование, но данные элементы защиты не всегда обеспечивают надежную безопасность сети:

- использование шифрования в несколько раз уменьшает скорость передачи данных по каналу, поэтому, нередко, шифрование сознательно не применяется администраторами сетей с целью оптимизации трафика;
- в компьютерных сетях зачастую применяется устаревшая технология шифрования. Существуют программы, которые могут достаточно быстро подобрать ключи для проникновения в сеть.

Каждый узел сети является самостоятельной компьютерной системой со всеми проблемами добавляются, связанные с линиями связи и процедурой передачи информации. С точки зрения безопасности компьютерные сети обладают следующими недостатками:

- недостаточный контроль над клиентскими компьютерами;
- отсутствие механизма настраиваемого доступа нескольких пользователей к разным ресурсам на одном компьютере;
- необходимость подготовленности пользователя к разным административным мерам — обновлению антивирусной базы, архивированию данных, определению механизмов доступа к раздаваемым ресурсам и т. д.;
- разделение ресурсов и загрузка распределяются по различным узлам сети, многие пользователи имеют потенциальную возможность доступа к сети как к единой компьютерной системе;
- операционная система, представляющая сложный комплекс взаимодействующих программ. В силу этого обстоятельство трудно сформулировать четкие требования безопасности, особенно к общецелевым сетям, разрабатывавшимся без учета безопасности;
- неопределенная периферия сильно влияет невозможность определения, в большинстве случаев, точных пределов сети. Один и тот же узел может одновременно работать в нескольких сетях, и, следовательно, ресурсы одной сети вполне могут использоваться с узлов, входящих в другую сеть. Такое широкомасштабное разделение ресурсов, несомненно, преимущество;
- не определённая распределение траектории доступа. Пользователь или захватчик может затребовать доступ к ресурсам некоторого узла сети, с которым данный узел не связан напрямую сетью. В таких случаях доступ осуществляется через некоторый промежуточный узел, связанный с обоими узлами, или даже через несколько промежуточных узлов. В

компьютерных сетях весьма непросто точно определить, откуда именно пришел запрос на доступ, особенно если захватчик приложит немного усилий к тому, чтобы скрыть это;

- слабая защищенность линии связи. Сеть тем и отличается от отдельной системы, что непременно включает в себя линии связи, по которым между узлами передаются данные. Это может быть элементарный провод, а может быть линия радиосвязи, в том числе и спутниковый канал. При наличии определенных условий (и соответствующей аппаратуры) к проводу можно незаметно (или почти незаметно) подсоединиться, радиолинию можно успешно прослушивать — т.е. ничто не препятствует тому, чтобы «выкачивать» передаваемые сообщения из линий связи и затем выделять из всего потока требуемые.

На основе анализа угрозы безопасности компьютерных сетей можно сделать выводы о свойствах и функциях, которыми должна обладать система обеспечения безопасности локальных и корпоративный сетей (КС).

1. Идентификация защищаемых ресурсов, т.е. при подключении компьютерным сетям присвоение защищаемым ресурсам, по которым в дальнейшем система производит аутентификацию.
2. Аутентификация защищаемых ресурсов.
3. Применение парольной защиты ресурсов во — всей части компьютерной сети.
4. Регистрация всех действий: вход пользователя в сеть, выход из сети, нарушение прав доступа к защищаемым ресурсам и т. д.
5. Обеспечение защиты информации при проведении сканирование сети от вредоносных программ и ремонтно-профилактических работ.

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ[1]

Никольская К. Ю.

Федеральное государственное автономное образовательное учреждение высшего образования «Южно-Уральский государственный университет (национальный исследовательский университет)»

Аннотация: В статье рассмотрено понятие компьютерная сеть. Дана классификация существующим компьютерным сетям. А также описана актуальность развития новых средств защиты информации в компьютерных сетях.

Ключевые слова: компьютерные сети, защита информации, защита компьютерных сетей.

Компьютерная сеть – это система связи между компьютерами и/или вычислительным оборудованием, позволяющая им совместно разделять общие информационные и вычислительные ресурсы [1].

Компьютерные сети стали логическим результатом эволюции компьютерных и телекоммуникационных технологий. Их можно рассматривать с двух сторон:

1. Компьютерные сети как частный случай распределенных компьютерных систем.
2. Компьютерные сети как средство передачи информации на большие расстояния.

Компьютерные сети классифицируются по территориальному признаку. Различают глобальные (Wide Area Network – WAN), локальные (Local Area Network – LAN) и городские (Metropolitan Area Network – MAN) сети.

Первыми появились сети WAN. Они объединяют компьютеры, которые рассредоточены на расстоянии сотен и тысяч километров. Первые глобальные компьютерные сети очень много унаследовали от телефонных сетей. В них часто использовались уже существующие и не очень качественные линии связи. Это приводило к низким скоростям передачи данных и ограничивало набор предоставляемых услуг передачей файлов в фоновом режиме и электронной почтой.

Сети LAN ограничены расстоянием в несколько километров. Эти сети построены с использованием высококачественных линий связи. Эти линии позволяют применять более простые методы передачи данных, чем в глобальных сетях. Также это позволяет достигать высоких скоростей обмена данными. Услуги предоставляются в режиме подключения и отличаются разнообразием.

[1] Статья выполнена при поддержке Правительства РФ (Постановление № 211 от 16.03.2013 г.), соглашение № 02.A03.21.0011 и при поддержке Совета по грантам Президента Российской Федерации (Соглашение № СП-5430.2018.5)

Сети MAN предназначены для обслуживания территории крупного города. При достаточно больших расстояниях между узлами (десятки километров) они обладают качественными линиями связи и поддерживают высокие скорости обмена. Сети MAN обеспечивают экономическое соединение локальных сетей между собой, а также доступ к глобальным сетям.

Важнейшим этапом развития компьютерных сетей стало появление сетевых технологий, таких как Ethernet, FDDI, Token Ring. Они позволяют быстро и эффективно объединить компьютеры различных типов.

В конце 80-х годов локальные и глобальные сети имели существенные отличия по протяженности и качеству линий связи, сложности методов передачи данных, скорости обмена данными, разнообразию услуг и масштабируемости. В дальнейшем в результате тесной интеграции LAN, WAN и MAAN произошло взаимопроникновение соответствующих технологий.

Компьютерные сети можно разделить на два класса по среде передачи в соответствии с технологическими признаками:

1. Проводные сети – сети, каналы связи которых построены с использованием медных и оптических кабелей.
2. Беспроводные сети – сети, в которых для связи используют беспроводные каналы связи [2].

В первое десятилетие своего существования компьютерные сети использовались исследователями университетов для обмена электронной почтой и сотрудниками компаний для совместного использования принтеров. Вопросы безопасности не привлекали много внимания. Однако теперь, миллионы человек используют сети для управления своими банковскими счетами, приобретения товаров через Интернет и многое другое. В данном аспекте проблема сетевой безопасности становится серьезной.

Развитие и широкое распространение компьютерных сетей повлекло за собой привлекательность их использования для злоумышленников. Безопасность компьютерной сети – это безопасность хранимой в ней информации.

Компьютерная сеть инструмент для обмена информацией. При создании и использовании различных компьютерных сетей возникает ряд взаимосвязанных проблем по обеспечению защиты информации, которая хранится на компьютерах пользователей или на серверах компьютерной сети. Современные сетевые операционные системы предоставляют различные варианты защиты от несанкционированного доступа к сетевым ресурсам. Часто штатных средств по защите информации вполне достаточно. Но если мы говорим о хорошо спланированной сетевой атаке, то штатные средства будут бессильны. Согласно сложившейся практике, злоумышленник, который обладает достаточным опытом в области сетевого и системного программирования, задавшись целью, может получить доступ к защищенным ресурсам сети. Исходя из этого возникает спрос на создание дополнительных аппаратных и программных средств для защиты сетевых

ресурсов от несанкционированного доступа. Причем эти средства не универсальные, они должны настраиваться согласно архитектуре и потребностям компании. Например, некоторым компаниям будет достаточно отслеживать атаки по сезонности, другим этого будет мало.

Библиографический список

1. Цуриков А.Н. Компьютерные системы и сети / А.Н. Цуриков. ФГБОУ ВО РГУПС. – Ростов н/Д, 2016. – 64 с.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2010. – 944 с.

INFORMATION ASSET INVENTORY WEB APPLICATION

Rodica Bulai, Daria Stupina
Technical University of Moldova

Summary: *This article informs about the concept and purpose of an information asset inventory as a part of an information security management system. It also gives a representation of an implemented application; which purpose is to automatize and ease asset inventory process.*

Introduction

An Information Security Management System (ISMS) is a systematic approach to the process of managing sensitive data at an organization. Commonly, it is based on a set of security policies and procedures. The main purpose of an ISMS is to minimize risk, limiting the impact of a security breach. Typically, an ISMS works with technologies, data, processes and human resources in an organization. An ISMS might be aimed to a particular data type, as customer data, business secret, employee data. Or it might also be implemented in a comprehensive way that becomes part of the company's culture.

There exists a specification, also called standard, for creating an ISMS – ISO 27001. ISO 27001 does not mandate specific actions, but includes recommendations for documentation, continual improvement, internal audits, corrective and preventive actions. That specification focuses on the integrity, availability and confidentiality provision. Inherent part of an ISMS process, according to ISO 27001 is asset inventory. Only knowing everything that has value to an organization it is possible to calculate and minimize risks and ensure business continuity.

The concept of an asset inventory (also called asset register) is based on collecting and classifying any object, person or information that is part of an organization with the condition that it might be valuable for business. Manually the easiest way to register assets is technique called "describe what you see", which implies interviewing heads of each department about listing that includes: any person at their department, any personal computer, laptop or work station, any physical or digital files, any hardware or software, any equipment they see.

According to ISO 27001 every asset has an owner – the person that is responsible for asset protection and operates that asset. Without knowledge about who is responsible for any kind of valuable information in an organization it's basically impossible to ensure security and information protection.

Application details

Asset Inventory Web Application is based on PHP, using MySQL database and AJAX based template for the interface. The main menu is represented in the figure 1.

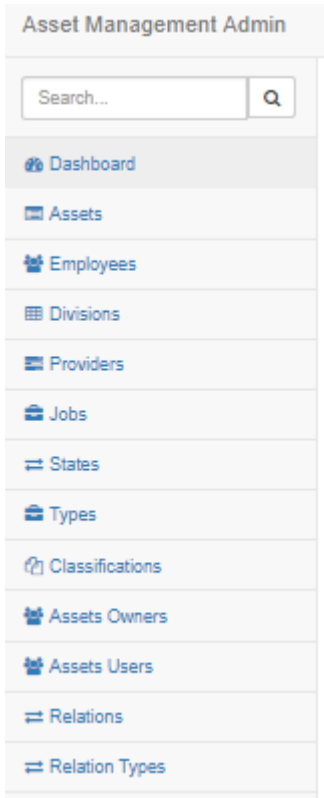


***Figure 1* – Main menu**

That software contains the most valuable information about any kind of assets in the organization:

- name – name of the asset, that is used for an asset subsequently;
- type – describes the type of asset, for example: hardware, software, human etc.;
- state – describes current state of an asset, for example: in production, in use;
- provider – describes provider of an asset;
- classification – describes current classification type of an asset, for example: critical, important, ordinary, not important;
- date of creation – contains creation date of an asset;
- date of last review – contains review date of an asset;
- relations between the assets – describes relations between assets, for example: PC1 uses Printer HP5;
- level of confidentiality, integrity, availability – describes the level from 1 to 5,
- resource value – is based on the level of confidentiality, integrity, availability and calculates automatic from1 to 10.

On the figure 2 is represented dashboard which allows users to see statistics about the levels of availability, confidentiality and integrity of the assets, number of assets by states, types and classification.

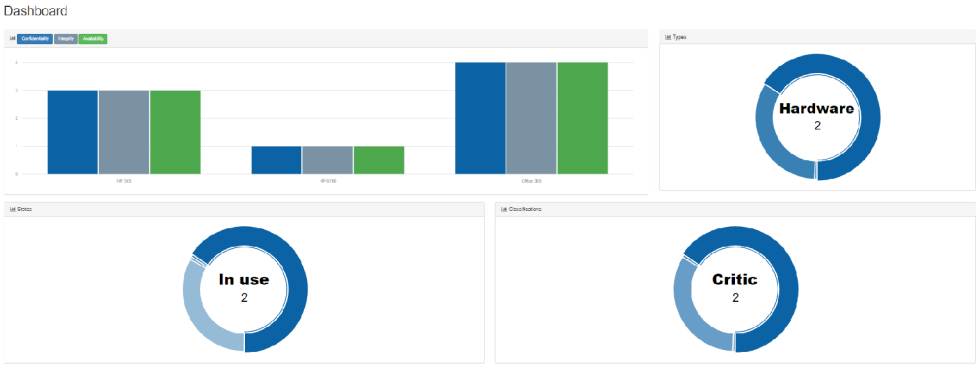


***Figure 2* - Dashboard**

An administrator or system manager has access to create the new asset, name it, choose the type and fill other fields as described above. On the figure 3 is shown a diagram, which represents the main functions of an administrator.

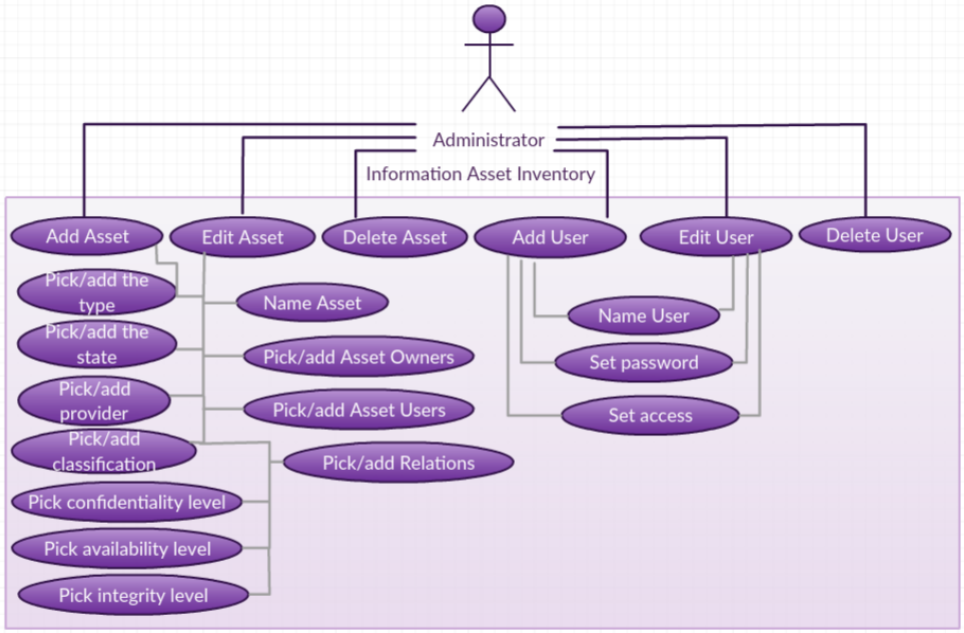


***Figure 3* – Use case diagram for an administrator**

Any part of the asset description might be modified by administrator, for example, an administrator can insert, edit or remove new types, states, relation types and all other fields. System manager is able to change only the limited number of fields or add an asset.

Application allows to choose the asset owners, as well as asset users, which can also be modified by an administrator or manager. Asset owners and asset users are chosen from the employee table, which might be filled by an administrator. On the figure 4 is shown list of the assets.

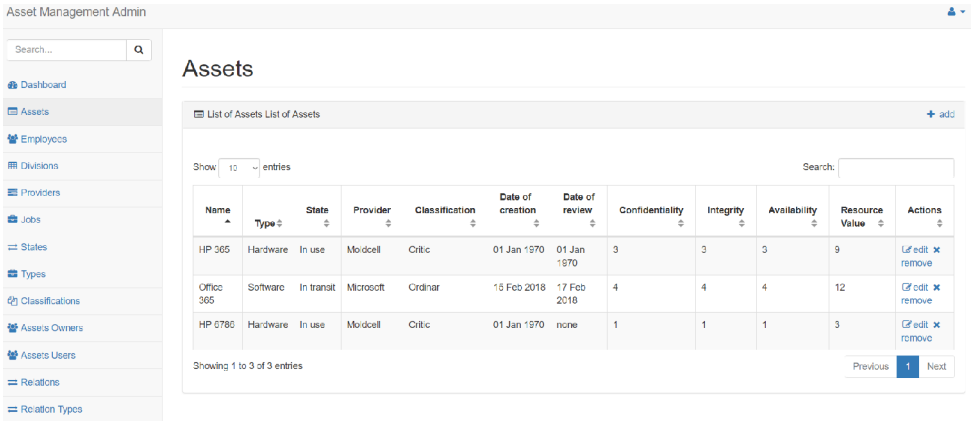


***Figure 4* – List of the assets**

There also exists an instrument, called `Asset Explorer` by Manage Engine, which allows user to discover all the assets in the network, manage and monitor software and hardware assets, manage the complete IT asset lifecycle, ensure software license compliance, make informed decisions about hardware and software purchases throughout the entire it life cycle, track purchase orders and contracts, know the total cost of ownership of an asset.

Within the 'Information Asset Register' software system by Informu Solutions user can establish a Business Classification Scheme, apply rules for retention periods, then tag the information assets to this scheme, with retention policies inherited. These assets could be applications and databases, electronic records, physical filing and backup tapes, computer equipment and mobile devices, books and magazines, audio and video materials etc. It also has the concept of asset collections that group together related sets of information.

Conclusion

On the first view, asset register seems to be a bureaucratic process, but in practice it the powerful and indispensable instrument in risk evaluation and protection of an organization.

As the plan for the future, Asset Inventory can wide to an Asset Inventory and Risk Management Processes, which should include risk identification (additional threats and vulnerabilities), analysis (impact and likelihood) and treatment part.

NOTIFICAREA VULNERABILITĂȚILOR

Rodica Bulai, Cucu Eugeniu, David Eugeniu
Universitatea Tehnică a Moldovei

Summary: *This talk is about a new system that is about to be implemented by us. It will be a new approach on vulnerability monitoring that will permit to reduce the amount of work for IT professionals and will be a easy to use tool for everyone that is concerned about security of their gadgets.*

Introducere

Ținând cont de trendurile actuale, tot mai multe dispozitive devin „smart" și devin tot mai accesibile oamenilor de rând. Aceste dispozitive, având necesitatea de a procesa ceva informație, vin cu sisteme de operare în care sunt înscrise comenzile care urmează să le poată îndeplini, însă puține din ele sunt elaborate și optimizate pentru a oferi securitate din start. Din acest motiv, apare necesitatea de a fi mereu la curent cu ultimele noutăți din domeniul IT și în special apare necesitatea de a fi la curent cu amenințările și vulnerabilitățile noi apaărute.

Astfel, dacă până la un moment, doar cei care erau nevoiți și impuși de responsabilitățile de serviciu, analizau situația la zi și erau la curent cu cele mai noi vulnerabilități, această necesitate apare astăzi și la utilizatorii de rând care utilizează lucruri „smart" (IoT).

Pentru aceasta vin în ajutor multe portaluri de noutăți din lumea IT, multe baze de cunoștințe despre vulnerabilități au RSS feed-uri care pot fi configurate, însă o astfel de soluție presupune ca utilizatorul să filtreze informația. Din cantitatea de informație obținută, să fie capabil să depisteze doar acele amenințări care îl afectează într-o oarecare măsură. Acest lucru fiind extrem de greu de realizat, multe din amenințări având diferiți vectori de atac și realizându-se prin diferite metode, utilizând vulnerabilități ale aplicațiilor, serviciilor, sistemelor de operare sau a componentelor hardware.

În lumea IT mereu a fost și va rămâne actuală necesitatea de a fi la curent cu toate noutățile tehnologice, iar pentru ofițerii de securitate, administratorii de rețea, administratorii de sistem și alte persoane responsabile de administrarea echipamentelor, este critic de a cunoaște care pot fi amenințările și prin ce vulnerabilități acestea se pot realiza. În ajutor vin scanerele de vulnerabilități, însă acestea consumă foarte multe resurse, necesită configurare și actualizare manuală, plus la rularea unei scanări, acestea consumă foarte mult trafic și adaugă un „stres" mare pe echipamentele verificate. Din acest motiv scanerele de vulnerabilități sunt setate de a rula la o perioadă stabilită pentru a nu întrerupe activitatea afacerii. Astfel scanerele de vulnerabilități sunt o măsură de control, însă nu este suficientă, răufăcătorii fiind mereu în căutarea noilor vulnerabilități, iar în lumea IT dacă nu mergi în pas cu răufăcătorii, devii victimă.

Sistem de notificare a vulnerabilităților

Un sistem de notificare a vulnerabilităților vine să rezolve unele probleme discutate mai sus, și anume:

- Realizează filtrarea informației pentru utilizatori.

- Dispune de un scaner, care rulează la inițierea sistemului, și care depistează echipamentele, sistemele de operare, serviciile și aplicațiile utilizate de către deținător. Totodată, utilizatorul poate introduce manual ceea ce nu a putut depista scanerul. Astfel, sistemul deținând informații despre resursele informaționale ale utilizatorului, poate notifica utilizatorul doar despre amenințările la care sunt supuse resursele sale. Aceasta permite micșorarea semnificativă a volumului de lucru oderind un mare avantaj nu doar persoanelor entuziasmate de lumea tehnologiilor moderne, ci și administratorilor de sisteme.
- Notificarea conține nu doar date despre vulnerabilitatea nou apărută, ci și recomandări de remediere a acesteia. Acest lucru, permite iarăși micșorarea volumul de lucru care urmează să fie realizat de administratorii de sisteme, cât și asistarea persoanelor cu cunoștințe mai reduse în domeniul securității informaționale.
- Sistemul oferă posibilitatea de a genera rapoarte, ceea ce poate fi util pentru utilizatori de rând și foarte util pentru administratori de sisteme. Rapoartele fiind personalizabile, oferă posibilitatea de a selecta ce informații să fie incluse și în ce format generate.
- Sistemul utilizează cele mai cunoscute și avansate baze de cunoștințe cu vulnerabilități: Exploit Database (exploit-db), National Vulnerability Database (NVD), CVESecurity Vulnerability Database și Rapid7 Vulnerability Database. Aceste baze de cunoștințe dețin informații despre vulnerabilități deja existente și sunt actualizate regulat cu noi vulnerabilități, datorită cooperării cu echipe de cercetare din domeniul securității informaționale.
- Datorită faptului că sistemul nu are necesitatea de a scana permanent rețeaua pentru depistarea vulnerabilităților, acesta nu consumă resurse, iar posibilitatea de a introduce manual date despre resurse informaționale oferă flexibilitate înaltă de întreținere și actualizare.

Sistemul conține o aplicație client prin care utilizatorii pot configura notificările și un API prin care sistemul poate fi integrat cu alte soluții proprii. Notificările despre vulnerabilități pot fi primite în cadrul aplicației client sau să fie expediate pe adresa de email a utilizatorului, figura 1.

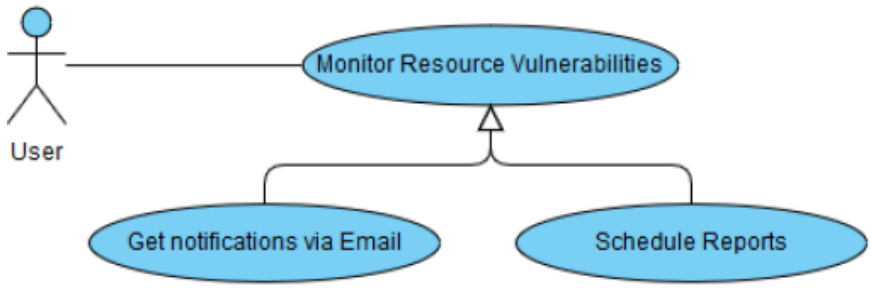


***Figura 1* – Diagramă generală de caz utilizare**

Aplicația este proiectată pentru a fi simplă în utilizare atât de profesionaliști din domeniul IT, cât și de utilizatorii de rând, iar API-ul poate fi de mare folos pentru întreprinderile care doresc să dezvolte propriile soluții sau doresc să integreze soluția dată cu alte proiecte.

Aplicația client poate fi utilizată pe mai multe platforme cur ar fi: platforma mobilă (Android, iOS), platforma desktop (Mac, Linux, Windows), sau pe platforma web. Acest lucru este posibil prin API GATEWAY care servește ca punct unic de intrare în aplicație și care comunică la fel cu toate platformele utilizând un API specific pentru fiecare din platforme, figura 2.

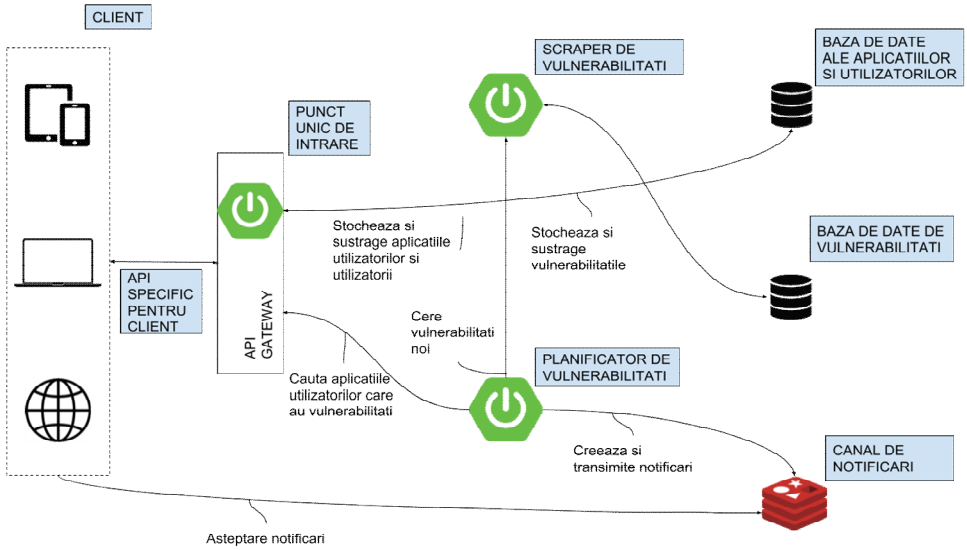


***Figura 2* – Diagrama comportamentală a sistemului**

Conform figurii 2 se poate de observat că în calitate de CLIENT poate fi utilizat orice dispozitiv pe orice platformă, client-ul comunicând cu API GATEWAY utilizând un API specific pentru fiecare platforma.

Clientul ce comunică cu API-ul poate înregistra aplicațiile sale în BAZA DE DATE DE APLICATII ŞI UTILIZATORI, după care primește o cheie unică pentru CANALUL DE NOTIFICARI de unde va primi notificarile.

La aceasta etapa acțiunile utilizatorului se încheie, și urmează partea de procesare a vulerabilităților de servicii PLANIFICATOR DE VULENERABILITĂȚI și SCRAPER DE VULNERABILITĂȚI, care găsind vulnerabilități noi le stochează în BAZA DE DATE DE VULNERABILITĂȚI, apoi găsind aplicațiile vulnerabile costruiește notificari și le transmite în canalul de notificări.

Cu toate că pe piață deja există unele soluții care oferă notificări despre vulnerabilități, acestea vin în formă de noutăți săptămânale sau la intervale stabilite de utilizator. De asemenea, informația expediată de aceste soluții nu poate fi filtrată ușor. De exemplu, *US-CERT Alarms* nu oferă nici un criteriu de filtrare, informația primită de

utilizator, cuprinde toate vulnerabilitățile noi apărute pe perioada stabilită. O altă soluție existentă, *CVE Details Vulnerability Feeds & Widgets*, oferă niște criterii de filtrare a informației, însă aceasta se limitează la tipurile de vulnerabilități și nu șa platforme, sisteme de operare sau servicii. Iar soluția *Secunia*, este una cu funcțional mai vast, pe lângă notificări, oferind suport tehnic și consultații și este o soluție contra plată orientată spre specialiștii în domeniul securității informației și infrastructuri ale companiilor IT.

Concluzii

Soluția dezvoltată și descrisă în acest articol vine ca un instrument potrivit pentru a asigura securitatea echipamentelor atât personale, pentru utilizatori de rând, cât și infrastructuri IT din cadrul întreprinderilor. Funcționalitățile oferite de sistem asigură notificarea în cel mai scurt timp despre noile amenințări, ceea ce poate fi critic în unele situații.

Tot odată, acest instrument nu consumă resurse și nu împiedică în nici un fel activitățile echipamentelor IT. Datorită faptului că utilizatorul introduce în sistem denumirea echipamentelor/aplicațiilor/SO-urilor deținute și versiunile acestora, soluția filtrează informația care urmează să fie expediată, ceea ce ușurează substanțial lucrul cu sistemul dat.

Sistemul oferă un API care permite încorporarea funcționalului în alte aplicații sau sisteme, acest lucru fiind un mare avantaj pentru companiile care au nevoie să modifice sau să adauge ceva componente, care să corespundă necesităților acestora.

Bibliografie:

1. Information security (infosec), Margaret Rouse - http://searchsecurity.techtarget.com/definition/information-security-infosec
2. Exploit Database - https://www.exploit-db.com/
3. National Vulnerability Database - https://nvd.nist.gov/
4. CVESecurity Vulnerability Database - https://www.cvedetails.com/
5. Rapid7 Vulnerability Database - https://www.rapid7.com/db

Materialele Conferinței "Securitatea Informațională 2017"
sunt publicate în redacția autorilor.

Semnat pentru tipar 07.03.2018.
Coli de tipar 12,06. Coli de autor 10,96.
Tiraj 50 ex.
Tipografia Departamentului Editorial-Poligrafic al ASEM