https://www.proconference.org/index.php/usc/article/view/usc11-01-007
DOI: 10.30888/2709-2267.2022-11-01-007

УДК 004.056

DEFINING REQUIREMENTS TO DEVELOP INFORMATION SECURITY CONCEPT N HYBRID THREATS CONDITIONS. PART 5

ВИЗНАЧЕННЯ ВИМОГ ЩОДО ПОБУДОВИ КОНЦЕПЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ. ЧАСТИНА 5

Borsukovskyi Y.V. / Борсуковський Ю. В.
c.t.s., as.prof. / к.т.н., доц.
ORCID ID 0000-0003-1973-2386
State University of Telecommunications, Kyiv, Ukkraine, Solomenska street, 7. 03110
Державний університет телекомунікацій, Київ, Україна, вул. Солом'янська, 7, 03110

Анотація. *В роботі розглянуто базові елементи, щодо формування окремих розділів концепції інформаційної безпеки бізнес-структур та державних організацій. Сформульовані вимоги щодо визначення подальших складових елементів при розробці концепції інформаційної та кібернетичної безпеки в умовах гібридних загроз, а саме типове визначення моделі порушника інформаційної та кібернетичної безпеки. Визначені типові категорії та типові припущення щодо кваліфікаційних параметрів можливих порушників інформаційної та кібернетичної безпеки.*

Ключові слова: *загрози, ризики, порушник безпеки, класифікація, кібербезпека, концепція.*

Abstract. *The paper examines the basic elements related to the formation of separate sections of the concept of information security of business structures and state organizations. Formulated requirements for the definition of further components in the development of the concept of information and cybernetic security in conditions of hybrid threats, namely the typical definition of the model of an information and cybernetic security violator. Typical categories and typical assumptions regarding qualification parameters of possible violators of information and cybernetic security are defined.*

Keywords: *threats, risks, security breacher, classification, cyber security, concept.*

Вступ

В перших частинах публікацій [4-7] були розглянуті визначення термінів, структура, загальні положення, опис об'єкта захисту, основні принципи забезпечення інформаційної безпеки, організаційна структура служби інформаційної безпеки, організація робіт щодо захисту інформації, заходи управління інформаційною безпекою, розподіл відповідальності і порядок взаємодії щодо питань інформаційної безпеки та порядок класифікації інформації, що захищається. Далі розглянемо типову структуру моделі порушника інформаційної та кібернетичної безпеки та припущення щодо

кваліфікаційних параметрів (навичок) потенційних порушників при побудові концепції інформаційної безпеки в умовах гібридних загроз [1-3, 9-11].

Аналіз останніх публікацій

До 2022 року ми аналізували як геополітична напруженість та глобальні технологічні ризики можуть негативно впливати на економічний потенціал технологій наступного покоління і призводити до серйозних інцидентів як в глобальному бізнесі так і в сфері персональних даних. З 24 лютого 2022 року ми побачили реальне використання інформаційних та кібернетичних загроз для нанесення значних фінансових збитків при розв'язанні неспровокованих військових дій проти України. Ми бачимо реальне використання кіберозброєння для виведення з ладу стратегічних комунікаційних ресурсів, атак на об'єкти критичної інфраструктури (ОКІ), зломи сторінок місцевих органів влади, кібератаки на сайти медіа та інше в умовах зовнішнього військового вторгнення. Все це уже не теоретичні припущення щодо можливих тенденцій успішних реалізацій ризиків сучасного технологічного суспільства, а використання можливостей в інформаційному та кібернетичному просторі для досягнення тактичних та стратегічних цілей в умовах реальної війни [18-19].

Результати дослідження

Модель порушника безпеки

Під порушником ІБ Організації розуміється особа, яка внаслідок навмисних чи ненавмисних дій може завдати шкоди інформаційним ресурсам Організації. Під атакою на ресурси корпоративної мережі розуміється спроба завдання шкоди інформаційним ресурсам систем, підключених до мережі. Атака може здійснюватися як безпосередньо порушником, і опосередковано з допомогою процесів, що виконуються від особи порушника, або шляхом впровадження у систему програмних чи апаратних закладок, комп'ютерних вірусів, троянських програм тощо. Відповідно до моделі всі порушники за ознакою належності до підрозділів, що забезпечують функціонування ІС Організації, діляться на зовнішніх та внутрішніх. Внутрішнім порушником може бути особа з таких категорій співробітників обслуговуючих підрозділів:

Обслуговуючий персонал (системні адміністратори, адміністратори БД, адміністратори додатків тощо, що відповідають за експлуатацію та супровід технічних та програмних засобів).

Розробники ПЗ (програмісти), що відповідають за розробку та супровід системного та прикладного ПЗ.

Технічний персонал (робітники підсобних приміщень, прибиральниці тощо).

Співробітники бізнес-підрозділів Організації, яким надано доступ до приміщень, де розташовано комп'ютерне або телекомунікаційне обладнання.

Співробітники підрядних організацій, яким надано доступ до приміщень Організації або доступ до ІС для виконання узгоджених робіт.

Передбачається, що несанкціонований доступ на об'єкти та доступ до ІС Організації сторонніх осіб виключається засобами фізичного захисту (охорона території, організація пропускного режиму тощо). Припущення про кваліфікацію внутрішнього порушника в загальному можна сформулювати таким чином:

- Внутрішній порушник є висококваліфікованим спеціалістом у галузі розробки та експлуатації ПЗ та технічних засобів.
- Знає специфіку завдань, які вирішують обслуговуючі підрозділи ІС Організації.
- Має навички системного програміста або є системним програмістом, здатним модифікувати роботу операційних систем.
- Правильно представляє функціональні особливості роботи системи та процеси, пов'язані зі зберіганням, обробкою та передачею критичної інформації.
- Може використовувати як штатне обладнання та ПЗ, що є у складі системи, так і спеціалізовані засоби, призначені для аналізу та злому комп'ютерних систем.

Залежно від способу здійснення доступу до ресурсів системи та наданих їм повноважень [12-17] внутрішні порушники можуть бути умовно поділені на п'ять категорій:

Категорія А: не зареєстровані в системі особи, які мають санкціонований доступ до приміщень з обладнанням. Особи, що належать до категорії «А», можуть: мати доступ до будь-яких фрагментів інформації, що поширюється внутрішніми каналами зв'язку корпоративної мережі Організації; мати у своєму розпорядженні будь-які фрагменти інформації про топологію мережі, про використовувані комунікаційні протоколи та мережеві сервіси; мати у своєму розпорядженні імена зареєстрованих користувачів системи та вести розвідку паролів зареєстрованих користувачів.

Категорія B: зареєстрований користувач системи, що здійснює доступ до системи з віддаленого робочого місця. Особи, що належать до категорії «B» мають у своєму розпорядженні всі можливості осіб, які належать до категорії «A»; знають, принаймні, одне легальне ім'я доступу; мають всі необхідні атрибути, що забезпечують доступ до системи (наприклад, паролі); мають санкціонований доступ до інформації корпоративної мережі, що зберігається в БД і на файлових серверах, а також на робочих місцях користувачів. Повноваження користувачів категорії «B» щодо доступу до інформаційних ресурсів корпоративної мережі Організації повинні регламентуватися безпековою політикою, прийнятою в Організації.

Категорія C: зареєстрований користувач, який здійснює локальний або віддалений доступ до систем, що входять до складу корпоративної мережі Організації. Особи, що належать до категорії «C», мають всі можливості осіб категорії «B», мають інформацію про топологію мережі, структуру БД і файлових систем серверів; мають можливість здійснення прямого фізичного доступу до технічних засобів ІС.

Категорія D: зареєстрований користувач системи з повноваженнями системного адміністратора. Особи, що відносяться до категорії «D», мають всі можливості осіб категорії «C», мають повну інформацію про системне та прикладне програмне забезпечення ІС; володіють повною інформацією про технічні засоби та конфігурацію мережі; мають доступ до всіх технічних та програмних засобів ІС та мають права налаштування технічних засобів та ПЗ. Концепція безпеки вимагає підзвітності осіб, які належать до категорії «D», та здійснення незалежного контролю за їх діяльністю.

Категорія E: програмісти, які відповідають за розробку та супровід загальносистемного та прикладного ПЗ, що використовується в ІС Організації. Особи, що належать до категорії «E», мають можливості внесення помилок, програмних закладок, встановлення троянських програм та вірусів на серверах корпоративної мережі; можуть мати у своєму розпорядженні будь-які фрагменти інформації про топологію мережі та технічні засоби ІС.

До зовнішніх порушників належать особи, перебування яких у приміщеннях з обладнанням без контролю з боку працівників Організації неможливе. Зовнішній порушник: здійснює перехоплення, аналіз та модифікацію інформації, що передається лініями зв'язку, які проходять поза контрольованою територією; здійснює перехоплення та аналіз

електромагнітних випромінювань від обладнання ІС. Припущення про кваліфікацію зовнішнього порушника в загальному може бути сформульованим в такий спосіб. Зовнішній порушник:

- Є висококваліфікованим спеціалістом у галузі використання технічних засобів перехоплення інформації.
- Знає особливості системного та прикладного ПЗ, а також технічних засобів ІС.
- Знає специфіку завдань, які розв'язують ІС.
- Знає функціональні особливості роботи системи та закономірності зберігання, обробки та передачі в ній інформації.
- Знає мережеве та канальне обладнання, а також протоколи передачі даних, що використовуються в системі.
- Може використовувати тільки спеціальне обладнання, що серійно виготовляється, призначене для знімання інформації з кабельних ліній зв’язку і з радіоканалів.
- Може використовувати спеціальне обладнання засобів РЕБ, призначене для знімання інформації з кабельних ліній зв'язку і з радіоканалів (потрібно враховувати, виходячи з аналізу застосування і можливих підходів до розвитку засобів РЕБ цілеспрямованих на здійснення атак на ОКІ).

При використанні моделі порушника для аналізу можливих загроз ІБ необхідно враховувати можливість змови між внутрішніми та зовнішніми порушниками.

Зрозуміло, що даний розділ концепції інформаційної безпеки тут поданий у дуже загальному вигляді і тільки для того, щоб зберегти цілісність викладення матеріалу. А також щоб окреслити основні параметри моделі порушника при формуванні реальної концепції інформаційної безпеки конкретної Організації.

Висновки та перспективи подальших досліджень

Сучасні тренди кібербезпеки безпосередньо пов'язані з моделями інформаційної безпеки, цілями і завданнями зловмисників, а також із застосуванням конкретних тактик та підтактик CSVV при проведенні кібератак на інформаційні ресурси, особливо при таргетованому здійсненні атак на ОКІ, що ми спостерігаємо в умовах військових дій проти України.

Очевидно, що аналіз результатів реалізації успішних кібератак (зокрема в умовах здійснення військових дій) однозначно вимагає переосмислення існуючих концепцій інформаційного та кібернетичного захисту, перегляду підходів до побудови сучасної системи протидії сучасним інформаційним та кібернетичним загрозам. Всі ці заходи повинні бути орієнтовані в першу чергу на створення нових концептуальних моделей побудови архітектури ІС, зокрема ОКІ, та систем управління інформаційною безпекою, що відповідають сучасним викликам в умовах активного протистояння в кіберпросторі.

Враховуючи вищесказане, подальші дослідження варто зосередити на таких складових частинах концепції політики ІБ як:

- формування вимог щодо побудови моделі порушника безпеки систем ІТ та ІКБ;
- аналіз вимог щодо забезпечення інформаційної та кібернетичної безпеки.

Література

1. Борсуковський Ю.В., Борсуковська В.Ю., Бурячок В.Л. «Напрямки формування політик кібербезпеки для державного, банківського та приватного секторів», Modern Methodologies, Innovations, and Operational Experience on the Field of Technical Science: Conference proceedings, December 27-28, 2017, Radom, Republic of Poland, с. 8-11

2. Борсуковська В.Ю., Борсуковський Ю.В. «Безперервність бізнесу: новий тренд або необхідність», Економіка. Менеджмент. Бізнес. - 2017, № 2(20), с. 48-52

3. Борсуковський Ю.В., Бурячок В.Л., Борсуковська В.Ю. «Базові напрямки забезпечення кібербезпеки державного та приватного секторів», Сучасний захист інформації, - 2017, № 2(30), с. 85-89

4. Борсуковський Ю.В. «Визначення вимог щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. Частина 1», Кібербезпека, освіта, наука, техніка, - 2019, №1(5), с. 61-72

5. Борсуковський Ю.В. «Визначення вимог щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. Частина 2», Кібербезпека, освіта, наука, техніка, - 2019, №2(6), с. 112-121

6. Борсуковський Ю.В. «Визначення вимог щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. Частина 3», Кібербезпека, освіта, наука, техніка, - 2020, №4(8), с. 34-48

7. Борсуковський Ю. В., Гайдур Г.І. «Визначення вимог щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. Частина 4», SWorld Journal, Issue 9, Part 1, p.36-42, September 2021.

8. ДСТУ ISO/IEC 27000:2015. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою (ISO/IEC 27000:2014 IDT).

9. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності.

10. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки ТЗ на створення КСЗІ в автоматизованій системі.

11. CERT-UA. Computer Emergency Response Team of Ukraine. Посилання: https://cert.gov.ua.

12. Chris Sanders. How Analysts Approach Investigations with Diagnostic Inquiry. Посилання: https://chrissanders.org/2016/05/how-analysts-approach-investigations.

13. The Cyber Kill Chain: A LOCKHEED MARTIN OVERVIEW. Посилання: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

14. Аналіз вторгнень по моделі DIAMOND. Посилання: https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf.

15. CYBERSECURITY& INFRASTRUCTURE SECURITYAGENCY. Defense in Depth. Посилання: https://www.us-cert.gov/bsi/articles/knowledge/principles/defense-in-depth.

16. Chris Sanders. The Role of Evidence Intention. Посилання: https://chrissanders.org/2018/10/the-role-of-evidence-intention.

17. Процес реагування на інциденти (PICERL). Посилання: https://www.sans.org/media/score/504-incident-response-cycle.pdf.

18. НАТО на кіберзахисті: як Альянс допомагає Україні вберегтися від хакерських атак РФ. Посилання: https://www.eurointegration.com.ua/articles/2022/07/6/7142651.

19. Кіберфронт. Як РФ атакує Україну та чи готові ми захищатися. Посилання: https://biz.nv.ua/ukr/experts/kiberataki-rosiji-na-ukrajinu-yak-prohodyat-ta-chim-zagrozhuyut-ostanni-novini-50236927.html.

Стаття відправлена 09.07.2022 р.

©Борсуковський Ю.В