УДК 004.946.5:005.334

ВИНИКНЕННЯ ЗАГРОЗ У КІБЕРПРОСТОРІ ЯК РЕЗУЛЬТАТ ТЕХНОЛОГІЧНОГО РОЗВИТКУ СУСПІЛЬСТВА

Марина Саєнко
Полтавський державний медичний університет
saenkomarina89@ukr.net

Кібербезпека – це важливий пріоритет системи української національної безпеки, яка може бути забезпечена завдяки посиленню можливостей системи кібербезпеки у процесі її протидії кіберзагрозам, що можуть бути характерними для сучасного безпекового середовища. У процесі формування сучасної української Стратегії кібербезпеки враховуються світові тренди, які присутні у глобальному кіберсередовищі як фактори, які мають вплив на процес розбудови державної системи кібербезпеки XXI століття. При цьому суспільство зустрічає низку ризиків, які є пов'язаними із застосуванням сучасних технологій, зокрема у кіберпросторі. Стратегією кібербезпеки в Україні визначено головні пріоритети, цілі та завдання по забезпеченню кібербезпеки для того, щоб створити умови для такого функціонування кіберпростору, який би був безпечним як для конкретної особи, так і для суспільства та держави в цілому.

Метою даної роботи є дослідження виникнення загроз у кіберпросторі як результату технологічного розвитку суспільства.

Загальна кількість кіберзагроз, які можливі у спектрі загроз національній безпеці країн, поступово збільшується. Дана тенденція і надалі буде посилюватися через те, що інформаційні технології бурхливо розвиваються, відбувається конвергенція з технологіями штучного інтелекту (ШІ). У результаті того, що такий вплив на діяльність національних та транснаціональних структур управління збільшується, формується абсолютно нова безпекова ситуація, пов'язана із викликами нового технологічного рівня. Протягом останнього часу можна спостерігати, що у кіберпросторі відбувається розподіл сфер впливу. Завдяки такому поділу реалізується прагнення людства реалізувати геополітичні інтереси, які постійно зростають.

Вважається, що кіберпростір у поєднанні з іншими фізичними просторами є одним із можливих сценаріїв, за яким відбуватиметься розгортання військових дій. Через це здатність держави захищати національні інтереси є надзвичайно важливою складовою кібербезпеки. Актуальним питанням за сучасних умов є створення нового війська – кібервійськ. Основне їхнє завдання полягає утому, щоб забезпечити захист критичної інформаційної інфраструктури від можливих кібератак. Проте, крім цього, вони також відповідають за здійснення превентивних наступальних операцій у кіберпросторі, які направлені на те, щоб знищити

обчислювальні мережі та інформаційні системи збройних сил противника. Їхнім завданням є також порушення нормальної роботи об'єктів противника, які є критично важливими. Це можливо досягнути, зруйнувавши інформаційні системи, які забезпечують управління таких об'єктів.

На думку експертів, поступово у кіберпросторі інтенсивність протистояння і розвідувально-підривної діяльності буде лише зростати. Ці явища будуть проявлятися, перш за все, у тому, що буде розширюватися кількість країн, які докладатимуть зусиль для того, щоб організувати діяльність своєї кіберрозвідки, опанувати сучасні технології розвідувально-підривної діяльності у кіберпросторі, сприяти збільшенню державного контролю за національними сегментами всесвітньої мережі. За таких умов більш поширеним буде розробка такого інструментарію, який буде здатним передбачати нагромадження значних інформаційних масивів, які відображатимуть особливості людської поведінки та різних груп у соціумі. При цьому буде використовуватися досвід у сфері ШІ.

На даний момент присутнім є такий розвиток технологій, який пов'язаний із надзвичайно швидким поширенням цифрових технологій, поступово розширюється Інтернет-середовище. Проте цей процес володіє негативною ознакою, яка полягає у тому, що технічний рівень інструментарію реалізації кіберзагроз критично збільшується. У результаті цього такі загрози все більше поширюються на різні сфери життєдіяльності. Кібератаки та їхні різновиди стають все більш інтелектуальними та небезпечними, при цьому вони створюють реальну загрозу для критично важливої інфраструктури. Увага зловмисників зосереджується на тому, щоб знайти вразливі місця активів (систем управління). Для цього розробляються багатофункціональне шкідливе програмне забезпечення, віруси-шифрувальники, ботнети. Враховуючи темпи розвитку технологій ШІ, у найближчі роки розміри та наслідки таких втручань будуть лише збільшуватися.

Все більш глобальним стає використання кіберпростору терористичними організаціями, тобто будемо говорити про кібертероризм. На це впливає цифрова трансформація систем управління та життєзабезпечення, яка постійно розширює цільову аудиторію кібертероризму та спектр потенційних об'єктів кібератак. До пріоритетних об'єктів терористичних кібератак відносять об'єкти атомної енергетики, системи, які відповідають за управління електропостачання, авіа- та залізничного транспорту, системи постачання водою, хімічні та біологічні об'єкти.

У результаті поширення ймовірних загроз та ускладнення інструментарію їх реалізації уряди провідних країн світу змушені були удосконалювати архітектуру національних систем кібезбезпеки, змінювати стратегію і тактику протидії кіберзагрозам. При цьому вдосконалюються моделі протидії кіберзагрозам. Ці зміни пов'язані з тим, що має місце розуміння того, що ті можливості, які є на сьогоднішній день, є недостатніми для того, щоб побудувати такі системи захисту, які були б абсолютно невразливими. Як показує досвід, кібератаки можуть бути

здійснені на будь-які інформаційно-комунікаційні системи незалежно від того, який рівень захисту у них присутній. З огляду на це більш значимим стає те, щоб найбільш швидко виявити кібератаки, зреагувати на них та поширити інформацію про такі випадки, щоб мати можливість мінімізувати їх можливу шкоду.

Отже, світ цифрових технологій, який швидкими темпами змінюється, вимагає того, щоб була сформована збалансована та ефективна національна система кібербезпеки, яка була б здатною до гнучкої адаптації до тих змін, які мають місце у безпековому середовищі. Таким чином, вона б гарантувала громадянам країни те, що національний сегмент кіберпростору буде безпечно функціонувати, а також передбачала б нові можливості цифровізації усіх сфер суспільного життя.

УДК 32.973.202 (004.8)

STRATEGY OF COUNTERING PHISHING ATTACKS ON THE CRYPTOCURRENCY EXCHANGE AS PART OF THE ENDLESS ANTAGONISTIC GAME SCHEME

Lakhno V.A.[1], Malyukov V.P.[1], Akhmetov B.S.[2], Alimseitova Zh.K.[3], Ogan A.[3]
National University of Life and Environmental Sciences of Ukraine[1], Kazakh National Pedagogical University named after Abai[2], Satpayev University[3]
[1]lva964@nubip.edu.ua, [1]volod.malyukov@gmail.com, [2]bakhytzhan.akhmetov.54@mail.ru, [3]zhuldyz_al@mail.ru, [3]atkeldi@mail.ru

As the scale of the use of various Internet technologies develops, the number of cybernetic threats, as well as all kinds of attacks aimed at computer systems, also increases. Computer attackers are not only inventing new ways and scenarios of conducting cyber attacks, but also improving old proven schemes. For example, despite the rapid development of various intrusion detection systems, the threat of phishing, which occupies a significant share among computer attacks, has not disappeared anywhere. These attacks make it possible for cybercriminals to steal user account data from various Internet sites. At the same time, attackers do not particularly bother to develop new phishing attack scenarios [1]. And, indeed, such methods of phishing are still effective for attackers, such as: sending fake emails, faking websites, etc.

Phishing has not bypassed such a popular type of commercial activity in recent years as trading in digital cryptocurrencies and, accordingly, affected online exchanges engaged in such transactions. With the development and growing popularity of exchanges engaged in trading digital cryptocurrencies, the problem of detecting and predicting the consequences of such attacks, including those based on phishing, remains relevant. In [1], examples of a number of fraudulent attacks aimed at the digital cryptocurrency exchange are considered. Information security specialists are looking for ways to ensure the interaction of all interested parties in order to counter fraud using phishing attack techniques and increase privacy for individual citizens and businesses. However, many