АНАЛІЗ БЕЗПЕКОВИХ РІШЕНЬ ЗАХИСТУ ШКІЛЬНИХ МЕРЕЖ

Волос Ігор Петрович
здобувач другого (магістерського) рівня вищої освіти спеціальності Комп'ютерні науки,
Тернопільський національний педагогічний університет імені Володимира Гнатюка,
igorvo3310@gmail.com
Василенко Ярослав Пилипович
викладач кафедри інформатики та методики її навчання,
Тернопільський національний педагогічний університет імені Володимира Гнатюка,
yava@fizmat.tnpu.edu.ua

У сучасному освітньому середовищі використання цифрових технологій стало невід'ємною частиною навчального процесу та адміністративної діяльності шкіл. Шкільні мережі забезпечують доступ до освітніх платформ, електронних журналів, баз даних учнів і вчителів, а також до мережевих ресурсів інтернету. Проте, із зростанням цифровізації постає питання захисту інформаційної інфраструктури навчальних закладів від кіберзагроз, несанкціонованого доступу та витоків даних.

Загрози, з якими стикаються шкільні мережі, включають вірусні атаки, фішинг, несанкціонований доступ, DDoS-атаки та внутрішні загрози через недостатню обізнаність користувачів щодо правил безпечного використання цифрових технологій. Це створює потребу у впровадженні комплексних безпекових рішень, які охоплюють як технічні, так і організаційні аспекти кіберзахисту.

Інформаційна інфраструктура шкільної мережі включає апаратне забезпечення, програмне забезпечення, мережеві ресурси та дані, що використовуються у навчальному та адміністративному процесах освітніх закладів.

Ця інфраструктура охоплює: локальні мережі навчальних закладів; сервери та робочі станції; хмарні сервіси, що застосовуються у школі; канали зв'язку та точки доступу до інтернету; бази даних з персональною та навчальною інформацією.

Об'єкт дослідження спрямований на вивчення загроз, які можуть впливати на безпеку шкільної мережі, а також механізмів та рішень, що дозволяють забезпечити її надійний захист.

Для досягнення поставленої мети у роботі було розглянуто: основні види загроз для шкільних мереж та їхні можливі наслідки; сучасні технології та методи забезпечення безпеки освітніх інформаційних систем; організаційні підходи до підвищення рівня кібербезпеки у школах; практичні аспекти впровадження безпекових рішень у навчальних закладах.

У процесі розробки та впровадження безпекових рішень для захисту шкільної мережі використовуються такі методи дослідження:

Метод аналізу та синтезу: аналіз існуючих безпекових рішень та підходів до захисту мереж; синтез отриманих даних для визначення оптимальних стратегій кіберзахисту.

Емпіричні методи: спостереження за роботою шкільної мережі та виявлення її вразливих місць; тестування мережі на стійкість до різних видів кіберзагроз (пенетраційне тестування).

Моделювання та прогнозування: створення моделей потенційних загроз та їх впливу на роботу мережі; прогнозування наслідків впровадження запропонованих заходів захисту.

Експериментальні методи: впровадження та тестування розроблених безпекових рішень у реальних умовах; оцінка ефективності запропонованих технологій та процедур.

Методи системного підходу: комплексний аналіз усіх елементів мережі як єдиної системи; розробка інтегрованих рішень, які враховують технічні, організаційні та освітні аспекти захисту.

Ці методи дозволяють комплексно підійти до вирішення проблеми захисту шкільної мережі, забезпечуючи її надійність та безпеку.

Найбільш поширені загрози для шкільних мереж включають зовнішні та внутрішні фактори, що можуть призвести до витоку даних, порушення роботи системи чи навіть фінансових втрат.

Основні види загроз та їхні можливі наслідки:

Вірусні та шкідливі програми (Malware, Ransomware, Spyware, Trojans). Можливі наслідки: зараження пристроїв, втрата чи шифрування даних (викупні віруси), викрадення конфіденційної інформації, порушення роботи навчальних платформ.

Фішинг (Phishing). Можливі наслідки: отримання зловмисниками паролів та персональних даних через підроблені електронні листи чи сайти, несанкціонований доступ до акаунтів учнів і вчителів, поширення дезінформації.

DDoS-атаки (Distributed Denial of Service). Можливі наслідки: перевантаження серверів шкільної мережі, відмова у доступі до освітніх ресурсів, нестабільна робота онлайн-систем.

Несанкціонований доступ (Hacking, Brute Force, Man-in-the-Middle Attacks). Можливі наслідки: отримання контролю над обліковими записами користувачів, модифікація або видалення важливої інформації, перехоплення мережевого трафіку, зміна оцінок та особистих даних учнів.

Соціальна інженерія (Social Engineering). Можливі наслідки: маніпуляції користувачами для отримання паролів або іншої конфіденційної інформації, розповсюдження шкідливого ПЗ через довіру до знайомих джерел.

Атаки на освітні установи із застосуванням ШІ, глибокі фейки (deepfake), які можуть використовуватись для дискредитації викладачів або учнів.

Витік або компрометація даних (Data Breaches). Можливі наслідки: несанкціоноване розповсюдження персональних даних учнів і вчителів, порушення законодавства щодо захисту інформації, ризики для безпеки дітей.

Використання незахищених пристроїв та мереж (BYOD, Open Wi-Fi, IoT-уразливості). Можливі наслідки: проникнення зловмисного коду через особисті пристрої учнів або вчителів, можливість підключення до внутрішньої мережі

сторонніх осіб, ризик атаки на IoT-пристрої (камери, електронні дошки, маршрутизатори).

Недостатній рівень кіберграмотності персоналу та учнів. Можливі наслідки: невиконання базових правил безпеки, використання слабких паролів, збереження паролів у відкритому доступі, завантаження небезпечних файлів, що збільшує ймовірність успішних атак.

Загальні наслідки для школи: зниження ефективності навчального процесу через збої у роботі онлайн-платформ; фінансові витрати на усунення наслідків атак та відновлення даних; порушення конфіденційності та прав учасників освітнього процесу; ризик юридичної відповідальності у разі витоку персональних даних.

Щоб мінімізувати ці загрози, необхідно впроваджувати комплексні безпекові рішення, що включають технічні заходи (захист мережі, антивіруси, резервне копіювання), організаційні механізми (регламенти безпеки, контроль доступу) та навчання користувачів основам кібербезпеки.

Основні загрози для шкільних мереж включають як зовнішні, так і внутрішні фактори, що можуть призвести до витоку даних, порушення роботи системи чи навіть фінансових втрат. Для ефективного захисту шкільних мереж використовуються різноманітні технології та методи, які можна поділити на кілька основних категорій:

1. Технології для захисту мережі: мережеві брандмауери (Firewall) – використовуються для моніторингу і фільтрації вхідного та вихідного трафіку в межах шкільної мережі. Вони допомагають блокувати несанкціонований доступ, знижуючи ризик атак через інтернет. Віртуальні приватні мережі (VPN) – дозволяють забезпечити захищене з'єднання для віддалених користувачів (наприклад, для вчителів, які працюють вдома). Вони шифрують передавання даних, що робить їх непомітними для потенційних хакерів.

2. Захист від вірусів та шкідливих програм: антивірусні програми та антишпигунські програми. Встановлення на всіх пристроях антивірусних та антишпигунських програм дозволяє своєчасно виявляти і знешкоджувати віруси, троянські програми та інші типи шкідливих програм, які можуть потрапити в мережу школи через інтернет або ззовні. Системи детекції програм-вимагачів (Ransomware Detection Systems) – дозволяють своєчасно виявляти та зупиняти активність шкідливого ПЗ, що може зашкодити даним або зашкодити роботі системи.

3. Шифрування з'єднань. Для забезпечення конфіденційності даних, що передаються через інтернет, використовуються протоколи SSL/TLS. Вони гарантують, що всі дані, які передаються між учасниками освітнього процесу (наприклад, між учнями, вчителями та адміністрацією), будуть зашифровані та захищені від несанкціонованого доступу.

4. Аутентифікація та контроль доступу: багатофакторна аутентифікація (MFA) – забезпечує додатковий рівень захисту облікових записів. Наприклад, для доступу до шкільних інформаційних систем необхідно використовувати не лише пароль, а й код, надісланий на мобільний телефон чи інший додатковий

фактор. Системи контролю доступу (Access Control Systems) – обмежують доступ до певних ресурсів і інформації на основі ролей користувачів. Наприклад, учні не повинні мати доступ до адміністративних даних, а вчителі – до фінансових або медичних даних. Це запобігає несанкціонованому використанню системи.

5. Захист від соціальної інженерії: освітні програми для підвищення обізнаності про кібербезпеку. Навчання учнів, вчителів та адміністрації правилам безпеки в інтернеті, розпізнаванню фішингових атак, важливості надійних паролів та безпечного користування онлайн-ресурсами є необхідним елементом захисту від соціальної інженерії. Політики та процедури безпеки. Встановлення чітких політик щодо використання шкільних пристроїв, інтернет-ресурсів та обміну інформацією дозволяє мінімізувати ризики, пов'язані з людським фактором.

6. Резервне копіювання та відновлення даних гарантує, що у разі втрати або пошкодження даних можна швидко відновити роботу системи.

7. Безпека хмарних сервісів. Якщо школа використовує хмарні платформи для зберігання даних чи проведення онлайн-уроків, важливо забезпечити захист цих сервісів через використання шифрування даних, багатофакторну аутентифікацію та регулярний моніторинг доступу.

У результаті проведеного дослідження на тему «Розробка та впровадження безпекових рішень для захисту шкільної мережі» було визначено основні загрози, з якими стикаються шкільні мережі, а також було проаналізовано сучасні технології та методи забезпечення безпеки освітніх інформаційних систем. Зростання використання цифрових технологій у навчальному процесі ставить перед школами необхідність забезпечення надійного захисту своїх інформаційних систем від різноманітних кіберзагроз. Вірусні атаки, фішинг, DDoS-атаки, а також соціальна інженерія є основними ризиками, які можуть негативно вплинути на функціонування мережі та збереження персональних даних. Розглянуті безпекові рішення включають впровадження мережевих брандмауерів, систем виявлення та запобігання вторгненням (IDS/IPS), антивірусного програмного забезпечення, шифрування даних, а також застосування багатофакторної аутентифікації та контроль доступу. Ці технології дозволяють ефективно захистити шкільні мережі від зовнішніх і внутрішніх загроз.

Освітні програми для учнів та вчителів, які спрямовані на підвищення рівня обізнаності про кібербезпеку, є важливим елементом для запобігання загрозам. Навчання основам безпечного користування мережею, правилам щодо паролів і боротьби з фішингом значно знижує ймовірність успішних атак.

Сучасні технології забезпечення безпеки освітніх інформаційних систем дозволяють ефективно захищати мережі навчальних закладів від різноманітних загроз, таких як несанкціонований доступ, вірусні атаки чи витоки даних.

Комплексний підхід до захисту шкільної мережі не лише мінімізує ризики, але й створює безпечне освітнє середовище, що сприяє розвитку цифрової грамотності всіх учасників навчального процесу.

Список використаних джерел

1. Білан Л. Безпека інформаційних систем в освіті. К. : Вид-во «Освіт. літ-ра», 2020. 198 с.
2. Інструкція для учнів та батьків з безпеки в мережі Інтернет. Наказ Міністерства освіти і науки України 26 грудня 2017 року, № 1669. URL: https://osvita-docs.com/node/176 (дата звернення: 30.03.2025).
3. Методичні рекомендації з інформаційної безпеки навчального комп'ютерного комплексу ; Укл. Дем'яненко В. М., Ковальчук В. Н. К. : ІІТЗН НАПН України, 2014. 39 с.
4. Положення «Про цифрову безпеку закладу освіти» Запорізької гімназії № 41. URL: http://www.znvk41.school.social/storage/polozhennya-pro-cifrovu-bezpeku-zakladu.pdf (дата звернення: 30.03.2025).

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, ЯК ІНСТРУМЕНТ РОЗВИТКУ КРИТИЧНОГО МИСЛЕННЯ В ОСВІТНЬОМУ ПРОЦЕСІ

Гавришків Надія Григорівна
викладач циклової комісії інформатики та комп'ютерних дисциплін,
Галицький фаховий коледж імені В'ячеслава Чорновола,
n.gavrychkiv@gmail.com
Слєпцова Ольга Ярославівна
викладач циклової комісії інформатики та комп'ютерних дисциплін,
Галицький фаховий коледж імені В'ячеслава Чорновола,
olgasleptcova30@gmail.com

Швидкісний розвиток інформаційних технологій суттєво змінює способи навчання, зміст освітніх програм і педагогічні методики у сучасному освітньому середовищі. В умовах глобалізації, трансформація освіти актуалізує потребу не лише у професійних знаннях, а й у розвитку м'яких навичок (soft skills), які стають ключовим чинником успішної професійної реалізації на сучасному ринку праці [3, с. 269]. Важливо розвивати як професійні компетентності, безпосередньо пов'язані зі спеціальністю («hard skills»), так і універсальні навички («soft skills»), що є актуальними в будь-якій сфері діяльності. Сучасні роботодавці розраховують на те, що кандидат матиме безліч різноманітних вмінь: здатність креативно мислити й управляти часом, навички комунікації, критичного мислення, керування проєктами та ефективної роботи в команді.

Розвиток критичного мислення є однією з ключових компетентностей XXI століття, що дозволяє аналізувати інформацію, робити обґрунтовані висновки, ухвалювати зважені рішення та розв'язувати нестандартні завдання [1, с. 95]. Однак традиційні методи навчання не завжди забезпечують належний рівень розвитку цієї навички у здобувачів освіти. У зв'язку з цим виникає необхідність дослідити, яким чином інформаційні технології можуть стати ефективним інструментом розвитку критичного мислення під час навчання студентів.

Традиційні методи навчання, спрямовані переважно на репродуктивне засвоєння знань, часто виявляються недостатніми для ефективного формування навичок критичного мислення. Водночас застосування інформаційних