МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

УДК 316.77
DOI: https://doi.org/10.32840/1814-1161/2020-5-22

Гарькава В.Ф.
кандидат економічних наук, доцент,
перший проректор
Міжнародного класичного університету імені Пилипа Орлика

Мишелов М.В.
старший викладач
Міжнародного класичного університету імені Пилипа Орлика

Harkava Viktoriia
Candidate of Economic Sciences, Associate Professor,
First Vice-rector
Pylyp Orlyk International Classic University

Myshelov Mikhail
Senior Instructor
Pylyp Orlyk International Classic University

ВИКЛИКИ ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

CHALLENGES OF STATE INFORMATION SECURITY

Безпека – це тема, яка набуває все більшої зацікавленості з боку організацій та державних установ. Кількість даних, з якими щодня доводиться мати справу організаціям, зростаюча кількість онлайн-транзакцій та відсутність обізнаності про комп'ютерну безпеку є більшими мотиваціями не лише для використання програмних уразливостей, а й для використання людських вразливостей. Узагалі користувачі, як правило, приймають нові технології з повним ігноруванням своїх уразливих місць безпеки, якщо отримують від них достатню вигоду. Виховання і постійне заохочення культури безпеки та усвідомлення того, що люди все ще є і завжди будуть найслабшою ланкою, безумовно, допоможуть організаціям досягти належного рівня безпеки і, таким чином, наблизитися до своїх бізнес-цілей. Більше того, моніторинг та раннє виявлення також відіграють важливу роль, оскільки це дає змогу організаціям та урядовим установам швидше реагувати на події, які важче знайти та зрозуміти з погляду управління безпекою. Швидке реагування на події, пов'язані з безпекою, та здійснення превентивних заходів з управління безпекою починають перетворюватися на конкурентну стратегію для організацій. У даній статті ми висвітлюємо деякі концепції та принципи інформаційної безпеки, щоб забезпечити діючу інформацію для осіб, що приймають рішення, щодо управління їхніми корпоративними активами та забезпечення їх стійкості.

Ключові слова: *інформаційна безпека, управління інформаційною безпекою, стандарти безпеки, методології безпеки.*

Безопасность – это тема, которая приобретает все большую заинтересованность со стороны организаций и государственных учреждений. Количество данных, с которыми ежедневно приходится иметь дело организациям, растущее количество онлайн-транзакций и отсутствие осведомленности о компьютерной безопасности являются большими мотивациями не только для использования программных уязвимостей, но и для использования человеческих уязвимостей. Вообще пользователи, как правило, принимают новые технологии с полным игнорированием своих уязвимых мест безопасности, если получают от них достаточную выгоду. Воспитание и постоянное поощрение культуры безопасности и осознание того, что люди все еще есть и всегда будут самым слабым звеном, безусловно, помогут организациям достичь надлежащего уровня безопасности и, таким образом, приблизиться к своим бизнес-целям. Более того, мониторинг и раннее выявление также играют важную роль, поскольку позволяют организациям и правительственным учреждениям быстрее реагировать на события, которые труднее найти и понять

с точки зрения управления безопасностью. Быстрое реагирование на события, связанные с безопасностью, и осуществление превентивных мер по управлению безопасностью начинают превращаться в конкурентную стратегию для организаций. В данной статье мы освещаем некоторые концепции и принципы информационной безопасности, чтобы обеспечить действующую информацию для лиц, принимающих решения, по управлению их корпоративными активами и обеспечению их устойчивости.

Ключевые слова: *информационная безопасность, управление информационной безопасностью, стандарты безопасности, методологии безопасности.*

Security is a topic that is gaining more and more interest from organizations and government agencies. The amount of data that organizations have to deal with on a daily basis, the growing number of online transactions, and the lack of knowledge about computer security are greater motivations not only for exploiting software vulnerabilities but also for exploiting human vulnerabilities. Responding quickly to security developments and taking preventive safety management measures are beginning to become a competitive strategy for organizations. In this article, we highlight some concepts and principles of information security to provide valid information for decision makers on how to manage their corporate assets and ensure their sustainability. For example, a security vulnerability, such as credit card leaks, can have negative consequences for card payment companies through the cancellation and reissuance of compromised cards. Of course, this is expensive, which greatly affects the reputation of the organization and consumer confidence. In fact, one of the fastest growing information crimes is the theft of personal information, including customer data, lost by the organizations responsible for managing it. Such cases have originated around the world and have led to the imposition of strict national and international data protection laws in many countries, which require organizations to protect the personal information of stakeholders. Therefore, it is very important for organizations to develop efforts to ensure their ability to securely protect their information assets and IT infrastructure. OCTAVE assessment is a process-driven methodology used to assess and plan risk-based information security. It helps organizations identify, prioritize, and manage information security risks. In general, to address all aspects of security, organizations first define their core security objectives, then apply adequate methods to formalize and verify their management, and finally develop procedures to achieve their objectives. In practice, protecting a security program is much more than that, and requires several variables. Security standards and methodologies provide a solid foundation for an information security program.

Keywords: *information security, information security management, security standards, security methodologies.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Поширення програм, що базуються на Інтернеті, змінило спосіб ведення бізнесу організаціями. Організації глибоко зацікавлені у пошуку нових технологічних ініціатив із низькою експлуатаційною вартістю, щоб запропонувати кращі та інноваційні послуги і, таким чином, отримати конкурентні переваги. Однак зі збільшенням залежності від технологій для отримання конкурентних переваг інформаційна безпека є й була однією з найважливіших і найскладніших вимог для ведення успішного бізнесу. Нові технологічні рішення завжди мають вразливі місця, які більшу частину часу виявляють несподівані ризики для безпеки. У цьому контексті організації повинні визначати, впроваджувати, контролювати та оцінювати найефективніший набір засобів контролю, щоб забезпечити адекватний рівень безпеки. Стандарти безпеки ISO/IEC_JTC1 (Міжнародна організація зі стандартизації/Міжнародна електротехнічна комісія_Спільний технічний комітет та NIST (Національний інститут стандартів і технологій) є важливим посиланням у сфері інформації про безпеку, й у цілому організації визначають свою програму безпеки відповідно до Міжнародних стандартів безпеки. Однак ці стандарти мають інформативний характер, не мають практичної інформації та покладаються на інтерпретацію експерта з питань безпеки, переважно на основі їхнього досвіду та уявлення про безпеку. Стандарти безпеки ISO/IEC 27002 та NIST 800–100 повинні надавати задокументовану інформацію, щоб допомогти користувачам зрозуміти їхні потреби в комп'ютерній безпеці і, таким чином, дати їм змогу вибрати відповідні засоби управління із широкого переліку існуючих засобів контролю. Однак ці стандарти не містять директив, процедур чи рекомендацій щодо здійснення заходів безпеки, але швидше сприяє більш або менш довільний, розроблений практиками індивідуально, не маючи жодної можливості порівняння результатів. У цьому документі висвітлено деякі концепції та принципи інформаційної безпеки щодо надання дієвої інформації особам, що приймають рішення, щодо управління їх корпоративними активами та забезпечення їх стійкості.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спираються автори. Дослідженню умов забезпечення інформаційної безпеки як стратегічного складника економічної безпеки держави присвячено праці В. Тамбовцева, В. Сенчагова, В. Ткаченка, Т. Іванюти, В. Похилюка, В. Третяк, А. Татаркіна.

Формулювання цілей статті **(постановка завдання)**. Метою статті є систематичний аналіз наукових підходів до основних проблем захисту інформаційної безпеки в державному управлінні.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Сьогодні організаціям доводиться стикатися з різними ризиками інформаційної безпеки. Терористичні атаки, пожежі, повені, землетруси та інші катастрофи можуть знищити засоби обробки інформації та важливі документи. Крадіжки та втрата організаційної інформації можуть спричинити серйозні наслідки для репутації бізнесу, прибутковості, довіри споживачів та загального економічного зростання. Наприклад, недолік безпеки, такий як витік кредитної картки інформації, може мати негативні результати для платіжних компаній-карток через скасування

та перевипуск компрометованих карток. Звичайно, це дорого коштує, що сильно впливає на репутацію організації та довіру споживачів. Насправді одним із найбільш швидкозростаючих інформаційних злочинів є крадіжка особистої інформації, включаючи дані про клієнтів, утрачені організаціями, які відповідали за їх управління. Такі випадки є в усьому світі та призвели до запровадження суворих національних та міжнародних законів про захист даних у багатьох країнах, які вимагають від організацій захисту персональної інформації зацікавлених сторін. Тому для організацій дуже важливо розвивати зусилля, щоб забезпечити свою здатність надійно захищати свої інформаційні активи та IT-інфраструктуру.

Оцінка OCTAVE – це керована процесом методологія, що використовується для оцінки та планування інформаційної безпеки на основі ризиків. Це допомагає організаціям визначати пріоритети та управляти ризиками інформаційної безпеки.

Підхід OCTAVE був розроблений Інститутом програмної інженерії (SEI) Університету Карнегі-Мелона в 2001 р. для вирішення проблем дотримання інформаційної безпеки, з якими стикається Міністерство оборони США. Він призначений допомогти організаціям (Alberts et al., 2001):

– розробити якісні критерії оцінки ризику на основі допусків на операційний ризик;

– визначити активи, які є критично важливими для місії організації;

– виявляти вразливості та загрози критично важливим активам;

– визначити та оцінити потенційні наслідки для організації, якщо загрози будуть здійснені;

– ініціювати коригувальні дії для зменшення ризиків та створити стратегію захисту, засновану на практиці.

OCTAVE працює у три етапи:

Етап 1: Створення профілів загроз на основі активів.

Етап 2: Визначення вразливостей інфраструктури.

Етап 3: Розроблення стратегії та планів безпеки.

Сфери стратегічної практики, запропоновані OCTAVE, коротко описуються так (Alberts et al., 2001):

1. Поінформованість про безпеку та навчання – зрозумійте, як практика інформаційної безпеки вдосконалюється завдяки навчанню.

2. Стратегія безпеки – фокусується на інтеграції питань інформаційної безпеки в бізнес-стратегію організації.

3. Управління безпекою – визначає ролі та відповідальність за інформаційну безпеку, а також підтримку керівництвом діяльності з інформаційної безпеки.

4. Політика та правила безпеки – стосується організаційних та управлінських напрямів інформаційної безпеки, включаючи відповідні норми. Ця сфера також стосується розуміння персоналом політики та забезпечення її виконання.

5. Спільне управління безпекою – включає створення передового досвіду під час роботи з третіми сторонами (підрядниками, постачальниками Інтернет-послуг, керованими постачальниками послуг, партнерами тощо).

6. Планування дій на випадок надзвичайних ситуацій/відновлення після катастроф – розглядає плани щодо протидії перебоям у бізнесовій діяльності та в системах і мережах.

Сфери оперативної практики, запропоновані OCTAVE, визначені нижче (Alberts et al., 2001):

1. Фізична безпека – включає плани та процедури фізичної безпеки; фізичний контроль доступу; моніторинг та аудит фізичної безпеки.

2. Безпека інформаційних технологій – охоплює декілька сфер, а саме: (1) управління системою та мережею; (2) засоби адміністрування системи; (3) моніторинг та аудит IT-безпеки; (4) автентифікація та авторизація; (5) управління вразливістю; (6) шифрування; (7) архітектура та дизайн безпеки.

3. Безпека персоналу – включає управління інцидентами та практику загального персоналу.

Однак існує низка державних та напівпублічних установ, які надають найкращі практики управління захистом безпеки, такі як:

1. Форум інформаційної безпеки (ISF) (https://www.securityforum.org) – надає публікацію під назвою «Стандарт належної практики», де викладаються найкращі практики інформаційної безпеки.

2. Координаційний центр із питань комп'ютерного реагування на надзвичайні ситуації (CERT/CC) при Університеті Карнегі-Меллона (http: //www.cert.org/). CERT/CC надає детальну та конкретну допомогу щодо впровадження методології безпеки.

3. Асоціація аудиту та контролю над інформаційними системами (http://www.isaca.org) – організовує кілька семінарів та занять із найкращих практик.

4. Міжнародна асоціація професійних консультантів із питань безпеки (http: //www.iapsc.org/) та Global Grid Forum (http://www.ogf.org/) – надають перелік найкращих практик.

5. Портал SearchSecurity.com (http://searchsecurity.techtarget.com/) та Центр комп'ютерних ресурсів NIST (http://csrc.nist.gov/) – це безкоштовні портали, присвячені безпеці, що включають збірки найкращих практик.

Висновки з цього дослідження і перспективи подальших розвідок. Безперечно, важливість цих стандартів створює міцну основу для програми захисту інформації. Однак потрібно кілька вдосконалень, особливо через мінливий характер цього домену. Більше того, незважаючи на обмеження методології OCTAVE, згадані раніше, вона забезпечує більш практичний підхід. Він базується на аналізі ризику активу, який чітко визначає реалістичний цільовий стан програми інформаційної безпеки.

Загалом для вирішення всіх аспектів безпеки організації спочатку визначають свої основні цілі безпеки, потім застосовують адекватні методи формалізації та перевірки свого управління і, нарешті, розробляють процедури для досягнення своїх цілей. На практиці захист програми безпеки набагато більше, ніж це, і вимагає залучення кількох змінних. Стандарти та методології безпеки дають змогу створити міцну основу для програми інформаційної безпеки.

Бібліографічний список:

1. Ткач В.О. Економічна безпека регіону як складова економічної безпеки держави. *Вісник Дніпропетровського університету. Серія «Економіка».* 2015. Вип. 4 (1). С. 113–120.

2. Варналій З. Проблеми та шляхи забезпечення економічної безпеки України. URL: http://www.rnbo.gov.ua/news /25.html (дата звернення: 20.06.2019).
3. Музиченко А.С. Організаційно-економічний механізм стимулювання інноваційної діяльності в АПК. *Економіка АПК.* 2017. № 11. С. 38–43.
4. Про основи національної безпеки України : Закон України від 19.06.2003 № 964-IV. URL : http://zakon2.rada.gov. ua/laws/show/964-15 (дата звернення: 19.06.2019).
5. Руссо Ж.Ж. Об общественном договоре. Москва : КАНОН-пресс, 1998. 416 с.
6. Корнійчук Л.Я. Історія економічних учень. URL : http://library.if.ua/book/87/6134.html (дата звернення: 01.07.2019).
7. Власюк О.С. Теорія і практика економічної безпеки в системі науки про економіку. Київ : Нац. ін-т пробл. міжнар. безпеки при Раді нац. безпеки і оборони України, 2016. 48 с.
8. Рузвельт Ф.Д. Беседы у камина Москва : ИТРК, 2017. 408 с.
9. Ермошенко Н.Н. Определение угрозы национальным интересам в финансово-кретитной сфере. *Экономика Украины.* 1999. № 1. С. 4–12.
10. Афонцев С.А. Национальная экономическая безопасность: на пути к теоретическому консенсусу. *Мировая экономика и международные отношения.* 2016. № 10. С. 30–39.
11. Татаркин А. Экономическая безопасность как объект регионального исследования. *Вопросы экономики.* 1996. № 5. С. 78–89.
12. Павловський М.А. Засади національної безпеки Україні на перехідному етапі. *Голос України.* 1997. 3 квітня.
13. Система економічної безпеки держави : монографія / за заг. ред. А.І. Сухорукова. Київ : Національний інститут проблем міжнародної безпеки при РНБО України, 2017. 685 с.

References:

1. Tkach V.O. (2015) *Ekonomichna bezpeka rehionu yak skladova ekonomichnoyi bezpeky derzhavy* [Economic security of the region as a component of economic security of the state]. Dnipropetrovsk. (in Ukrainian)
2. Varnaliy Z. (2016) *Problemy ta shlyakhy zabezpechennya ekonomichnoyi bezpeky Ukrayiny* [Problems and ways of economic security of Ukraine]. URL: http://www.rnbo.gov.ua/news /25.html. (accessed: 20.06.2019)
3. Muzychenko A.S. (2017) *Orhanizatsiyno-ekonomichnyy mekhanizm stymulyuvannya innovatsiynoyi diyalnosti v APK* [Organizational and economic mechanism of stimulation of innovation activity in agroindustrial complex]. Kyiv. (in Ukrainian)
4. "Pro osnovy natsionalnoyi bezpeky Ukrayiny" (2003) [On the Fundamentals of National Security of Ukraine]: http://zakon2.rada.gov.ua/laws/show/964-15. (accessed 19 June 2019)
5. Russo Zh.Zh. (1998) *Ob obshchestvennom dohovore.* [About a public contract]. Moskov: «KANON-press». (in Russian)
6. Korniychuk L.Ya. (2014) *Istoriya ekonomichnykh uchen* [History of Economic Studies] /: http://library.if.ua/book/87/6134.html. (accessed: 01.07.2019)
7. Vlasyuk O.S. (2016) *Teoriya i praktyka ekonomichnoyi bezpeky v systemi nauky pro ekonomiku* [The theory and practice of economic security in the system of science of economics] Kyiv. (in Ukrainian)
8. Ruzvelt F.D. (2017) *Besedy u kamyna* [Conversations at the fireplace] Moskov: YTRK. (in Russian)
9. Ermoshenko N.N. (1999) *Opredelenye uhrozy natsyonalnym ynteresam v fynansovo-kretytnoy sfere* [Definition of a threat to national interests in the financial and credit sphere] Kyiv : Ekonomyka Ukrayny. (in Ukrainian)
10. Afontsev S.A. (2016) *Natsyonalnaya ekonomycheskaya bezopasnost: na puty k teoretycheskomu konsensusu* [National Economic Security: Towards a Theoretical Consensus]. Kyiv. (in Ukrainian)
11. Tatarkyn A. (1996) *Ekonomycheskaya bezopasnost kak obekt rehionalnoho yssledovanyya* [Economic security as the object of regional research]. Kyiv. (in Ukrainian)
12. Pavlovskyy M.A. (1997) *Zasady natsionalnoyi bezpeky Ukrayini na perekhidnomu etapi* [Principles of National Security of Ukraine at the Transitional Stage] Kyiv: Holos Ukrayiny. (in Ukrainian)
13. Sukhorukova A.I. (2017) *Systema ekonomichnoyi bezpeky derzhavy* [System of economic security of the state] . Kyiv: VD «Stylos». (in Ukrainian)