3. Хакери – хто вони? *Портал освітньо-інформаційних послуг «Студентська консультація».* URL: http://studcon.org/hakery-hto-vony (дата звернення 06.10.2023).
4. Єсіна О. Г., Варналій А. О. Хакерство як соціальне явище. *Інформатика та інформаційні технології:* студ. наук. конф., 20 квітня 2015 р.: матер. конф. Одеса: ОНЕУ, 2015. С. 107–110.
5. Що таке хакерська етика? *Визначення з техопедії.* URL: https://uk.theastrologypage.com/hacker-ethic
6. Грінік Р. О., Пилипенко В. М. Кібертероризм як нова форма міжнародного тероризму. *Науковий блог Львівського державного університету безпеки життєдіяльності.* URL: https://sci.ldubgd.edu.ua/bitstream/123456789/3203/1/13.pdf (дата звернення 09.10.2023).
7. Що таке хактивізм? *Фінансова енциклопедія.* URL: https://ua.nesrakonk.ru/hacktivism (дата звернення 10.10.2023).
8. Фінська модель розвитку інформаційного суспільства. *Розвиток інформаційного суспільства.* URL: http://elbib.in.ua/finska-model-informatsiynogo-suspilstva-rozvitok-informatsiynogo-suspilstva.html (дата звернення 10.10.2023).
9. Трансформаційні процеси у суспільній та соціокультурній сферах України / О. М. Анісімова, Л. А. Ковальська, Г. П. Лукаш, О. В. Прігунов, О. С. Щербіна, Т. М. Яворська. Вінниця: ДонНУ імені Василя Стуса, 2021. 176 с.

УДК 004.056.53

БЕЗПЕКА ТА КОНФІДЕНЦІЙНІСТЬ У БАЗАХ ДАНИХ

І. С. Діброва, Т. В. Січко

Анотація. Дослідження зосереджено на аспектах забезпечення інформаційної безпеки в організаційному середовищі. Пояснюється, наскільки важливо розуміти загрози та вразливості для ефективного захисту інформаційних активів. Також проаналізовано важливі принципи доступності інформаційних ресурсів, як-от: політика безпеки та надійний захист, безперебійна робота систем і послуг. До того ж вказано важливість дотримання низки правил, стандартів, законів і рекомендацій для ефективного управління ризиками та підвищення рівня кібербезпеки.

Ключові слова: захист баз даних, екосистема баз даних, кібербезпека, кіберзлочинність, ризики, аутентифікація, авторизація.

Безпека бази даних має важливе значення для запобігання доступу, зміні або знищенню секретних даних організації. Бази даних містять важливу інформацію, як-от дані про клієнтів, фінансову інформацію та інтелектуальну власність. Усі ці дані є цінними цілями для хакерів і злочинців. Отже, підтримка надійної системи безпеки бази даних має вирішальне значення для підтримки точності даних, дотримання правил захисту даних та завоювання довіри клієнтів і зацікавлених сторін.

Дані – це цінний корпоративний актив для будь якого підприємства. База даних – це організований набір даних, до якого можна отримати доступ, вивчити та реалізувати за допомогою СКБД (системи керування базами даних). Бази даних необхідно захищати та регулярно оцінювати ефективність цього захисту. За допомогою спеціальних методів і програм можна запобігти несанкціонованому доступу до бази даних у локальних мережах або оприлюдненню інформації, не призначеної для широкого загалу [1, 4].

Жодна організація, корпорація чи держава не може уникнути використання інформаційної системи (клієнти, препарати, правила, продукти, фінансові звіти). Ці масиви майже завжди складаються з особистої, інституційної та конфіденційної інформації. Їх втрата може мати серйозні наслідки – як фінансові, так і народні.

Два основні фактори спонукають компанії та державні установи виділяти все більше ресурсів на захист баз даних.

Перший і найважливіший – це кіберзлочинність. Постійна еволюція інструментів зловмисників, поява нових програм-вимагачів, розвиток безфайлових методів проникнення та постійна можливість вчинення дій, які створюють загрозу секретній інформації. Згідно зі звітом про витоки даних, лише у 2019 році було розкрито понад 9 мільярдів облікових записів з особистою інформацією. З огляду на розвиток кримінальних технологій, суттєву увагу слід приділяти заходам, що гарантують захист конфіденційної інформації. Важливим етапом є впровадження превентивних заходів, як-от налаштування брандмауера, який обмежує доступ до сумнівного

вхідного та вихідного трафіку; а також визначення рішень і процедур у разі можливого порушення безпеки.

Другим важливим аспектом, є відповідність міжнародним нормам та законодавству щодо захисту персональної інформації, який постійно удосконалюється. Організації, що здійснюють збір і обробку інформації, несуть відповідальність за її надійний захист. Водночас нормативні вимоги можуть варіюватись залежно від галузі та характеру оброблюваної інформації. Для забезпечення безпеки баз даних українських компаній дуже важливо відповідати цим вимогам, що може потребувати значних фінансових витрат [2, 5].

Основні концепції забезпечення безпеки баз даних – це конфіденційність, цілісність і доступність. Ця тріада виступає фундаментальним базисом у створенні бази даних. Англійською звучить як: confidentiality, integrity and availability, або CIA.

Конфіденційність – властивість інформації, яка полягає в тому, що доступ до інформації мають тільки авторизовані користувачі; навпаки, неавторизовані користувачі в жодний спосіб не мають права доступу до інформації. Також передбачено, що будь-яка інформація має право на зберігання конфіденційності. Вона передбачає недопущення несанкціонованого доступу до конфіденційної інформації.

Цілісність визначає, що дані, які зберігаються в базі даних, не можуть бути змінені та зруйновані без санкційного доступу до них. Цілісність забезпечує роботу даних у встановлений спосіб, що сприяє стійкої роботи всієї системи загалом, автоматичному відновленню системи в разі виявлення помилки, а також автоматичному використанню альтернативних компонентів замість тих, що вийшли з ладу. Одним зі способів забезпечення цілісності є використання цифрових підписів для перевірки автентичності та захисту транзакцій. Воно широко використовується державними установами та організаціями в медичній сфері.

Доступність – це характеристика інформаційних ресурсів. Вона полягає в тому, що користувачі та/або процеси з відповідними привілеями можуть використовувати цей ресурс, не чекаючи більше певного (прийнятного) періоду часу, відповідно до правил, зазначених у політиці безпеки. Контрольні засоби, комп'ютерні системи та програмне забезпечення повинні функціонувати належно, щоб забезпечити доступність послуг та інформаційних систем у разі потреби. Наприклад, якщо фінансову базу даних вимкнено, відділ бухгалтерського обліку може бути не в змозі вчасно подавати або оплачувати рахунки-фактури, що потенційно може порушити важливі бізнес-процеси. Отже, важливо забезпечити надійний захист, а для цього слід розглянути чотири аспекти безпеки.

Перший етап управління даними – це розробка ефективної політики безпеки бази даних. На цьому етапі слід встановити різні рівні конфіденційності даних та виставити пріоритети відповідно до їх важливості. Наступним кроком у плануванні політики баз даних буде визначення із технологіями захисту. Наприклад, це буде шифрування чи встановлення ключів, або ж це можуть бути вірусні сканери та файрволи. Далі слід подбати про встановлення та налагодження каталогів, що містять перелік даних та інформацію про них. Перший етап управління даними є фундаментом для ефективного забезпечення системи бази даних. Слід постійно оновлювати бази даних відповідно до їх змін, вчасно вживати заходів для виявлення порушень чи несправностей. Такий підхід допомагає встановити відповідний рівень захисту та уникнути потенційних загроз і можливих недоліків в управлінні.

Другим важливим етапом є розробка системи виявлення IDS (Intrusion Detection System) – програмних або апаратних засобів, призначених для виявлення незвичайної або підозрілої активності у комп'ютерній мережі чи системі. Основна мета цих систем – вчасно виявляти можливі загрози та інциденти з безпекою, щоб негайно реагувати на них.

Існують два основні типи IDS: система виявлення IDS та система реагування IPS.

IDS – детекторна підсистема, метою якої є накопичення подій мережі або комп'ютерної системи. Вона виявляє підозрілу активність мережі та кібератаки. Також вона виступає сховищем накопичення інформації про події в мережі та результат різних несанкціонованих дій. Також за допомогою IDS можна стежити за станом системи, проводити системний аналіз системи та мати доступ до інформації про систему.

IPS – система реагування та запобігання. Це розширений, більш функціональний різновид IDS. Головне завдання цієї системи – виконувати захисні функції. Відмінною рисою IPS є те, що вони працюють у режимі онлайн і можуть автоматично блокувати атаки.

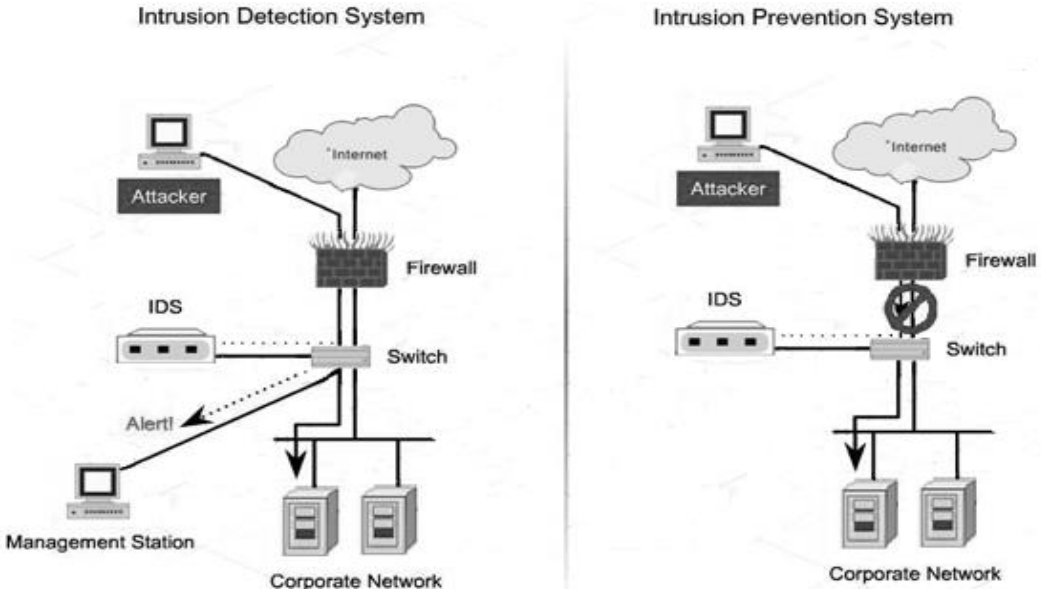

Рис. 1. Поведінка системи виявлення вторгнення (ліворуч), поведінка системи запобігання вторгнення (праворуч)

Третім етапом є захист бази даних. Процес захисту даних інформаційної бази передбачає активні дії щодо забезпечення безпеки. Захист систем баз даних – це сукупність методів, програмних засобів, процесів, програм та технологій, застосування яких забезпечує безпеку інформації, що зберігається, і запобігає несанкціонованому електронному доступу до неї, модифікаціям, випадковому розкриттю, порушенню, знищенню, копіюванню. Ось кілька ключових аспектів захисту бази даних:

- шифрування даних;
- моніторинг;
- захист від SQL-ін’єкцій та інших атак;
- резервне копіювання та відновлення (допомагає уникнути втрати даних);
- безпека стільникових мереж.

Четвертий важливий крок – відповідність. Відповідність (Compliance) в інформаційній безпеці означає дотримання організацією набору правил, стандартів, законів та політик, які регулюють обробку та зберігання даних. Це включає внутрішні політики компанії, регулятивні вимоги галузі та національні, або міжнародні закони. Сюди входить розробка та впровадження певних політичних стандартів, встановлення процедур відповідності, яких організація повинна дотримуватися. Основним завданням такого підходу є забезпечення певного регламенту, який призведе до злагодженої роботи усіх розробників [3].

Якщо виконати усі чотири кроки – отримаємо створення безпечної бази даних, своєрідну екосистему, яка може функціонувати подібно до колообігу в природі. Захищена екосистема баз даних – це комплексний підхід до захисту інформації, що зберігається та обробляється в базах даних організації. Ця екосистема допомагає компаніям створювати надійні механізми захисту важливої інформації, що зберігається в їх базах даних, і зменшувати ризик несанкціонованого доступу, втрати чи пошкодження даних.

Важливо розуміти, що будь-який елемент у базі даних із перелічених не може функціонувати самостійно. Створення якісної екосистеми баз даних вимагає певного підходу та цілісного погляду. Не треба розглядати окремий елемент у базі даних як окреме ціле, також не слід розглядати лише структуровані файли й не зважати на неструктуровані. Цілісне уявлення має вирішальне значення, також розробка правильної архітектури і створення потрібних компонентів з використанням відповідних технологій та їх інтеграція буде мати вирішальне значення.

У межах цього дослідження були проаналізовані важливі аспекти забезпечення інформаційної безпеки з погляду управління базами даних. На основі аналізу було визначено та обговорено чотири основні кроки забезпечення інформаційної безпеки бази даних. Загалом наведені в роботі етапи та методи забезпечення інформаційної безпеки баз даних є важливими елементами управління ризиками та збереження конфіденційної інформації. Їх впровадження може значно підвищити рівень кібербезпеки та запобігти потенційним загрозам.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Smith J. The Impact of Modern Technologies on Communication Skills. *Journal of Communication Studies.* 2021. Vol. 45, № 2. P .78–92.
2. Anderson R. Et al. Insider Threats to Database Security: Case Studies and Mitigation Strategies. *Information Security Symposium.* 2023. P. 75–88.
3. Davis L. The Role of Human Error in Database Security Breaches. Security Management Magazine. 2023. Vol. 22, № 3. P. 60–73.
4. Мазур Ю. О., Зелінська О. В. Особливості захисту сучасної інфосфери в умовах стороннього кібернетичного впливу. *Прикладні аспекти сучасних міждисциплінарних досліджень:* матеріали І Всеукраїнської науково-практичної конференції (м. Вінниця, 26 листопада 2021 р.). Вінниця: ДонНУ імені Василя Стуса. 2021. С. 102–104. URL: https://jpasmd.donnu.edu.ua/issue/view/403
5. Денисюк В. В. Важливість кібербезпеки в сучасному світі. *Комп'ютерні технології обробки даних:* матеріали ІІ Всеукраїнської науково-практичної конференції (м. Вінниця, 10 грудня 2021 р.). Вінниця: ДонНУ імені Василя Стуса. URL: https://jktod.donnu.edu.ua/article/view/11614
6. Степанюк О. С., Січко Т. В. Особливості використання реляційних та нереляційних баз даних в Big Data. *Комп'ютерні технології обробки даних:* матеріали всеукр. наук.-практ. конф., м. Вінниця, 2020. С. 103–106.

УДК 004.056-028.63:37.091.2

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯЯ ЦИФРОВОЇ БЕЗПЕКИ ПІД ЧАС РЕАЛІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ В ЗАКЛАДАХ ОСВІТИ

О. В. Дорош, В. Ю. Василенко

Анотація. У статті досліджується питання цифрової безпеки в освітньому процесі, аналізується законодавча база та стратегічні документи, які визначають цифрову трансформацію української освіти. Акцентовано на розвитку цифрових компетентностей учасників освітнього процесу та наголошено на важливості забезпечення безпеки цифрового середовища. Були зазначені проблеми низького рівня цифрової грамотності, обмеженого доступу до комп'ютерного обладнання та інтернету, а також відсутності високоякісного цифрового освітнього контенту.

Ключові слова: цифрова безпека, цифрова грамотність, освіта, цифрові навички.

Вступ. У сучасному світі, де цифрові технології відіграють важливу роль, освіта є основою будь-якого суспільства. Освіта не тільки дає людині знання та навички, але й визначає її здатність адаптуватися до середовища, що швидко змінюється. Оскільки технології продовжують розвиватися і стають все більш взаємопов'язаними, ризик загроз для освітнього процесу є найвищим. У цьому контексті цифрова безпека стає важливою частиною освіти.

Основний розділ. Освіта – важливий аспект соціального життя, безпеки та стабільності країни, які все більше набувають числового формату. Часто інформаційний контент є засобом маніпулювання свідомістю, причиною конфліктів і негативних проявів. Питання свідомого споживання інформації, особливо в освіті, критичного аналізу та якості інформації стали стратегічними для розвитку країн на національному та міжнародному рівнях. Отже, розвиток цифрових технологій стимулює створення цифрової безпеки в закладах освіти. Сучасна освіта з березня 2020 року в основному реалізовувалась у дистанційному та/або онлайн-форматі, через це питання цифрової безпеки у вищій освіті має пріоритетне значення [1]. В умовах реформування та модернізації освітнього середовища за допомогою цифрових технологій цифрова безпека освітніх систем є основною тенденцією. Це забезпечується шляхом підвищення грамотності у використанні сучасних цифрових технологій, удосконалення правового регулювання відповідальності за порушення законодавства у сфері інформаційної безпеки молоді. Особливе значення відіграє впровадження дистанційних методів навчання на всіх рівнях освіти, активі-