DOI 10.18372/2310-5461.54.16746

УДК 621.396

Р. В. Хращевський, д-р техн. наук, професор
Національний авіаційний університет
orcid.org/0000-0003-4210-8135
e-mail: rimvidas.krashchevskyi@npp.nau.edu.ua;

К. С. Нестеренко, д-р техн. наук, професор
Національний авіаційний університет
orcid.org/0000-0001-7672-7386
e-mail: kateryna.nesterenko@npp.nau.edu;

В. В. Козловський, д-р техн. наук, професор
Національний авіаційний університет
orcid.org/0000-0002-8301-5501
e-mail: vvkzeos@gmail.com;

О. І. Ткаля
Національний авіаційний університет
orcid.org/0000-0001-6687-2416
e-mail: 5824892@stud.nau.edu.ua

ЗАХИСТ БАЗ ДАНИХ ЗА ДОПОМОГОЮ ПРОГРАМНОГО КОМПЛЕКСУ DBPROTECT

Вступ

Стрімкий розвиток інформаційних технологій веде до збільшення кількості інформації, що своєю чергою призводить до зростання кількості загроз інформації.

Оскільки інформація — це найважливіший ресурс у сучасному світі цілком очевидним є питання з удосконалення її захисту, щоб запобігти збитку інтересів власника інформації.

В останні роки у світі набуває розвитку відносно новий напрямок інформаційна індустрія що поєднує в собі всі сфери життя людини, такі як наукова, підприємницька, комерційна чи розважальна діяльність.

У зв'язку з цим зростає чисельність несанкціонованих втручань та зломів з метою викрадення конфіденційної інформації для подальшого отримання вигоди. Тому потреба захисту цієї інформації є пріоритетною для багатьох спеціалістів індустрії в різних країнах.

Щоб розв'язувати питання з оптимізації матеріальних та трудових ресурсів та в роботі з неймовірно великими обсягами інформації, що нині циркулює у просторі організації державного, наукового, освітнього чи приватного характеру впроваджують використання баз даних. База даних — це найкращий метод для роботи з великим обсягом інформації, що являє собою систематизовану сукупність матеріалів різного типу для обробки за допомогою комп'ютера.

Постановка проблеми та її актуальність

Нині зі зростанням розвитку всіх сфер інформаційної індустрії збільшується і застосування баз даних у різних підприємствах та організаціях. Разом з цим розвивається і злочинна сфера і в зв'язку з цим сьогодні можна знайти багато матеріалів та програм хакерів які є у вільному доступі та дозволяють будь-кому використовувати вразливості баз даних для злому та отримання конфіденційної інформації з метою подальшого її використання у корисних цілях.

Статистика говорить, що в останні роки кількість зломів та витоку інформації дуже зросла. Є багато випадків витоку особистої інформації користувачів банку чи рієлторський організацій що призвели до великих фінансових збитків. Також відомі випадки витоку даних з державних організацій що призвело до оприлюднення паспортних даних та інших особистих документів. У науковій та комерційній сфері витоки інформації через несанкціоновані доступи призводять до присвоєння чужих робіт та розкриття комерційних таємниць що завдає великих збитків. Тому конфіденційна інформація потребує захисту та контролю для забезпечення безпеки.

Аналіз останніх досліджень і публікацій

Кількість випадків злому, як приватних копаній, так і державних організацій на сьогодні неймовірно велика, багато прикладів і досліджень є у відкритому доступі, це дає змогу будькому самостійно провести аналіз проблеми неза-

хищеності баз даних порівняно з розвитком і збільшенням загроз.

Наприклад 2020 році було зафіксовано 1 120 витоків і кібератак. Більшість цих інцидентів було оприлюднено провідними ЗМІ, в цілому близько 20 120 074 547 записів було зламано [1].

У грудні 2020 року фахівцями з інформаційної безпеки було зафіксовано атаки та злив інформації компаній та організації що користувалися сервісом Accellion FTA. Загалом від атак постраждало близько 100 компаній, однією з яких стала канадська машинобудівна компанія Bombardier [3]. У 2021 році була проведена атака на бази даних однією з найбільших компаній виробників комп'ютерів Acer та як повідомляють фахівці шахраї запросили один з найбільших на сьогодні викупів у розмірі 50 млн доларів США [4]. У серпні 2019 року зазнала атаки одна з німецьких бонусних програм Mastercard. В результаті цього номери телефонів, банківські рахунки та електронні пошти були у відкритому доступі, постраждало близько 90 тисяч користувачів що стали учасниками програми [5].

Асоціація індустрії обчислювальних технологій «CompTIA» провела дослідження та опублікувала статистику яка показує, що порівняно з 2020 роком у 2021 році кількість людей котрі вважають, що стан кібербезпеки, а разом з тим і захищеність баз даних покращується зменшилася на 11 %. [2] (рис. 1).

Рис. 1. Стан кібербезпеки з 2020 на 2021 рік

Хоча кількість зафіксованих та підтверджених випадків зломів неймовірна велика, багато випадків замовчуються для збереження репутації. Адже компанії котрі постраждали від несанкціонованого доступу до своїх баз даних зазнають не тільки фінансових збитків, а й псування іміджу що може призвести навіть до банкрутства та повного закриття у майбутньому (рис. 2).

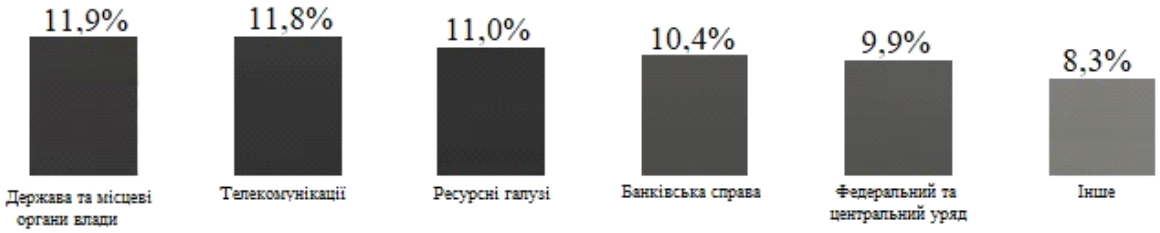

Рис. 2. Галузі з найшвидшим зростанням витрат на безпеку в усьому світі

Компанія Accenture провела дослідження у результаті якого стало відомо що станом на 2021 р. 82 % з опитаних компаній прийняли рішення збільшити бюджет на забезпечення інформаційної безпеки [6].

Платформа FinancesOnline зібрала дані для створення статистики яка показує різні сфери людської діяльності та їх витрати на забезпечення інформаційної безпеки.

Мет ою даної статті є розглянути програмний комплекс DbProtect, як один з методів захисту баз даних та визначити його ефективність.

Виклад основного матеріалу

Необхідність оперувати великими обсягами інформації з'явилася вже давно, як один з методів роботи з інформаційним ресурсом став комп'ютер який зараз вже є невід'ємною частиною сучасного життя. Але і поява комп'ютера не полегшує роботи з неймовірними обсягами неорганізованих даних саме тому і використовують бази даних щоб структурувати та упорядкувати дані задля зручного користування ними надалі.

База даних — це один або кілька файлів даних, призначених для збереження і оброблення великих масивів взаємозалежної інформації [7]. На практиці частіше можна зустріти використання систем баз даних.

Система баз даних — це комп'ютерна система, у якій зберігається один тип запису, який можна розглядати як електронний файл, що зберігаються в пам'яті комп'ютера. Система баз даних дає змогу зручно користуватися та оперувати необхідною інформацією.

Система управління базою даних являє собою набір мовних та програмних засобів, призначених для створення, обслуговування, підтримки та забезпечення централізованої інтеграції, а також спільного контролю над використанням бази даних.

Важливою особливістю систем управління базами даних є наявність систем доступу та зберігання як даних, а й описи їх структури та взаємозв'язків між ними.

Бази даних класифікуються за різними ознаками: за типом збереженої інформації записи поділяються на фактографічні та текстові. Якщо малювати ілюстрації та приклади опису інформації, описані вище, то картотеки фактографічної бази даних, а текстові файли — це текстові файли. Звичайно, база даних зберігає коротку інформацію у чітко визначеному форматі. Документарні бази даних містять усі типи документів. Причому це можуть бути не лише кольорові записи, а й графіка, відео та звук (мультимедіа).

Організовані за способом зберігання даних, який поділяє базу даних на середню та розподільну. Вся інформація в центральному сховищі зберігається на іншому комп'ютері. Це може бути автономний комп'ютер або мережевий сервер, якого клієнти можуть отримати доступ. Розподілені бази даних використовуються локально та по всьому світу комп'ютерними мережами. І тут різні частини бази даних зберігаються різних комп'ютерах. Третій показник конфігурації бази даних залежить від організації даних.

Якщо учні ніколи не схоплювали ідею створення даних, вчителю слід зупинитись на цій темі або повторити знайомий досвід учнів. Фасилітатор повинен розповісти про три способи організації даних: табличний, ієрархічний і мережевий. Бази даних використовують відповідний метод організації інформації, званий реляційними (табличні БД), ієрархічними та мережевими базами даних. База даних є важливим компонентом корпоративного соусу, який необхідно підтримувати відповідними способами та засобами. Щоб вжити негайних заходів щодо зниження ризику, тобто ризику втрати або пошкодження даних, необхідно вивчити відповідну загрозу. Концепція захисту даних стосується не лише даних, що зберігаються у базі даних. Дефекти імунної системи також можуть виникати у деяких її областях, що поставить під загрозу основу. Тому безпека повинна повністю охоплювати кожен аспект інформаційної діяльності (компанії та організації): інструменти, програмне забезпечення, користувачів і дані (див. таблицю)

Таблиця

Види загроз та їх наслідки для бази даних

Загроза	Втрата доступності	Порушення недоторканності особистих даних	Втрата конфіденційності	Викрадення і фальсифікація даних	Втрата цілісності
Необдумані методики й процедури, що допускають змішування конфіденційних і звичайних даних в одному документі		+	+	+	
Створення «лазівок» у системі		+	+	+	
Уведення хакерами некоректних даних		+	+	+	
Використання прав доступу іншої людини		+	+	+	
Недостатня кваліфікація персоналу	+	+	+		+
Несанкціонована зміна або копіювання даних				+	+
Викрадення даних, програм і устаткування	+	+	+	+	
Відмова системи захисту, що викликає перевищення припустимого рівня доступу		+	+	+	
Обрив або від'єднання кабелів	+				+
Руйнування даних у результаті відключення або перенапруги в мережі електроживлення	+				+
Впровадження комп'ютерних вірусів	+				+
Зміна програм	+			+	+
Підключення до кабельних мереж		+	+	+	
Шантаж		+	+	+	
Нестача персоналу й страйки	+				+
Перегляд і розкриття засекречених даних		+	+	+	
Електронні наведення й радіація				+	+

Ця потенційна загроза пояснює основні способи, якими менеджери повинні робити кроки для зниження рівня ризику, тобто можливості втрати або пошкодження даних. У деяких випадках, всі спостереження за пошкодженням даних пов'язані між собою. Таким чином, дії, спрямовані на порушення безпеки системи тим чи іншим чином, часто призводять до зниження її безпеки у всіх інших. Крім того, деякі інциденти, такі як порушення конфіденційності або помилкова інформація, можуть бути результатом навмисних та ненавмисних дій. І зовсім не важливо, чи супроводжуватимуться вони будь-якими змінами, поміченими якимось чином у базі даних або системі.

Крадіжка даних та шахрайство можуть відбуватися не лише в області баз даних – із цим ризиком стикається вся організація. Таким чином, акти крадіжки або помилкової інформації, як правило, здійснюються самими людьми, тому основну увагу слід приділяти зменшенню їх загального розміру та простоті участі у таких діях. Крадіжка та шахрайство пов'язані не тільки зі зміною будь-яких даних, що також вірно для втрати конфіденційності або порушення ваших даних.

Втрата недоторканності приватного життя та порушення недоторканності приватного життя призводить до руйнування конкуруючих позицій та правових наслідків, що є результатом анти організаційних скарг, поданих постраждалими людьми. У випадку дані, важливі для всієї організації, вважаються конфіденційними, у своїй конфіденційність даних передбачає виконання вимог захисту особистої інформації.

Втрата довіри та втрата доступу до даних призводять до пошкодження або знищення даних, що може призвести до серйозних наслідків майбутньої роботи організації.

Втрата доступу до даних – це коли дані або система, або те й інше недоступні для користувачів, що може поставити під загрозу безперервність організації. У деяких випадках події, що спричинили переміщення системи в недоступне місце, можуть одночасно призвести до знищення бази даних. В даний час більшість організацій працюють у безперервному режимі, пропонуючи свої послуги клієнтам 24 години на добу та сім днів на тиждень. Тому втрата доступності даних призводить до значних збитків через відплив платоспроможних клієнтів.

Одним з варіантів захисту своїх даних для компаній та організацій є використання різних платформ створених спеціально для виявлення уразливостей баз даних та запобігання несанкціонованих втручань. Є надзвичайно велика кількість таких платформ, програм та комплексів і щоб знайти та обрати підходящу для своєї організації потрібно провести аналіз якщо не кожної то більшості та обрати найкращу, яка буду виконувати всі поставлені перед нею задачі.

Програмний комплекс DbProtect служить для того, щоб вирішувати питання безпеки баз даних та для того щоб всі вимоги були виконані згідно з нормативними актами. Дана платформа створена для того, щоб можна було виконувати всі потреби різних систем баз даних.

DbProtect контролює процеси забезпезпечення безпеки та допомагає компаніям, виставити правильну пріоритетність задля захисту інформації. Зараз, під час стрімкого розвитку баз даних, коли з кожним разом все більше і більше додаються нові прикладні програми, бази, користувачі та оновлюється ПО, компаніям стає важче захищати інформацію, що циркулює в їх базах даних.

Є п'ять критичних вимог до захисту баз даних за, які відповідають компанії:

1. Прибрати бази даних, які є нестійкі. Підтримка всіх баз, які працюють в компанії, і виявлення в них, інформації, яка може бути нестійкою.

2. Усунення вразливостей. Завжди проводити аналіз та усунення всіх можливих вразливостей, які можуть вплинути на бази даних.

3. Дотримання правил та контроль. Зробити, та вказати те, що має можливість робити користувач для того, щоб користувач не мав доступ до інформації з обмеженим доступом та баз даних, які відповідають за роботу.

4. Моніторинг відхилень. Виконання правил та політики компанії, також перевірка всіх можливих вразливостей.

5. Реакція на підозрілі дії/поведінку. Попередження та реагування в реальному часі, на любі дії, які є підозрілими, або які відхилені від норми поведінки користувача.

DbProtect використовується для контролю забезпечення ІБ баз даних.

Контролює збір, аналіз, контроль та усунення.

Даний комплекс включає в себе збір даних та надає повну характеристику баз даних кампанії. Після збору інформації, він починає аналіз для того, щоб знайти вразливі місця, або можливі витоки інформації та ризики, також знаходить вразливості які потрібно модернізувати. Таким чином, даний комплекс надає повну інформацію та інструкції для усунення вразливостей в базах даних. Після цього, DbProtect контролює безпеку баз даних, через моніторинг та реагуючи на підозрілі активності.

Точний моніторинг баз даних платформи DbProtect.

Даний комплекс допомагає компаніям сконцентрувати увагу на підозрілій активності та несанкціонованому доступу до баз даних, окрім цього упорядкувати дії по забезпеченню безпеки баз даних.

Системи для управління вразливостями та правами, також які служать для аналізу ризику, які підтримуються базою SHATTER, знаходять, перевіряють і надсилають звіт по перевірці, також знешкоджують можливі канали, через які може витекти інформація та невірні конфігурації, які є в базах даних цієї компанії.

За допомогою цього, компанія, прибирає можливі вразливості через які можна зламати базу даних, покращити параметри ризикозахищеності.

Система активного реагування DbProtect забезпечує автоматичні відповіді на певні типи підозр та несанкціоновані дій. Відповіді включають: IT-повідомлення, запити SIEM, запити на відновлення, сканування шкідливих програм, зловмисне програмне забезпечення або завершення сеансу. Переваги системи DbProtect Active Response включають:

1. Припинення підозрілої активності в реальному часі.
2. Проведення комп'ютерного аналізу та покращення безпеки бази даних.
3. Введення додаткових заходів безпеки для забезпечення конфіденційної інформації.

Ретельний моніторинг усуває турботи, необхідні ресурси та ціни, пов'язані зі сховищем, що знаходиться у сховищі бази даних.

DbProtect – одна з небагатьох програм, призначених для використання у малих та середніх компаніях, а також у великому бізнесі. Модульний дизайн та гнучкі ціни дозволяють організаціям додавати інструменти, а також встановлювати та додавати DbProtect для задоволення поточних та майбутніх потреб.

Управління вразливістю є основою DbProtect AppSec. Виконує безпрецедентний тест бази даних. Безкоштовна проксі-програма DbProtect дозволяє знаходити, аналізувати та безпосередньо оцінювати відповіді, а також виправляти порушення та неточності у будь-якій базі даних.

Система управління вразливістю підтримується інформаційною базою SHATTER, яка є повним набором систем управління ризиками, доступними на ринку. ASAP Upgrade за допомогою AppSec забезпечує найновіший рівень захисту. Оскільки нові типи вразливостей та можливостей для крадіжки можуть бути виявлені, а також розроблені безпечні інструменти бази даних, DbProtect розроблений для забезпечення кліматичного захисту цінних ресурсів бази даних. Система управління вразливістю включає:

Інформація про структуру даних. Перший у створенні ефективного управління безпекою даних з їх отриманням та підтримкою точного переповнення всіх баз даних, що діють на підвідомчих підприємствах. Пошукова оптимізація є найкращим способом вийти на провідний ринок нерухомості в решті країни. Орієнтовані на бізнес, а також обмін фотографіями, живі IT та корпоративні онлайн-конкурси. У підсумку вони створюють ризик без подачі, радіють падінням хакерів, чиї дані намагаються проникнути в мережу і отримати доступ до інших баз даних, які є відчутною інформацією. DbProtect змінює правила гри для широкого кола реальних сценаріїв. Перевірка входу в систему за допомогою функцій безпеки та моніторингу системи Наступним кроком у реалізації ефективного захисту бази даних є виявлення та усунення дефектів та неправильних систем, які продовжують порушувати роботу бази даних. Існує безліч можливостей вкрасти докладну інформацію. Ненадійні паролі, відсутність функцій безпеки, безпечні паролі безпеки та відсутність контролю доступу дають хакерам можливість вкрасти конфіденційну інформацію. DbProtect забезпечує непередбачуваний аналіз нестабільності бази даних, що дозволяє організаціям усувати невідповідності та неточності при діагностиці та усуненні нестабільності у будь-якій базі даних. Система термінового оновлення DbProtect надає останній рівень захисту бази даних.

Вдосконалена політика. Рушійною силою системи управління вразливістю є сильний спосіб встановлення правил. Це дозволяє створювати функціональні та певні макети, призначені для екосистеми конкретної бази даних. Політика оновлення DbProtect, яка підтримується простим у використанні допоміжним функціональним модулем, дає користувачеві тристоронній підхід до допоміжних технологій. Це дозволяє організаціям ідентифікувати будь-яку конкретну подію, яку слід відслідковувати, а також отримувати доступ до будь-якої конфіденційної інформації, яку необхідно контролювати, та будь-яких припущень, що потребують активації системи Active Response. DbProtect ініціює оновлення системи за допомогою налаштованих шаблонів, сумісних із затвердженою бібліотекою користувача. Шаблони включають SOX, PCI-DSS, NIST 800.53, DISA STIG, HIPAA та багато інших. Application Security Inc. Разом зі своїми російськими дочірніми компаніями також розробляє стандартний блок STOBRIBBS. Щоб увімкнути фільтрацію та бізнес-правила, ефективний модуль довідки надає каталог усіх елементів бази даних. Це допоможе організаціям визначити

конкретні таблиці та стовпці, що становлять інтерес, а також визначити типи ризиків. Цей метод дозволяє шукати всі можливі покращення на рівні стовпця, забезпечуючи більш глибоке розташування та усуваючи будь-які хибні чи посилені заперечення.

База знань SHATTER. База знань SHATTER реалізує промислові заходи змішаної нестабільності та видимості загроз. Його підтримує TeamSHATTER, дуже велика та досвідчена організація з пошуку баз даних. Система термінового оновлення DbProtect надає щомісячні оновлення бази знань SHATTER з останніми відомостями про нестабільність сигнатур та загроз, доступ до найсучасніших даних про розгортання SQL і високотехнологічні злами з використанням постійних загроз. Кожне опитування надає детальну та зручну для інтерпретації інформацію, яка забезпечує спільне розуміння між адміністраторами баз даних (ABD), відділами IT-безпеки та іншими організаціями.

Звіти та аналітика. Система звітів та аналітики DbProtect надає вичерпну інформацію про нестабільність, загрози та відповідність вимогам у різних системах баз даних у сучасних компаніях. Простий у використанні інтерфейс складається з інтерактивних інформаційних панелей та зведених звітів, у яких система збирає дані за допомогою великої фільтрації, організації та детальної обробки, забезпечуючи потужні можливості звітності. Ця технічна можливість дозволить менеджерам швидко визначити, куди і як слід спрямувати ресурси для кращого зниження ризиків, а також виконати адміністративні вимоги до бази даних. Детальні та докладні звіти створюють повну картину ситуації у кожній базі даних або групі баз даних. Аналітики АБД та IT-безпеки отримують інформацію з необхідним рівнем знань, не обтяжуючи менеджерів та менеджерів організації недійсним досвідом. звіти про політику користувача та події. Організовано надсилання електронних звітів кваліфікованому персоналу за необхідності.

Оцінка ризиків. Система аналізу ризиків DbProtect (додатково) допомагає організаціям оцінити ефективність системи управління ризиками для боротьби з безпосередніми загрозами. Система аналізу ризиків розраховує «фактор ризику» нестабільності бази даних на основі здійсненності, ефективності та помилок під час ведення бізнесу. За такого підходу незахищеність бази даних можна порівняти з IT-ризиками, що допоможе організаціям розставити пріоритети у роботі з усунення вразливостей.

Управління повноваженнями. Надійна система управління DbProtect забезпечує докладний аналіз власника даних організації, управління доступом та прав на отримання детальної інформації. Згодом права користувачів можуть значно збільшуватися та вийти з-під контролю. Просування по службі, передача, придбання та злиття, а також успадкування можуть призвести до того, що користувачі отримують більше привілеїв, ніж потрібні працівники для виконання їхніх обов'язків. Ця ситуація може призвести до небезпечних наслідків з привілеїв, що дозволяє крадіжку даних або злочинну заміну інформації усередині. Важливим кроком у реалізації функціональної бази даних підтримки шаблонів є контролю над дотриманням малих привілеїв. Простіше кажучи, це означає давати лише ті привілеї, які має людина для виконання своєї роботи. Управління правами користувачів та моніторинг підозрілої активності вважаються найважливішими етапами, визначеними майже у всіх законах, включаючи закони Сарбейнса-Окслі (SOX), PCI-DSS, NIST-800, DISA STIG, HIPAA та інші.

Відстеження подій бази даних. Система моніторингу активності бази даних DbProtect (MABD) відслідковує зловмисних користувачів, сповіщає та попереджає про незвичайну або підозрілу поведінку, а також блокує зломи та спроби використання вразливостей бази даних. Правила проектування DbProtect дозволяють організаціям зосередитись на конкретних подіях бази даних, що потребують особливої уваги. Системи моніторингу можна визначити як певні дії реальних користувачів, які намагаються отримати доступ до певної інформації в інших базах даних. Цей метод дозволяє перевірити всі способи для використання вразливостей і надати кілька правил для усунення цих проблем чи конфліктів. SOX, PCI-DSS, NIST 800.53, DISA STIG, HIPAA та багато інших рівнів допомагають продемонструвати можливості загальних систем безпеки для моніторингу всієї інформації, допомагаючи організаціям визначати набір автоматичних подій на підозрілу активність. Система Active Response може бути адаптована до екосистеми баз даних та включає:

1. Надсилання попереджень IT-персоналу для подальшого розслідування.
2. Надсилання попереджень до системи SIEM, щоб зв'язати підозрілі бази даних з вебконтентом для криміналістичного аналізу.
3. Надсилання запитів на виправлення для відстеження системних порушень.
4. Визначення підозрілої та несанкціонованої події.

Шифрування, яке надається в системі Active Response (також відоме як система віртуальної нейтралізації або запобігання вторгненням), за-

хищає від крадіжки та несанкціонованого доступу до конфіденційної інформації. Закриття може включати автоматичну зупинку підозрілих сеансів користувача або закриття декількох облікових записів злому. В основі системи Active Response лежить потужна правоохоронна система DbProtect, яка дозволяє організаціям бачити відповідні дії у відповідь на певну подію, коли фактичні користувачі намагаються отримати доступ до певної інформації у певних базах даних. З такими високими рівнями організації можуть запобігти ризикам, пов'язаним з неправильним реагуванням на затверджену подію.

Висновки

У всі часи інформація була одним з найважливіших ресурсів людства та потребувала захисту. З появою та розвитком інформаційних технологій стало набагато легше користуватися цим ресурсом. Але разом з розвитком інформаційних та комп'ютерних технологій збільшується і кількість загроз, котрі постійно вдосконалюються та все частіше з'являються в загальному доступі для звичайних користувачів, що дає змогу у майбутньому будь-кому зламати незахищену базу даних задля отримання конфіденційної інформації компанії чи організації.

Тому кожна організація повинна заздалегідь вирішити проблему несанкціонованого доступу щоб не постраждати від злому та несанкціонованого доступу. Великі підприємства і компанії та державні організації витрачають величезні суми свого бюджету на забезпечення безпеки. Проте і для менш фінансованих організацій є неймовірно велика кількість платформ та комплексів направлених на захист баз даних різного типу. Щоб захистити свою організацію від загроз зараз можна просто провести детальний аналіз таких комплексів та обрати підходящий.

Програмний комплекс DbProtect підходить, як для невеликих компаній так і для організацій середнього та великого розміру. Модульний дизайн та гнучкі ціни дозволяють організаціям додавати інструменти, встановлювати та додавати DbProtect для задоволення поточних та майбутніх потреб.

ЛІТЕРАТУРА

[1] Статистика з кібербезпеки за 2020 рік https://10guards.com/ua/articles/2020-cybersecurity-statistics/#contacts (дата звернення 10.02.2022)

[2] State of cybersecurity 2021 https://www.comptia.org/content/research/cybersecurity-trends-research (access data 10.02.2022)

[3] Engineering company Bombardier fell victim to a ransomware attack https://howtofix.guide/bombardier-fell-victim-to-a-ransomware-attack/ (access data 10.02.2022)

[4] Acer hit with up to $50m ransom https://www.securitymagazine.com/articles/94870-acer-hit-with-up-to-50m-ransom (access data 10.02.2022)

[5] Datenleck bei Mastercard-Bonusprogramm https://www.spiegel.de/netzwelt/web/mastercard-datenleck-bei-bonusprogramm-a-1282697.html (access data 10.02.2022)

[6] The state of cybersecurity resilience 2021 https://www.accenture.com/us-en/insights/security/invest-cyber-resilience (access data 10.02.2022)

[7] Редько М.М., Ярмуш О.В., Редько Н.С. Інформатика та комп'ютерна техніка. Навчально-методичний посібник, 2002. С. 50.

[8] Кузин, А.В., Левонисова С.В. Базы данных: Учебное пособие для студ. высш. учеб. Заведений. М.: ИЦ Академия, 2012.

[9] Есин В. И., Кузнецов А. А., Сорока Л. С. Безопасность информационных систем и технологий. Х. : ЭДЭНА, 2010.

[10] Cybersecurity Statistics: 2021/2022 Data & Market Analysis https://financesonline.com/cybersecurity-statistics/#:~:text=55%25%20of%20business%20executives%20plan,2024%20(Forbes%2C%202020) (access data 15.04.2022)

[11] DbProtect Analytics 1.0 Installation and User's Guide http://www.appsecinc.com/update/docs/DbProtect_Analytics_Users_Guide.pdf (access data 15.04.2022)

[12] База даних. Поняття системи баз даних. Схема бази даних. Дані. Апаратне та програмне забезпечення. Користувачі баз даних https://www.bestprog.net/uk/2019/01/16/the-concept-of-a-database-system-database-schema-data-hardware-and-software-database-users-ua/#q01 (дата звернення 15.04.2022)

[13] База даних. http://infohmc10.blogspot.com/p/blog-page_11.html (дата звернення 15.04.2022)

[14] Микитюк І. С., Баришев Ю. В. Підхід до захисту баз даних: тези на наукову конференцію. Матеріали XLVII Науково-технічної конференції факультету інформаційних технологій та комп'ютерної інженерії. Вінниця. 2017. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/index/pages/view/ (дата звернення 15.04.2022)

Хращевський Р. В., Нестеренко К. С., Козловський В. В., Ткаля О. І.

ЗАХИСТ БАЗ ДАНИХ ЗА ДОПОМОГОЮ ПРОГРАМНОГО КОМПЛЕКСУ DBPROTECT

Інформація — це один з найважливіших ресурсів у сучасному світі. Оскільки інформаційні технології розвиваються збільшується і кількість загроз, тому очевидним є питання з удосконалення її захисту, щоб запобігти збитку інтересів власника інформації.

Так, як зараз у інформаційному просторі циркулює неймовірно велика кількість інформації для зручності її використання організації впроваджують бази даних. База даних — це найкращий метод для роботи з великим обсягом інформації, що являти собою систематизовану сукупність матеріалів різного типу для обробки за допомогою комп'ютера.

Розвивається злочинна сфера про що говорить і статистики відповідно до якої за останні роки кількість зломів та витоку інформації дуже зросла. Хоч кількість зафіксованих та підтверджених випадків зломів неймовірна велика, багато випадків замовчуються для збереження репутації. Тому конфіденційна інформація потребує захисту та контролю для забезпечення безпеки.

Одним з варіантів захисту своїх даних для компаній та організацій є використання різних платформ створених спеціально для виявлення вразливостей баз даних та запобігання несанкціонованих втручань. Програмний комплекс DbProtect чудово підходить, як для невеликих компаній так і для організацій середнього та великого розміру. DbProtect служить для того, щоб вирішувати питання безпеки баз даних та для того щоб всі вимоги були виконані згідно з нормативними актами. Дана платформа створена для того, щоб можна було виконувати всі потреби різних систем баз даних.

Ключові слова: бази даних, інформаційна безпека, програмний комплекс захисту, система управління базою даних

Khryshchevsky R., Nesterenko K., Kozlovsky V., Tkalya O.

DATABASE PROTECTION USING DBPROTECT SOFTWARE

Information is one of the most important resources in the modern world. Since information technologies are developing and the number of threats is increasing, therefore, the question of improving its protection is obvious in order to prevent damage to the interests of the information owner.

Statistics show that in recent years, the number of hacks and information leaks has greatly increased. which leads to large financial losses or to the disclosure of passport data and other personal documents. In the scientific and commercial spheres, leaks of information through unauthorized access lead to the appropriation of other people's works and the disclosure of commercial secrets, which causes great losses. Therefore, confidential information needs protection and control.

Since an incredibly large amount of information is now circulating in the information space for ease of use, organizations are implementing databases. A database is the best method for working with a large amount of information, which is a systematized collection of materials of various types for processing using a computer.

The criminal sphere is developing as evidenced by the statistics, according to which in the last years the number of hacks and information leaks has increased greatly. Although the number of recorded and confirmed cases of hacking is incredibly high, many cases are hushed up to preserve reputation. Therefore, sensitive information requires protection and control to ensure security.

One of the options for companies and organizations to protect their data is to use various platforms created specifically to identify database vulnerabilities and prevent unauthorized interventions. The DbProtect software package is perfect for both small companies and medium and large organizations. DbProtect serves to resolve database security issues and ensure that all requirements are met in accordance with regulations. This platform is designed to be able to fulfil all the needs of various database systems.

Keywords: databases, information security, software protection, database management system.

Стаття надійшла до редакції 17.04.2022 р.
Прийнято до друку 15.06.2022 р.