KAPITEL 3 / *CHAPTER 3* [3]
CYBERSECURITY IN E-LEARNING SYSTEMS

DOI: 10.30890/2709-2313.2023-17-02-029

Вступ

Введення воєнного стану в Україні змусило академічне співтовариство звернутися до нових методів навчання, включаючи дистанційне і онлайн-навчання, також це підштовхнуло вищі навчальні заклади (ВНЗ) швидше рухатися в напрямку цифрового перетворення, поміщаючи дані в хмарі і використовуючи передові аналітичні засоби для поліпшення навчального процесу. Ризики в цьому цифровому світі набагато вищі, ніж в інших сферах, ми не можемо просто зупинити навчальний процес, щоб переконатися, що всі системи використовуються належним чином. Насправді будь-які зміни до систем, що потребуються навчальними закладами, вважаються досить ризикованими через «закон ненавмисних наслідків». ВНЗ навіть не хочуть застосовувати стандартні засоби сканування мережі та засоби виявлення вразливості проти своїх систем, визнаючи ризики перевантажити мережі, вплинути на доступність своїх ресурсів та збільшити затримку зв'язку.

Існує цілий ряд факторів, які стимулюють зростання атак на інфраструктуру установи. Наприклад, коли вони використовують нові аналітичні платформи на своїх ресурсах і переміщують дані в хмару, де вони можуть застосовувати сучасне машинне навчання, щоб досягти підвищення продуктивності. У той же час більшість установ мають користувальницькі інтерфейси, які працюють під управлінням Windows, що необхідно для спрощення контролю. Ці інтерфейси на базі Windows, як правило, працюють на набагато старіших операційних системах, які мають більше вразливих місць безпеки, ніж можна допустити. Автори загроз зосереджуються на використанні цих застарілих систем, які часто не виправляються через небажання IT співробітників вносити зміни, побоюючись, що виправлення або перезапуск систем може призвести до зупинки навчального процесу. Крім того, багато з цих систем вже не мають підтримки і більше не оновлюються. Порушники це знають і розуміють, що вони нарешті можуть легко отримати доступ до цих вразливих систем.

На сьогодні виділяють декілька тенденцій, що стосуються методів і методології атак-вимагачів. З них найбільше занепокоєння викликає новий

[3] ***Authors:*** *Viunenko Olexander Borisovich*

акцент на змішаних атаках з простим вимаганням та вимаганням в якому автори загроз викрадають конфіденційну інформацію компанії, перш ніж її зашифрувати. Якщо жертви відмовляться платити за ключ розшифровки, зловмисники погрожують публічно розповсюдити вкрадену інформацію [1].

Навіть якщо жертви і зможуть відновити зашифровані файли з резервної копії, вони можуть зазнати порушення цілісності своїх даних, втрати своїх даних та записів клієнтів, і їм доведеться платити законодавчі штрафи, не кажучи вже про відновлення пошкодженої репутації. У деяких випадках зловмисників підозрювали в тому, що вони виправдовують свої вимоги щодо викупу посилаючись на регуляторні штрафи, які організації мали б сплатити, тобто використовуючи це як ще одну тактику тиску, щоб змусити їх розглянути можливість сплати. Всі ці тенденції змушують співробітників, які відповідають за безпеку переоцінювати ризик та відповідно скорегувати свою реакцію на аварії, аварійне відновлення та плани безперервності роботи установи.

Здебільшого атаки на державні установи - це грубі атаки на відмову в обслуговуванні, або блокування, які переважно захоплюють ресурси та загрожують вивести їх з-під контролю. Для зловмисників може бути простіше діяти, якщо вони використовують готовий експлойт Windows, який вже має велику кількість посилань на літературу в Інтернеті, щоб скомпрометувати рівень інтерфейсу управління. Атаки, які установа може бачити, виявляються як одна або декілька відмов критичних систем управління, які раптово перестають реагувати, а інформація, що надходить від цих систем, стає підозрілою або ненадійною. Для цих атак вирішальним є час швидкого реагування, оскільки вони можуть почати поширюватися і ставати складнішими для стримування.

Виходячи з вище наведеного все більше стає актуальною організація навчання з питань кібербезпеки, які можуть допомогти створити та протестувати команди реагування на аварії, а також навчальні ігрові ресурси. Досвідчені викладачі також сприятимуть практичному досвіду та зможуть продемонструвати найефективніші практики, зібрані в зрілих галузях та організаціях. Вони дозволять провести такі команди через реалістичні сценарії порушення, які допоможуть їм засвоїти навички управління кризовими ситуаціями та сформувати кращу культуру безпеки, яка покращить стан кібербезпеки в навчальній установі.

3.1. Проблеми з кібербезпекою у ВНЗ

Програми-вимагачі - не єдина загроза кібербезпеці ВНЗ. Там, де є програми-вимагачі, майже завжди присутній фішинг. Проблема як з програмами-вимагачами, так і з фішингом полягає в тому, що цифрові зловмисники можуть використовувати ці загрози для викрадення даних своїх жертв. Зловмисники можуть скомпрометувати бази даних установи і використовувати ці деталі для подальших атак, таких як порушення цілісності даних. Вони також можуть використовувати його для власної атаки, яка може скомпрометувати бізнес-процеси установи.

Зараз більшість установ мають цифрову присутність. Потреби кібербезпеки для ВНЗ загалом не відрізняються від потреб виробництва. Вони також хочуть отримувати дані в режимі реального часу, щоб вони могли стежити за станом своїх інформаційних процесів. Але, є проблема. Багато інформаційних процесів недостатньо обладнані для захисту від сьогоднішніх загроз. Деякі з цих систем використовуються вже десятки років, тобто ми маємо справу із застарілими системами які використовують власні протоколи для спілкування між собою. Таким чином, вони не можуть легко отримувати віддалені оновлення і це також сприяє зростанню рівня цифрових загроз для навчальних закладів [2].

3.2. Як зловмисники використовують вразливості

Вищі навчальні заклади стикаються з постійним потоком кібератак. Після інциденту в 2015 році Кевін Муроні, колишній віце-проректор з інформаційних технологій в Університеті штату Пенсильванія - заявив The New York Times, що штат Пенсильванія стикається із середньою кількістю 20 мільйонів атак на день, що є "типовим для дослідницького університету". Як зазначив Кім Мілфорд, виконавчий директор Центру обміну інформацією та аналізу інформаційних і освітніх мереж при університеті Індіани, університети зараз "потрапили в дорогу гонку озброєнь", оскільки вони досліджують нові способи боротьби з нинішніми атаками та намагаються бути на крок попереду атак, які ще мають відбутися. Незалежно від того, чи успішні кібератаки, на думку Мілфорда, вони представляють дорогу і постійно актуальну проблему, яку університети змушені вирішувати [3].

Але ризики, спричинені кібератаками, можуть виходити за рамки фінансових втрат для ВНЗ. В інформаційних системах університетів міститься величезний обсяг конфіденційних даних - від номерів документів до цінної інтелектуальної власності, яка в разі викрадення чи компрометації може завдати значної шкоди далеко за стінами ВНЗ. Тобто вони можуть бути більш значними, ніж потенційні фінансові втрати і представляти серйозну загрозу репутації університету та безпеці його студентів.

Хоча практично кожна велика галузь стикається зі значними проблемами кібербезпеки, вища освіта є особливо вразливою з ряду ключових причин. Загалом це пов'язано з унікальною культурою академічних кіл, яка пишається тим ступенем відкритості та прозорості, якого бракує більшості галузей. Сучасні ВНЗ історично зосереджували зусилля на забезпеченні того, щоб факультети, студенти і громадськість мали можливість швидкого і вільного спілкування. Це робить комп'ютерні мережі ВНЗ такими ж відкритими та привабливими, як і університетські містечка. Інша причина пов'язана з історією - зокрема, як довго ВНЗ працюють в Інтернеті. Вони завжди були головними мішенями для кібератак, в основному тому, що ВНЗ були одними з перших місць, де був відкритий доступ до Інтернету, а раніше і до міжнародних аматорських некомерційних комп'ютерних мереж, тобто завдяки відносно тривалому доступу до Інтернету ВНЗ вже давно стали помітними мішенями, і тому їх слабкі сторони дуже відомі та зрозумілі для порушників. Сучасні кібератаки використовують найсучасніші технології та методи для використання інформаційних систем ВНЗ, які, в деяких випадках, дуже застарілі та нестандартні. Університетські ІТ-системи часто характеризуються децентралізованою і безсистемною архітектурою, яку зловмисники можуть легко використати і хоча з операційної точки зору окремим підрозділам має сенс діяти у власних ІТ-структурах, але такий тип поступового налаштування створює чіткі вразливості інформаційної безпеки для ВНЗ. Для великої кількості самостійних підрозділів є велика ймовірність, що принаймні в одному з них може існувати якась комбінація застарілих пристроїв, застарілої ОС, неадекватної фільтрації електронної пошти, антивірусного захисту, несправного резервного копіювання даних або недостатнього рівня підготовки та політики користувачів.

Хоча ці проблеми характерні не тільки для вищої освіти, проте дефіцит фахівців у галузі кібербезпеки є значною перешкодою, яку ВНЗ повинні подолати для вирішення вищезазначених проблем. Недавнє дослідження, яке

було проведене консалтинговою фірмою Frost & Sullivan, відмічає, що очікується 1,8 млн незаповнених робочих місць в галузі кібербезпеки в 2020 році, і що цей дефіцит кваліфікованих кадрів існує в глобальному масштабі, так майже 70 відсотків фахівців у всьому світі відмічають, що занадто мало працівників в галузі кібербезпеки присутні серед персоналу установ. Оскільки попит на фахівців з кібербезпеки значно випереджає пропозицію, компанії часто платять значні гроші за досвід у галузі кібербезпеки. Це, ймовірно, ставить університети у серйозний невигідний стан, коли вони намагаються заманити таких фахівців із високооплачуваних робочих місць у приватному секторі, таких як Alphabet, Facebook тощо [3].

Сучасні зловмисники застосовують різноманітні тактики та інструменти під час запуску кібератак. Загалом можна виділити дві найпоширеніші методи:

•SQL-ін'єкції (SQLi) – це імовірно найсерйозніша проблема для веб-додатків. SQLi являють собою атаки, які призначені для обходу захисту із використанням паролів шляхом атаки баз даних, що лежать в основі різних додатків. SQL-ін'єкції працюють завдяки використанню слабких сторін коду, який лежить в основі коду сторінок введення даних (наприклад, сторінок введення імені користувача та пароля), вони змушують базу даних повертати конфіденційну інформацію. ВНЗ мають безліч захищених паролем онлайн-додатків - від звітів студентів до інформації про роботу викладачів, які теоретично можуть бути зламані із використанням SQL-ін'єкцій. До тих пір, поки вищі навчальні заклади матимуть слабкі місця в свої базові бази даних, ін'єкції SQL, ймовірно, залишатимуться поширеними і занадто легкими для використання хакерами.

•Фішинг. Фішинг-атаки характеризуються використанням електронної пошти або веб-сторінок, які призначені для того, щоб обдурити користувачів при введенні конфіденційних даних, таких як паролі або дані кредитних карток. Як правило, фішер надсилає електронне повідомлення великій групі осіб, адреси яких він захопив з адресних книг та веб-сайтів через Інтернет. Таке повідомлення завжди добре сформоване, виглядає офіційно, та може стверджувати, що воно надійшло від фінансової установи, постачальника послуг або будь-якої іншої організації, яка добре відома одержувачам. Часто одержувача просять надати інформацію, натиснувши посилання на веб-сайт в електронному листі, але хоча посилання на веб-сайт може виглядати законним, посилання, яке відображається,

не обов'язково є фактичним сайтом, який ви плануєте відвідати. Ряд досліджень показують, що за останній рік більш ніж 30 відсотків користувачів в освітній галузі стали об'єктами атак із застосуванням фішингу.

Фішинг-атаки можуть мати широкий спектр кінцевих цілей - від викрадення даних користувачів, до встановлення програми-вимагача на комп'ютер жертви та отримання фінансових платежів. Хоча ці атаки можуть здатися очевидними та їх легко уникнути, але багато досліджень показують, що значна частина підприємств вже стала жертвою фішинг-шахрайства.

Хоча вищезазначені тактики виявилися досить ефективними, але існує декілька простих стратегій, які допоможуть їм запобігти: зупинка атак SQLi через підготовлені запити, збережені процедури та перевірки вводу.

Підготовлені запити. ВНЗ повинні побудувати свої основні бази даних із використанням підготовлених запитів. Підготовлені оператори гарантують, що зловмисник не може змінити ціль запиту, навіть якщо зловмисник вставляє команди SQL. По суті, підготовлені оператори можуть зробити команди SQL, що використовуються як вхідні дані користувача (імена користувачів та паролі), безсилими.

Збережені процедури. Збережені процедури можуть мати той самий ефект, що і підготовлені оператори, основна відмінність полягає в тому, що код SQL для збереженої процедури визначається і зберігається в самій базі даних, а потім викликається із програми, але збережені процедури не завжди можуть бути придатними для захисту від атак SQLi, але можуть бути життєздатним варіантом для ВНЗ, коли вони написані та реалізовані належним чином.

Перевірка вводу. Атаки із використанням SQL-ін'єкцій використовують програми та бази даних, які не використовують перехресні посилання та перевірку введених даних. Отже, логічним кроком на шляху запобігання цим атакам є визнання того, що побудована база даних вимагає обов'язкової перевірки всіх вхідних даних. Корпорація Майкрософт також називає перевірку вхідних даних ключовим методом уникнення атак SQLi в рамках своєї моделі веб-розробки ASP.net.

На відміну від запобігання атакам SQLi, які можна зробити за допомогою внутрішніх технічних виправлень ВНЗ, запобігання шахрайству в основному покладається на кінцевих користувачів - викладачів, персонал та студентів. Існує кілька кроків, які повинні зробити ВНЗ, щоб забезпечити необхідну пильність всіх своїх кінцевих користувачів:

1. Кампанії з підвищення кваліфікації. ВНЗ повинні вимагати від кінцевих користувачів пройти відповідне навчання, яке охоплює питання пов'язані з фішингом та методами його розпізнавання. Такі тренінги слід повторювати регулярно і вони повинні піддавати користувачів різному спектру фішингових атак. Надання прикладів реальних атак та створення репозиторію для таких атак, також може підвищити обізнаність користувачів.

2. Фільтри електронної пошти. В першу чергу ВНЗ повинні встановити фільтри для електронної пошти, які надсилають підозрілі не-університетські електронні листи до папки спаму користувача. Незважаючи на те, що це далеко не надійне рішення, це перший важливий крок, який може запобігти використанню зловмисних електронних листів.

Хоча перелічені вище стратегії не можуть бути всеосяжними і не зможуть запобігти кожному нападу, але вони являють собою відносно прості кроки, які можуть дати значні переваги у боротьбі ВНЗ з потенційними кіберзагрозами. Проте кіберзагрози постійно розвиваються, і немає жодних гарантій того, що загрози, з якими стикаються сьогодні і стратегії їх пом'якшення, будуть нагадувати ті, що будуть виникати в майбутньому.

Довгострокові рішення з питань кібербезпеки повинні включати принципові зміни в написанні та розробці програмного забезпечення. Розробка програмного забезпечення повинна бути посилена так, щоб люди брали до уваги ризики безпеки та вразливості інформаційних систем. Ще одним ключем до вирішення майбутніх викликів в галузі кібербезпеки, є залучення надійної та стабільної групи експертів у цій галузі. І хоча бюджет ВНЗ зазвичай досить обмежений, проте існує ряд способів вирішити цю проблему, включаючи використання послуг експертів-фрілансерів та фахівців бажаючих працювати віддалено.

Хоча проблеми з кібербезпекою, що стоять перед вищою освітою, великі, а вартість їх вирішення величезна, потенційні фінансові та репутаційні ризики, які виникають при недостатньому захисті, ймовірно, будуть ще більшими. Тому заклади вищої освіти можуть виявити, що ефективні рішення з кібербезпеки в кінцевому рахунку можуть окупитись.

3.3. Створення стратегії кібербезпеки для ВНЗ

Керівники кібербезпеки у вищій освіті витрачають лише невеликий відсоток свого часу на розробку стратегії, але ця діяльність, ймовірно, матиме найбільший вплив на ВНЗ в самий найближчий час. Як правило, вони не усвідомлюють, що поєднання основних цінностей вищої освіти - автономії, конфіденційності та експериментів саме по собі створює значні проблеми для кібербезпеки ВНЗ.

Першим кроком у вирішенні цих проблеми кібербезпеки у ВНЗ є розробка та реалізація відповідної дієвої стратегії. Багато підходів, які користувачі називають стратегіями, насправді складно віднести до стратегій. Сюди входять "програми безпеки на основі ризику" або "стратегії на основі ризику". Ризик - це лише одна складова стратегії, тому зосередження уваги лише на ризику веде до прийняття лише тактичних рішень. Інші компоненти включають посилення норм регулювання та відповідності. Виконання нормативних вимог та вимог дотримання має бути стратегічною метою, але знову ж таки, це не повинна бути сама стратегія. Загалом термін стратегія може бути визначено наступним чином: "Довгостроковий план, який розподіляє ресурси та встановлює основу для прийняття рішень для досягнення довгострокових цілей в умовах невизначеності" [4].

Бізнес стратегія. Бізнес-стратегії дещо простіші, ніж стратегії вищої освіти, оскільки майже кожна діяльність, яку здійснює бізнес, може бути повністю простежена. Майкл Тресі та Фред Вірсема виділяють три типи бізнес-стратегії: близькість клієнтів, лідерство продукції та операційну досконалість [5]. Кожен з них пропонує структуру, яка відповідає викладеному вище визначенню стратегії.

ІТ-стратегія. Визначення технологічної стратегії у Вікіпедії: "загальний план, який складається з цілей, принципів і тактик, що стосуються використання технологій у певній організації". Tech Target заявляє, що ІТ-стратегія - це "всеосяжний план, який окреслює, яку технологію слід використовувати для досягнення ІТ-цілей та бізнес-цілей" [6]. Основна концепція, на яку слід звернути увагу, полягає в тому, що ІТ-стратегія сама по собі не є конкурентною. У бізнес-стратегії, навпаки, компанії прагнуть досягти успіху над конкурентами, а ІТ-стратегія повинна підтримувати стратегії організації та забезпечувати те, що потрібно цій організації. Багато ІТ-стратегій - це просто тактичний перелік найкращих практик. ІТ-стратегії, як правило, передбачають пріоритетність ресурсів як в організації, так і в ІТ-відділі. Довгострокові цілі зазвичай діляться

на дві категорії: ті, що забезпечують досягнення бізнес-цілей, і ті, що звільняють ресурси для ведення бізнесу. Наприклад, роздрібний бізнес може мати стратегію близькості клієнтів. Для виконання цієї стратегії він може вибрати збір та аналіз даних. Компанія може прийняти рішення про збільшення інвестицій в інформаційні технології з метою збільшення доставки та якості інформації як бізнес-мети. Прикладом стратегії звільнення ресурсів може бути консолідація IT, яка може зменшити скорочення реагування на ресурси, які можна витратити деінде.

Ризик повинен бути частиною IT-стратегії. Ризики включають такі очевидні, як аварійне відновлення та безперервність бізнесу. Управління ризиками передбачає визначення того, скільки ризику може переносити бізнес у порівнянні із витратами, необхідними для вирішення цих ризиків. Доступність також є центральним елементом кібербезпеки. Ризики конфіденційності, цілісності та доступності є стрижнем кібербезпеки, тому це очевидне місце, де IT-стратегія та стратегія кібербезпеки повинні узгоджуватися. Однак внесення стратегії кібербезпеки до IT-стратегії є помилкою. Ці дві функції занадто різні, щоб бути повністю інтегрованими.

Стратегічний аналіз у бізнесі, як правило, організовується за допомогою сильних, слабких сторін, можливостей та загроз – він також відомий як SWOT-аналіз, SWOT-аналіз також може бути застосований і для кібербезпеки. Але існує три характеристики кібербезпеки, які пропонують інший підхід. По-перше, кібербезпека завжди буде функцією стратегії організації. По-друге, кібербезпека реактивна, а не ініціативна. Нарешті, кібербезпека є асиметричною.

Кібербезпека завжди буде функцією стратегії організації. Метою кібербезпеки є захист інформаційних активів організації. Організація володіє інформаційними активами, щоб вона могла виконати свою місію та надати їй перевагу перед конкурентами.

Кібербезпека реактивна, а не ініціативна. Багато експертів заохочували нас активно мислити про кібербезпеку та називали свої стратегічні підходи ініціативними. Але ми не можемо розшукати порушників і заарештувати їх, або порушити їх наміри, перш ніж вони нападуть на нас. Активна стратегія означає діяти раніше, ніж це роблять супротивники - або попередити їх, або погіршити їх здатність досягти своїх цілей. Ми можемо підготуватися до нападів до того, як вони трапляться, але також ми не можемо діяти, доки такі атаки не відбудуться. Тобто порушники все ще вибирають час, місце та спосіб нападу.

Кібербезпека є асиметричною. Це тому, що у порушників є варіанти, яких немає у ВНЗ. Мета ВНЗ - захистити свою інформацію. Цілі порушників - викрасти або змінити інформацію, або перешкодити установі мати доступ до неї.

Таким чином замість розгляду SWOT, стратегічний аналіз кібербезпеки повинен розглядати загрози та обмеження. По суті, метою програми кібербезпеки є пом'якшення загроз (ризиків), з якими вона стикається, працюючи в рамках своїх обмежень. Хороша стратегія кібербезпеки фокусується на виявленні найбільших загроз, для того щоб створити необхідні ресурси для захисту установи і захисту від цих загроз.

Загалом стратегія кібербезпеки повинна зосереджуватись на тих загрозах, які були визнані найбільш серйозними, враховуючи численні обмеження, що обмежують програми кібербезпеки у вищій освіті:

Правила та закони. Програма кібербезпеки повинна відповідати нормам та законам. Ресурси, які були витрачені на відповідність нормативним вимогам, недоступні для інших цілей.

Фінансування. Це обмеження стосується капітальних і операційних витрат, а також суми та строків для грошей, які ВНЗ можуть витратити.

Накладні витрати на бізнес. Індивідуальна культура різних груп користувачів у ВНЗ визначатиме, скільки можна досягти за допомогою контролю безпеки. Процес присвоєння рейтингів високої, середньої або низької толерантності для різних груп може забезпечити кращу картину про загальну толерантність організації до накладних витрат на безпеку.

Час та компетентність персоналу. Можливості персоналу та можливість наймати та утримувати фахівців для ВНЗ досить обмежені. Плинність кадрів і спроможність персоналу засвоїти нові навички - все це приклади обмежень щодо часу та компетентності персоналу.

Політичний капітал. Це обмеження дещо збігається із накладними витратами на бізнес, але тут акцент робиться на лідерство та підтримку з боку колег в галузі ІТ. Наприклад, якщо ВНЗ нещодавно зазнав серйозних порушень безпеки, то команда фахівців по безпеці може мати значний політичний капітал перед вищим керівництвом.

Календарний час. Це обмеження включає виявлення будь-яких обмежень у часі, а також визначення послідовності рішень з урахуванням календарного часу.

Підзвітність. Усвідомлення культури підзвітності в установі має вирішальне значення для розробки успішної стратегії кібербезпеки.

Управління. Якщо управління покладається і на кібербезпеку, то це є обмеженням. Якщо управління може бути створене фахівцем з інформаційної безпеки, то це є складовою стратегії кібербезпеки.

Подібно до того, як поєднуються відповідні шаблони дизайну програмного забезпечення при створенні дизайну програми, підбір правильних стратегічних шаблонів також може допомогти оперативно створити чи змінити стратегію кібербезпеки ВНЗ. Колекція стратегічних зразків кібербезпеки, в свою чергу формує стратегію більш високого рівня. Матриця - це природний спосіб охопити всі рівні стратегічного плану.

На сайті Національного інституту стандартів і технологій (NIST) наведена матриця з п'ятьма стратегічними функціями кібербезпеки, яка містить наступні елементи: ідентифікація, захист, виявлення, реагування та відновлення - на лівій стороні та з людьми, процесами та технологіями на її вершині [7]. Це візуальне уявлення показує, як вирішуються ці п'ять основних функцій, а також компроміси, які при цьому приймаються. П'ять функцій верхнього рівня також може бути поділений на більшу кількість областей. Наприклад, захист може бути деталізований як контроль доступу, обізнаність та навчання, безпека даних, процеси захисту інформації, технічне обслуговування та захисна технологія. Ще один аспект, яким може бути корисна стратегічна матриця кібербезпеки - це розуміння нових пріоритетів та закономірностей. Оскільки компроміси проводяться з метою розподілу ресурсів у межах обмежень, може стати очевидним, що початкові думки та плани просто не практичні. Може стати зрозумілим кращий спосіб розподілу ресурсів або інша стратегічна модель.

Висновки

На сьогодні кібератаки представляють серйозну загрозу репутації ВНЗ та безпеці його студентів. Кібербезпека вимагає стратегічного підходу, оскільки вона досить складна, швидко змінюється і потенційно може стримувати розвиток ВНЗ. Кібербезпека відрізняється від ІТ або ділових операцій, оскільки вона є змагальною, реактивною та асиметричною. Зусилля з кібербезпеки повинні бути тісно узгоджені із загальною стратегією установи та повинні доповнювати її ІТ-стратегію. Нездатність ВНЗ мислити та діяти стратегічно призводить до неефективного використання ресурсів та збільшує інституційний ризик.

Стратегія кібербезпеки повинна визначати інформаційні активи установи та вплив на них можливих кібератак. ВНЗ мають обмежені ресурси для витрат на кібербезпеку. Ці ресурси включають не лише фінансування та персонал, а й такі нематеріальні активи, як політичний капітал та підзвітність. Ефективна стратегія повинна боротися з найсерйознішими загрозами, залишаючись в рамках обмежень ВНЗ. Загалом стратегія кібербезпеки повинна бути довгостроковою, ефективною в умовах невизначеності, а також визначати пріоритети на ресурси та забезпечувати основу для узгодження дій персоналу в усьому ВНЗ. Ефективний план кібербезпеки можна розробити шляхом побудови стратегічних схем кібербезпеки побудови стратегічних схем кібербезпеки. Крім того, матриця кібербезпеки, яка відповідає функціям NIST - людям, процесам і технологіям, може забезпечити наочне представлення реалізації всієї стратегії кібербезпеки ВНЗ. Нарешті, послідовність змісту цієї матриці може створити дорожню карту проектів, ініціатив та зусиль для реалізації стратегії.

Кібератаки на ВНЗ стають все частішими та завдають все більшої шкоди. Кіберзагроза вищій освіті в цілому є значною і, ймовірно, буде постійно зростати в найближчому часі. Для вирішення цієї проблеми, особливо у ВНЗ, потрібне стратегічне мислення, і така стратегія повинна виходити із стратегічного мислення, яке орієнтоване на кібербезпеку.