Отже, правильне налаштування доступу до цілого електронного курсу та його ресурсів є основною вимогою для забезпечення кібербезпеки електронних ресурсів системи дистанційного навчання Moodle.

Список використаних джерел

1. Віртуальний університет Львівського державного університету безпеки життєдіяльності. URL: https://virt.ldubgd.edu.ua
2. Козяр М.М. Віртуальний університет: перспективи переходу на новий тип освіти / Козяр М.М. // Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: ме-тодологія, теорія, досвід, проблеми: зб. наук. праць. − Київ-Вінниця: ТОВ фірма "Планер", 2010. – Вип. 23. − С. 40-46.
3. Офіційний сайт розробників системи Moodle. URL: https://moodle.org
4. Полотай О.І., Бойко К. Програмно-технічний захист інформації за допомогою охоронної системи. Зб. тез. III Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів “Захист інформації в інформаційно-комунікаційних системах” (м. Львів, 28 листопада 2019 р.). Львів : ЛДУБЖД, 2019. С. 76–78.
5. Полотай О.І., Кухарська Н.П. Розроблення електронних курсів у віртуальному навчальному середовищі. Львів : СПОЛОМ, 2021. 172 с.

ПРОПОЗИЦІЇ ЩОДО БЕЗПЕКИ ІНФОРМАЦІЙНИХ ПОТОКІВ ЗАКЛАДУ ВИЩОЇ ОСВІТИ

Полотай Орест
к.т.н., доцент
Львівський державний університет безпеки життєдіяльності
Пузир Андрій
здобувач вищої освіти
Національний університет Львівська політехніка

Загрози кіберзлочинності, такі як фішинг, вірусні атаки, порушення даних через вразливості системи та загрози інформації в локальній мережі закладу вищої освіти, загрожують не лише конфіденційності даних навчального процесу, але й безпеці всього закладу вищої освіти. Існує ціла низка загроз, які притаманні закладам вищої освіти [3], зокрема вони, як і будь які інші учасники бізнес процесів вразливі до витоку конфіденційних даних, які у вигляді інформаційних потоків циркулюють в межах організації та можуть вийти назовні. Така втрата даних може призвести до серйозних втрат, як фінансових так і втрат репутаційних.

Збереження конфіденційності даних стало не просто питанням безпеки, а й важливим елементом стратегії конкурентоспроможності організацій.

Одним із найбільш ефективних способів забезпечення безпеки конфіденційної інформації є використання закладами вищої конкретних систем

захисту, зокрема системи запобігання витоку конфіденційної інформації (Data Loss Prevention, DLP). DLP-системи дають змогу контролювати та обмежувати несанкціоноване використання і передачу конфіденційних даних через різноманітні канали зв'язку, такі як електронна пошта, мережа Інтернет, зовнішні носії тощо.

Системи запобігання витоку даних (DLP — Data Loss Prevention) є важливим компонентом інфраструктури інформаційної безпеки, призначеним для захисту конфіденційної та критично важливої інформації організації від несанкціонованого доступу, витоків або крадіжок (рис. 1).

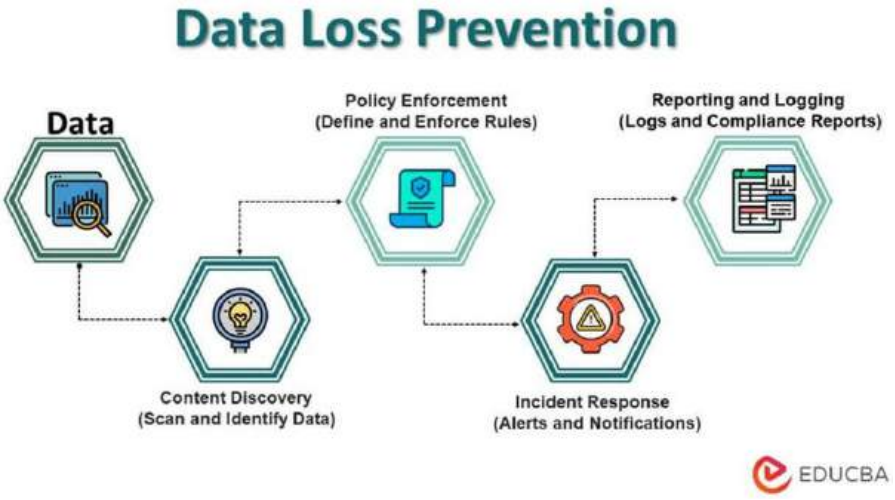

Рис. 1. Принцип роботи DLP систем.

DLP-системи дозволяють не лише попередити витік даних, а й контролювати їх переміщення, зберігання та обробку на різних рівнях організації. Це включає контроль за передачею даних через мережу, взаємодію з кінцевими пристроями, електронною поштою, використання зовнішніх носіїв та інші канали комунікації.

Одним з перших кроків у роботі DLP-системи є виявлення та класифікація чутливих даних, які потребують захисту. Це включає визначення важливих документів і файлів, таких як фінансова інформація, особисті дані співробітників, комерційні таємниці та інші типи конфіденційної інформації. Визначення таких даних здійснюється за допомогою алгоритмів, які можуть використовувати шаблони або спеціальні метадані для виявлення формату інформації. Класифікація даних дозволяє розподілити їх за рівнями конфіденційності: «високий», «середній», «низький». Така класифікація дає змогу застосовувати різні рівні захисту та політики доступу в залежності від важливості даних. Наприклад, дані, що належать до «високого рівня конфіденційності», можуть мати більш жорсткі заходи захисту, ніж менш чутливі матеріали.

DLP-система постійно моніторить потоки даних по всіх каналах зв'язку в межах організації. Це може бути як внутрішній трафік, так і зовнішні зв'язки — мережа Інтернет, електронна пошта, обмін файлами, використання зовнішніх носіїв, USB-пристроїв та інше. Вона здатна виявляти підозрілі або аномальні дії, які можуть вказувати на спроби витоку даних. Такий моніторинг дозволяє

виявляти, наприклад, спроби несанкціонованого копіювання або пересилання конфіденційної інформації, переміщення великих обсягів даних за межі корпоративної мережі чи несанкціоноване використання зовнішніх пристроїв для зберігання або передавання чутливої інформації. У разі виявлення загрози система може миттєво реагувати, запобігаючи витоку.

Коли система виявляє можливий витік даних, вона ініціює автоматичні заходи для його блокування. Це може бути повне блокування спроби пересилання інформації, шифрування даних або ж примусова аутентифікація користувача перед виконанням певної дії. Наприклад, якщо користувач намагається надіслати конфіденційний файл через електронну пошту, система може заблокувати цю операцію або вимагати підтвердження її необхідності.

Існує кілька типів DLP-систем, які відрізняються своїм призначенням, можливостями та принципом роботи. За загальноприйнятою класифікацією їх можна поділити на три основні категорії: мережеві DLP-системи, DLP-системи кінцевих точок та хмарні DLP-системи (рис. 2). Вони працюють за допомогою кількох основних принципів: ідентифікація, класифікація та моніторинг чутливих даних, контроль за їхнім переміщенням, блокування витоків і формування звітності. Завдяки класифікації DLP-систем на мережеві, кінцевих точок та хмарні, організації можуть вибирати відповідну систему залежно від типу своїх потреб, інфраструктури та специфіки діяльності.

Рис. 2. Типи DLP систем та їх рішення.

Серед можливостей DLP систем, які ефективно працюють в специфічному середовищі закладу вищої освіти, є моніторинг у реальному часі, шифрування та звітність про інциденти, а також можливостіі систем DLP для запобігання втраті та витоку даних, забезпечення відповідності нормативним вимогам та підвищення загальної безпеки. Незважаючи на безліч переваг, DLP-рішення не безмежні. Ефективність цих систем може бути знижена через складні кібератаки, внутрішні загрози та їх вплив на продуктивність роботи закладів вищої освіти. Однак при ретельному впровадженні і постійному вдосконаленні DLP-системи можуть забезпечити надійний захист від витоків і несанкціонованої передачі даних (рис. 3).

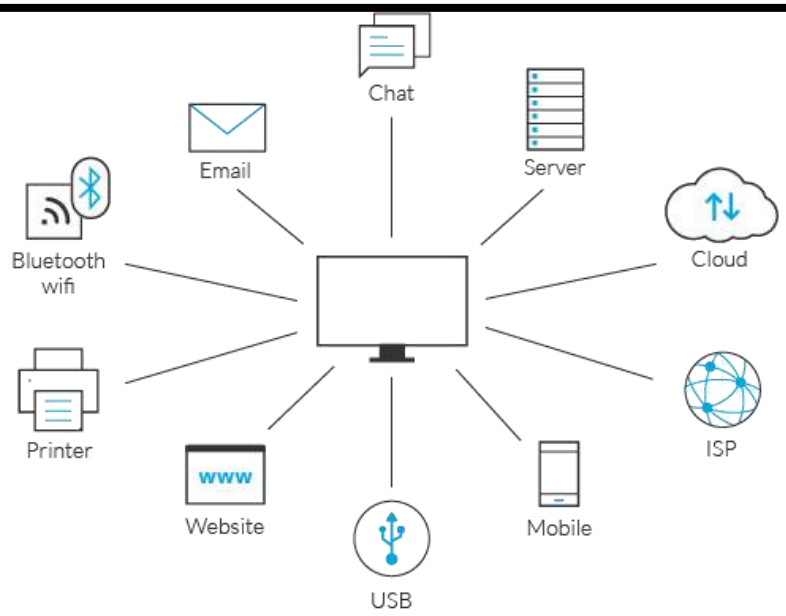

Рис. 3. Можливості моніторингу DLP систем.

Найоптимальнішим місцем роботи DLP систем є відділи топ-менеджменту закладу вищої освіти, відділи персоналу, бухгалтерія, оскільки саме там, зберігається та «живе» конфіденційна інформація. І коли працівники цих відділів працюють з цією інформацією то вони створюють інформаційні потоки, які виходять за межі середовища закладу вищої освіти та ризикують попасти в руки зловмисників. Тому важливим є контроль цих інформаційних потоків, за допомогою DLP систем.

На рис. 4 показано сфери та потоки даних, на які спрямована робота DLP-систем [4].

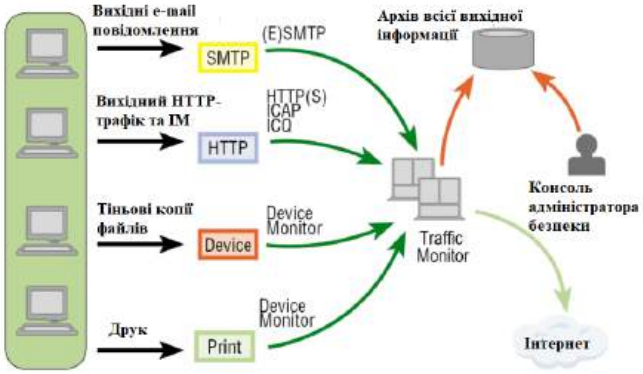

Рис. 4. Робота DLP-системи

Системи DLP можуть стати невід'ємною частиною стратегії інформаційної безпеки в закладах вищої освіти. Вони допоможуть виконати три основні функції, які дадуть змогу організаціям ідентифікувати, захищати та реагувати на загрози, пов'язані з конфіденційною інформацією.

Список використаних джерел

1. Вовчановський П.П., Демчинський В.В. Архітектура DLP-систем в умовах політики BYOD. Системи та технології кібернетичної безпеки. 2020. 151-154.
2. Полотай О.І., Бойко К. Програмно-технічний захист інформації за допомогою охоронної системи. Зб. тез. III Всеукр. наук.-практ. конф. молодих

учених, студентів і курсантів “Захист інформації в інформаційно-комунікаційних системах” (м. Львів, 28 листопада 2019 р.). Львів : ЛДУБЖД, 2019. С. 76–78.
3. Полотай О.І., Кухарська Н.П. Розроблення електронних курсів у віртуальному навчальному середовищі. Львів : СПОЛОМ, 2021. 172 с.
4. Що таке DLP-система і навіщо вона потрібна? 2020. URL: https://falcongaze.com/ua/pressroom/publications/dlp-sistemy/what-is-dlp.html

МЕТОДИКА ПРОГНОЗУВАННЯ РИЗИКУ РОЗЛУЧЕННЯ НА БАЗІ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Левицький Всеволод Володимирович
здобувач вищої освіти магістерського рівня
Кафедра інформаційних систем
Національний університет «Одеська Політехніка», Одеса, Україна

Завдання розробки та вивчення методики прогнозування ризику розлучення за допомогою методів машинного навчання є надзвичайно актуальним через складність і багатогранність цього явища, а також його значний вплив на різні аспекти суспільного життя – соціальний, економічний та психологічний. Розлучення є однією з найпоширеніших криз у сімейних стосунках, яка впливає не лише на подружжя, а й на дітей, родичів та соціальне середовище [1]. Це створює додаткове навантаження на соціальні інститути, такі як правова система, освітні організації та служби психологічної підтримки. Завдяки прогнозуванню ризиків розлучення можна вчасно виявляти проблеми у стосунках і допомагати у їх вирішенні за допомогою цілеспрямованих заходів.

Машинне навчання відкриває нові можливості для аналізу великих масивів даних, які включають соціальні, економічні, психологічні, культурні та поведінкові аспекти стосунків. Використовуючи сучасні алгоритми, можна виявити приховані закономірності та ключові фактори, що впливають на міцність шлюбу [2]. Це дозволяє створювати високоточні моделі прогнозування, які враховують не тільки прямі, а й непрямі зв’язки між різними аспектами життя подружньої пари. Наприклад, такі моделі можуть аналізувати вплив фінансових труднощів, рівень взаєморозуміння, сумісність цінностей, наявність стресових ситуацій або роль соціального оточення [3].

Ця тематика є особливо цікавою для наукових досліджень через можливість поєднання методів машинного навчання із знаннями з інших дисциплін, таких як психологія, соціологія та економіка. Вивчення цього питання сприяє глибшому розумінню впливу різних чинників на стійкість шлюбу та відкриває нові горизонти для розвитку теоретичних і прикладних підходів [4].

Практичне значення моделей прогнозування ризику розлучень полягає в їх застосуванні для консультування сімей, розробки програм підтримки та