DOI: **10.33099/2311-7249/2019-34-1-109-114**

УДК: 355.424:004.056

Михайло Миколайович Алексєєв

Національний університет оборони України імені Івана Черняховського, Київ, Україна

АНАЛІЗ МЕТОДОЛОГІЧНИХ ПІДХОДІВ ЩОДО ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ УПРАВЛІННЯ РИЗИКАМИ У СФЕРІ КІБЕРБЕЗПЕКИ

Широке застосування сучасних інформаційних технологій у секторі безпеки і оборони водночас обумовлює виникнення нових загроз національній та міжнародній безпеці. Актуальними сьогодні стають таки поняття як "кіберзброя" та "кібервійна". Поряд із інцидентами природного походження зростає кількість та потужність кіберзагроз. Найважливішим завданням для нашої держави стає напрацювання теоретичних основ для визначення оптимальних, в умовах обмежених можливостей, кроків на шляху створення ефективної системи забезпечення кібербезпеки України.

Оцінюючи високий ступінь кіберзагроз для держави та суспільства впродовж останніх років все більше підштовхують фахівців у сфері кібернетичної безпеки до застосування технологій управління ризиками. Тому в статті проводиться аналіз методологічних підходів щодо застосування технологій управління ризиками у сфері кібербезпеки.

***Ключові слова**: кібербезпека, управління ризиками, стратегії управління ризиками.*

Вступ

Тенденції розвитку сучасних світових подій все частіше свідчать про зростання ескалації не лише в традиційному геостратегічному просторі, але й перенесення протиборства провідних держав у штучно створену "віртуальну" реальність – кібернетичний простір, світ електронних засобів масової комунікації та управління.

Постановка проблеми. Відповідно до ключових положень Стратегії національної безпеки США [1] сучасні кібернетичні загрози є одним з найбільших викликів державній, суспільній та економічній безпеці, що повстали перед нацією. У рамках зв'язків із суспільством посадовці Агенції національної безпеки США (АНБ) постійно фокусують увагу американського населення на зростанні масштабів кібернетичних атак проти Сполучених Штатів. При цьому, на думку фахівців АНБ, найбільш небезпечними з них є такі, що спрямовуються на порушення функціонування систем енергозабезпечення та водопостачання, фінансів, транспорту, комунікації, оборонної промисловості, військового управління, безперебійної роботи мережі Інтернет, від якої залежить економіка країни [2].

Аналіз останніх досліджень і публікацій. Одним з останніх прикладів важливості згаданої проблематики є факт таємного доступу невідомих осіб (або держави) до американської захищеної бази даним (БД), відомої як "Державний перелік дамб", виявлений у травні 2013 року співробітниками Агенції національної безпеки. Як повідомляється в [2], зазначена БД налічує наявні вразливості 13 397 небезпечних гідроспоруд країни, включаючи приблизну кількість осіб, які можуть загинути у разі аварії на них.

Таким чином сьогоднішні кібернетичні загрози вже можна порівняти із загрозами військового та (або) терористичного характеру. Тому в [3] кіберпростір вже об'явлено п'ятою середою для ведення бойових дій, поряд із сушею, морем, повітряним та космічним просторами. При цьому автори дослідження передбачають, що у найближчі чотири роки США та інші провідні країни світу значно збільшать власні інвестиції в розвиток кіберзробї як для оборони, так і для нападу (Рис. 1).

У свою чергу, відповідно до [4] країни-учасниці НАТО також постійно розробляють нові заходи та посилюють захист своїх інформаційно-комунікаційних систем від кібернападів. Ці зусилля, а також можливості надавати допомогу країнам у захисті їхніх мереж від масштабних нападів, обумовлюють практичну реалізацію політики НАТО щодо кібернетичного захисту, яку було ухвалено країнами-членами НАТО в січні 2008 року після масштабних кібернападів на Естонію в 2007 році.

На Лісабонському саміті НАТО 2010 року кіберзагрози визначено головним викликом НАТО в сфері безпеки. У ході проведення саміту були опрацьовані подальші кроки та завдання щодо кіберзахисту, які потребуватимуть докладного аналізу сучасної політики в кібернетичній сфері.

В рамках даного процесу в Естонії було створено Центр передового досвіду в галузі кіберзахисту, а Військовий комітет НАТО нещодавно затвердив Концепцію кіберзахисту, яка передбачає практичні програми дій [5].

Метою статті є проведення аналізу методологічних підходів щодо застосування технологій управління ризиками у сфері кібербезпеки.

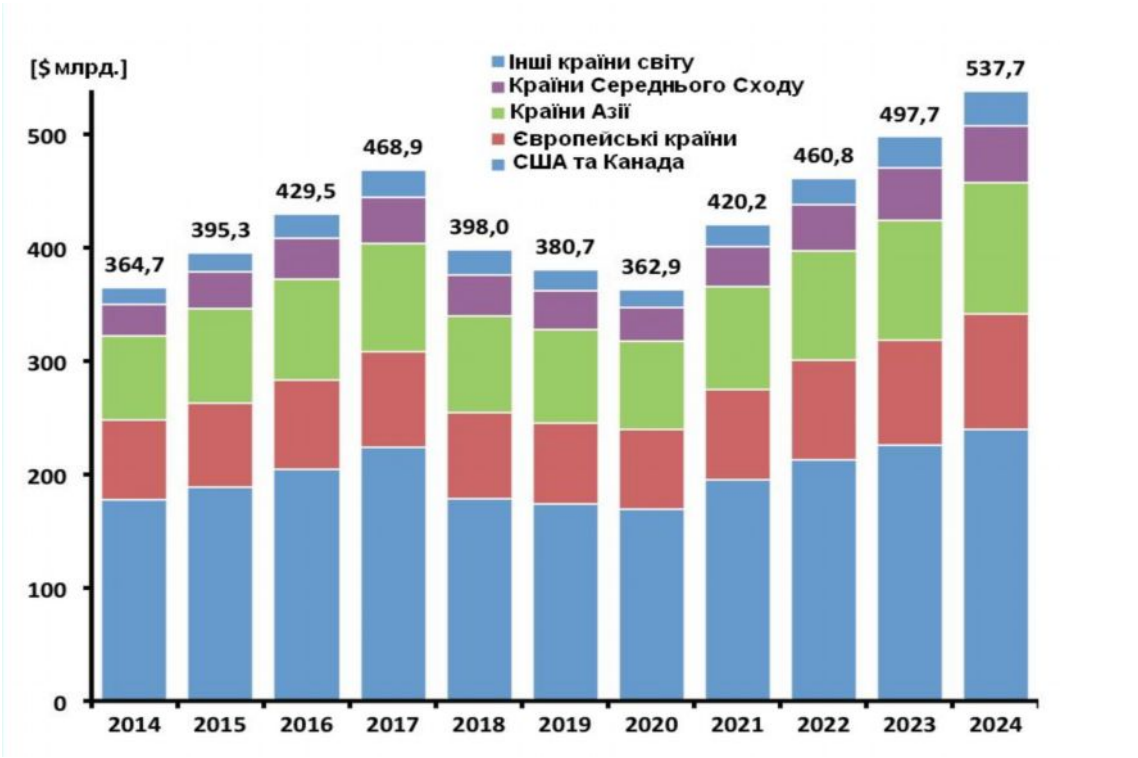

Рис. 1. Прогнозовані показники передбаченого зростання глобального ринку кіберзброї на наступні 10 років (витрати по регіонах світу в мільярдах доларів США)

Виклад основного матеріалу дослідження

Станом на сьогодні існує ціла екосистема, яка оперує відмінним набором високоспеціалізованих інструментів, що дозволяють атакувати кібернетичні системи незалежно від їх стану захищеності. При цьому, з розвитком "хмарних" технологій та ринку так званих "Інтернету речей" (IoT), зникає таке поняття, як мережевий периметр безпеки організації. Відповідно, традиційний підхід до забезпечення кібербезпеки, який існував тривалий час до цього, стає не ефективним.

Виклики, з якими ми стикаємося сьогодні, – це складні цільові атаки (APT) з боку потужних хакерських об'єднань (за якими часто приховуються державні спеціальні служби); розподілені відмови в наданні послуг (DDoS атаки), які здійснюються за допомогою т.з. "ботнетів", які складаються з величезного набору інтернет-пристроїв, заражених шкідливими програмами та контрольованих злочинними угрупуваннями; застосування кіберзброї, яка здатна виводити з ладу об'єкти критичної інфраструктури, призводить до вкрай негативних наслідків для економік окремих регіонів, цілих держав та часто навіть всього розвинутого світу.

Викладені факти, а також автоматизація, розповсюдження та постійне удосконалення механізмів кібернетичних атак все більше підштовхують фахівців у сфері кібернетичної безпеки до застосування технологій управління ризиками.

Ризик – це наявність загрози, пов'язаною з існуючою вразливістю, що може завдати шкоди визначеному активу.

Управління ризиками – це безперервний, ітеративний та еволюційний процес. Кожна ітерація поділяється на три етапи (Рис. 2):

- визначення ризиків,
- зменшення ризиків;
- оцінка ризиків.

В рамках першого етапу необхідно визначити ризик та його компоненти, такі як загрози, вразливості та його ймовірність в межах чітко визначеної сфери, тобто здійснити ідентифікацію ризику. Далі аналізується його вплив. Тобто метою визначення ризику є формування його повного опису та оцінка його важливості на основі визначених імперативів (характеризація ризику).

Розглянемо приклад із сфери IT – безпеки: сканування вразливості (Penetrationtest) – тест на проникнення, який є інструментом для ідентифікації та аналізу недоліків кібернетичної системи, що можуть бути використані для шкідливої атаки на певний об'єкт кібрезахисту.

вразливість становить проблему для вказаного об'єкту здійснюється оцінка ступеню її негативного впливу на конкретний об'єкт. Цей процес дозволяє з'ясувати результати сканування в контексті визначеної організації.

На даному етапі зазвичай використовується структурований ітераційний підхід, який визначається загальним набором термінів та системних показників.

Рис. 2. Цикл управління ризиками

Зважаючи на той факт, що викладений метод не дозволяє оцінювати результати тестування поза межами вказаної організації, так як структура відповідної оцінки має якісну (а не кількісну) структур, він не може бути стандартизованим. Проте на даному етапи більш важливим завданням є визначення найбільш важливих ризики, ніж з'ясування їх вплив на конкретну кібернетичну систему.

Для того, щоб визначити, чи дійсно така вразливість становить проблему для вказаного об'єкту здійснюється оцінка ступеню її негативного впливу на конкретний об'єкт. Цей процес дозволяє з'ясувати результати сканування в контексті визначеної організації.

На даному етапі зазвичай використовується структурований ітераційний підхід, який визначається загальним набором термінів та системних показників.

Зважаючи на той факт, що викладений метод не дозволяє оцінювати результати тестування поза межами вказаної організації, так як структура відповідної оцінки має якісну (а не кількісну) структур, він не може бути стандартизованим. Проте на даному етапи більш важливим завданням є визначення найбільш важливих ризики, ніж з'ясування їх вплив на конкретну кібернетичну систему.

На наступному етапи, враховуючи можливий вплив визначених ризиків, приймається рішення щодо конкретної політики стосовно кожного з них. За своєю природою такі заходи можуть бути юридичними або адміністративними, організаційними або процедурними, технічними або технологічними.

З цього моменту починається фаза зменшення ризиків – етап під час якого дуже важливо здійснити правильне визначення пріоритетів та раціонально розподілити наявні ресурси. Головною метою фази зменшення ризиків є планування та реалізація заходів, спрямованих на протидію визначеним ризикам або контроль за ними, на основі економічної ефективності.

Після імплементації запланованих заходів починається фаза оцінки ризиків, яка полягає в постійному моніторингу визначеного ризику та аналізі ефективності вжитих заходів. Якщо ризик зменшується до допустимого рівня, захід вважається ефективним. В іншому випадку, або в разі появи нового ризику, запускається новий управлінський цикл з його першого етапу – визначення ризиків.

При цьому, на відміну від реактивного (подія – реакція) підходу, який застосовувався в минулому (наприклад: у разі зараження комп'ютера вірусом необхідно було вжити низку термінових заходів: по-перше, обмежити шкоду, по-друге, оцінити збитки, далі, визначити причину та усунути їх в подальшому шляхом оновлення політики чи процедури) сьогодні часто використовується так званий проактивний режим, коли з'являється час для завчасної, обґрунтованої та раціональної відповіді на можливі кіберзагрози, або, в ідеалі, взагалі усуваються передумови до їх виникнення.

Проактивний режим перш за все передбачає підготовку плану реагування на виникнення ймовірних надзвичайних ситуації, своєчасну та регулярну перевірку конфігурації системи, визначення рівня оновлення програмного продукту, з'ясування ефективності системних і програмних обмежень від несанкціонованого доступу до самої кіберсистеми та її ресурсів, проведення аудиту системних та мережевих журнальних записів (логів).

Такий алгоритм роботи, у більшості ситуацій, дозволить своєчасно викрити місце виникнення можливої кібератаки та з'ясувати ресурси, які зазнали ураження. Після чого для поновлення

нормального режиму функціонування відповідної кіберсистеми вживаються заходи, визначені у завчасно розробленому плані реагування на надзвичайні ситуації.

Останнім часом, коли масштаби та частота виникнення кібернетичних інцидентів драматично зростає, фахівцями з кібрезахисту накопичено величезний досвід, що дозволяє прогнозувати ймовірні вектори кібератак у майбутньому та своєчасно готуватися до усунення їх можливих деструктивних наслідків.

У контексті роботи в проактивному режимі існує два шляхи, що допомагають визначати ризики. Один з них базується на кількісній оцінці, інший характеризується якісними показники [6].

Як показано вище ризики оцінюються шляхом виявлення загроз та вразливостей, потім визначаються їх ймовірності та впливи на кожний асоційований з ним ризик. Це складне завдання, зазвичай засноване на недосконалій інформації. Отже, оцінка ризиків передбачає обробку величезної кількості даних, часто сотні або навіть тисячі сценаріїв.

Відповідним аналітикам потрібно враховувати необхідний рівень деталізаціїв результатах оцінки ризику перед самим початком відповідного процесу. Станом на сьогодні існує ціла низка методологій, які дозволяють забезпечити повторювальний та послідовний результат.

Кількісна оцінка ризиків, за правило, спирається на методологію, що використовується фінансовими установами та страховими компаніями. Зазвичай у таких випадках головним критерієм оцінки є вартість відповідних інформаційних систем, бізнес-процесів, кошторис робіт відновлення працездатності всієї організації тощо. Таким чином негативний вплив на систему, тобто – ризик, може бути визначений у термінах прямих та побічних фінансових витрат.

Метод якісної оцінки ризику спрямований на максимально точне описання ризику в парадигмі прийняття повноваженою особою відповідного управлінського рішення.

При цьому, не заважаючи на той факт, що в більшості випадків цей метод вимагає глибокого дослідження, тобто є достатньо ресурсномістким та потребує відповідного рівня досвіду від фахівців (експертів), які залучаються до його проведення, у сфері кібербезпеки він є більш поширеним у порівнянні з кількісним методом.

Зазначене пов'язано із суттєвими недоліками та складнощами застосування кількісних оцінок у визначеній сфері. Величезний масштаб відкритості та високий рівень взаємопов'язаності в сучасному кіберпросторі, наявність таких різнопланових, часто прихованих факторів, як глобальні операції, геополітична напруженість між країнами, все це явища, вплив яких на стан кібербезпеки практично не можливо виміряти у кількісних параметрах.

Окрім викладеного, станом на сьогодні, не існує формальних і суворих способів ефективного обчислення ціннісних значень для таких фундаментальних понять кібербезпеки, як актив та контроль. До того ж застосування кількісних методів, у порівнянні з якісними, вимагає значно більшого часу та суттєвих матеріальних і людських ресурсів.

У свою чергу в основу якісного оцінювання ризиків вже покладена наявність великої ступені невизначеності в імовірності та значенні впливу на об'єкту, який підлягає дослідженню, та визначає ризики в суб'єктивних або якісних термінах. Більш того відповідні значення необхідно описати таким чином, щоб ті ж самі шкали (масштаби) могли бути уніфіковані для різнорідних оцінок.

Якісне оцінювання ризиків зазвичай проводиться шляхом комбінування анкет та спільних семінарів за участю експертів з різних дисциплін або групи всередині організації.

При цьому оцінка ризику зазвичай має наступні значення: високий, середній та низький рівень, або масштаб від одного до п'яти (або більш дрібну шкалу у залежності від характеру потрібної точності), виходячи з суб'єктивної оцінки експерта щодо ймовірності та впливу конкретного ризику.

Таким чином, у випадках якісної оцінки ризику кібербезпеки, як правило, використовується так звана матриця ризиків, в якої горизонтальна вісь визначає імовірність виникнення конкретного ризику, а вертикальна – його вплив (рис. 3.).

Рис. 3. Матриця ризиків

У такому разі події з високою вірогідністю та високим впливом – це верхній правий кут. У свою чергу ризики, що мають низьку ймовірність та низький вплив, займають протилежний кут.

Ідея полягає в тому, що чим вище експертна оцінка, тим важливіше відповідний параметр. Таке прямолінійне та інтуїтивно зрозуміле зображення забезпечує чудову видимість і розуміння рівня ризику, особливо для людей, які приймають рішення, але не є експертами з питань безпеки.

При цьому у сфері управління ризиками (рис. 4)загально визнаними є чотири наступні стратегії [7]:

1. Зменшення ризику;

2. Трансформація ризику;
3. Прийняття ризику;
4. Уникнення ризику.

Рис. 4. Стратегії управління ризиками

Для кожного визначеного ризику слід обрати свою стратегію. При цьому, найбільш поширеним шляхом управління ризиками є стратегія їх зменшення (пом'якшення негативних наслідків).

Вона передбачає фіксацію нанесеної шкоди та застосування певного типу компенсаторного контролю, спрямованого на зменшення вірогідності виникнення визначеного ризику або пом'якшення пов'язаних з ним негативних наслідків до прийнятного рівня. В IT сфері найбільш поширеною практикою, яка відноситься до згаданої стратегії, є своєчасне оновлення програмного продукту, яке на постійної основі пропонується його виробником.

Трансформація ризику це, фактично, процес страхування (перекладання відповідальності за настання негативних наслідків у разі реалізації певних ризиків на іншу сторону). Прикладами застосування відповідної стратегії є страхування життя або власності. У сфері IT таку функцію можуть виконувати хмарні технології, антивірусні компанії тощо.

Прийняття – це практика, коли свідомо допускається робота системи з відомим ризиком. Багато ризиків з низьким впливом просто приймаються. Така ж політика може застосовуватись до ризиків, зменшення негативних наслідків від яких може мати надзвичайно високу вартість.

У кожному випадку рішення щодо застосування відповідної стратегії приймається безпосередньо керівником, або уповноваженою та компетентною для цього особою, часто у письмовому вигляді.

У свою чергу уникнення ризику – це практика усунення вразливого аспекту системи, або навіть самої системи в цілому.

Наприклад, під час оцінки ризику одного з веб-сайтів було виявлено можливість, що дозволяє постачальникам переглядати свої рахунки-фактури за допомогою ідентифікатора постачальника, вбудованого в назву HTML-файлу, що явним чином порушувало загально прийняті правила авторизація та автентифікації. Після повідомлення про встановлену вразливість керівництво організації вирішило видалити відповідні веб-сторінки та надавати рахунки-фактури постачальникам за допомогою іншого механізму.

Висновки і перспективи подальших досліджень

Таким чином управління ризиками кібербезпеки є строга дисципліна, яка спирається на низку принципів, має послідовну термінологію та систему показників, використовує ітераційний, проактивний структурний процес.

Подальші дослідження доцільно спрямувати на формування індикаторів оцінки рівнів кібербезпеки інформаційно-телекомунікаційних систем військового призначення та покращення методики оцінки готовності їх до виявлення та відбиття атак.

Література

1. National security strategy USA, may 2010, The White House, Washington. URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.
2. The Secret War, by James Bamford, 06.12.13. URL: http://www.wired.com/threatlevel/2013/06/general-keith-alexander-cyberwar **3. Offensive** and Defensive Cyber Weapons for Government and Private Sectors Global Market and Technologies Forecast - 2014-2024, Published: Oct 18, 2013. URL: http://www.giiresearch.com/report/mig287441-offensive-defensive-cyber-weapons-government.html. **4. NATO** and cyber defence. URL: http://www.nato.int/cps/en/natolive/topics_78170.htm
5. Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn 2012. URL: http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf. **6. Guide** for Conducting Risk Assessments, National Institute of Standards and Technology, NIST Special Publication 800-30. **7. Managing** Information Security Risk: Organization, Mission, and Information System View, National Institute of Standards and Technology, NIST Special Publication 800-39

АНАЛИЗ МЕТОДОЛОГИЧЕСКИХ ПОДХОДОВ ПО ПРИМЕНЕНИЮ ТЕХНОЛОГИЙ УПРАВЛЕНИЯ РИСКАМИ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

Михаил Николаевич Алексеев

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

Широкое применение современных информационных технологий в секторе безопасности и обороны одновременно обусловливает возникновение новых угроз национальной и международной безопасности. Актуальными сегодня становятся таки понятие как "кибероружие" и "кибервойна". Наряду с инцидентами природного происхождения растет количество и мощность киберугроз. Важнейшей задачей для нашего государства становится наработки теоретических основ для определения оптимальных, в условиях ограниченных возможностей, шагов на пути создания эффективной системы обеспечения кибербезопасности Украины.

Оценивая высокую степень киберугроз для государства и общества в последние годы все больше подталкивают специалистов в сфере кибернетической безопасности к применению технологий управления рисками. Поэтому в статье проводится анализ методологических подходов по применению технологий управления рисками в сфере кибербезопасности.

Ключевые слова: *кибербезопасность, управление рисками, стратегии управления рисками.*

ANALYSIS OF METHODOLOGICAL APPROACHES TO APPLICATION OF RISK MANAGEMENT TECHNOLOGIES IN THE FIELD OF CYBERNETIC SECURITY

Mykhailo Aleksieiev

National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

The widespread use of modern information technologies in the security and defense sector simultaneously creates new threats to national and international security. The concepts of "cybernetic weapons" and "cybernetic warfare" are becoming relevant nowadays. Along with natural incidents, the number and power of cybernetic threats increases. The most important task for our state is to develop the theoretical foundations for identifying the optimal, under limited opportunities, steps towards establishing an effective system for ensuring cybernetic security of Ukraine.

Assessing the high degree of cybernetic threats to the state and society over the past years has increasingly pushed cyber security experts to apply risk management technologies. Therefore, the article analyzes methodological approaches to the application of risk management technologies in the field of cybernetic security.

Keywords: *cybernetic security, risk management, risk management strategies.*

References

1. National security strategy USA, may 2010, The White House, Washington. URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

2. The Secret War, by James Bamford, 06.12.13. URL: http://www.wired.com/threatlevel/2013/06/general-keith-alexander-cyberwar **3. Offensive** and Defensive Cyber Weapons for Government and Private Sectors Global Market and Technologies Forecast - 2014-2024, Published: Oct 18, 2013. URL: http://www.giiresearch.com/report/mig287441-offensive-defensive-cyber-weapons-government.html. **4. NATO** and cyber defence. URL: http://www.nato.int/cps/en/natolive/topics_78170.htm

5. Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn 2012. URL: http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf. **6. Guide** for Conducting Risk Assessments, National Institute of Standards and Technology, NIST Special Publication 800-30. **7. Managing** Information Security Risk: Organization, Mission, and Information System View, National Institute of Standards and Technology, NIST Special Publication 800-39.