КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (18), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.18.623
УДК 004.946.5.056

Лахно Валерій Анатолійович
доктор технічних наук, професор, завідувач кафедри комп'ютерних систем та мереж
Національний університет біоресурсів і природокористування України, м.Київ, Україна
ORCID ID: 0000-0001-9695-4543
lva964@gmail.com

Каламан Єрболат
Кафедра кібербезпеки, обробки та зберігання інформації
Сатбаєвський університет, Алмати, Казахстан
ORCID ID: 0000-0002-8607-737X
kalaman.erbolat@gmail.com

Ягалієва Багдат Есеновна
PhD, доцент, декан факультету науки та техніки
Університет Єсенова, м.Актау, Казахстан
ORCID ID: 0000-0001-9695-4543
lva964@gmail.com

Криворучко Олена Володимирівна
доктор технічних наук, професор, завідувач кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет, м.Київ, Україна
ORCID ID: 0000-0002-7661-9227
kryvoruchko_ev@knute.edu.ua

Десятко Альона Миколаївна
PhD in Computer Sciences, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет, м.Київ, Україна
ORCID ID: 0000-0003-2860-2188
desyatko@knute.edu.ua

Цюцюра Світлана Володимирівна
доктор технічних наук, професор, завідувач кафедри інформаційних технологій
Київський національний університет будівництва і архітектури, м.Київ, Україна
ORCID ID: 0000-0002-4270-7405
svtsutsura@gmail.com

Цюцюра Микола Ігорович
доктор технічних наук, доцент, доцент інформаційних технологій
Київський національний університет будівництва і архітектури, м.Київ, Україна
ORCID ID: 0000-0003-4713-7568
mitsiutsiura@gmail.com

МОДЕЛЬ ЗАХИСТУ ЛОКАЛЬНОЇ МЕРЕЖІ НАВЧАЛЬНОГО ЗАКЛАДУ СЕРВЕРНОЇ СИСТЕМИ ВІРТУАЛІЗАЦІЇ

Анотація. Запропоновано новий підхід для удосконалення інформаційної безпеки (ІБ) мережі навчального закладу. Пропонований підхід – структурований і системний. Ще дозволяє оцінити захищеність мережі навчального закладу (наприклад, університету) в цілому, а також її підсистем та компонентів, які забезпечують ІБ навчального закладу. Для оцінювання ступеня захищеності використовуються статистичні, експертні, евристичні та інші показники. Запропонована модель дозволяє описати процедуру забезпечення ІБ мережі університету. Пропонується збалансована система показників ІБ, що дозволить оцінювати ефективність захисту мережі університету. Також в рамках дослідження, біло побудовано модель захищеної мережі навчального закладу, де мережеві пристрої були з'емульовані у віртуальній машині (ВМ) зі встановленим додатком EVE-NG. Інші ресурси мережі відтворені

ISSN 2663 - 4023

завдяки серверній системі віртуалізації Proxmox VE. На хостах під управлінням PVE було розгорнуто систему виявлення загроз IPS Suricata, платформу Splunk та фільтр DNS-адрес Pi-Hole.
Новий механізм селекції на відміну від традиційної, передбачає створення проміжної популяції. Формування проміжної популяції відбувається в кілька етапів. На першому етапі перша половина популяції формується на основі метрики - частка вразливостей об'єкта інформатизації, які усунуті в установлені терміни. На другому етапі друга половина проміжної популяції формується на основі метрики - частка ризиків, які неприпустимі для інформаційних активів об'єкта інформатизації. Далі ці частини проміжної популяції змішуються. Після змішування формується масив номерів і виробляється змішування. На заключному етапі селекції для схрещування будуть братися екземпляри (індивіди) за номером з цього масиву. Номери вибираються випадково. Ефективність застосування даної методики підтверджена практичними результатами

Ключові слова: розподілені мережі, навчальний заклад, інформаційна безпека, віртуалізація, IDS, SIEM

ВСТУП

Тема захисту інформації завжди була важливою, коли справа стосувалася державних таємниць, бізнесу, та приватних секретів. Тема інформаційної безпеки (ІБ) у навчальному закладі також актуальна тому що говорячи про таку суспільну групу, як діти та підлітки варто зазначити, що це ті, хто найчастіше завантажує собі нові застосунки на смартфони, планшети та комп'ютери. Частіше за все цими застосунками є ігри. А такі застосунки далеко не завжди проходять перевірку в онлайн-магазинах застосунків, не кажучи вже про ті, які завантажуються з інтернету/торентів та ін. У багатьох випадках подібні контрафактні застосунки містять потенційні загрози та можуть бути розповсюджені через локальну мережу навчального закладу (школи, коледжу, університету). В навчальних закладах зазвичай слабкий рівень безпекових налаштувань, через що мережі шкіл, коледжів та університетів можуть бути одним з місць розповсюдження шкідливого програмного забезпечення (ПЗ) [1, 2].

В даній статті стоїть задача як завдяки засобам віртуалізації змоделювати мережу навчального закладу та розробити надійну систему захисту (інформаційної безпеки), що допомогла б вирішити дані проблеми та при цьому не вимагала великих вкладень, через часто недостатній рівень інвестування державою ресурсів у навчальні заклади. Ідеальними для цього є системи з відкритим кодом, які не вимагають вкладень та часто мають широку підтримку від користувачів, що значно спрощує впровадження таких систем на практиці.

Постановка проблеми. Без сумніву в умовах війни з рф потребують просиляння захисту від комп'ютерних атак обчислювальні мережі всіх державних та приватних об'єктів інформатизації. Саме тому запропоновано підхід для удосконалення інформаційної безпеки (ІБ) мережі навчального закладу. Пропонований підхід – структурований і системний. Ще дозволяє оцінити захищеність мережі навчального закладу (наприклад, університету) в цілому, а також її підсистем та компонентів, які забезпечують ІБ навчального закладу. Для оцінювання ступеня захищеності використовуються статистичні, експертні, евристичні та інші показники.

Аналіз останніх досліджень і публікацій. Ландшафт кіберзагроз та методи забезпечення ІБ, та кібербезпеки, зокрема, доволі швидко змінюються. Це стало ще більш очевидно з початком пандемії COVID-19, особливо в корпоративних бізнес-операціях та IT-архітектурі компаній. Зловмисники почали активно користуватися цими

ISSN 2663 - 4023

змінами, спрямовуючи свої атаки на вразливі місця у сфері віддаленого доступу, хмарних обчислень та інших рішень, прийнятих в межах нових політик ІБ. Зростають також і такі загрози, як багатовекторні атаки, зараження вірусами-вимагачами комп'ютерів кінцевих користувачів, атаки на ланцюги поставок. А складні атаки, такі як використання вразливості Log4j, впливають на мільйони компаній, в тому числі Amazon, Tesla і Cisco [3, 4]. Вище наведені приклади еволюції ландшафту кіберзагроз мають значний вплив на тенденції розвитку кібербезпеки, оскільки організації мусять адаптуватися до новітніх загроз. Програми-вимагачі стали однією з найпоширеніших і найпомітніших загроз кібербезпеки останніх років. За даними Cybersecurity Ventures, прогнозується, що збитки від програм-вимагачів складуть 11,5 мільярдів доларів США. Поточний обсяг загрози призводить до появи нової жертви кожні 14 секунд. Реалізація полягає у зараженні комп'ютера жертви шкідливим програмним забезпеченням, що призначене для шифрування файлів у системі та вимагання викупу в обмін на ключ дешифрування, необхідний для відновлення доступу до цих файлів. В останні роки загроза вірусів-вимагачів зростає та еволюціонує, оскільки суб'єкти кіберзагроз вдосконалюють свої інструменти та методи. Сучасні атаки вимагачів є цілеспрямованими і вимагають багатомільйонні викупи. Ці атаки також еволюціонували і включають в себе різні способи вимагання, такі як крадіжка даних перед їх шифруванням і загроза розподіленої атаки на відмову в обслуговуванні (DDoS), щоб надати зловмиснику додаткові важелі впливу на жертву, щоб змусити її задовольнити вимогу викупу [5, 6].

Як показано у [7, 8, 23-32] фішинг та компрометація ділової електронної пошти залишаються найпопулярнішими низько-технологічними методами, які використовують кіберзлочинці для отримання доступу до мереж. Фішингові електронні листи виглядають як звичайні, щоденні електронні листи від компаній, керівників та довірених осіб. При переході за шкідливими посиланнями або наданні інформації на фальшивих цільових сторінках на пристрої завантажується шкідливе програмне забезпечення, що дозволяє кіберзлочинцям отримати доступ до критично важливих мереж. З широким розповсюдженням хмарних сервісів, таких як Gmail та Office 365, хакери стають все більш витонченими у своїх навичках самозванства та соціальної інженерії. Хмарні сервіси не можуть адекватно захистити ваші конфіденційні дані. Вжиття додаткових заходів безпеки електронної пошти з шифруванням та аналізом загроз - це розумний спосіб захистити співробітників від витончених атак електронною поштою [9].

До наступної категорії кіберзагроз, що набирають популярність, належать злами систем ланцюгів постачання. Так, злом SolarWinds у 2020 році був першим з багатьох таких нещодавніх атак. Часто для їх реалізації використовувались довірчі відносини, що існують між організаціями [10]. Метод реалізації такої атаки полягає у наступному: кожна компанія має набір довірених клієнтів, постачальників та інших партнерів. Зловмисники використовують дані довірчі відносини, та завдяки наявному доступу до систем партнера, проводять атаку на IT-активи іншої організації або здійснюють фішингову атаку. За [11], 75% опитаних IT-фахівців визнали, що ризик проникнення через третю сторону є небезпечним і зростає. Зокрема, за даними Soha Systems, 63% всіх витоків даних можуть бути прямо або опосередковано пов'язані з доступом третіх осіб.

Злом SolarWinds та подібні атаки базувалися на тому, що всі компанії використовують у своїх мережах довірене стороннє програмне забезпечення. Шкідливий код, що вбудовувався в програмне забезпечення або оновлення наявного програмного забезпечення, був встановлений і запущений без додаткових перевірок автентичності, забезпечуючи внутрішній доступ до мережі організації.

ISSN 2663 - 4023

Використання Інтернету речей (IoT) зростає з кожним днем (за даними Statista.com, очікується, що до кінця 2022 року кількість пристроїв, підключених до Інтернету речей, досягне майже 31 мільярда). Більше підключених пристроїв означає більший ризик. Потрапивши під контроль хакерів, пристрої Інтернету речей можуть бути використані для перевантаження мереж, отримання доступу до конфіденційних даних або блокування важливого обладнання з метою отримання фінансової вигоди.

Все частіше суб'єкти кіберзагроз вдаються до багатовекторних атак. Ще десятиріччя назад програми-вимагачі були зосереджені виключно на шифруванні даних, а тепер включають в себе крадіжку даних, DDoS та інші загрози. Основним викликом у проведенні більшості кібератак є отримання доступу до цінних даних організації.

Наведені приклади атак на ІТ-ресурси компаній мають вплив на визначення трендів у протидії інформаційним загрозам, зокрема у навчальних закладах. Таким чином, враховуючи все що було розглянуто вище, тема нашого дослідження є вкрай актуальною.

Мета статті. Мета дослідження - розробка моделі інформаційної безпеки розподіленої мережі навчального закладу.

Завдання дослідження:

1. розробка моделі ІБ розподіленої мережі навчального закладу;
2. побудовано та дослідити модель ІБ мережі, де мережеві пристрої з’емульовані у віртуальній машині зі встановленим додатком EVE-NG, а інші ресурси відтворені завдяки серверній системі віртуалізації Proxmox VE.

МОДЕЛІ ТА МЕТОДИ ДОСЛІДЖЕННЯ

Модель інформаційної безпеки розподіленої мережі навчального закладу. Нехай ресурси кожного компонента розподіленої обчислювальної мережі (РОМ), наприклад, навчального закладу, мають потенційну небезпеку класу CL_l, кожна з яких cl_{kl} має реалізації $\{x_{jkl}\}$ [12, 13]. Питома ефективність для засобу захисту інформації (ЗЗІ) (метод, програмне забезпечення (наприклад, антивірусне програмне забезпечення, або IDS/IPS, SIEM), апаратура) конкретної реалізації загрози дорівнює EFA_{ijkl}, де $i-$ індекс засобів захисту $(i=1,2,...,I)$, $j-$індексу способу реалізації загрози для ІБ $(j=1,2,...,J)$, з індексом $k=1,2,...,K$.

Ефективність ЗЗІ для мережі навчального закладу вимірюється динамічно, за одиницю часу [14, 15].

Ефективність заходів захисту інформації у мережі навчального закладу (EFE_{ijkl}) залежить від методу нейтралізації загрози $i-$им ЗЗІ. Можна визначити залежність ефективності захисту EFE_{ijkl} від кількості застосованих ЗЗІ одного типу (класу): $EFE_{ijkl}=f\left(EFA_{ijkl},n_i\right)$, де n_i- кількість використовуваних $i-$их ЗЗІ для забезпечення інформаційної безпеки РОМ навчального закладу.

Будуємо залежність періоду T функціонування окремої компоненти РОМ від ефективності захисту EFE_{ijkl} і визначаємо максимум $n_{i\max}$ одночасно застосовуваних ЗЗІ у складі підсистеми ІБ РОМ навчального закладу.

На наступному рівні захисту ресурсів РОМ навчального закладу ЗЗІ взаємодіють паралельно. Тому доцільно застосувати мультиплікативну модель [16, 17]. Наприклад, ступінь ефективності ЗЗІ на цьому рівні можна описати виразом:

ISSN 2663 - 4023

$$Q_{ikj} = 1 - \prod_{i=1}^{I} \left[1 - EFE_{ijkl}\left(EFA_{ijkl}, n_i\right)\right], \quad (1)$$

де I – множина індексів всіх ЗЗІ для мережі навчального закладу.

Наприклад, функціями виду:

$$Q_{ikj} = \prod_{i=1}^{I} \zeta_i^{\alpha_i}, \quad (2)$$

де $\zeta_i^{\alpha_i}$ – функція, яка враховує вплив $\left(EFA_{ijkl}, n_i\right)$ на показник Q_{ikj}.

Параметри ідентифікуються зміненим методом найменших квадратів, шляхом логарифмування функціоналу адекватності. З огляду на ідентифіковані параметри визначаємо ступінь ефективності захисту даного рівня.

Залежність ймовірності реалізованості j – го способу для k – ої загрози другою рівні – W_{jk} залежить від міри захищеності Q_{kj} від загрози. При цьому використовуємо принцип: більш ефективніший захід захисту – менша ймовірність реалізованості загрози для ІБ.

Залежність $W_{jk} = W_{jk}\left(Q_{kj}\right)$ дозволяє оцінювати ефективність підсистеми безпеки РОС навчального закладу.

Оцінимо показник ризику порушення інформаційної безпеки для РОМ навчального закладу. Цей показник визначається величиною R_{jkl}, де l – з множини компонентів РОМ навчального закладу:

$$R_{jkl} = 1 - \left[W_{jk}\left(Q_{kj}\right) \cdot \left(1 - Q_{kj}\right)\right], \quad (3)$$

На наступному рівні ставиться мета забезпечення рівної (захищеності) від усіх методів і підходів реалізації окремої загрози для ІБ РОМ навчального закладу. Тобто, ризик порушення ІБ R_{jkl} (від k – ой загрози) визначається мінімальною якістю захисту серед усіх способів реалізації захисту.

Далі ставиться мета забезпечити рівну надійність захисту окремих компонентів РОМ навчального закладу від всіх загроз за умов рівноцінності загроз та ранжування цих загроз за ступенем небезпеки. Ранжування загроз можна виконати за допомогою рангових коефіцієнтів Q_{kl}.

У першому випадку ризик визначатиметься таким виразом:

$$R_l = \max R_{kl}, \quad \forall k \in K_l, \quad (4)$$

де $\{R_{kl}\}$ – множина показників ризику ІБ по множині для загроз l – ої компоненти РОМ навчального закладу.

У другому випадку аналізований ризик для ІБ РОМ визначається виразом:

$$R_l = \max_{\{R_{kl}\}} R_{kl} Q_{kl}, \quad \forall k \in K_l, \quad (5)$$

Основна мета функціонування захисту РОМ навчального закладу – забезпечення рівної надійності захисту компонентів РОМ від всіх загроз. Що можна подати так: $\{R_{kl} Q_l\}$, $\forall l \in L$, де Q_l – коефіцієнт важливості компонента l у складі РОМ навчального закладу. Оцінки важливості компонента l у складі РОМ навчального закладу – експертні чи евристичні.

ISSN 2663 - 4023

Ефективність EF ризик-управління ІБ РОМ навчального закладу можна оцінити формулою:

$$EF = \frac{100\left(R - \overline{R}\right)}{R}, \quad (6)$$

де $\overline{R}$ – міра ризику по максимуму (за аналізованим набором ризиків для РОМ навчального закладу).

Мірою захищеності сегмента РОМ може бути показник загроз ІБ на основі розрахункових формул, що враховують складові інформаційного домену сегмента безпеки.

Наприклад, $R_d = \max\left(R_{md}E_{md}\right)$ по множині $\{R_{md}E_{md}\}$, $\forall m \in M$, де M – множина сегментів РОМ навчального закладу, що включають також сегмент d, який розглядається як поточний.

Аналогічно визначається показник загальної захищеності для всієї університету:

$R = \max\left(R_d F_d\right)$, $\forall d \in D$, де D – кількість об'єктів системи, яка підлягає захисту, F_d – ступінь важливості захищеності об'єкта.

Можливе додаткове завдання, наприклад експериментально виявити ефективність використовування того чи іншого компоненту захисту. Наприклад, у наступному підрозділі статі розглядається можливість використовування IPS Suricata та SIEM Splunk на базі серверной системі віртуалізації. При цьому на хостах під управлінням PVE було розгорнуто систему виявлення загроз IPS Suricata, платформу Splunk та фільтр DNS-адрес Pi-Hole.

Створення середовища для моделювання мережі. На практиці, для проактивного захисту інформації найчастіше компанії не здатні інвестувати достатньо ресурсів, або не бачать в цьому потреби. Стосується це не лише обладнання, але і кваліфікованих кадрів. Виражається дана проблема в тому, що ті фахівці з кібербезпеки, що працюють в такій компанії, не мають змоги захистити мережу перевіреними рішеннями відповідно до вимог часу, та змушені постійно шукати діючі методи захисту даних без необхідності великих вкладень. Через що, часто захист корпоративних мереж займає місце між моделями «льодяника» та «цибулини», маючи більше ніж один рівень захисту, але менше, ніж цього вимагають реалії. Часто мережі навчальних закладів також потерпають від недостатнього інвестування.

Такі мережі, зазвичай, не мають налаштувань відмово стійкості компонентів, що є дуже важливим для стабільної роботи. Через високу вартість фаєрволів, систем запобігання вторгненню, систем аналізу трафіку, зазвичай їх роботу виконують маршрутизатори з налаштованими ACL-списками фільтрації трафіку. Однак маршрутизатори часто нездатні глибоко аналізувати трафік, через що є захист від запитів з відомих небезпечних доменів, однак відсутній захист від вірусів. Також на маршрутизаторах налаштовують блокування портів, що не використовуються та адрес, з яких надходить надмірна кількість трафіку, що може свідчити про початок атаки «відмова в обслуговуванні».

На рівні ядра мережі також часто відсутнє резервування комутаторів 3 рівня, через що трафік з різних мереж проходить через один комутатор та при його відмові не можна буде не лише обмінюватися даними з мережею Інтернет, а і отримати доступ до локальних ресурсів (корпоративної пошти, файлового сервера, внутрішніх веб-ресурсів).

Мережеві пристрої рівня доступу найменш потерпають від проблем нестачі вкладень, однак також відчувають його вплив. Так, в 2022 році переважна частина

комп'ютерів користувачів випускаються з мережевими адаптерами, що підтримують швидкість 1 Гбіт/с, однак часто комутатори, до яких вони під'єднуються мають на LAN-портах швидкість 100 Мбіт/с, що не відповідає сучасним вимогам [18].

Wi-Fi мережі в навчальних закладах часто використовують застарілі протоколи передачі даних g/n та вже втрачаючий актуальність протокол IEEE 802.11ac, через що швидкість доступу до інформації лишає бажати кращого, а користувачі починають користуватися мобільним інтернетом та вмикають точки роздачі Wi-Fi, тим самим забиваючи доступні канали та ще більше зменшуючи швидкість передачі даних по бездротовій мережі і радіус дії точок доступу.

Що ж стосується мережевого сховища, то часто воно будується на базі не призначених до цього серверів, що не тільки не можуть надати необхідну продуктивність при читанні/запису інформації, але і не мають резервування дискового контролера, що створює небезпеки втрати інформації.

Модель «цибулини» [19] показує, що чим більше шарів захисту мають дані, тим зловмиснику складніше викрасти дані з неї. Через що експерти рекомендують будувати мережу з декількома рівнями апаратного та програмного захисту.

Окрім маршрутизаторів в мережі обов'язково мають бути фаєрволи, система розпізнавання вторгнень та глибокого аналізу трафіку, а також локальний захист кожного пристрою від атак на 2 та 3 рівнях моделі OSI.

Дуже важливою частиною захищеної мережі є резервування пристроїв. Це запобігає не лише втраті доступу до ресурсів при виході з ладу певного мережевого пристрою, але і при атаці на відмову обслуговування.

Також важливим є підключення ключових пристроїв мережі (маршрутизаторів, фаєрволів та інших систем захисту, комутаторів ядра та серверів) до джерел безперебійного живлення та дизельних/бензинових генераторів, що здатні живити мережу струмом навіть при відключенні централізованого електропостачання [20].

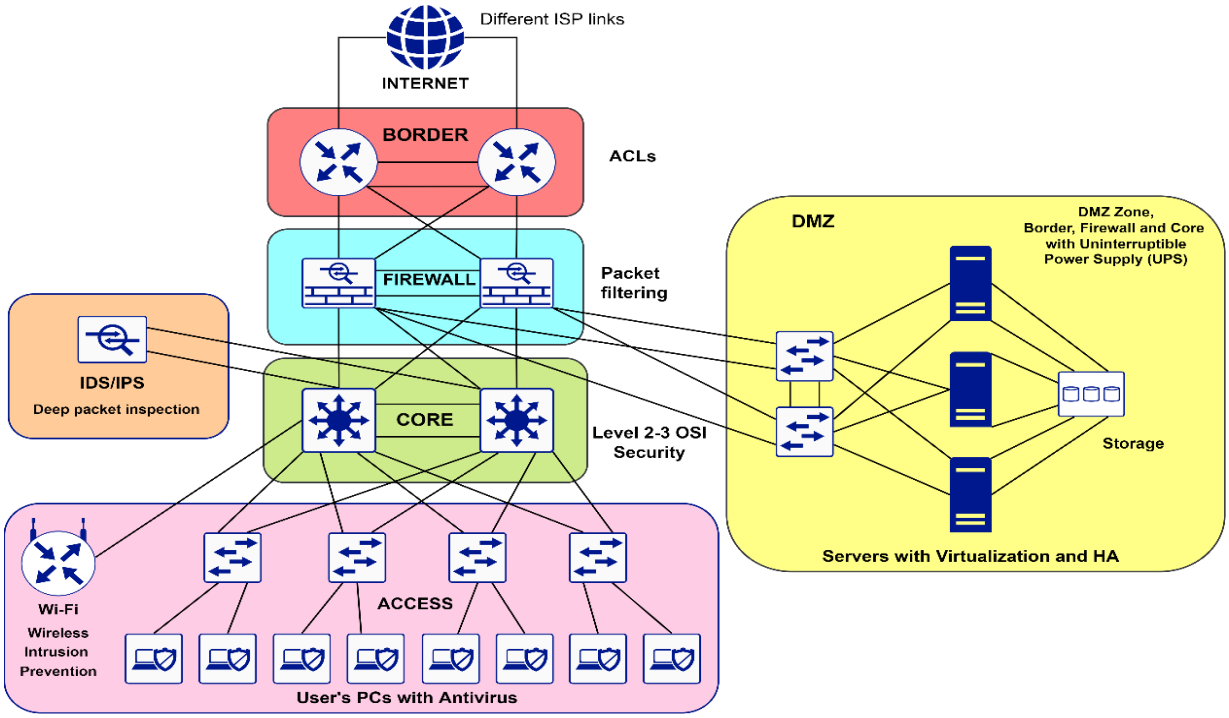

Рис. 1. Захищена локальна мережа

ISSN 2663 - 4023

Не менш важливим є підключення маршрутизаторів до різних провайдерів або одного провайдера, але з різними точками підключення. При відмові одного з лінків, мережа все ще матиме змогу функціонувати через другий канал підключення.

Для моделювання мережі навчального закладу було створено середовище для цього. В якості бази була обрана платформа VmWare Workstation, встановлена на комп'ютер під керуванням ОС Windows 10. Сам комп'ютер побудований на базі серверного процесора Intel Xeon E5 1650 та має встановлену пам'ять ОЗП об'ємом 32 Гб, що достатньо для операцій зі створення віртуальних машин та моделювання роботи систем.

Загалом було створено 3 віртуальні машини, з них 2 – під керуванням ОС Proxmox VE, що виступає гіпервізором для розгортання на ньому інших віртуальних машин. На третю ВМ було встановлено Ubuntu Server та додаток для моделювання мереж EVE-NG. Для створення віртуальної машини було обрано кастомізоване створення в налаштуваннях.

Для більш зручного керування інфраструктурою використовують кластерні рішення – об'єднання декількох серверів в одну систему для забезпечення можливості резервування ресурсів та централізованого адміністрування. Proxmox VE також підтримує дану функцію. Було вирішено об'єднати 2 сервери в один кластер. Після того, як кластер створено, переходячи на адресу будь якого з хостів, можна побачити інформацію про обидва сервери та всі їх ресурси (віртуальні машини, контейнери, сховища та ін.), див. рис. 2.

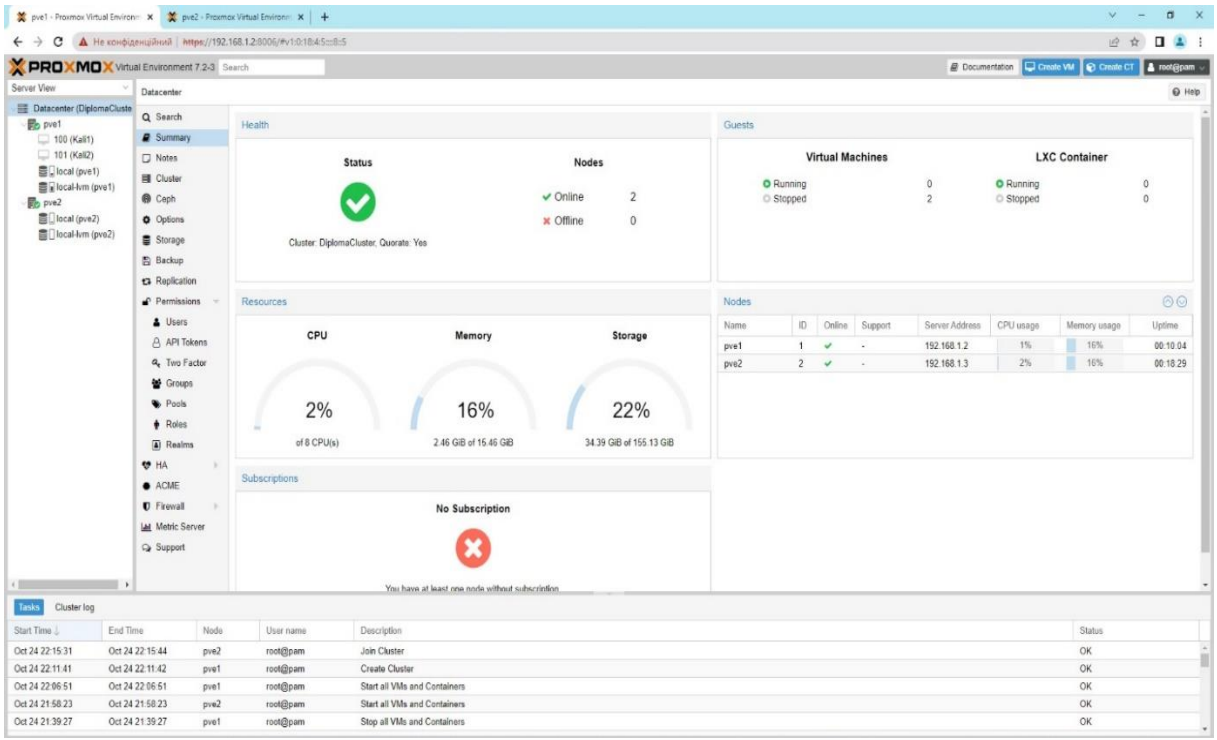

Рис. 2. Інформація про ресурси кластеру

Створення кластеру надає велику кількість переваг, одна з яких – можливість міграції віртуальних машин, що містяться на серверах, на інші вузли кластеру.

Для побудови моделі мережі на мережевих пристроях слід перейти на веб-сторінку створеної раніше віртуальної машини EVE-NG та додати необхідні пристрої.

ISSN 2663 - 4023

В даному випадку, виходячи з досвіду налаштування мережі факультету інформаційних технологій Національного університету біоресурсів та природокористування України, на робочу поверхню було додано 1 маршрутизатор (який виступає в ролі і фаєрвола) і 2 комутатори ядра, один з яких відповідає за серверний сегмент, а інший – за користувацький. Також були додані комутатори доступу, що підключені до комутатора ядра, що відповідає за користувацький сегмент, де в свою чергу є 2 групи: 1 – комутатори, що розміщені в навчальних лабораторіях, 2 – розміщені на кафедрах факультету. Відповідно до цього, політики доступу для користувачів з цих 2 сегментів відрізняються – користувачі, що приєднані через комутатори кафедр мають більше прав доступу до локальних ресурсів, що знаходяться на серверах факультету, див. рис. 3.

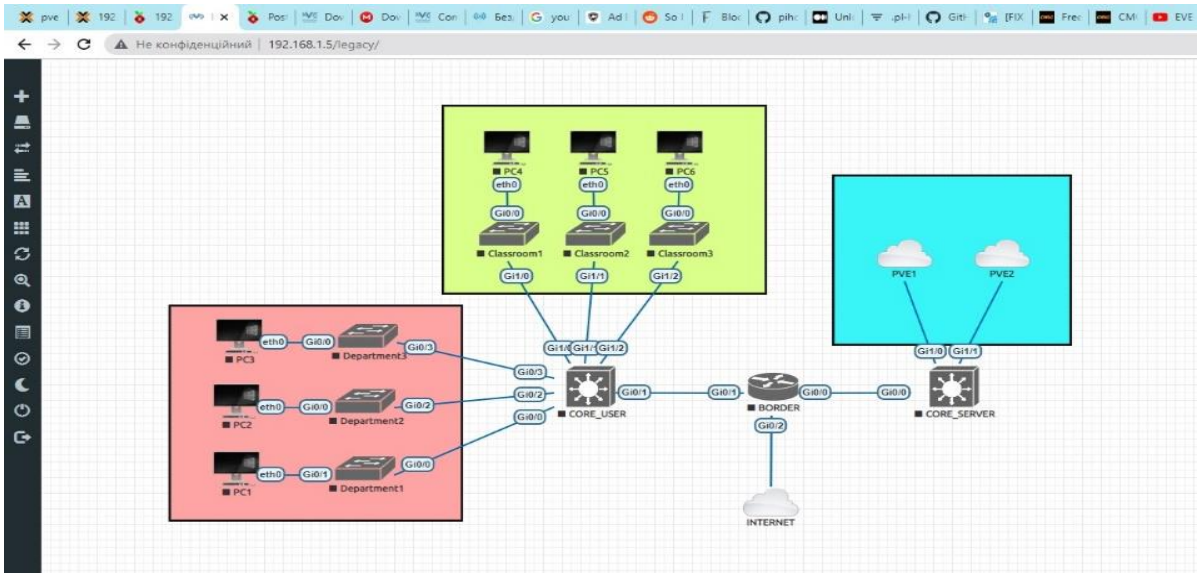

Рис. 3. Схема мережі навчального закладу

Фактично, підключення наших пристроїв в моделі мережі навчального закладу виглядають так, як подано на рисунку 4.

ISSN 2663 - 4023

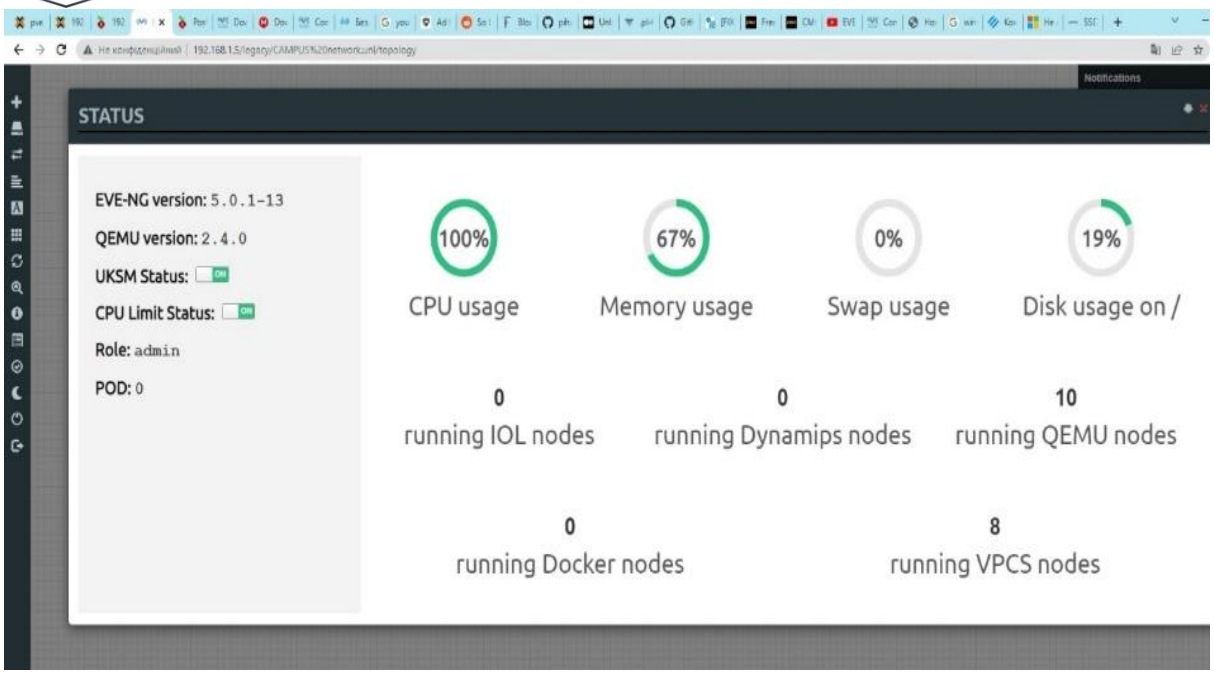

Рис. 4. Завантаженість ВМ при запуску вузлів мережі

Всі пристрої підключаються до віртуальних інтерфейсів VmWare, яка в свою чергу до мережевого інтерфейсу персонального комп'ютера. Сам ПК, який використовувався під час експериментального дослідження, був приєднаний до маршрутизатора, який вже підключений до мережі провайдера, див. рис. 5.

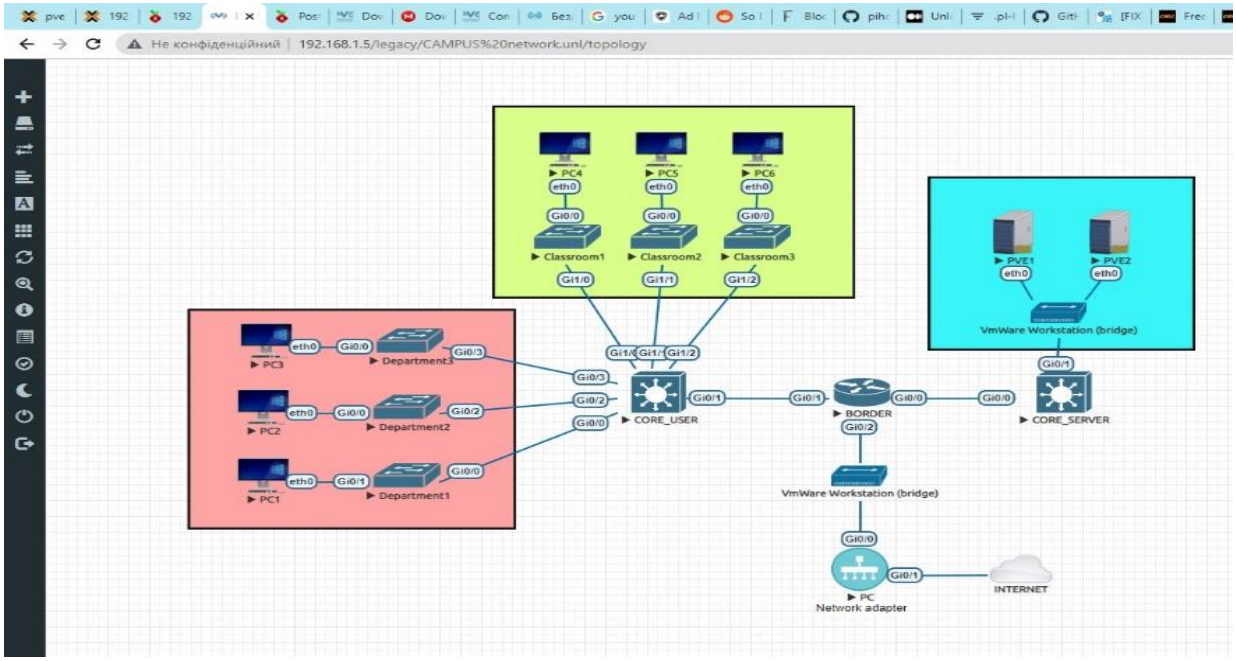

Рис. 5. Реальні підключення пристроїв

В межах дослідження захисту інформації в начальному закладі було обрано одразу змінити налаштування мережі, аби зробити її більш захищеною. Одна з характеристик захисту інформації – доступність ресурсів. Якщо один з ключових пристроїв вийде з ладу, аби вся система не втратила працездатність. В реаліях навчальних закладів України на сьогодні навряд чи можна зробити повноцінне резервування всіх ключових вузлів

ISSN 2663 - 4023

мережі, однак на наведеній вище схемі мережі можна зробити резервування комутаторів ядра та їх зв'язків між собою та маршрутизатором. Для цього слід провести зв'язки від серверів та комутаторів доступу користувачів до обох комутаторів ядра. Більшість комутаторів доступу, на сьогодні, для цього мають 2–4 висхідних порти, так само як і сервери – мережеві карти на мінімум 2 порти, див рис. 6.

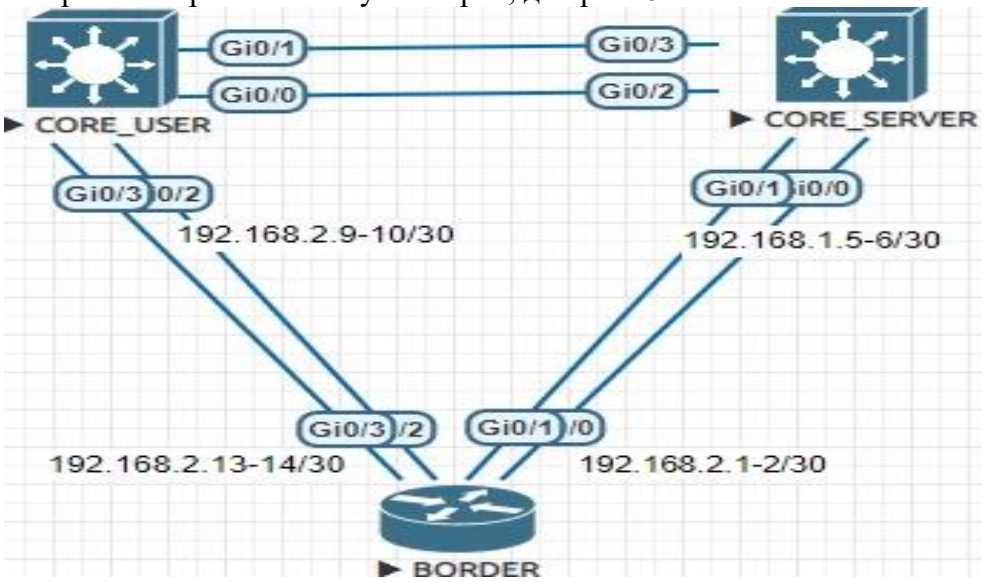

Рис. 6. Забезпечення відмово стійкості комутаторів

Для того, щоб ще більше посилити захист мережі, окрім забезпечення безпеки на окремих її вузлах та фільтрації DNS-адрес, бажано додати до системи віртуальну машину, яка б аналізувала трафік на предмет свідчень про початок кібератаки. Існує декілька таких систем з відкритим кодом, найпопулярнішою з яких є IPS Suricata [21].

Експериментальні дослідження захищеної мережі навчального закладу. Для перевірки працездатності захищеної мережі навчального закладу ВМ з Pi-Hole була вказана як основний DNS-сервер на всіх пристроях, та на крайньому маршрутизаторі. Сам додаток Pi-Hole дозволяє в режимі реального часу переглядати, які запити блокуються, а які дозволяються. Зручно виводить статистику у формі діаграм та дозволяє переглядати їх деталі, див. рис. 7.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (18), 2022
ISSN 2663 - 4023

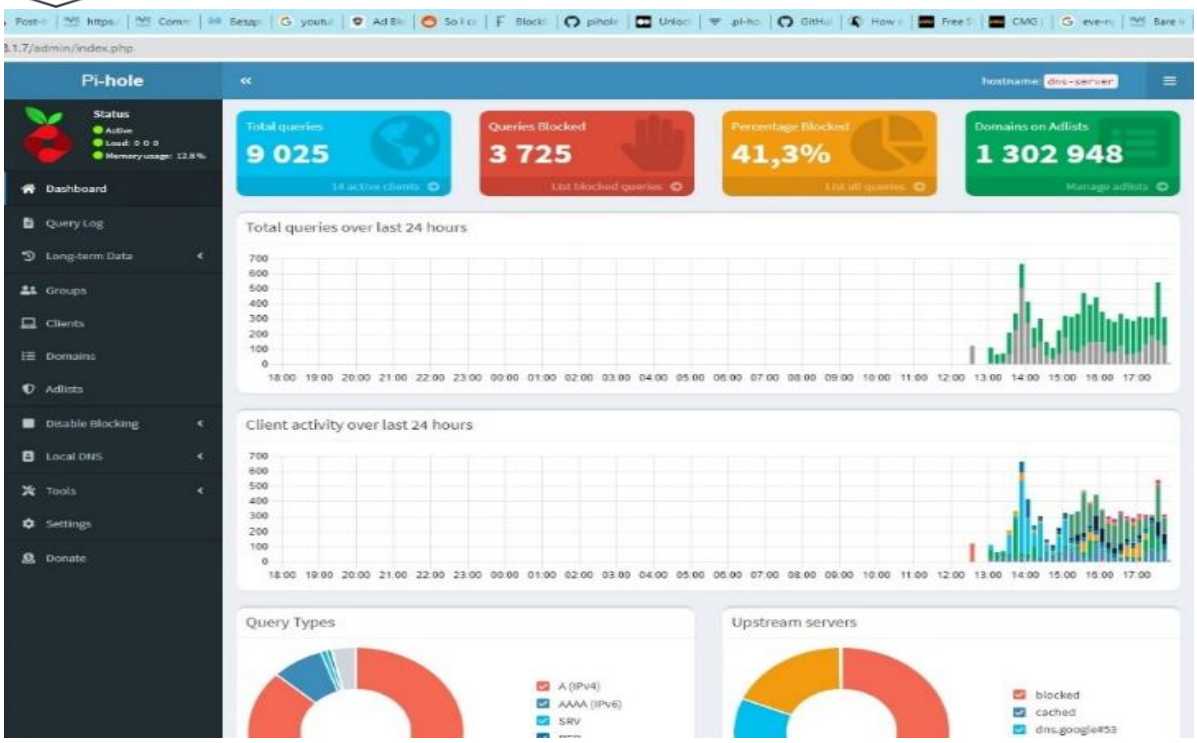

Рис. 7. Загальна статистика роботи Pi-Hole

Після того, як було налаштовано зв'язку системи виявлення вторгнень Suricata та SIEM Splunk [22] остання почала отримувати системні сповіщення від першої, див. рис. 8.

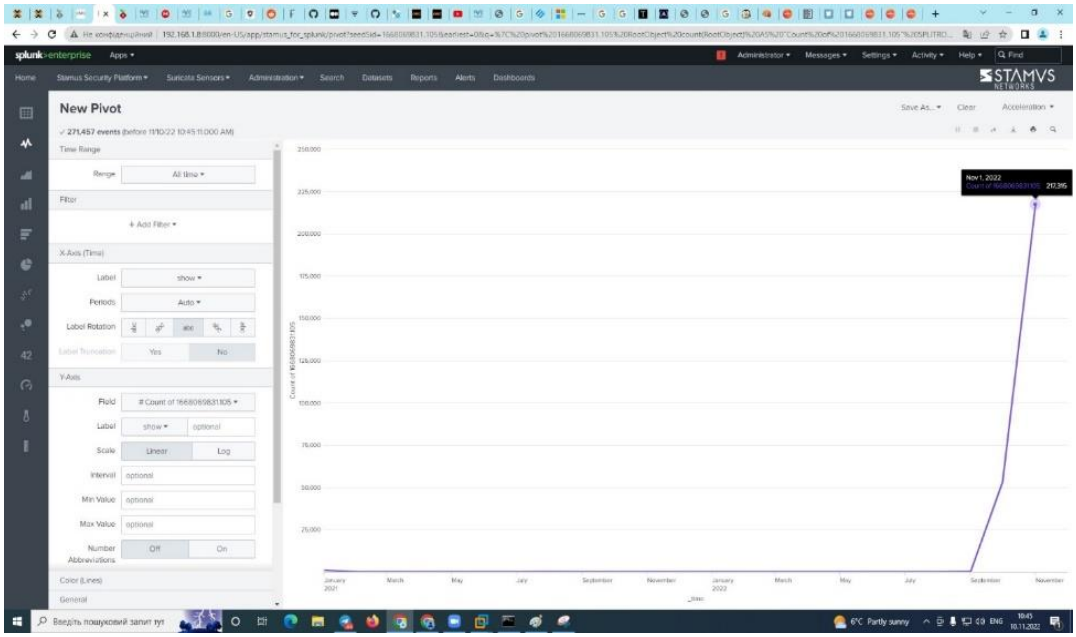

Рис. 8. Графічне відображення сповіщень від Suricata в SIEM Splunk

Обговорення результатів експериментальних досліджень захищеної мережі навчального закладу. З отриманих результатів, показаних на рис. 7, видно, що система за 5 годин роботи заблокувала більше 3700 шкідливих запитів, що складає більш ніж 41% від усього трафіку, що заходив в мережу навчального закладу. Окрім загальної інформації про заблоковані загрози Pi-Hole надавав можливість перегляду інформації по

тому, до яких заборонених доменів йде найбільше звертань, від яких клієнтів йде найбільше запитів – як в цілому, так і шкідливих зокрема. Всього за годину SIEM Splunk було надіслано 20 сповіщень про порушення правил інформаційної безпеки та блокування відповідного трафіку. Ще дає змогу стверджувати, що така SIEM є необхідною частиною мережі будь якого крупного навчально закладу, зокрема університету. Сама SIEM Splunk надає можливість відсортувати сповіщення зручним чином, аби як найдетальніше оцінити стан безпеки мережі навчального закладу, див. рис. 8. Окрім можливості сортувати сповіщення, Splunk також надавав можливість будувати графіки для розуміння динаміки зміни поведінки трафіку в мережі та вчасного реагування на це.

На наш погляд, запропонований підхід – структурований і системний, що дозволяє оцінити захищеність мережі навчального закладу (наприклад, університету) в цілому, а також її підсистем та компонентів.

Використовування засовів моделювання та віртуалізації дало можливість не лише дослідити захист мережі навчального закладу, а й скоротило затрати часу та фінансових ресурсів на розбудову реальної мережі, яка наразі позабудовується на фізичних серверах Національного університету біоресурсів та природокористування України, а також на базі університету Єсенова (Казахстан).

Подяки. Дослідження фінансується Казахським національним педагогічним університетом імені Абая (договір № ППС-ДН-01 від 12.02.2020), а також гранта AP19174716 «Розробка системи підтримки прийняття рішень на основі байєсівських мереж для підвищення ефективності виявлення вторгнень у комп'ютерні системи». Експериментальні дослідження виконувалися на базі кафедр комп’ютерних систем, мереж та кібербезпеки Національного університету біоресурсів та природокористування України, а також на базі кафедри комп’ютерних наук університету Єсенова (Казахстан).

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В ході роботи було отримано наступні результати:

3. досліджено методи захисту інформації в локальних мережах, зокрема навчальних закладів;
4. побудовано модель мережі, де мережеві пристрої були з’емульовані у віртуальній машині зі встановленим додатком EVE-NG, а інші ресурси відтворені завдяки серверній системі віртуалізації Proxmox VE. На хостах під управлінням PVE було розгорнуто систему виявлення загроз IPS Suricata, платформу Splunk та фільтр DNS-адрес Pi-Hole.

За результатами експериментальних досліджень встановлено: 1) фільтр DNS-адрес Pi-Hole за 5 годин роботи заблокував більше 3700 шкідливих запитів, що складає більш ніж 41% від усього трафіку, що заходив в мережу навчального закладу; 2) за годину системою IPS Suricata було надіслано 20 сповіщень про порушення правил інформаційної безпеки та блокування відповідного трафіку, що дає змогу стверджувати, що така система є необхідною частиною мережі будь якого закладу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Wijayanto, H., Prabowo, I. A. (2020). Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic. *Jurnal Sisfokom (Sistem Informasi dan Komputer), 9*(3), 395-399.

2 Ulven, J.B.; Wangen, G. A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet 2021, 13*, 39. https://doi.org/10.3390/fi13020039

3 Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), tyy006.

4 Oreyomi, M., Jahankhani, H. (2022). Challenges and Opportunities of Autonomous Cyber Defence (ACyD) *Against Cyber Attacks. Blockchain and Other Emerging Technologies for Digital Business Strategies*, 239-269.

5 Watney, M. (2022). Cybersecurity Threats to and Cyberattacks on Critical Infrastructure: a Legal Perspective. *European Conference on Cyber Warfare and Security*, *21*(1), 319–327. https://doi.org/10.34190/eccws.21.1.196

6 Laghari, S. U. A., Manickam, S., Al-Ani, A. K., Rehman, S. U., Karuppayah, S. (2021). SECS/GEMsec: A Mechanism for Detection and Prevention of Cyber-Attacks on SECS/GEM Communications in Industry 4.0 Landscape. *IEEE Access, 9*, 154380-154394.

7 Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., Costabile, M. F. (2021). Human factors in phishing attacks: a systematic literature review. *ACM Computing Surveys (CSUR), 54*(8).

8 Zahra, S. R., Chishti, M. A., Baba, A. I., Wu, F. (2022). Detecting Covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system. *Egyptian Informatics Journal*, *23*(2), 197-214.

9 Топ 10 cyber risks for business URL: https://10guards.com/en/articles/2022-top-10-cyber-risks-for-business/ (date of access: 13.08.2022).

10 Alkhadra, R., Abuzaid, J., AlShammari, M., Mohammad, N. (2021, July). Solar winds hack: In-depth analysis and countermeasures. In *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE.

11 Sheehan, B., Murphy, F., Kia, A. N., Kiely, R. (2021). A quantitative bow-tie cyber risk classification and assessment framework. *Journal of Risk Research, 24*(12), 1619-1638.

12 Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez-Fonseca, G., Quiroz, D. (2021). Information security management frameworks and 1 institutions: a systematic review. *Annals of Telecommunications, 76*(3), 255-270.

13 Alexei, L. A., Alexei, A. (2021). Cyber security threat analysis in higher education institutions as a result of distance learning. *International Journal of Scientific and Technology Research*, (3), 128-133.

14 Landoll, D. (2021). *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC Press.

15 Leszczyna, R. (2021). Review of cybersecurity assessment methods: Applicability perspective. *Computers & Security, 108*, 102376.

16 Ferrari, R. M., Teixeira, A. M. (2021). Detection of Cyber-Attacks: A Multiplicative Watermarking Scheme. In *Safety, Security and Privacy for Cyber-Physical Systems* (pp. 173-201). Springer, Cham.

17 Naurazova, E. A., SHamilev, S. R. (2016). Model informacionnoj bezopasnosti v raspredelennyh setyah. *Ekonomika. Biznes. Informatika, 2*(4), 27-37.

18 What switches are best for school districts URL: https://info.hummingbirdnetworks.com/blog/bid/315722/what-switches-are-best-for-school-districts (date of access: 26.08.2022).

19 Moraliyage, H., Sumanasena, V., De Silva, D., Nawaratne, R., Sun, L., Alahakoon, D. (2022*). Multimodal Classification of Onion Services for Proactive Cyber Threat Intelligence using Explainable Deep Learning*. IEEE Access.

20 What is a UPS and How Does it Protect Your Network? https://ltnow.com/blog/ups-protect-network/ (дата звернення: 25.08.2022).

21 Suricata: home URL: https://suricata.io/ (date of access: 03.10.2022).

22 SPLUNK короткий посібник https://coderlessons.com/tutorials/bolshie-dannye-i-analitika/vyuchit-splunk/splunk-kratkoe-rukovodstvo (date of access: 20.10.2022).

23 Lakhno, V., Akhmetov, B., Smirnov, O., Chubaievskyi, V., Khorolska, K., Bebeshko, B. (2023). Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm. *Lecture Notes on Data Engineering and Communications Technologies, 131*, 21-34.

24 Lakhno, V., Kasatkin, D., Desiatko, A., Chubaievskyi, V., Tsuitsuira, S., Tsuitsuira, M. (2023). Indicators Systematization of Unauthorized Access to Corporate Information. *Lecture Notes on Data Engineering and Communications Technologies, 131*, 569-580.

25 Lakhno, V., Akhmetov, B., Mohylnyi, H., Blozva, A., Chubaievskyi, V., Kryvoruchko, O., Desiatko, A. (2022). Multi-criterial optimization composition of cyber security circuits based on genetic algorithm. *Journal of Theoretical and Applied Information Technology, 100*(7), 1996-2006.

26 Lakhno, V., Blozva, A., Kasatkin, D., Chubaievskyi, V., Shestak, Y., Tyshchenko, D., Brzhanov, R. (2022). Experimental studies of the features of using waf to protect internal services in the zero trust structure. *Journal of Theoretical and Applied Information Technology, 100*(3), 705-721.

27 Nashynets-Naumova A. Yu., Buriachok V. L., Korshun N. V., Zhyltsov O. B., Skladannyi P. M., Kuzmenko L. V. (2020). Technology for information and cyber security in higher education institutions of Ukraine. *Information Technologies and Learning Tools, 77*(3), 337–354. https://doi.org/10.33407/itlt.v77i3.3424

28 Buriachok, V. L., Bogush V. M., Borsukovskii, Y. V., Skladannyi, P. M., Borsukovska, V. Y. (2018). Training model for professionals in the field of information and cyber security in the higher educational institutions of Ukraine. *Information Technologies and Learning Tools, 67*(5), 277–291. https://doi.org/10.33407/itlt.v67i5.2347

29 Buriachok, V., Shevchenko, S., ZhdanovaY., Skladannyi, P. (2021). Interdisciplinary approach to the development of is risk management skills on the basis of decision-making theory. *Cybersecurity: Education, Science, Technique, 3*(11), 155-165. https://doi.org/10.28925/2663-4023.2021.11.155165.

30 Buriachok, V., Korshun, N., Shevchenko, S., Skladannyi, P. (2020). Application of ni multisim environment in the practical skills building for students of 125 CYBERSECURITY SPECIALTY. *Cybersecurity: Education, Science, Technique, 1*(9), 159-169. https://doi.org/10.28925/2663-4023.2020.9.159169

31 Buriachok, V. L., Shevchenko, S. M., Skladannyi, P. M. (2018). Virtual Laboratory for Modeling of Processes in Informational and Cyber Securities as a form of Forming Practical Skills of Students. *Cybersecurity: Education, Science, Technique, 2*(2), 98-104. https://doi.org/10.28925/2663-4023.2018.2.98104.

32 Shevchenko, S., Zhdanova, Y., Spasiteleva, S., Skladannyi, P. (2020). Conducting a swot-analysis of information risk assessment as a means of formation of practical skills of students specialty 125 CYBERSECURITY. *Cybersecurity: Education, Science, Technique, 2*(10), 158–168. https://doi.org/10.28925/2663-4023.2020.10.158168.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (18), 2022
ISSN 2663 - 4023

Valery Lakhno
Doctor of Technical Sciences, Professor of Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine Kyiv, Ukraine
ORCID ID: 0000-0001-9695-4543
lva964@gmail.com

Kalaman Yerbolat
Department of Cybersecurity, Information Processing and Storage
Satbayev University Almaty, Kazakhstan
ORCID ID: 0000-0002-8607-737X
kalaman.erbolat@gmail.com

Yagaliyeva Bagdat
PhD, Associate Professor, Dean of Faculty of Science and Technology
Essenov University, Aktau, Kazakhstan
ORCID ID: 0000-0001-9695-4543
lva964@gmail.com

Olena Kryvoruchko
Doctor of Technical Sciences, Professor, Head of Department of Software Engineering and Cyber Security Kyiv National University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0002-7661-9227
kryvoruchko_ev@knute.edu.ua

Alona Desiatko
PhD in Computer Sciences, Associate Professor of Department of Software Engineering and Cyber Security
Kyiv National University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0003-2860-2188
desyatko@knute.edu.ua

Tsiutsiura Svitlana
Doctor of Technical Sciences, Professor, Head of Department of Information Technologies
Kyiv National University of Construction and Architecture, Kyiv, Ukraine
ORCID ID: 0000-0002-4377-0916
svtsutsura@gmail.com

Tsiutsiura Mykola
Doctor of Technical Sciences, Associate Professor, Associate Professor of Department of Information Technologies
Kyiv National University of Construction and Architecture,Kyiv, Ukraine
ORCID ID: 0000-0003-1658-7822
mitsiutsiura@gmail.com

THE MODEL OF SERVER VIRTUALIZATION SYSTEM PROTECTION IN THE EDUCATIONAL INSTITUTION LOCAL NETWORK

Abstract. A new approach for the information security (IS) improvement of the educational institution's network has been proposed. The proposed approach is structured and systematic. It allows one to assess the security of the network of an educational institution (for example, a university) as a whole, as well as its subsystems and components that provide IS of an educational institution. Statistical, expert, heuristic and other indicators have been used to assess the degree of security. The proposed model allows one to describe the procedure for securing the IS network of the university. A balanced system of IS indicators has been proposed, which will allow the effectiveness evaluation of the university's network protection. Also as part of the research, a model of a secure network of an educational institution has been built, where network devices were emulated in a virtual machine (VM) with the EVE-NG application installed. Other network resources have been reproduced with the server virtualization system Proxmox VE. The IPS Suricata threat detection system, the Splunk platform, and the Pi-Hole DNS filter have been deployed on PVE-managed hosts.

Keywords: distributed networks, educational institution, information security, virtualization, IDS, SIEM

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Wijayanto, H., Prabowo, I. A. (2020). Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic. *Jurnal Sisfokom (Sistem Informasi dan Komputer), 9*(3), 395-399.
2 Ulven, J.B.; Wangen, G. A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet 2021, 13*, 39. https://doi.org/10.3390/fi13020039
3 Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), tyy006.
4 Oreyomi, M., Jahankhani, H. (2022). Challenges and Opportunities of Autonomous Cyber Defence (ACyD) *Against Cyber Attacks. Blockchain and Other Emerging Technologies for Digital Business Strategies*, 239-269.
5 Watney, M. (2022). Cybersecurity Threats to and Cyberattacks on Critical Infrastructure: a Legal Perspective. *European Conference on Cyber Warfare and Security, 21*(1), 319–327. https://doi.org/10.34190/eccws.21.1.196
6 Laghari, S. U. A., Manickam, S., Al-Ani, A. K., Rehman, S. U., Karuppayah, S. (2021). SECS/GEMsec: A Mechanism for Detection and Prevention of Cyber-Attacks on SECS/GEM Communications in Industry 4.0 Landscape. *IEEE Access, 9*, 154380-154394.
7 Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., Costabile, M. F. (2021). Human factors in phishing attacks: a systematic literature review. *ACM Computing Surveys (CSUR), 54*(8).
8 Zahra, S. R., Chishti, M. A., Baba, A. I., Wu, F. (2022). Detecting Covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system. *Egyptian Informatics Journal*, *23*(2), 197-214.
9 Top 10 cyber risks for business URL: https://10guards.com/en/articles/2022-top-10-cyber-risks-for-business/ (date of access: 13.08.2022).
10 Alkhadra, R., Abuzaid, J., AlShammari, M., Mohammad, N. (2021, July). Solar winds hack: In-depth analysis and countermeasures. In *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE.
11 Sheehan, B., Murphy, F., Kia, A. N., Kiely, R. (2021). A quantitative bow-tie cyber risk classification and assessment framework. *Journal of Risk Research, 24*(12), 1619-1638.
12 Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez-Fonseca, G., Quiroz, D. (2021). Information security management frameworks and 1 institutions: a systematic review. *Annals of Telecommunications, 76*(3), 255-270.
13 Alexei, L. A., Alexei, A. (2021). Cyber security threat analysis in higher education institutions as a result of distance learning. *International Journal of Scientific and Technology Research*, (3), 128-133.
14 Landoll, D. (2021). *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC Press.
15 Leszczyna, R. (2021). Review of cybersecurity assessment methods: Applicability perspective. *Computers & Security, 108*, 102376.
16 Ferrari, R. M., Teixeira, A. M. (2021). Detection of Cyber-Attacks: A Multiplicative Watermarking Scheme. In *Safety, Security and Privacy for Cyber-Physical Systems* (pp. 173-201). Springer, Cham.
17 Naurazova, E. A., SHamilev, S. R. (2016). Model informacionnoj bezopasnosti v raspredelennyh setyah. *Ekonomika. Biznes. Informatika, 2*(4), 27-37.
18 What switches are best for school districts URL: https://info.hummingbirdnetworks.com/blog/bid/315722/what-switches-are-best-for-school-districts (date of access: 26.08.2022).
19 Moraliyage, H., Sumanasena, V., De Silva, D., Nawaratne, R., Sun, L., Alahakoon, D. (2022*). Multimodal Classification of Onion Services for Proactive Cyber Threat Intelligence using Explainable Deep Learning*. IEEE Access.
20 What is a UPS and How Does it Protect Your Network? https://ltnow.com/blog/ups-protect-network/ (date of access: 25.08.2022).
21 Suricata: home URL: https://suricata.io/ (date of access: 03.10.2022).

22 SPLUNK короткий посібник https://coderlessons.com/tutorials/bolshie-dannye-i-analitika/vyuchit-splunk/splunk-kratkoe-rukovodstvo (date of access: 20.10.2022).

23 Lakhno, V., Akhmetov, B., Smirnov, O., Chubaievskyi, V., Khorolska, K., Bebeshko, B. (2023). Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm. *Lecture Notes on Data Engineering and Communications Technologies, 131*, 21-34.

24 Lakhno, V., Kasatkin, D., Desiatko, A., Chubaievskyi, V., Tsuitsuira, S., Tsuitsuira, M. (2023). Indicators Systematization of Unauthorized Access to Corporate Information. *Lecture Notes on Data Engineering and Communications Technologies, 131*, 569-580.

25 Lakhno, V., Akhmetov, B., Mohylnyi, H., Blozva, A., Chubaievskyi, V., Kryvoruchko, O., Desiatko, A. (2022). Multi-criterial optimization composition of cyber security circuits based on genetic algorithm. *Journal of Theoretical and Applied Information Technology, 100*(7), 1996-2006.

26 Lakhno, V., Blozva, A., Kasatkin, D., Chubaievskyi, V., Shestak, Y., Tyshchenko, D., Brzhanov, R. (2022). Experimental studies of the features of using waf to protect internal services in the zero trust structure. *Journal of Theoretical and Applied Information Technology, 100*(3), 705-721.

27 Nashynets-Naumova A. Yu., Buriachok V. L., Korshun N. V., Zhyltsov O. B., Skladannyi P. M., Kuzmenko L. V. (2020). Technology for information and cyber security in higher education institutions of Ukraine. *Information Technologies and Learning Tools, 77*(3), 337–354. https://doi.org/10.33407/itlt.v77i3.3424

28 Buriachok, V. L., Bogush V. M., Borsukovskii, Y. V., Skladannyi, P. M., Borsukovska, V. Y. (2018). Training model for professionals in the field of information and cyber security in the higher educational institutions of Ukraine. *Information Technologies and Learning Tools, 67*(5), 277–291. https://doi.org/10.33407/itlt.v67i5.2347

29 Buriachok, V., Shevchenko, S., ZhdanovaY., Skladannyi, P. (2021). Interdisciplinary approach to the development of is risk management skills on the basis of decision-making theory. *Cybersecurity: Education, Science, Technique, 3*(11), 155-165. https://doi.org/10.28925/2663-4023.2021.11.155165.

30 Buriachok, V., Korshun, N., Shevchenko, S., Skladannyi, P. (2020). Application of ni multisim environment in the practical skills building for students of 125 CYBERSECURITY SPECIALTY. *Cybersecurity: Education, Science, Technique, 1*(9), 159-169. https://doi.org/10.28925/2663-4023.2020.9.159169

31 Buriachok, V. L., Shevchenko, S. M., Skladannyi, P. M. (2018). Virtual Laboratory for Modeling of Processes in Informational and Cyber Securities as a form of Forming Practical Skills of Students. *Cybersecurity: Education, Science, Technique, 2*(2), 98-104. https://doi.org/10.28925/2663-4023.2018.2.98104.

32 Shevchenko, S., Zhdanova, Y., Spasiteleva, S., Skladannyi, P. (2020). Conducting a swot-analysis of information risk assessment as a means of formation of practical skills of students specialty 125 CYBERSECURITY. *Cybersecurity: Education, Science, Technique, 2*(10), 158–168. https://doi.org/10.28925/2663-4023.2020.10.158168.