Рейнська В. Б., к.е.н., доцент,
Національний університет водного господарства та природокористування

КІБЕРБЕЗПЕКА ЗАКЛАДІВ ВИЩОЇ ОСВІТИ ЯК НЕОБХІДНИЙ ВИКЛИК СУЧАСНОСТІ

Кількість інтернет-користувачів за останні 10 років збільшилася більш ніж удвічі – з 2,18 млрд. на початок 2012 року до 4,95 млрд. на початку 2022 року [5]. Кількість інтернет-користувачів і висока залежність від інтернету викликали певні занепокоєння щодо безпеки. Перші загрози стосувалися фізичної інфраструктури інтернету. Однак зараз загрози варіюються від шкідливих кодів і програмного забезпечення до комп'ютерних вірусів. Однією з проблем, з якою стикаються в рамках кібербезпеки, є баланс між свободою і кібербезпекою. Намагаючись підтримувати кібербезпеку, необхідно також зберігати право на вільний доступ до інформації та боротися з кіберцензурою [3]. Кібербезпека стосується всіх політик, концепцій безпеки, інструкцій з безпеки, підходів до управління ризиками, навчальних заходів, які слугують меті збереження інституцій у кіберпросторі. Установи, залежні від інформаційних технологій, зберігають інформацію про свій персонал, інфраструктуру, практики та послуги в кіберпросторі. Кібербезпека передбачає формування властивостей безпеки таким чином, щоб протистояти ризикам безпеки в кіберпросторі. Крім того, основною метою кібербезпеки є забезпечення доступності, цілісності та конфіденційності інформації. Під доступністю інформації розуміється можливість отримання інформації в разі потреби, навіть якщо відбуваються зловмисні кібератаки. Цілісність інформації означає повноту та незмінність інформації. Особливо для секторів, які є чутливими до правильності інформації, таких як охорона здоров'я та промисловий дизайн, цілісність інформації є життєво важливою. Конфіденційність інформації відповідає запобіганню потрапляння інформації до сторонніх осіб.

Кібербезпека – це термін, який увійшов у наше життя після закінчення холодної війни як реакція на поєднання технологічного розвитку і зміни географічних умов. Вперше термін "кібербезпека" був запропонований вченими-комп'ютерниками на самому початку 1990-х років, щоб підкреслити різноманітні загрози, пов'язані з мережевими комп'ютерами. Кібербезпека – це здатність зберігати і захищати використання установою кіберпростору від кібератак, скоєних через кіберпростір з метою "порушення, виведення з ладу, знищення або зловмисного контролю над комп'ютерним середовищем /інфраструктурою; або знищення цілісності даних чи крадіжки контрольованої інформації" [2].

Кінцевими цілями кіберзагроз є наступні:

- Несанкціонований доступ до інформаційних і комунікаційних систем,
- Заміна, знищення та розголошення даних,
- Відмова в наданні послуг.

Кіберзагроза – це не лише кібератака, шкода або незаслужена вигода в результаті цієї атаки. Крім того, інтернет може використовуватися кібертерористами як засіб комунікації та пропаганди.

Можна визначити ризики кіберзагроз наступним чином:

- Розкриття конфіденційних даних про рахунки або клієнтів – ризик підриву найбільш цінних для установи відносин,
- Втрата когнітивної та розумової власності,
- Руйнування центральної інфраструктури,
- Фінансові втрати,
- Руйнування кібер-активів фінансової організації,
- Спричинення незручності та репутаційних ризиків організаціям.

Доступність і поширення цифрової інформації, доступної в інформаційних технологіях, а також збільшення кількості інфраструктур і систем, залежних від інформаційних технологій, зробили інформаційні технології вразливими до кібер-ризиків і атак. Залежність від інформаційних технологій створила загрозу для соціальних, політичних, економічних і військових інститутів. Тому масштаби кібератак і ризиків зробили поняття "кібербезпека" і "захист критичної інформації та інфраструктури" центральними питаннями у сфері інформаційних технологій.

Випадки кіберзагроз відбуваються у наступних випадках:

- Видалення головних сторінок загальнодоступних інтернет-сайтів,
- Захоплення файлів, доступних на вищезгаданих інтернет-сайтах, та їх викрадення,
- Зміна доступних файлів,
- Зробити інтернет-сайти недоступними за допомогою кібератак,
- Завантаження вірусів або шкідливого програмного забезпечення на персональні або інституційні комп'ютери,
- Ведення кіберпропаганди або розголошення конфіденційної інформації про установи.

Електронні дані знаходяться в основі університетської інфраструктури. Як наслідок, захист і безпека цих електронних даних є ключовим фактором з ряду причин:

- Університети створюють дані як основний інтелектуальний ресурс, який необхідно зберігати, отримувати і використовувати належним чином, щоб зрозуміти його академічну цінність,
- Університети залежать від доступу до конфіденційних даних від сторонніх організацій,
- Університети збирають дані, які стосуються їхньої робочої діяльності, такі як дані про студентів, бюджет або персонал.

Оскільки університети є виробниками та користувачами великих обсягів даних, вони є більш вразливими до кіберзагроз та атак. Саме тому для них необхідно розвивати засоби кібербезпеки.

Навчання є одним з ефективних способів боротьби з кіберзагрозами. Оснащення персоналу, студентів та викладачів інформацією про кібербезпеку як на індивідуальному, так і на інституційному рівні може мінімізувати кіберзагрози. Необхідно передбачити оцінку ризиків і ймовірних кібератак, а також розробити можливі плани дій. На даний час актуальної є пропозиція створити лабораторії кібербезпеки, щоб дати студентам можливість реалізувати новітні заходи з кібербезпеки. Крім того, можна створити кібер-клуб і запланувати курси з кіберзахисту. У клубі можна було б використовувати практичні заняття та інструменти. Крім того, заклади вищої освіти можуть підготувати плани дій з кібербезпеки, програми безпеки, спрямовані на захист університетських або пов'язаних з університетами інтернет-сторінок від кіберзагроз або атак. Крім того, можуть бути створені групи втручання з питань кібербезпеки. Обмежена інформація або дані можуть надаватися стороннім особам.

Джерело [4] рекомендує десять правил кібербезпеки:

- Правило територіальності: принцип територіальності робить інституції та нації більш потужними, щоб нав'язати своє домінування над інформаційною інфраструктурою, яка знаходиться на їхній території.
- Правило відповідальності: стосується того факту, що кібератака, яка була здійснена з інформаційної системи, розташованої на території держави, є доказом того, що цей акт може бути приписаний цій державі або установі.
- Правило співробітництва: стосується того факту, що кібератака, яка була здійснена через інформаційні системи, розташовані на території держави, призводить до обов'язку співпрацювати з державою-жертвою.
- Правило самозахисту: кожна нація та організація має право на самооборону.
- Правило збереження даних: дані, доступні на інтернет-сайті установи чи організації, повинні сприйматися як особисті, якщо тільки вони не надаються для інших людей чи організацій.
- Місія "правила турботи": кожна організація зобов'язана забезпечити належний рівень кібербезпеки в своїй інформаційній інфраструктурі.
- Правило раннього попередження: необхідно попереджати можливих жертв про невідомі та ймовірні кіберзагрози.
- Правило доступності інформації: громадськість має право бути поінформованою про загрози її життю та безпеці.
- Правило про правопорушення: кожна країна зобов'язана включити найбільш поширені кіберзлочини до свого кримінального законодавства та законодавства про правопорушення.
- Правило мандату: кожна установа зобов'язана співпрацювати і координувати свою діяльність у сфері глобальної кібербезпеки.

У закладах вищої освіти системи безпеки повинні бути створені з урахуванням наступних пропозицій [1]: Користувачі повинні бути ідентифіковані; Доступ до систем повинен контролюватися; Слід використовувати альтернативні сервери; Користувачі повинні бути під наглядом; IP-адреси комп'ютерів повинні зберігатися.

Оскільки освітні установи стають все більш залежними від кіберпростору, вони, відповідно, стають вразливішими до кіберзагроз. Обсяги даних, які навчальні заклади зберігають у своїх базах даних, та вразливі до кіберзагроз студенти цих закладів спонукають кіберзлочинців обирати навчальні заклади в якості мішеней для атак. Для того, щоб захистити навчальні заклади та студентів від кіберзлочинців і не замикати навчальні заклади, слід вжити вищезгаданих кіберзаходів.

Список використаних джерел

1. Çetin H., Gundak İ. And Çetin H.H. A researchon e-business security and cyberattacks. Çankırı Karatekin University Journal of Institute of Social Sciences, 2015. 6(2), 223 – 240.
2. IIROC. *Cybersecurity best practices guide for IIROC dealermembers*. Technical report. 2015.
3. Öğün M.N. and Kaya A. The importance of cybersecurity interms of national security and measures that canbe taken. Security Strategies, 2013. 9(18), 145-181.
4. Tikk E. Ten rules for cybersecurity. *Survival*, 2011. 53(3), 119-132.

63% людей зараз онлайн. Великий звіт Digital 2022 про користувачів інтернету. URL: https://ain.ua/2022/04/30/zvit-digital-2022/