4. Sierpinski W. Sur une courbe dont tout point est un point de ramification // Comptes rendus hebdomadaires des séances de l'Académie des sciences. – Paris. – Tome 160, Janvier – Juin 1915. – Pp. 302–305.
A. Dewdney K. Computer recreations: The cellular automata programs that create Wireworld, Rugworld and other diversions // Reviews of Scientific American : journal – 1990 – January.
5. David Darling. The Universal Book of Mathematics: From Abracadabra to Zeno's Paradoxes. – John Wiley & Sons, 2004. – P. 180–181.

Ключові слова: клітинні автомати, гра «Життя», Wireworld, код Вольфрама, мураха Ленгтона.
Key words: cellular automata, Conway's Game of Life, Wireworld, Wolfram code, Langton's ant.

ТРОФИМЕНКО ОЛЕНА ГРИГОРІВНА

Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат технічних наук, доцент

КІБЕРБЕЗПЕКА ОСВІТНЬОГО СЕКТОРА

Разом з повсюдною інформатизацією суспільства ІТ-інфраструктура стає все більш вразливою для кіберзлочинності. Переважно кібератаки спрямовані на дані й активи фінансових установ, урядів, корпорацій, різних підприємств і компаній. Проте не стали винятком у цьому переліку університети та академічні установи.

За даними Microsoft [1] сектор освіти найбільше страждає від корпоративних зіткнень зі шкідливим програмним забезпеченням і посідає перше місце (82,6 %) по кількості випадків виявлення зловмисного програмного забезпечення, порівняно з галузями торгівлі (8,41 %), медицини (3,93 %), телекомунікацій (2,39 %), фінансів (1,52 %) та інших. При цьому поняття кібербезпеки охоплює всі ресурси вишу, враховуючи студентів, співробітників, філіалів і партнерів. Адже будь-яка сфера діяльності або активності, яка може притягнути загрозу реалізації вищезазначених ризиків, формує повне охоплення кіберризиків [2].

Інтерес кіберзлочинності до освітнього сектора зумовлений наявністю значної кількості персональних даних як студентів, так і штату працівників. Крім того, багато навчальних закладів мають інформацію про передові дослідження, технологічні інновації та інтелектуальну власність, яку також цінують потенційні хакери. При цьому традиційно освітні установи вищої школи дотримуються академічної відкритості та сприяють вільному обміну інформацією під час співпраці з іншими дослідниками як всередині, так і за межами університету. І з часом такі взаємозв'язки в університетах продовжують зростати, а відтак пропорційно зростає поле доступу для кібератак. Все це є викликами

кібербезпеки, які не спостерігаються в інших галузях. Іронія ситуації полягає в тому, що численні науковці вишів досліджують сучасні проблеми кібербезпеки і публікують свої дослідницькі статті щодо її забезпечення, тоді як сам сектор вищої освіти часто має проблеми з кіберзахистом і потребує втручання відповідних технічних спеціалістів. Але через обмежені бюджети такі штатні фахівці може собі дозволити далеко не кожен університет чи то академія.

Спектр кіберзагроз для сектора вищої освіти доволі широкий: від крадіїв персональних даних та комерційних таємниць до програм-вимагачів, від несегментованих мереж віддалених працівників та студентів до взаємовідносин між структурними підрозділами, філіалами та комерційними партнерами. Наявність численних комп'ютерних лабораторій у різних структурних підрозділах цих закладів, де для великої кількості студентів і викладачів з різним ступенем технічних знань розміщені комп'ютери та системні пристрої з вільним доступом, ніяк не сприяє забезпеченню інформаційної безпеки університетів. Як наслідок, заходи кібербезпеки часто послаблюються на користь зручності та функціональності. Крім того, вільний потік робочої сили та щорічна ротація нових студентів і співробітників також додають вразливості освітньому сектору.

Суттєвий вплив на послаблення рівня кібербезпеки університетів відбувся унаслідок швидкого переходу до віддаленої роботи, електронного навчання та онлайн-викладання на початку пандемії COVID-19, що порушило архітектуру мереж освітніх організацій, зробивши дані всередині мереж набагато більш відкритими. Адже вдома студенти і працівники можуть використовувати незахищені чи застарілі пристрої, які більш уразливі для атак, що ненавмисно створює додаткові вразливості.

Суттєво те, що багато викладачів університетів для онлайн-викладання вибрали платформу Zoom, оскільки вважають її економічно ефективною і зручною як для себе, так і для студентів. Нині Zoom продовжує покращувати захист від зовнішнього втручання і навіть пропонує наскрізне шифрування для забезпечення конфіденційності відеодзвінків, проте наявне зараз шифрування не є наскрізним у загальноприйнятому його розумінні, коли тільки користувачі мають доступ до криптографічних ключів, необхідних для розшифрування вмісту. Випадки масових «зумбомбінгів» та передачі даних користувачів Facebook і Google без їх згоди були визнані компанією та для задоволення претензій колективного позову виплачені відповідні, призначенні судом багатомільйонні кошти [3]. Відтак варто зважати на те, що поки що платформа Zoom не надає надійний захист для дзвінків і формує додаткові проблеми кібербезпеки.

Для навчальних закладів від початку пандемії COVID-19 віртуальні технології стали важливим фактором у навчанні, і тому вкрай важливо вживати заходів для подолання ризиків. З іншого боку, дослідження [4] показали, що під час пандемії певна невизначеність і невпевненість у «завтрашньому дні», різної природи страхи підвищують емоційний

стан людей, роблять їх більш сприйнятливими до шахрайства. Через це за даними Всесвітньої організації охорони здоров'я (ВООЗ) кількість кібератак під час пандемії COVID-19 зросла вп'ятеро [5]. Розуміючи фактори, які роблять людей більш вразливими до кібератак, можна краще підготуватися та навчитися реагувати на можливі кіберінциденти.

Знання основних загроз освітніх мереж і систем, розуміння поширених способів злому і витоків конфіденційних даних студентів, викладачів та інших співробітників дозволить вибрати й застосовувати навчальним закладам найбільш ефективні інструменти і стратегії на всіх рівнях кіберзахисту. ЗВО мають оцінити свій профіль кіберризиків, зважаючи на те, які саме бізнес-активи та процеси піддаються зовнішньому впливу, і відповідно до цього вибирати програмне забезпечення, інструменти та методології безпеки, які контролюватимуть доступ до даних, наприклад, брандмауери або шифрування, щоб краще захистити великі обсяги цінних досліджень і персональних даних. Розбудувати всеосяжну і надійну систему кіберзахисту при обмеженому бюджеті не реально. Саме тому освітні академічні установи для забезпечення своєї діяльності повинні робити більше за менші кошти, тобто засоби і підходи до зменшення поверхні атаки та її складності мають вибиратись і реалізуватись саме з точки зору їх ефективності. А вже надалі робити все можливе щодо розширення і посилення захисту своїх програм, мереж і систем, поглибленого моніторингу кіберризиків та забезпечення безпеки для кожного пристрою своєї IT-інфраструктури від несанкціонованого доступу.

Список використаних джерел:

1. Most affected industries. URL: https://www.microsoft.com/en-us/wdsi/threats (дата звернення: 04.05.2022).
2. Кіберризики: як розуміти та управляти https://10guards.com/ua/articles/cyber-risks/ (дата звернення: 04.05.2022).
3. Zoom to pay $85M for lying about encryption and sending data to Facebook and Google. URL: https://arstechnica.com/tech-policy/2021/08/zoom-to-pay-85m-for-lying-about-encryption-and-sending-data-to-facebook-and-google/ (дата звернення: 04.03.2022).
4. Naidoo R. A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*. 2020. Vol. 29(3). P. 306–321. DOI: 10.1080/0960085x.2020.1771222
5. WHO reports fivefold increase in cyber attacks, urges vigilance. World Health Organization. URL: https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance (дата звернення: 04.05.2022).

Ключові слова: кіберризики, кібератака, кіберзахист, кібербезпека, освітній сектор.

Key words: cyber risks, cyberattack, cyber defense, cybersecurity, educational sector.