СЕКЦІЯ 13

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ У СУЧАСНОМУ СВІТІ

Керівник секції: *завідувач кафедри кібербезпеки, доктор економічних наук, професор С. А. Горбаченко*

Секретар секції: *лаборант кафедри кібербезпеки Є. Р. Кулешова*

ГОРБАЧЕНКО СТАНІСЛАВ АНАТОЛІЙОВИЧ

Національний університет «Одеська юридична академія», завідувач кафедри кібербезпеки, доктор економічних наук, професор

КУЛЕШОВА ЄВГЕНІЯ РОМАНІВНА

Національний університет «Одеська юридична академія», здобувач вищої освіти

ТРАНСФОРМАЦІЯ МЕНЕДЖМЕНТУ БЕЗПЕКИ В КОНТЕКСТІ АКТУАЛЬНИХ КІБЕРЗАГРОЗ

Глобальний розвиток сфери інформаційних технологій з постійним впровадженням інноваційних продуктів, ресурсів і послуг призвів до тектонічних змін та виникнення принципово нових суспільних відносин. Проте, одночасно, кіберсередовище спричинило й появу нових загроз, в першу чергу – загроз безпеці.

В менеджменті загрози безпеці розглядають як певні чинники, що формують небезпеку, тобто наявну та об'єктивну ймовірність негативного впливу на систему. Якщо мова йде про кіберзагрози, можна зазначити наступне. Тривалий час кіберзлочинність функціонувала на принципах, дуже схожих з принципами законного бізнесу, який намагається отримати найвищий рівень прибутку. Відтак, ефективно знижувати рівень кіберзагроз, як ключових загроз безпеці, означало систематично знищувати бізнес-модель, за якою в умовах невисокого ризику нескладні для застосування інструменти використовуються для отримання значних прибутків [1].

У вказаній ситуації метою ефективного кіберзахисту було зробити кібератаку невигідною (в першу чергу у фінансовому аспекті). Задля цього суб'єкти господарювання намагалися не тільки безпосередньо забезпечувати технологічну підтримку системи кібербезпеки,

а й проводити систематичну оцінку активів з огляду на їхню вразливість у кіберсередовищі та розмір потенційних збитків. Насамперед, оцінювалися можливі репутаційні втрати, збитки від крадіжки фінансової інформації, персональних даних працівників та клієнтів, блокування роботи серверів, проблем з функціонуванням сайту.

Проте в останні роки використання інформаційних технологій в процесі гібридної війни обумовило виникнення принципово нових кіберзагроз вищого рівня, які спрямовано на національну та міжнародну безпеку. Зокрема, зростає кількість та потужність кібератак, вмотивованих геополітичними інтересами окремих держав, груп та осіб. І при їхньому здійсненні вже не враховуються такі поняття як фінансова ефективність чи рентабельність атаки.

Спектр сучасних кібератак є досить різнорідним, тож доцільно їх класифікувати за такими базовими ознаками, як: інструментальний засіб, що використовується при проведенні; специфіка реалізації; міра складності; умова ініціалізації; дистанційність; процес автоматизації; зовнішній прояв; спрямованість кінцевого результату та специфіка порушення базових характеристик системи інформаційної безпеки [2].

Найбільш масштабні кібератаки здійснюються на об'єкти критичної інфраструктури, тобто підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство. Вони є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, а виведення з ладу або руйнування їх може вплинути на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків та, навіть, людських жертв. У контексті кіберзагроз слід додати, що зазначені об'єкти повинні мати у своєму складі комп'ютерні системи та/або телекомунікаційні мережі, порушення функціонування яких напряму відбивається на інтересах суспільства і держави.

Це корелює із основним завданням кібербезпеки щодо захисту життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [3].

На рівні підприємств та організацій під безпекою розуміють такий стан господарюючого суб'єкта, що характеризується організованою сукупністю концептуальних і прагматичних чинників, які забезпечують: результативність та ефективність менеджменту, чесну конкурентну боротьбу, захист від небажаного втручання, сталий розвиток, безперервність ключових бізнес-процесів, незалежність функціонування. Тому в якості об'єктів кіберзахисту виступають усі ключові складові

підприємницької діяльності: репутація, бренд, клієнти, фінанси, бізнес-процеси тощо.

Процеси безпеки на підприємстві чи в організації мають забезпечуватися та підтримуватися за допомогою ефективної системи менеджменту безпеки. Під останнім слід розуміти систематизовані та скоординовані методи, засоби та інструменти за допомогою яких організація намагається максимально ефективно управляти власними ризиками і пов'язаними з ними потенційними загрозами.

Система менеджменту безпеки являє собою процес, заснований на циклі управління PDCA (Plan-Do-Check-Act): «Планування», «Виконання», «Контроль» і «Корекція» і спрямований на постійне поліпшення безпеки організації з використанням об'єктивно вимірюваних індикаторів [4].

Інформаційна складова менеджменту безпеки має забезпечувати: конфіденційність (доступ до інформації тільки авторизованих користувачів), цілісність (достовірність і повноту інформації та методів її обробки) та доступність (доступ до інформації та зв'язаних з нею активів авторизованих користувачів).

Основним інструментом при цьому виступає система кіберзахисту на основі наявних організаційних та технологічних можливостей, фінансових та людських ресурсів, а також нормативно-правового базису. Відповідальним за побудову вказаної системи на локальному рівні найчастіше виступає системний адміністратор. На великих підприємствах побудова комплексу протидії кіберзагрозам є вже управлінською проблемою як потребує залучення профільних фахівців. Незалежно від конкретних інструментів, які планується використовувати, менеджмент безпеки здійснюється згідно з наступними принципами: локалізація людського фактору; розуміння критичних місць та джерел небезпеки; моніторинг ризиків; можливість оперативного реагування.

Крім того, враховуючи те, що значна частина кібератак ґрунтується на використанні прийомів соціальної інженерії, завдання сучасної системи менеджменту безпеки полягає у створенні на підприємстві чи в організації культури інформаційної та кібербезпеки, норм поведінки працівників, а також відповідного інформаційного середовища.

Список використаних джерел:

1. Полторак А. С., Сухорукова А. Л., Бурковська А. І. Кібербезпека в системі трансформації управління бізнес-організацією. Трансформація менеджменту бізнес-організацій: сучасні тренди та виклики : колективна монографія / за заг. ред. Сагайдака М. П., Соболєвої Т. О., 2021. С. 158–176.
2. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту : монографія / О. Д. Довгань, І. М. Доронін; НАПрН України, НДІІП – К. : Видавничий дім «АртЕк». – 2017. – 107 с.
3. Про основні засади забезпечення кібербезпеки України : закон України від 05.10.2017 р. № 2163-VIII / Верховна Рада України. 2017. URL: http://zakon3.rada.gov.ua/laws/show/2163-19

4. Новик І. В. Менеджмент безпеки як невід'ємний складник інтегрованої системи менеджменту підприємства. URL: http://www.marketinfr.od.ua/journals/2019/30_2019_ukr/31.pdf

Ключові слова: менеджмент, безпека, кіберзагроза, ризики.
Key words: management, security, cyber threat, risks.

ВАСИЛЕНКО МИКОЛА ДМИТРОВИЧ

Національний університет «Одеська юридична академія», професор кафедри кібербезпеки, доктор фізико-математичних наук, доктор юридичних наук, професор

СЛАТВІНСЬКА ВАЛЕРІЯ МИКОЛАЇВНА

Міжнародний гуманітарний університет, викладач кафедри кримінального права, процесу та криміналістики

СОЦІАЛЬНА ІНЖЕНЕРІЯ ЯК ЗБРОЯ ХАКІНГУ З ПІДВИЩЕНИМ РИЗИКОМ

Соціальна інженерія досліджує причини поведінки людини, обставин і середовища, що впливають на формування системи її цінностей та на саму поведінку [1]. Звісно, що поведінка людей в воєнному стані або під час війни відрізняється від їх поведінки у мирний час. При цьому важливою стає створена самою людиною небезпечна (безпечна) ситуація, що проявляється, в першу чергу, в ризиках, пов'язаних з діяльністю людей. Відбувається проникнення ризику в усі сфери людської діяльності, що стає закономірним під час війни. В цьому випадку ризики реально пов'язані з несприятливими умовами життєдіяльності та небезпечними подіями та явищами (форс-мажором), що створюють небезпечні (катастрофічні) ситуації, що реалізуються. В зазначених вище умовах виникає ситуація реальної невизначеності, яка представляє собою сукупність обставин та умов, за яких можливі зміни стану об'єкта ризику стають абсолютно непередбачуваними. Ця ситуація виключає можливість об'єктивного оцінювання ризику. Однак певне зменшення невизначеності до рівня так званої статистичної невизначеності породжує ризикову ситуацію (РС), яка характеризується, існуванням кількох можливих станів (як варіант – множини станів, що сягає нескінченості), ймовірність реалізації кожного з яких відома, але в цілому невизначеність все ж таки залишається. Якщо реалізацію на об'єкт ризику будь-якого з можливих станів вважати подією, РС визначається існуванням множини варіантів можливого розвитку подій, ймовірність кожного з яких характеризується відповідною кількісною або якісною оцінкою. За умов виникнення ризикової ситуації стає актуальним проведення