странах. Использованы основные общеизвестные группы методов: философские методы научного познания, общенаучные и специальные методы и подходы. В частности, применены анализ, синтез, дедуктивный метод, междисциплинарный, концептуальный подход. Комплексный подход помог выявить тенденции и закономерности формирования информационной элиты, предвидеть последствия и возможное развитие политических событий с учетом особенностей информационной эпохи.

Ключевые слова: инфократия, нетократии, новая элита, информация.

Mytko Antonina, Shuliak Nazarii. Specification for the Formation of New Political Elits in the Information Education. The article examines the influence of media communication, information and knowledge on the formation of a new elite of infocracy and netocracy. The role of the media for the construction of a new elite in the information age is revealed. The modern information technologies (Internet, computer communication, multimedia, etc.) were described, which allowed the transnational organizations to generate a new elite in different countries. The basic well-known groups of methods are used: philosophical methods of scientific knowledge, general scientific and special methods and approaches. In particular, analysis, synthesis, deductive method, interdisciplinary, conceptual approach were applied. The comprehensive approach helped to identify the trends and patterns of the formation of the information elite, to predict the consequences and possible development of political events, taking into account the peculiarities of the information age.

Key words: infocracy, netocracy, new elite, information.

Стаття надійшла до редколегії
04.05.2017 р.

УДК 351:004.65

Ярослава Пахольчук,
Антоніна Митко

Безпека інформаційних систем організацій

У статті вказано причини, які зумовлюють потребу безпеки інформаційних систем, зазначено основні цілі управління їх безпекою. Крім підтримки конфіденційності, цілісності та доступності, сучасне суспільство

вимагає дотримання й інших цілей: установлення відповідальності, інтегрованості людей, достовірності та етичності. Завдання та цілі цього дослідження досягнуті завдяки аналізу інформаційних джерел із цієї теми. Ідентифіковано заходи, які потрібно вжити, описано важливість безпеки ІС. У процесі наукового дослідження застосовано такі методи: метод наукового узагальнення, метод аналізу інформації, узагальнення. Практичну цінність цієї роботи становить детермінація заходів безпеки ІС організацій. Результати дослідження можуть бути використані в подальших дослідженнях із цієї тематики.

Ключові слова: інформаційні системи (ІС), управління системою безпеки, інформація, технічний рівень, інформаційні технології.

Постановка наукової проблеми та її значення. За останні кілька років простежували значну тенденцію розвитку технологій, яка створила нові можливості для робочих місць, розваг, якщо йдеться про наше повсякденне життя, та навіть зробила доступною величезний обсяг інформації, який зосереджено в наших руках. Те, що ми постійно обмінюємось інформацією, змусило компанії й організації активізувати свою гру також, тому безпека інформаційних систем стала, як ніколи, гострою проблемою, щоб тримати інформацію під контролем для її безперебійної роботи та обробки.

Аналіз досліджень цієї проблеми. Інформаційні системи та їхню безпеку вивчали і зарубіжні, і вітчизняні науковці. Серед українських можна виділити роботи О. В. Грицунова, Т. М. Басюка, П. І. Жежнича, В. Звасса. У роботах іноземних учених проблемне питання досліджено значно ширше, багатогранніше. Можна відзначити Р. Ватсона, Д. Боржву, А. Слоуна, Дж. Валачича, К. Шнайдера, Р. Робертса та ін.

Мета статті – дослідити закономірності покращення безпеки інформаційних систем й обґрунтувати їх важливість.

Завдання статті – виявити причини, які зумовлюють зміцнення ІС; визначити основні цілі управління безпекою інформаційних систем; узагальнити комплекс заходів для захисту ІС.

Швидкий розвиток інформаційних технологій, цивілізації й кіберзлочинності зумовлює **актуальність** цього дослідження.

Для докладного вивчення тематики статті використано такі теоретичні **методи** наукових досліджень, як порівняння, системний

підхід, метод наукового узагальнення, а також емпіричні методи – вивчення літератури з теми роботи та метод аналізу інформації.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження. Інформаційні системи, як відомо, розгляддають як сукупність організаційних і технічних засобів для збереження та опрацювання інформації для забезпечення інформаційних потреб користувачів. Проблема гарантування безпеки інформаційних систем завжди займала важливе місце в роботі відомих фірм, підприємств, організацій. Саме тому такі інциденти минулих років, як крах Barings Bank, Enron і провали безпеки в ChoicePoint, Банку Америки, T-Mobile, набули широкої публічності серед громадськості, а отже, привернули увагу засобів масової інформації. На сьогодні зміцнення безпеки інформаційних систем у середовищі високих технологій зумовлене взаємодією декількох технологічних і соціальних факторів.

По-перше, залежність окремих осіб, організацій та товариств від інформації й комунікаційних технологій досягла високого рівня. Ми як окремі особистості використовуємо ці технології для виконання широкого спектра завдань – від спілкування з іншими людьми, покращуючи нашу продуктивність роботи, маючи доступ до різних джерел інформації, до бронювання квитків і покупки книг. Для організацій інформаційні та комунікаційні технології є не просто головним компонентом основних операційних систем і створення сприятливих умов для підвищення продуктивності, а й засобом для отримання конкурентних переваг, розвитку нового бізнесу, а також просування нових методів управління [7].

По-друге, унаслідок використання інформаційних та комунікаційних можливостей у бізнес-сфері уся бізнес-модель багатьох організацій трансформувалася. У минулому компанії покладалися на певну географічно визначену територію, щоб виконувати свою діяльність. Однак глобальний масштаб взаємозв’язку, розподілена обробка, швидкий ріст Інтернет-мережі, лібералізація ринків телекомунікації та поширення електронної комерції різко змінили спосіб ведення бізнесу. Сьогодні співробітники проживають в ері підвищення мобільності, яка приводить до потреби отримання доступу до інформації з використанням різноманітних засобів, у несхожих ситуаціях, будучи

за межами організації, у віддалених місцях. Незалежність організації від місця локації – вагома перевага для неї [7].

Важливість інформації підтверджують передові досягнення у сфері інформаційних технологій та мінливі зміни кордонів фірми. Саме інформація допомагає компаніям реалізувати свої цілі, тримаючи їх у контакті із їхнім середовищем, вона виступає як інструмент спілкування, допомагає менеджерам приймати доцільні рішення та забезпечує підтримку для обміну знаннями між робочим складом.

Раніше інформація зберігалася в певному місці, куди обмежувався доступ тих, хто авторизувався, тому було відносно легко підтримувати її конфіденційність. Оскільки інформацію обробляли в головному офісі, то на певному рівні це давало можливість зберігати її цілісність, тобто обмежити можливості несанкціонованої модифікації її змісту й форми, а також підтримку доступності інформації та пов'язаних із нею ресурсів [4, с. 118].

Підтримка конфіденційності, цілісності й доступності були основними цілями управління безпекою. Це й створювало своєрідний трикутник безпеки ІС (наведено нижче).

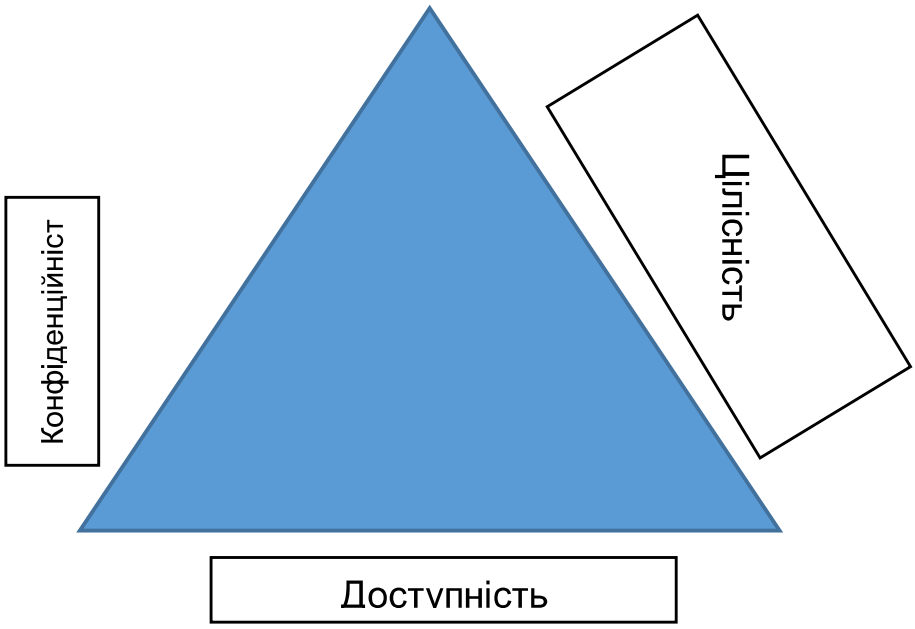

Рис. 1. **Трикутник безпеки ІС**

Сьогодні, ураховуючи трансформовану природу організацій і розширену сферу обробки інформації, управління інформаційною

безпекою не обмежується лише цими трьома пунктами, тому наразі потрібно акцентувати на встановленні відповідальності, інтегрованості людей, достовірності та етичності.

Сьогодні захист інформаційних систем – нелегке завдання: дуже часто відсутня унікальна й чітко визначена мета захисту цих активів. Сучасне інформаційне середовище вимагає підтримки секретності даних, пов'язаних зі співробітниками, клієнтами та партнерами; мінімізації наслідків, спричинених залежністю від недовірчих або зовсім ненадійних систем та організацій; стійкості до технологічних неполадок в управлінні безпекою інформаційних систем.

Для того щоб керувати безпекою інформаційних систем, організації повинні об'єднувати широкий набір факторів, починаючи від суто технічних і закінчуючи розглядом бізнес-середовища, культурою організації, очікуваннями й обов'язками колективу, смислами різних дій та пов'язаних із ними закономірностями поведінки. Це означає, що безпека інформаційних систем досліджується з погляду мінімізації ризиків, які виникають через непослідовну та неорганізовану поведінку щодо обробки інформації компанією.

Ці суперечності та неузгодженості в діяльності можуть призвести до виникнення побічних ефектів. Крім утрат, завданих природними чинниками (наприклад пожежі, повені), більшість побічних ефектів пов'язана з навмисно чи ненавмисно неналежною поведінкою окремих осіб у вигляді індивідуальної помилки або з недоліками системного аналізу чи дизайну, порушенням гарантій довіреним персоналом, системою зловмисників або шкідливими програмами, такими як віруси, черв'яки та троянські коні.

Для запобігання, виявлення й реагування на такі події організації можуть застосовувати комплекс заходів, відомий як управління системою безпеки. Оскільки обробку інформації в організаціях здійснюють на трьох рівнях – технічному, формальному, неформальному, то безпека інформаційних систем може бути досягнута тільки завдяки координації та підтримці цілісності операцій у межах і між цими трьома рівнями [9, с. 75]. Це означає, що організація повинна зайняти комплексну позицію в управлінні безпекою інформаційних систем саме через реалізацію комплексу

управління системою безпеки, яка загалом підтримує цілісність інформаційних систем організації.

На технічному рівні організація може вжити такі заходи управління безпекою, як антивірусне програмне забезпечення, систему обмеження доступу, системи виявлення несанкціонованих вторгнень, пристрої контролю доступу та криптографічне управління. На неофіційному рівні вимагається проведення таких заходів, як упровадження ознайомчих програм, перехід на належну практику управління, розвиток культури безпеки працівників, яка сприяє захисту інформаційних активів [4, с. 121].

Упродовж минулих років організації не досягнули своєї мети в охороні інформаційних систем, тобто розроблення заходів інформаційної безпеки не виправдала себе в розв'язанні проблем інформаційної безпеки. Різні дослідження повідомили про значні втрати у вигляді зареєстрованих порушень, а саме комп'ютерних злочинів, які були вчинені через порушення та недотримання заходів щодо забезпечення безпеки співробітниками організацій.

Висновки й перспективи подальших досліджень. Конфіденційність, цілісність, доступність – це ключові атрибути безпеки інформаційних систем. Із технічного погляду, безпека може бути досягнута тільки у випадку, якщо ці три аспекти чітко зрозумілі та дотримані. В умовах збільшення випадків комп'ютерних злочинів, проблем інформаційної безпеки й утручання шахраїв у ІС будь-які спроби розв'язання проблем вимагають адекватного розуміння положень, які допоможуть організації протистояти порушенню її мережевої безпеки, а саме:

– створення ефективних методів управління;

– установлення політики безпеки й процедур, які відображатимуть організаційний контекст та нові бізнес-процеси;

– інформування працівників щодо правил безпеки ІС;

– установлення спеціальних програм, які унеможливлюють уторгнення в мережу організації;

– створення відповідного плану дій у надзвичайних ситуаціях тощо.

Отже, перед підприємствами стоїть безліч правил, яких потрібно дотримуватись, і здійснення низки заходів, які допоможуть розв'язати проблеми щодо захисту інформаційних систем.

Обчислювальні й мережеві ресурси збільшують свою роль у нашому житті та бізнесі, водночас збільшується і їх важливість, а отже, усе частіше вони стають ціллю для злочинців. Саме тому організаціям потрібно бути пильними в тому, як вони захищають свої ресурси та інформацію.

Список використаних джерел

1. Грицунов О. В. Інформаційні системи та технології : навч. посіб. / О. В. Грицунов. – Харків : ХНАМГ, 2010. — 222 с.
2. Методи та засоби мультимедійних інформаційних систем : навч. посіб. / Т. М. Басюк, П. І. Жежнич ; Нац. ун-т «Львів. політехніка». – Львів : Вид-во Львів. політехніки, 2015. – 426 с.
3. Гайдамакин Н. А. Автоматизированные системы, базы и банки данных. Вводный курс : учеб. пособие / Н. А. Гайдамакин. – Москва : Гелиос АРВ, 2002. – 368 с.
4. David T. Bourgeois, Ph.D. Information Systems for Business and Beyond / David Thomas Bourgeois // Biola University. – Pub Date : 2014. – P. 167.
5. Backhouse, J., & Dhillon, G. (1996). Structures of Responsibility and Security of Information Systems / J. Backhouse // European Journal of Information Systems. – 5(1), 2–9.
6. Dhillon, G. (1997). Managing Information System Security / G. Dhillon. – London : Macmillan.
7. Dhillon, G. (2007). Principles of Information Systems Security: Text and Cases / G. Dhillon. – Hoboken, NJ : John Wiley & Sons.
8. Garg, A. (2003). The Cost of Information Security Breaches / A. Garg. – The SGV Review. – P. 202.
9. Hitchings, J. (1994). The Need for a New Approach to Information Security / J. Hitchings. – Paper presented at the 10th.
10. International Conference on Information Security (IFIP Sec '94), 23–27 May. – Curacao, NA.

Пахольчук Ярослава, Мытко Антонина. Безопасность информационных систем организаций. В статье указаны причины, обуславливающие необходимость безопасности информационных систем, указаны основные цели управления безопасностью таких систем. Кроме поддержки конфиденциальности, целостности и доступности, современное общество требует соблюдения и других целей – установление ответственности, интегрированности людей, достоверности и этичности. Задачи и цели данного исследования были достигнуты путем анализа

информационных источников по данной теме. Идентифицированы меры, которые нужно соблюдать, описана важность безопасности ИС. В процессе научного исследования были использованы следующие методы: метод научного обобщения, метод анализа информации, обобщения. Практическую ценность этой работы составляет детерминация мер безопасности ИС организаций. Результаты исследования могут быть использованы в дальнейших исследованиях по данной тематике.

Ключевые слова: информационные системы (ИС), управление системой безопасности, информация, технический уровень, информационные технологии.

Paholchuk Yaroslava, Mytko Antonina. Security of Information Systems in the Organizations. The article stated reasons which demand the necessity of information systems security, stated the main goals of safety management systems. In addition to maintaining the confidentiality, integrity and availability, modern society requires compliance of other goals, such as responsibility, integration of people, credibility and ethics. Tasks and objectives of this study were achieved by analysis of information sources on the topic. Identified steps to be followed, described the importance of information systems security. During the research were used the following methods: a method of scientific analysis, the method of analysis of information, synthesis. The practical value of this work is determination precautions of information systems security of organizations. Results of the study can be used in further research on the subject.

Key words: information systems (IS), security system management, information, technical level, information technologies.

Стаття надійшла до редколегії
10.05.2017 р.

УДК 35.01:328

Наталія Подвірна

Комунікативний складник у відносинах між владою та суспільством

Розвиток нових інформаційних технологій, мобільний зв'язок, Інтернет і соціальні мережі дали можливість світу на зламі XX–XXI ст. по-