ТЕХНІЧНІ НАУКИ

DOI: https://doi.org/10.32839/2304-5809/2019-11-75-142
УДК 004.056.53

Архипов О.Є., Теплицька Т.П.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

АДАПТИВНИЙ ПІДХІД ДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Анотація. У статті сформульовано основні аспекти адаптивного підходу до управління інформаційною безпекою. Виділено чотири рівні адаптації відповідно до моделей потенційного атакуючого. Запропоновано спосіб обчислення прийнятного (ефективного) обсягу інвестицій у систему захисту інформації (СЗІ), структура і функції якої формуються виходячи із принципу адаптивного управління ІБ організації. В залежності від існуючих умов, для захисту від потенційного атакуючого, означеного як Scriptkiddie, найбільш прийнятними є інвестиції у СЗІ в обсязі до 25% від вартості активів, що підлягають захисту, для професіонала цей обсяг збільшується до 50%. Аналізуючи отримані результати, приходимо до висновку, що, в залежності від цінності інформаційних активів організації, рівня її зрілості, характеристик потенційного атакуючого, можна розрахувати прийнятний обсяг інвестицій в СЗІ для будь-якої організації індивідуально. Отримані розрахунки дають можливість побудувати для організації найбільш ефективну та економічно виправдану стратегію захисту.

Ключові слова: адаптивний підхід, управління інформаційною безпекою, обсяг інвестицій, атака, захист.

Arkhypov Oleksandr, Teplytska Tetiana
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"

ADAPTIVE APPROACH TO INFORMATION SECURITY MANAGEMENT

Summary. The continued growth of successful cyber attacks on information systems and resources of enterprises and institutions is, on the one hand, a consequence of the increase in the aggressiveness of cybercriminals, which causes a direct increase in the total number of attacks, and on the other – a testimony to the qualitative enhancement of the potential of these attacks, in particular the improvement of the software and organization of the attacking party, support of the attack, its level of intellectual support. Under these conditions, the protection party must develop and implement information security policies that are adequate in content and level to attack. The article outlines the main aspects of an adaptive approach to information security management. Four levels of adaptation are identified according to the models of the potential attacker. A method of calculating an acceptable (effective) amount of investment in the construction of an information security system is proposed, the structure and functions of which are formed on the basis of the principle of adaptive management of the organization's IB. Methods of game theory are considered, among which the game with nonzero sum is chosen for solving the problem. For the first two levels of adaptation, the chosen type of games is built and with the help of the Nash equilibrium an acceptable level of investment in the construction of the defense system is obtained. Depending on the current conditions, to protect against a potential attacker referred to as Scriptkiddie, the most appropriate investment is up to 25% of the value of the assets to be protected, for a professional, this amount increases to 50%. Analyzing the results, we conclude that, depending on the value of the information assets of the organization, the level of its maturity, the characteristics of the potential attacker, it is possible to calculate an acceptable amount of investment in the GIS for any organization individually. The calculations obtained make it possible to build for the organization the most effective and economically justified defense strategy.

Keywords: adaptive approach, information security management, investment volume, attack, defense.

Постановка проблеми. Триваюче зростання успішних кібератак на інформаційні системи та ресурси підприємств і установ з одного боку є наслідком росту агресивності кіберзлочинців, що обумовлює пряме збільшення загальної кількості атак, а з іншого – свідоцтвом якісного підсилення потенціалу цих атак, зокрема покращенням програмно-технічного забезпечення атакуючої сторони, організаційного супроводу атаки, рівня її інтелектуальної підтримки. За цих умов сторона захисту мусить розробляти і впроваджувати політики інформаційної безпеки, за своїм змістом та рівнем адекватні атакуючим діям.

Аналіз останніх досліджень та публікацій. Аналізуючи розвиток стандартів у області інформаційної безпеки, можна розділити існуючі документи на дві групи [1]. Першу започатковано від найстарішого стандарту в галузі інформаційної безпеки – «Помаранчевої книги». Сюди також належать розроблені пізніше «Федеральні критерії», «Канадські критерії», а сучасним представником даної гілки виступають «Загальні критерії оцінки безпеки інформаційних технологій» – ISO/IEC 15408. Основною концепцією стандартів цієї групи є захист «із повним перекриттям», орієнтація на статичні, замкнуті системи, що зазвичай типові для військової сфери, однак вкрай нехарактерні для комерційної.

До другої ж групи віднесемо стандарти, що базуються на стандартах серії BS 7799 (British Standards) і за своїм змістом інтегруються із

стандартами якості менеджменту серії ISO 900X. Саме з даної групи стандартів беруть початок основні принципи управління інформаційною безпекою. Сучасними представниками документів цієї групи є серія стандартів ISO/IEC 2700X. Важливою відмінністю даних стандартів від першої групи є регламентування ризик-орієнтованого підходу до управління інформаційною безпекою (УІБ). Проте застосування даного підходу на практиці викликає певну кількість запитань. Зокрема для великих організацій із складною ієрархічною структурою розрахунок їх інтегральних ризиків являє трудомістку довготривалу процедуру, результати якої виявляться приблизними та неоднозначними. Крім того, вельми суб'єктивним є формування переліку адекватних загроз: перестраховка, намагання не пропустити істотної загрози призводить до невиправданого розширення складу переліку загроз, що у свою чергу тягне за собою надлишкові інвестиції у створення системи захисту інформації (СЗІ).

Це питання є дуже болісним і важливим для комерційних організацій, виникає потреба у перегляді використовуваних підходів до формування базових принципів побудови СЗІ та політик УІБ в цілому, підсиленні в них ваги економічної складової, формування цих політик залежно від потенціалу та спроможності атакуючої сторони, адаптуючись до особливостей її поведінки, ймовірних намірів та можливостей.

Виділення нерозв'язаних раніш частин загальної проблеми. Аналізуючи дослідження та публікації, можна прийти до висновку, що однією із нерозв'язаних досі задач УІБ є визначення оптимального рівня інвестицій в побудову системи захисту, адекватну за своїм рівнем ступеню загроз, існуючих з боку атакуючої сторони.

Мета статті. Ціллю статті є формулювання основних аспектів адаптивного підходу до УІБ та визначення оптимального рівня інвестицій в побудову СЗІ.

Виклад основного матеріалу. Існуючі механізми захисту, що вже реалізовані на серверах автентифікації, системах розмежування доступу, є дієвими лише під час здійснення атаки. По суті дані механізми захищають від атак, що вже перебувають в процесі реалізації. Проте для організацій значно більш доцільним та ефективним є попередження атак, тобто запобігання самих передумов необхідних для реалізації вторгнення.

Поняття управління з адаптацією (адаптивне управління) – це управління в системі з неповної апріорної інформацією про керований процес, яке змінюється (адаптується) в міру накопичення інформації і застосовується з метою поліпшення якості роботи системи [2]. В даній роботі адаптація розглядається як залучення додаткових відомостей про потенційного зловмисника при побудові стратегії управління інформаційною безпекою.

Оскільки, результативність реалізації загроз багато в чому залежить від компетенції та ресурсів атакуючого, врахування цих факторів є обов'язковою умовою при визначенні рівня інвестицій в розробку СЗІ. Одним із перспективних рішень для врахування «інтересів» атакуючої сторони може стати застосування рефлексивних моделей ризику. Такий підхід вже розглядався у роботах [3; 4]. В залежності від характеристик потенційного атакуючого, формуються моделі, що відображають специфічні характеристики поведінки атакуючої сторони. Аналіз сформованих рефлексивних моделей дозволяє для кожної відповідної ситуації оцінити необхідний обсяг інвестицій в СЗІ. В залежності від характеристик потенційного атакуючого можна виділити наступні рівні адаптації:

Рівень 1. В ролі атакуючої сторони розглядається «повсякденний хакер» (скрипткідді, scriptkiddie) – одинак з доволі невеликим досвідом проведення атак (або взагалі без досвіду), обмежений у фінансових ресурсах, без достатньої підготовки та знань для написання експлойта або складної програми, який використовує для реалізації атаки на комп'ютерні системи і мережі вже існуючі скрипти або програми, загалом розуміючи механізм їх дії, але не здатний до самостійної реалізації ефективних рішень для здійснення атак. Таким чином, атаками, очікуваними від даного атакуючого, є найбільш популярні і вже відомі атаки. Організаціям, для яких потенційним атакуючим є скрипткідді достатньо реалізувати базовий рівень захисту. До методів, що дозволяють організувати даний рівень захисту можна віднести: аутентифікація, розмежування доступу, використання антивірусного програмного забезпечення, брендмауерів, протоколювання та аудит, реагування на інциденти ІБ і т.д.

Рівень 2. Атакуючу сторону представляє професіонал або група професіоналів, що володіє необхідними знаннями, навичками і достатнім досвідом реалізації атак. Для такого зловмисника хакинг – це основна діяльність, що носить відверто комерційний характер. Атакуючий-професіонал зазвичай у своєму розпорядженні має достатні фінансові ресурси, але для нього, існують певні обмеження, що накладаються можливими наслідками розкриття. Для такого атакуючого, окрім найпопулярніших атак, мають місце соціальна інженерія, фішинг. Як зазначено у роботі [5], людина є найменш надійною ланкою в системі захисту інформації. З усіх відомих вдалих спроб злочинів у сфері комп'ютерної інформації переважна більшість була скоєна за допомогою спільників в установі (інсайдерів), або за допомогою недостатньо кваліфікованих в галузі інформаційної безпеки працівників, які не змогли розпізнати загрозу і зловмисника. Наслідками таких злочинів зазвичай є порушення конфіденційності корпоративної інформації фірм, підприємств, установ і закладів. Найчастіше соціальну інженерію надзвичайно недооцінюють в процесі створення організаційних заходів та комплексних систем захисту інформації, а також у процесі самої діяльності організації. На людський чинник звертають дедалі менше уваги. Тому на даному рівні адаптації важливим аспектом протидії атакуючому, окрім базового рівня захисту, є підвищення рівня обізнаності персоналу у сфері інформаційної безпеки. Також важливим аспектом є побудова проактивного захисту – використання поведінкових аналізаторів та блокувачів, що допомагають розпізнати та заблокувати підозрілі дії. Застосування таких технологій потребує грамотного налаштування та вчасного коригування.

Рівень 3. Атакуюча сторона – «Професіонал-виконавець». В такому сценарії для досягнення своїх цілей зловмисник користується послугами найманого виконавця, зобов'язаного за будь-яких обставин виконати свою роботу. Як правило, в попередніх сценаріях для ситуації «атака-захист» сторони в своїх діях керуються принципом економічної доцільності. Особливість професіоналу в тому, що, як правило, у зв'язку з особливою важливістю поставленого перед професіоналом-виконавцем завдання, він може розраховувати на залучення для підтримки своїх дій різні додаткові ресурси: фінансові, технічні, інформаційно-аналітичні, оперативні. На практиці це означає можливість реалізації дуже високозатратних та складних атак. При цьому успішність реалізації загрози атакуючою стороною являється практично гарантованою. Типовим прикладом подібної ситуації є виконання особливо важливого завдання співробітником спецслужби, що є професіоналом, підготовленим до здійснення дій в кіберпросторі [3].

При проведенні цільових атак такі зловмисники часто використовують так звані загрози нульового дня. Тобто віруси або експлойти, що були написані спеціально для атаки на конкретну організацію і ще не потрапили в сигнатурні бази традиційних засобів захисту. Важливою складовою СЗІ на даному рівні можна вважати пісочниці, що дозволяють виявити шкідливі дії в безпечному середовищі, де злочинна програма може намагатися нашкодити наскільки можливо і без будь-якого результату. Пісочниця – ізольоване безпечне середовище, яке імітує операційну систему з усіма її компонентами – драйверами, налаштуваннями, поширеним ПЗ і т. д. У пісочниці можна запускати підозрілі файли і програми, щоб відстежувати їх поведінку і розбиратися в призначенні, не піддаючи небезпеці мережу організації і кінцеві точки. Таким чином це безумовно важливий елемент в системі інформаційної безпеки кожної організації.

Пісочниці можуть працювати як окреме апаратне рішення, так і в якості віртуального або хмарного сервісу (застосовується і комбінація цих методів). При цьому вважається, що найефективнішим рішенням є саме апаратне забезпечення. Апаратні рішення поставляються і як самостійні засоби, і як частина комплексних продуктів по боротьбі з цільовими атаками та іншими загрозами. Тому для реалізації даного методу захисту (як і на попередньому рівні) важливим є грамотний підхід до обрання та конфігурації пісочниць.

Рівень 4. «Хактивіст» – це ідейний хакер («кібер-активіст»). Головною метою такого зловмисника є просування в кіберпростір політичних або соціальний ідей (нерідко досить сумнівного характеру), що організує акції громадської «електронної» непокори в кіберпросторі, який намагається привернути увагу оточення, влади (іноді в досить жорсткій формі) до тих чи інших питань і проблем сучасного суспільства шляхом синтезу соціальної активності і хакерства. На даному рівні пісочниці можуть виявитися не досить ефективними, адже існують спеціальні «детектори», що дозволяють виявити пісочниці. Одним із можливих варіантів засобів захисту для даного сценарію можуть стати пастки та помилкові інформаційні системи. Такі системи імітуючи тематичне наповнення справжніх комп'ютерних систем організації допомагають непомітно для атакуючого виявляти, спостерігати, досліджувати та запобігати спробам реалізації атак. Проте усі зазначені засоби захисту можуть виявитися малоефективними в тому випадку, коли атакуючий реалізовує сучасну складну спрямовану кібератаку (APT).

Важливим аспектом в управлінні інформаційною безпекою є визначення необхідного рівня інвестицій в побудову системи захисту інформації (СЗІ). Адаптивний підхід до УІБ, як вже було зазначено вище, дозволяє вирішити цю задачу за допомогою залучення додаткових відомостей про потенційного атакуючого. В якості методу визначення оптимального рівня інвестицій в СЗІ використаємо методи теорій ігор. Так, наприклад, побудуємо та розглянемо дві гри, що будуть відповідати першим двом рівням адаптації: скрипткідді та професіонал.

В даній грі беруть участь два гравця: атакуюча сторона (А) та організація, що захищається (З). Оскільки виграш зловмисника при вдалій спробі реалізації атаки далеко не завжди сумірний з програшем організації в даному сценарії – будемо розглядати гру з ненульовою сумою.

Для кожної із сторін визначимо набір стратегій в грі наступним чином: Стратегії захисту відрізнятимуться сумою інвестицій в побудову СЗІ, що представлена у вигляді відсотку від вартості захищаємого ресурсу. Оскільки інвестування в СЗІ не вважається ефективним при перевищенні вартості самого ресурсу, що захищається, будемо розглядати лише такі стратегії, за яких $c < q$, де c – сума інвестицій в побудову СЗІ у відсотках, q – вартість захищаємого ресурсу. Таким чином, стратегії гравця З (захист) можна представити у вигляді множини: *{0,05; 0,25; 0,5; 0,75; 0,95}*.

Стратегії атакуючих будуть відрізнятися витратами атакуючих на реалізацію атаки. За [6] витрати на реалізацію атак для Scriptkiddie та Професіоналу дорівнюють відповідно $100 і $1000. Проте в інших джерелах [7] вказуються інакші дані. Так, наприклад, вважається, що Scriptkiddie не вкладає ніяких фінансових капіталів в реалізацію атаки. Тому сформуємо стратегії таким чином: Scriptkiddie *{0, $50, $100}* та Професіонал *{$500, $750, $1000}*.

Очевидно, що виграш зловмисника в разі вдалої реалізації атаки складатиме різницю між вартістю отриманого в результаті ресурсу та витратами, задіяними на підготовку та реалізацію атаки. Оскільки виграш атакуючого залежить також від його мотивації, задіяних ресурсів та рівня захищеності ресурсу, при розрахунку виграшу будемо враховувати ймовірність успішної атаки. Визначимо функцію виграшу для гравця А наступним чином:

$$\pi_A = (g - D) P_{усп.},$$

де g – вартість атакуємого ресурсу для злочинника, D – витрати на реалізацію атаки, $P_{усп.}$ –імовірність успішної атаки.

Задамо функцію виграшу для грака З наступним чином:

$$\pi_З = -qP_{усп.} - cq.$$

Ймовірність успішної атаки будемо розраховувати за формулами, отриманими в роботі [3]. Відповідно для атакуючого Скрипткідді ймовірність успішної атаки визначатимемо за формулою:

$$P_{усп.} = \frac{q}{q + sc},$$

де s – рівень зрілості організації. Кількісну оцінку рівня зрілості можна отримати застосувавши методику, наведену в [8]. Для даних розрахунків було використано значення $s \in [20,60]$.

Ймовірність успішної атаки Професіоналом визначатимемо за допомогою формули [3]:

$$P_{усп.} = \frac{q}{q + s\frac{c^2}{D}},$$

Розглянемо декілька прикладів побудованих ігор.

Для вирішення гри було використано рівновагу Неша. Підкреслено стратегії, що є оптимальними за даною рівновагою. Отже, для потенційного атакуючого Scriptkiddie найбільш оптимальним

Таблиця 1

Результати гри з ненульовою сумою для атакуючого Scriptkiddie при *q = $1200*

	Scriptkiddie D = 0	**Scriptkiddie D = 50**	**Scriptkiddie D = 100**
c = 0,05*q	-860, 800	-860, 766	-860, 733
c = 0,25*q	-642, 342	-642, 328	-642, 314
c = 0,5*q	-800, 200	-800, 191	-800, 183
c = 0,75*q	-1041, 141	-1041, 135	-1041, 129
c = 0,95*q	-1254, 114	-1254, 109	-1254, 104

Джерело: розроблено авторами

Таблиця 2

Результати гри з ненульовою сумою для атакуючого Професіоналу при *q = $1200*

	Професіонал D = 500	**Професіонал D = 750**	**Професіонал D = 1000**
c = 0,05*q	-1192, 660	-1213, 432	-1225, 194
c = 0,25*q	-780, 280	-900, 225	-985, 114
c = 0,5*q	-771, 100	-840, 90	-900, 50
c = 0,75*q	-982, 48	-1020, 45	-1054, 25
c = 0,95*q	-1192, 30	-1217, 29	-1241, 16

Джерело: розроблено авторами

Таблиця 3

Результати гри з ненульовою сумою для атакуючого Scriptkiddie при *q = $1500*

	Scriptkiddie D = 0	**Scriptkiddie D = 50**	**Scriptkiddie D = 100**
c = 0,05*q	-1075, 1000	-1075, 966	-1075, 933
c = 0,25*q	-803, 428	-803, 414	-803, 400
c = 0,5*q	-1000, 250	-1000, 241	-1000, 233
c = 0,75*q	-1301, 176	-1301, 170	-1301, 164
c = 0,95*q	-1567, 142	-1567, 138	-1567, 133

Джерело: розроблено авторами

Таблиця 4

Результати гри з ненульовою сумою для атакуючого Професіонал при *q = $1500*

	Професіонал D = 500	**Професіонал D = 750**	**Професіонал D = 1000**
c = 0,05*q	-1470, 930	-1503, 714	-1520, 481
c = 0,25*q	-896, 338	-1041, 340	-1149, 258
c = 0,5*q	-926, 117	-1000, 125	-1065, 105
c = 0,75*q	-1208, 55	-1247, 61	-1283, 52
c = 0,95*q	-1478, 35	-1503, 39	-1528, 34

Джерело: розроблено авторами

Таблиця 5

Результати гри з ненульовою сумою для атакуючого Scriptkiddie при *q = $1800*

	Scriptkiddie D = 0	**Scriptkiddie D = 50**	**Scriptkiddie D = 100**
c = 0,05*q	-1290, 1200	-1290, 1166	-1290, 1133
c = 0,25*q	-964, 514	-964, 500	-964, 485
c = 0,5*q	-1200, 300	-1200, 291	-1200, 283
c = 0,75*q	-1561, 211	-1561, 205	-1561, 200
c = 0,95*q	-1881, 171	-1881, 166	-1881, 161

Джерело: розроблено авторами

Таблиця 6

Результати гри з ненульовою сумою для атакуючого Професіоналу при *q = $1800*

	Професіонал D = 500	**Професіонал D = 750**	**Професіонал D = 1000**
c = 0,05*q	-1741, 1192	-1788, 990	-1812, 765
c = 0,25*q	-1003, 400	-1170, 420	-1297, 376
c = 0,5*q	-1080, 130	-1157, 150	-1227, 145
c = 0,75*q	-1434, 61	-1474, 72	-1511, 71
c = 0,95*q	-1763, 38	-1789, 46	-1814, 46

Джерело: розроблено авторами

є обсяг інвестицій до 25% від вартості активів, що підлягають захисту. Для професіоналу необхідний обсяг інвестицій збільшується – до 50%. Також при проведенні розрахунків було виявлено, що при зростанні рівня зрілості організації до значень 40 балів та вище оптимальний обсяг інвестицій в СЗІ при потенційному атакуючому професіоналу зменшується майже до 25%.

Висновки і перспективи. Запропоновано спосіб обчислення прийнятного (ефективного) обсягу інвестицій у СЗІ, структура і функції якої формуються виходячи із принципу адаптивного управління ІБ організації. В залежності від існуючих умов, для захисту від потенційного атакуючого, означеного як Scriptkiddie, найбільш прийнятними є інвестиції у СЗІ в обсязі до 25% від вартості активів, що підлягають захисту, для професіонала цей обсяг збільшується до 50%. Аналізуючи отримані результати, приходимо до висновку, що, в залежності від цінності інформаційних активів організації, рівня її зрілості, характеристик потенційного атакуючого, можна розрахувати прийнятний обсяг інвестицій в СЗІ для будь-якої організації індивідуально. Отримані розрахунки дають можливість побудувати для організації найбільш ефективну та економічно виправдану стратегію захисту.

Список літератури:

1. Архипов О.Є., Теплицька Т.П. Еволюція методології захисту інформації на прикладі аналізу стандартів безпеки. Матеріали XVI Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених. «Теоретичні і прикладні проблеми фізики, математики та інформатики», т. ІІ (26-27 квітня 2018 р., м. Київ). Київ : КПІ ім. Ігоря Сікорського, Видавництво «Політехніка», 2018. С. 130–132.
2. Карпов Л.Е., Юдин В.Н. Адаптивное управление по пре-цедентам, основанное на классификации состояний управляемых объектов. URL: http://citforum.ru/consulting/BI/karpov/#ref_1 (дата звернення: 20.11.2019).
3. Архипов А.Е. Применение экономико-стоимостных моделей информационных рисков для оценивания предельных объемов инвестиций в безопасность информации. *Захист інформації.* 2015. Том 17, № 3. С. 21–218.
4. Архипов А.Е. Экономические аспекты информационной безопасности. Матеріали міжнародної наукової конференції. ISBN 978-617-7273-36-2. Херсон : Видавництво ПП Вишемирський В.С., ХНТУ, 2016. С. 23–25.
5. Саймон В., Митник К. Искусство вторжения. Москва : ДМК-Пресс, Компания АйТи, 2005. 282 с.
6. Вахний Т.В., Гуц А.К. Теория игр и защита компьютер-ных систем. Омск : Издательство ОмГУ, 2013. 160 с.
7. Dorothy E. Denning, Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influenc-ing Foreign Policy: Global Problem Solving Information Technology and Tools, 1999. URL: https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influen cing-foreign-pol-icy-2/ (дата звернення: 29.10.2019).
8. Руководство по управлению рисками безопасности. Группа разработки решений Майкрософт побезопасности и соответствию, регулятивным нормам и Центр Microsoft security center of excellence. URL: http://infoeto.ru/download/rukovodstvo-po-upravleniyu-riskami-bezopasnosti.doc (дата звернення: 28.10.2019).

References:

1. Arkhypov, O., & Teplytska, T. (2018). Evoliutsiia metodolohii zakhystu informatsii na prykladi analizu standartiv bezpeky [The evolution of information security methodology as an example of security standards analysis]. Materialy KhVI Vseukrainskoi naukovo-praktychnoi konferentsii studentiv, aspirantiv ta molodykh vchenykh. «Teoretychni i prykladni problemy fizyky, matematyky ta informatyky». Kyiv Igor Sikorsky KPI, «Politekhnika», pp. 130–132.
2. Karpov, L.E., & Yudyn, V.N. (2007). Adaptyvnoe upravlenye po pretsedentam, osnovannoe na klassyfykatsyy sostoianyi upravliaemykh obiektov [Adaptive case management based on the classification of states of managed objects]. URL: http://citforum.ru/consulting/BI/karpov/#ref_1 (accessed 20 November 2019).
3. Arkhypov, A.E. (2015). Prymenenye ekonomyko-stoymostnikh modelei informatsyonnikh ryskov dlia otsenyvanyia predelnikh obiemov investytsyi v bezopasnost informatsyy [Application of economic-cost models of information risks for estimation of the limits of investments in information security]. *Zakhyst informatsii*, vol. 17, no. 3, pp. 211–218.
4. Arkhypov, A.E. (2016). Ekonomycheskye aspekty informatsyonnoi bezopasnosty [Economic aspects of information security]. Materialy mizhnarodnoi naukovoi konferentsii. Kherson: PP Vyshemyrskyi V.S., KhNTU, pp. 23–25.
5. Saimon, V., & Mytnyk, K. (2005). Yskusstvo vtorzhenyia [The art of invasion]. Moskva: DMK-Press, Kompanyia AiTy, p. 282.
6. Huts, A. K., & Vakhnyi, T. V. (2013). Teoryia yhr y zashchyta kompiuternykh system [Game theory and computer system protection]. Omsk: OmHU, p. 160.
7. Dorothy, E. Denning (1999). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy: Global Problem Solving Information Technology and Tools. URL: https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-pol-icy-2/ (accessed 29 October 2019).
8. Rukovodstvo po upravlenyiu ryskamy bezopasnosty. Hruppa razrabotky reshenyi Maikrosoft po bezopasnosty y sootvetstvyiu, rehuliatyvnym normam y Tsentr Microsoft security center of excellence [Safety Risk Management Guide. Microsoft Security and Compliance, Regulatory Development Team, and Microsoft Security Center of excellence]. URL: http://infoeto.ru/download/rukovodstvo-po-upravleniyu-riskami-bezopasnosti.doc (accessed 28 October 2019).