УДК 330
DOI: 10.31891/2307-5740-2019-270-3-61-64

ГОНТАРЕВА І. В.
Харківський національний університет імені В.Н. Каразіна

ЕКОНОМІЧНА ОЦІНКА ВАРТОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ

Як будь-який інший економічний ресурс, інформація має вартість, яку треба не лише примножувати, але і уміти охороняти в процесі підприємницької діяльності. Найбільш розвиненим сучасним інструментом аналізу активів з такими характеристиками є методологія реальних опціонів. Кожен реальний опціон має свою специфіку, що обумовлює необхідність певної модифікації загальної методології. Оскільки за статистикою до 40 % усіх втрачань інформації пов'язані зі взаємовідносинами усередині організації і відношенням персоналу до роботи, то вартість ресурсу, що охороняється, повинна враховувати рівень і стан організаційної культури.

Ключові слова: рінго, волатильність, інформаційна безпека, структурний капітал, реальні опціони, підприємництво.

GONTAREVA I.
V. N. Karazin Kharkiv National University

ECONOMIC ASSESSMENT OF THE COST OF INFORMATION SECURITY OF ENTREPRENEURSHIP

The purpose of this article is to formulate ideas about the costs of ensuring the security of information resources for entrepreneurship as a real option value.

As any other economic resource, information has a cost, that needs not only to increase but also able to guard in the entrepreneurship process. The most developed modern instrument of analysis of assets with such descriptions is methodology of the real options. The real options are determined as valuable, rare and is difficult reproduction of capabilities or resources that create to the businessman exclusive possibilities on the choice of strategies of development of the activity. Every real option possesses the specific, that stipulates the necessity of certain modification of general methodology. For the practical use of this theory in an appendix to informative safety clarification of such her positions as expenses on an option, cost of asset and level of her is required volatility. At the choice of strategy of providing of informative safety it is necessary base to confess a structural capital, because a entrepreneur does not have legal ownership rights on employees and, accordingly, on their human capital. Nevertheless, expenses must be taken into account on defense of intellectual property arising up as a result of joint organizationally – labor activity. Because on statistics to 40 % all losses of information are related to the mutual relations into organization and relation of personnel to work, then the cost of the guarded resource must consider a level and state of organizational culture.

Coming from the features of informative safety it is necessary to come running to the indirect measuring of volatility of basic resource. Methods and indexes of the indirect measuring must follow from methodologies of estimation of basic resource in an option.

Keywords: ringo, volatility, information security, structural capital, real options, entrepreneurship

Постановка проблеми. Основною умовою прийняття ефективних рішень в підприємницькій діяльності є наявність достатньої, достовірної і своєчасної інформації. Інформація, як нематеріальний ресурс, має багато специфічних властивостей, які визначають умови її придбання і використання. В той же час, як будь-який інший економічний ресурс, вона має вартість, яку треба не лише примножувати, але і уміти охороняти. Прискорений розвиток інформаційно-комунікаційних технологій (ІКТ) значно ускладнили як традиційні проблеми інформаційної безпеки (достовірність і конфіденційність), так і створили нові мережеві загрози (хакерство і віруси).

Аналіз останніх досліджень та публікацій. Відповідно до міжнародних стандартів під інформаційною безпекою зазвичай розуміється забезпечення доступності, конфіденційності і цілісності інформації в процесі її отримання, зберігання і поширення. Якість інформації, що охороняється, характеризується поняттям її корисності для досягнення мети організації, проте методики оцінки корисності не визначені. Це утрудняє, по-перше, проведення рекомендованого стандартами функціонально-вартісного аналізу заходів по інформаційній безпеці, а, по-друге, обґрунтування економічної доцільності самих таких заходів через відсутність конвенціальної вартості ресурсу, що охороняється.

У рамках міжнародних стандартів оцінки вартості існує досить багато методів оцінки вартості нематеріальних ресурсів [3]. Виходячи з характеристик інформаційного ресурсу найбільш перспективним підходом для вирішення проблеми оцінки допустимої вартості інформаційної безпеки є теорія реальних опціонів. Для практичного використання цієї теорії в додатку до інформаційної безпеки потрібно уточнення таких її положень як витрати на опціон, вартість активу і рівень її волатильності.

Формулювання цілі статті. Метою статті є формування уявлення щодо прийняття рішень на основі витрат на забезпечення безпеки інформаційних ресурсів підприємницької діяльності як про вартість реального опціону.

Виклад основного матеріалу дослідження. В процесі підприємницької діяльності формується інформаційний актив, який корисний конкретній підприємницькій структурі, але може бути використаний і

іншими підприємницькими структурами, принаймні, в якості бази порівняння. Так, традиційний для японських підприємців спосіб прийняття інноваційних рішень «рінго». Будь-який співробітник може подати свою пропозицію, з ним зобов'язані ознайомитися і оцінити усі зацікавлені особи на усіх рівнях управління, оцінку думок і остаточне рішення по пропозиції приймає перша особа. Начебто нічого особливого, але успіхи японських фірм у безперервному поліпшенні продукції з використанням рінго загальновизнані. У плані менеджменту, рінго є накопиченим досвідом (рутиною), який приносить позитивний результат.

Цей досвід широко відомий і хоча, певною мірою, виступає як товарний знак, але не підлягає юридичному або будь-якому іншому захисту. В той же час, більшість рутин інформаційного активу підприємницької діяльності виступають елементами інтелектуальної власності конкретної підприємницької структури і можуть підлягати захисту в юридичному, технічному і організаційному планах. Раціональний рівень інформаційної безпеки залежить від внутрішньої і зовнішньої цінності ресурсу, величини збитку від порушення прав власності, вірогідності виникнення ризикових ситуацій і вартості заходів по їх відтворенню або отриманню компенсації за можливі втрати.

У економічному плані, витрати на захист інформації виступають непрямими чинниками дії на доходність підприємницької діяльності. Сама по собі інформаційна безпека не створює додаткових фінансових потоків, але сприяє збереженню наявних потоків при настанні екстремальних ситуацій типу вірусних, мережевих або спамових атак. Це утрудняє ухвалення інвестиційних рішень по проектах інформаційної безпеки з використанням методик чистого дисконтованого прибутку або коефіцієнтів капіталізації. Деякі переваги в такій ситуації має методологія реальних опціонів, яка оцінює не лише окупність проекту, але і можливі варіанти стратегічних рішень за об'ємом вирішуваних завдань, часу і етапам реалізації, допустимим витратам, мірі впливу невизначеності внутрішнього і зовнішнього середовища [3].

У загальному випадку під опціоном розуміється право на купівлю (кол-опціон) або продаж (пут-опціон) базового активу в певний момент за фіксованою ціною – строго на дату скінчення опціону (європейський опціон) або у будь-який момент до його закінчення (американський опціон). У разі інформаційної безпеки, під опціоном розумітимемо право вибору підприємця купувати або не купувати програмні і технічні засоби захисту власного інформаційного ресурсу, які дозволять йому використати цей ресурс в повному об'ємі при настанні ризикової ситуації. Виходячи з відмінностей між загальним визначенням опціону і визначенням автора, що використовується в цьому дослідженні, в доповненні до інформаційної безпеки витікає потреба в прив'язці ряду положень загальної методології опціонів до конкретної ситуації.

Реальні опціони визначаються як цінні, рідкісні і складновідторювані здібності або ресурси, які створюють підприємцеві ексклюзивні можливості по вибору стратегій розвитку своєї діяльності [4]. У відмінності від оцінок варіантів дій шляхом традиційного аналізу «витрати-результати», у вартість витрат включається ціна на право управляти ресурсом, а результати враховують допустимий рівень ризиків.

У методологічному плані теорія реальних опціонів базується на моделі фінансових опціонів Black - Scholes. Ця модель включає наступні елементи: а) біржову ціну основного ресурсу, що визначає вартість вибору стратегії; б) бажану вартість ексклюзивних прав (опціону) на продаж або купівлю основного ресурсу; в) термін дії опціону; г) волатильність біржових цін основного ресурсу; д) коефіцієнти дисконтування. Бажана вартість фінансового опціону обчислюється як різниця між вартістю ризикового і безризикового портфелів інвестицій.

У огляді J. J. Tan [5] показав, що у відомих випадках розрахунку реальних опціонів все або частина змінних вартості фінансового опціону замінюються на ті їх аналоги, які краще описують суть цілей конкретного підприємницького рішення. Зокрема, замість біржових цін можуть використовуватися ціни світового або локального ринку, а волатильність визначається через коливання загальних біржових індикаторів або обмінних курсів валют. Вартість реального опціону визначається як функція від різниці поточної вартості основного ресурсу і його очікуваної вартості з урахуванням коливання основних чинників, що впливають на ухвалення рішень.

Виходячи з мети цієї статті, надалі розглядатимемо структуру реального опціону, основним ресурсом якого є інформація, що вимагає спеціальних заходів по своєму захисту. На відміну від досліджень E. F.Brigham і J. F. Houston [0], в якості інформаційного ресурсу виступатиме не лише інтелектуальна власність, а увесь структурний капітал, наявний у підприємницькому бізнесі.

В процесі підприємницької діяльності інформація може: а) приймати різні форми – потік чуттєвої інформації, зафіксовані вимоги, систематизовані дані, апріорні і апостеріорні знання, ментальні моделі і практичні уміння; б) знаходиться на різних носіях – друкарські документи, аудіо і відео файли, постійна і оперативна пам'ять комп'ютера і, звичайно, людська пам'ять; в) мати специфіку на особовому і організаційному рівнях – по складу і якості, по способах і методах застосування. З певною мірою точності можна вважати, що об'єм і специфічність роботи з інформацією на особистому рівні є людським капіталом, а на організаційному – структурним.

При виборі стратегії забезпечення інформаційної безпеки базовим слід визнати структурний капітал, оскільки підприємець не має юридичних прав власності на співробітників і, відповідно, на їх людський капітал. Проте, мають бути враховані витрати на захист інтелектуальної власності, що виникла в результаті спільної організаційно-трудової діяльності. Зазвичай це робиться шляхом включення в структурний

капітал вартості організаційної культури в частини інформаційної безпеки. Окрім організаційної культури в структурний капітал входить: а) задокументовані дані про суб'єктів, об'єкти і процеси підприємницької діяльності; б) нормативно-правова, организационно-распорядительская, планова і методична документація; в) бази даних про моніторинг внутрішнього і зовнішнього середовища; г) аналітичні і експертні прогнози і оцінки; г) результати науково-дослідних, дослідно-конструкторських і проектних робіт; д) права на об'єкти інтелектуальної власності.

Починаючи з робіт Дж. Тобина різниця між ринкової і балансової вартостями компанії відносять на рахунок її нематеріальних, у тому числі інформаційних активів. Зараз розвиток методології оцінювання нематеріальних активів йде по напряму деталізації нематеріальних активів, уточнення їх зв'язку з рівнем капіталізації компанії, а також розширення баз порівняння при визначенні додаткової доходності. До найбільш відомих методик оцінки вартості структурного капіталу можна віднести наступні: метод коефіцієнтів вкладу матеріального людського і структурного капіталів в додану вартість підприємницької структури; метод порівняння інформаційної продуктивності менеджменту в галузі; метод доданої економічної вартості.

Вибір конкретного методу оцінки вартості нематеріального активу залежить від цілей такої оцінки і наявності інформації, що релевантна цьому методу. У розрахунках реальних опціонів вибір оцінки вартості основного ресурсу далі впливає на характеристики точності зробленої оцінки.

У моделі Блека-Шоулза волатильність ціни основного ресурсу визначається як передбачуваний діапазон відхилення поточного значення на термін виконання опціону. Для ресурсів, якими постійно торгують, очікуване максимальне і мінімальне відхилення приблизно симетричні відносно поточної ціни і пропорційні величині апріорного стандартного відхилення. Проте, для інформаційної безпеки ситуація інша. По-перше, структурні нематеріальні ресурси як і засоби їх захисту неоднорідні; по-друге, вони рідко є предметом торгу; по-третє, чекати додаткового прибутку від її придбання не доводиться, а ось збитки від їх відсутності цілком реальні.

Зокрема, за даними компанії «Лабораторія Касперского» [9] у підприємств малого і середнього бізнесу найчастіше викрадають операційні дані (рис. 1, *а*), а вони найбільше захищають інформацію про клієнтів (рис. 1, *б*). Більше того практично відсутній захист смартфонів співробітників, а через них проходить великий об'єм операційної інформації, особливо при роботі в системі Internet.

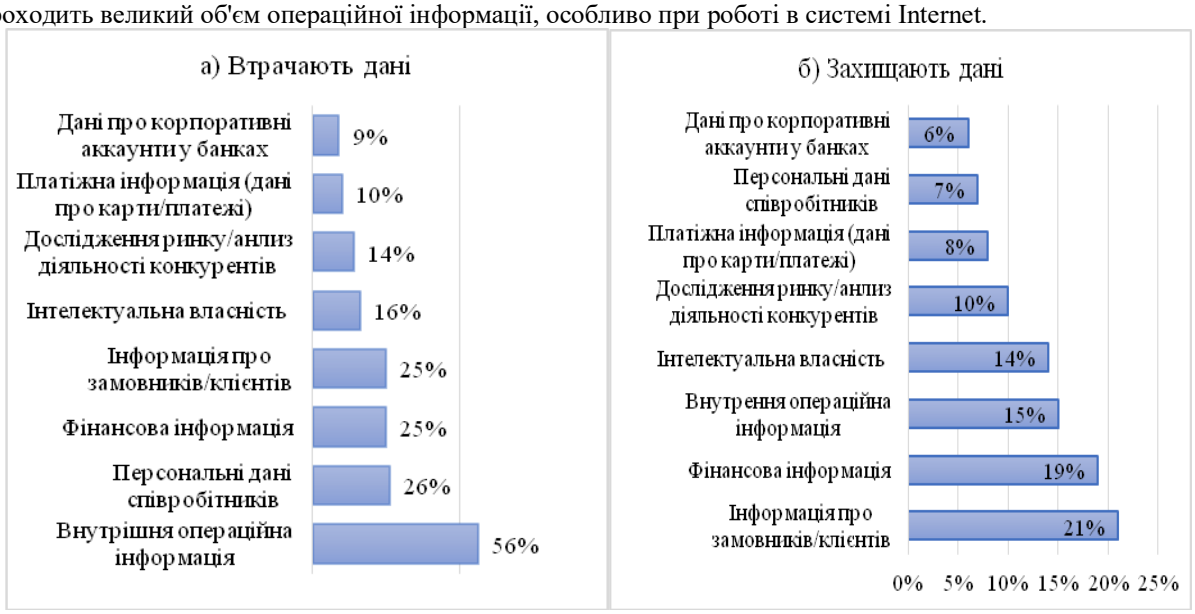

Рис. 1. Види даних, які компанії найбільше: *а*) втрачають; *б*) захищають [9]

Виходячи з особливостей інформаційної безпеки слід прибігати до непрямих вимірів волатильносі основного ресурсу. Способи і показники непрямих вимірів повинні витікати з методик оцінки основного ресурсу в опціоні.

Висновки. Забезпечення інформаційної безпеки обов'язкова умова здійснення підприємницької діяльності. При цьому корисність засобів захисту залежить від цінності того ресурсу, який вони захищають, – інформаційного (структурного) капіталу підприємства. Сама по собі інформаційна безпека не створює додаткових фінансових потоків, але сприяє збереженню наявних потоків при настанні екстремальних ситуацій типу вірусних, мережевих або спамових атак. Найбільш розвиненим сучасним інструментом аналізу активів з такими характеристиками є методологія реальних опціонів. Кожен реальний опціон має свою специфіку, що обумовлює необхідність певної модифікації загальної методології.

Оскільки за статистикою до 40 % усіх просочувань інформації пов'язані зі взаємовідносинами усередині підприємницької структури і відношенням персоналу до роботи, то вартість ресурсу, що охороняється, повинна враховувати рівень і стан організаційної культури. Виходячи з особливостей

інформаційної безпеки слід прибігати до непрямих вимірів волатильності основного ресурсу. Способи і показники непрямих вимірів повинні витікати з методик оцінки основного ресурсу в опціоні, що і буде напрямом подальших досліджень.

Література

1. Wood C. C. Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature // Computer Fraud & Security, 2004. – 1. – P. 16-17.

2. ISO/IEC 13335-1:2004 Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management [Electronic resource], 2004. Access mode: https://www.sis.se/api/document/preview/905483/

3. Damodaran A. Investment Valuation: Tools and Techniques for Determining the Value of Any Asset, Third Edition. New Jersey: John Wiley & Sons, Inc., 2012. 974 p.

4. McGrath R. G., Ferrier W. J., Mendelow A. L. Response: Real Options as Engines of Choice and Heterogeneity // The Academy of Management Review, 2004. Vol. 29, No. 1. P. 86-101.

5. Tan J. J. Interfaces for enterprise valuation from a real options lens // Strategic Change. January 2018, Volume27, Issue1, Special Issue: Mergers & Acquisitions, P. 69-80.

6. Brigham Eugene F., Houston Joel F. Fundamentals of Financial Management 12th Edition. — South-Western College, 2009. – 752 p.

7. Stewart T. A. Intellectual capital: the new wealth of organizations New York: . Doubleday, 1997. – 404 p.

8. Cyber Security Culture in organisations - The European Union Agency for Network and Information Security(ENISA) [Electronic resource], November 2017. Access mode: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations/at download/fullReport

9. Информационная безопасность бизнеса. Исследование текущих тенденций в области информационной безопасности бизнеса, Лаборатория Касперского [Электронный ресурс], 2014. – Режим доступа: https://media.kaspersky.com/pdf/IT_risk_report_ Russia_2014.pdf

References

1. Wood C.C. Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature // Computer Fraud & Security, 2004. – P. 16-17.

2. ISO/IEC 13335-1:2004 Information technology -- Security techniques - Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management [Electronic resource], 2004. Access mode: https://www.sis.se/api/document/preview/905483/

3. Damodaran A. Investment Valuation: Tools and Techniques for Determining the Value of Any Asset, Third Edition. New Jersey: John Wiley & Sons, Inc., 2012. 974 p.

4. McGrath R. G., Ferrier W. J., Mendelow A. L. Response: Real Options as Engines of Choice and Heterogeneity // The Academy of Management Review, 2004. Vol. 29, No. 1. P. 86-101.

5. Tan J. J. Interfaces for enterprise valuation from a real options lens // Strategic Change. January 2018, Volume27, Issue1, Special Issue: Mergers & Acquisitions. P. 69-80.

6. Brigham Eugene F. & Houston Joel F. Fundamentals of Financial Management 12th Edition. — South-Western College, 2009. – 752 p.

7. Stewart T. A. Intellectual capital: the new wealth of organizations New York: Doubleday, 1997. – 404 p.

8. Cyber Security Culture in organisations - The European Union Agency for Network and Information Security(ENISA) [Electronic resource], November 2017. Access mode: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations/at download/fullReport

9. Informatsionnaya bezopasnost' biznesa. Issledovaniye tekushchikh tendentsiy v oblasti informatsionnoy bezopasnosti biznesa, Laboratoriya Kasperskogo, [Elektroniy resurs], 2014. – Regim dostupa: https://media.kaspersky.com/pdf/IT_risk_report_Russia_2014.pdf

Рецензія/Peer review : 07.05.2019 Надрукована/Printed : 04.06.2019
Рецензент: д. е. н., проф. Орлов О. О.