УДК 004.056
DOI: 10.31673/2412-9070.2022.010310

Г. І. ГАЙДУР, доктор техн. наук, професор;
С. О. ГАХОВ, канд. військ. наук, доцент;
В. Є. ДМІТРІЄВ, ст. викладач;
М. І. ГАНЧЕНКО, здобувач,
Державний університет телекомунікацій, Київ

АКТУАЛЬНІСТЬ ТА ПЕРСПЕКТИВА РОЗВИТКУ PRIVILEGED ACCESS MANAGEMENT РІШЕНЬ

Досліджено інциденти кібербезпеки, пов'язані з порушенням прав привілейованих користувачів, та розвиток ринку PAM-рішень за останні п'ять років — 2017-2022. Також розглянуто процес безпечного та впевненого надання дозволів на доступ до інформаційних систем організації із забезпеченням і відстеженням безпечної діяльності користувачів у бізнес-мережі та хмарному середовищі компанії. Визначено актуальність та потребу в керуванні та контролі доступу адміністраторів, а також вивчено тенденції зростання ринку послуг PAM. Сформульовано перспективи розвитку стратегії впровадження PAM-рішень для або у хмарні середовища. Було застосовано методи прогнозування на основі аналізу ринку та висновків із поданих звітів міжнародних компаній щодо розвитку рішень PAM та підвищення попиту на такі системи в майбутньому, а також спостереження тенденцій переходу діяльності огранізацій у хмарне середовище із розвитком хмарних послуг: IaaS, PaaS, SaaS. Розглянуто звіти CIS Controls, OWASP, Balabit, Gartner, Allied Marked Research та дослідження світових вендорів: Heimdal security, Microsoft, IBM, що дало змогу дійти необхідних висновків та довести доцільність застосування і підвищення попиту на PAM-системи в найближчі десять років та обґрунтувати перспективність і потребу в упровадженні нової стратегії розвитку PAM у хмарі через інтеграцію та розмиття кордонів з IAM. Наукова новизна здобутих результатів дослідження ринку свідчить про те, що зацікавленість PAM-рішеннями з боку замовників, котрі усвідомлюватимуть потребу в засобах контролю доступу адміністраторів, визначає подальший розвиток та конкурентоспроможність таких систем. Збільшення площ атак, підвищені ризики безпеки, необхідність іти в ногу з сучасними робочими бізнес-процесами — усе це вимагає впровадження нових рішень PAM із підвищеним рівнем безпеки, автоматизацією, а також інтегрування для забезпечення комплексного захисту інформації, що стане невід'ємною частиною загальної стратегії інформаційної та кібернетичної безпеки як підприємств, так і державних установ.

Ключові слова: уразливість; інцидент; контроль доступу; PAM; привілейований доступ; привілейовані облікові записи; інформаційна безпека; хмарне середовище; хмарні послуги; IaaS; PaaS; SaaS; IAM.

ВСТУП

Системи моніторингу та керування привілейованим доступом останніми роками набирають дедалі більшої популярності, про що свідчить збільшення на світовому ринку таких рішень, як *Privileged Access Management* **(PAM)** та *Database Access Management* **(DAM)**, котрі призначені для контролю роботи адміністраторів та реалізації концепції Zero Trust. А визначення поняття привілейованого доступу від Heimdal security [3] подається з боку корпоративного контексту і відбиває втілення тих функцій або типів доступу, які перевищують стандартні доступи користувачів.

З огляду на подане визначення корпорація Microsoft надає рекомендації розроблень цілих стратегій привілейованого доступу задля зниження ризиків для організації, що можуть бути пов'язані з високим рівнем впливу і високою ймовірністю атак на привілейований доступ як такий [9]. І не дарма CIS Controls у своїй праці [2] одним із п'яти ключових критеріїв захисту виокремлюють «контрольоване використання адміністративних привілеїв», яке впливає з найбільшим ефектом на інформаційну безпеку (ІБ). Такий контроль гарантує, що співробітники мають лише системні привілеї, права та дозволи, потрібні їм для виконання лише саме своєї роботи.

Окрім того у 2021 році проєкт із безпеки вебзастосунків OWASP здійснив оновлення «Top 10 Web Application Security Risks» [1] уразливостей, і вразливість «Broken Access Control» було піднято з п'ятої позиції на першу (рис. 1) та зазначено, що 94% застосунків було перевірено на певну форму, включно з можливістю підвищення рівня привілеїв і діяльністю від імені адміністратора, зламаного контролю доступу.

Відтак варто зазначити, що збої в контролях доступу призводять до неавторизованого розкриття інформації, модифікації, знищення чи використання бізнес-функцій за межами обмежень користувача [1]. З чого випливає доцільність і потреба в запровадженні систем моніторингу та контролю всіх наявних прав і доступів, включно з правами адміністраторів та інших привілейованих користувачів. Отже, саме ці питання і розглядатимуться далі через дослідження тенденцій зростання ринку PAM-послуг, а також кількості інцидентів кібербезпеки, пов'язаних із порушенням прав привілейованих користувачів за останні п'ять років (2017–2022 рр.).

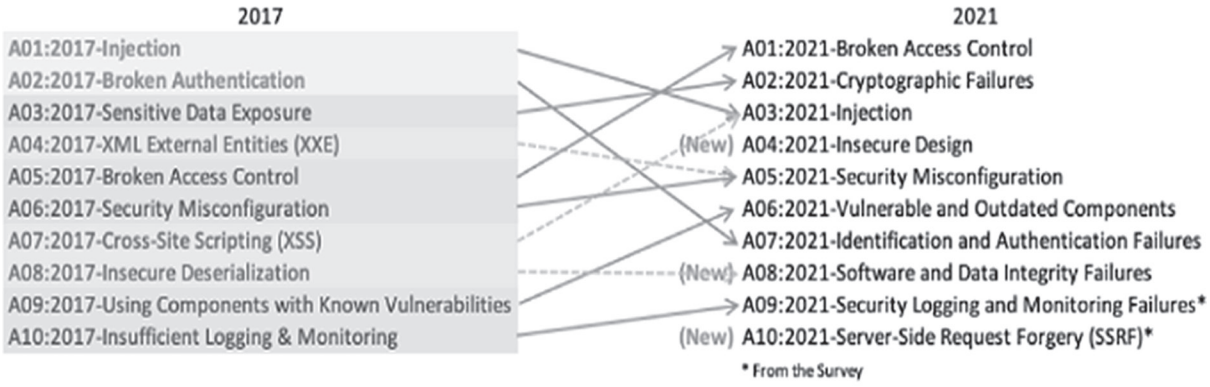

Рис. 1. Десять кращих вебзастосунків із ризиків безпеки

ОСНОВНА ЧАСТИНА

З появою хмарних обчислень потреби цифрового бізнесу у сфері безпеки значно зросли. Складність і висока вартість застарілих локальних систем потребують переходу до сучасної хмарної архітектури [19]. А багатохмарні цифрові середовища вимагають багатохмарної безпеки та керування, і цифрова трансформація сприяє зростанню робочого навантаження та створенню дедалі більшої кількості потрібних дозволів. Тож зусилля, які докладають вендори хмарних послуг для захисту даних і керування доступом, прогресують у формуванні нових відповідних вирішень. Такі вирішення являють собою централізоване керування користувачами та контроль доступу, забезпечуючи основні вимоги бізнесу — гнучкість та інновації [17], оскільки сьогодні підприємства потребують доступів для всіх типів користувачів до систем не лише локальних, а і хмарних.

Організаціям важливо безпечно та впевнено надавати дозволи на доступ, забезпечуючи і відстежуючи діяльність користувачів у бізнес-мережі [18]. Відтак керування доступом є основним компонентом сучасних стандартів кібербезпеки, зокрема GDPR, HIPPA, PCI-DSS [19]. А оскільки віддалена робота та хмарні послуги дедалі стають все буденнішими, керування доступом стає не розкішшю, а потребою.

Privileged Access Management (PAM) — це найкраще вирішення для зменшення ризиків, пов'язаних із використанням привілейованих облікових записів, оскільки останні є найбільшими вразливостями в організації за оцінкою Forrester і становлять 80% порушень безпеки [20]. Саме тому PAM-рішення корпоративного рівня призначені для захисту, моніторингу, визначення привілейованих облікових даних і реагування на загрози. Отже, відбувається максимальний захист складних розподілених середовищ [20]. А оскільки перехід на віддалену роботу додатково зменшує простір для контролю [21], PAM стає розв'язком для подібних проблем.

Привілейований доступ — найвищий пріоритет безпеки

Починаючи з 2019 року, під час сплеску захворюваності на коронавірус, відбувся масовий перехід на віддалену роботу, що, зі свого боку, лише збільшило тенденції росту світового ринку PAM-послуг, який спостерігається нині. І не мала зацікавленість до цих систем керування та моніторингу помітна з боку державних установ. Такий попит не є винятком і для України, особливо зважаючи на нинішній воєнний стан та постійні кібератаки з метою отримання доступу до державних реєстрів та інформаційної інфраструктури країни [13], для дестабілізації ситуації.

Отже, лише за перші місяці війни Україна зазнала 362 кібератаки, і більшу частину яких (рис. 2) у розмірі 85% було здійснено на урядові та місцеві органи влади, 49% — сектор безпеки, 26% — комерційні організації [13].

Рис. 2. Кібератаки на українську критичну інформаційну інфраструктуру протягом перших 1,5 місяці війни

За даними Balabit, ще у 2017 році 44% витоку даних у світі відбувались із використанням привілейованих облікових даних [15]. І лише в Україні на кінець 2021 року системою виявлення вразливостей і реагування на кіберінциденти на об'єктах моніторингу зафіксовано підозрілі події, де перші місця посідають інциденти з порушення прав адміністраторів — 22% від загальної кількості [13], а отже, спроб отримання привілейованого доступу.

Тож захист від несанкціонованого доступу (НСД) є найактуальнішим питанням у кіберзахисті, оскільки хакери постійно намагаються отримати доступ до облікових записів, аби використати їх для наступних атак [12]. А отже, безпека привілейованого доступу є вкрай важливою, оскіль-

ки вона є базою для всіх інших гарантій безпеки, маючи [9]:

• великий вплив на бізнес, а відповідно втрати репутації, даних;

• високу ймовірність ураження через виникнення, поширення нових методів та вразливостей.

Gartner визначає впровадження PAM пріоритетом номер один у проєктах безпеки на найближчі роки [15]. Адже своєчасне впровадження PAM-системи дає змогу вберегтись від можливих інсайдерських атак з боку адміністраторів і вищого керівництва компаній, а також контролювати діяльність аутсорсингових компаній і забезпечувати відповідність вимогам законів і стандартів у сфері ІБ.

Привілейовані облікові записи мають найвищий рівень захисту, оскільки в разі зламу здійснюють потенційний вплив на операції організації, тож беруть активну участь в інцидентах безпеки [8]. Як повідомляється в щорічному звіті IBM Security X-Force Insider Threat Report [4] за 2021 рік (рис. 3): 40% інцидентів стосується співробітників із привілейованими правами доступу до активів компанії (рис. 4), і у 100% інцидентів із поданих 40%, коли інсайдер був підтверджений або ж мав адміністративний доступ, де останній і зіграв свою роль у цьому інциденті (рис. 5).

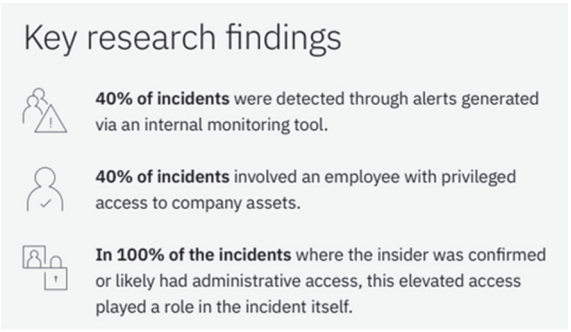

Рис. 3. Ключові результати дослідження, подані в IBM Security X-Force In-sider Threat Report

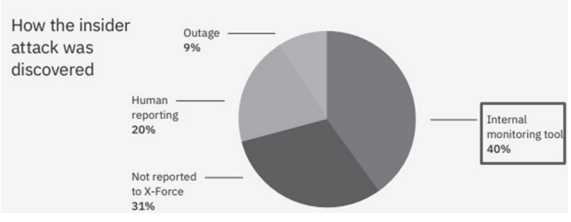

Рис. 4. Відсоток виявлення інсайдерських атак

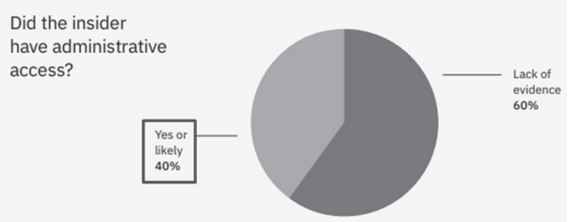

Рис. 5. Відсоток інсайдерських атак із привілейованим доступом

Тенденції росту ринку PAM послуг

У 2020 році в The Cost of Insider Threats: Global Report [5] зазначається, що лише 39% організацій прийняли ту чи іншу форму PAM (рис. 6).

Рис. 6. Звіт The Cost of Insider Threats: Global Report

А станом на лютий 2022 року лише 27% компаній країн СНД використовують PAM-системи (рис. 7) [14].

Рис. 7. Знайомство з PAM-системами

Такі цифри свідчать про те, що рівень ознайомленості та знань загальних принципів PAM перевищує реальний досвід експлуатації даних рішень. Така відсоткова різниця між частиною країн Америки і Європи та часткою країн СНД у застосуванні PAM-систем залежить саме від географічної сфери діяльності організації, бо так чи інакше останні підлягають під відповідність стандартам NIST SP 800-53, GDPR або ISO 27001, що охоплюють обов'язкові засоби контролю для безпечного керування привілейованими користувачами [7]. Отже, недостатньо розвинена практика поширення PAM призводить до того, що власники бізнесу не мають уявлення, що і для чого роблять привілейовані користувачі [15] у корпоративному середовищі компанії.

Відтак зростаюча потреба в захисті привілейованого доступу зумовлює стрімкий розвиток ринку рішень PAM. Згідно з даними Allied Marked Research [6] у 2020 році ринок оцінювався у 2,47 млрд дол., а до 2030 року очікується його зростання до 13,37 млрд дол. (рис. 8).

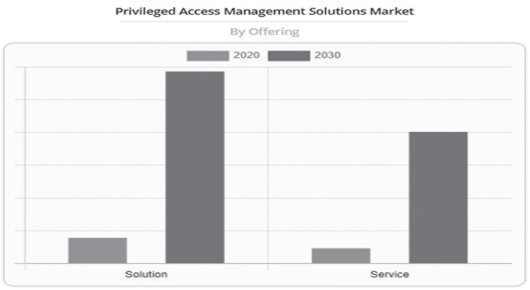

Рис. 8. Ринок рішень PAM

Окрім того ринкова частка державного та приватного секторів на відміну від IT, телекомунікацій, секторів охорони здоров'я, виробництва та енергетики тощо була найвищою у 2020 році і надалі зростатиме до 2030 року.

PAM у хмарі та PAM для хмари

Безліч факторів, серед яких економія коштів, зручність, відсутність довіри, віддалений доступ і віддалена робота, змусили більшість компаній повністю перейти у хмари. Організації використовують комбінації моделей SaaS, IaaS чи PaaS і розміщують свої програми у загальнодоступних чи приватних хмарах [24]. Та на жаль, локальна безпека компаній часто не переноситься до хмарного середовища, або захист для одного не завжди підходить чи сумісний з іншими хмарними середовищами.

Існує чотири основні проблеми в сучасній хмарі та хмарних середовищах для належного здійснення контролю доступу [24]:

- збільшення потужності привілейованих облікових записів;
- розширення поверхні атак зі створенням облікових записів хмарних платформ;
- невідставання від швидких і автоматизованих робочих процесів, що провокує призначення довгострокових дозволів;
- гібридні середовища потребують великої кількості різнорідних PAM для кожного, що не призначені для одного коректного функціонування.

Отже, зростає розуміння, що середовища постачальників хмарних технологій вимагають унікальних підходів до керування привілейованими доступами.

PAM у хмарі. PAM як послуга, або ж SaaS — це про керування привілейованим доступом у хмарі. Замість самостійного керування PAM локально, всі роботи щодо встановлення, обслуговування і оновлення покладаються на постачальника, який гарантує безпеку, доступність і своєчасність оновлень [22], гнучкість та масштабованість. І вже сьогодні сучасні хмарні розгортання PAM містять усі ті самі функції, що і локальні, а також керування політиками привілеїв.

За даними Gartner до 2021 року понад 70% організацій використовують безпеку як послугу [22]. А опитування, проведене Delinea, показало, що 21% компаній уже запровадили керування привілейованим доступом саме у хмарі або ж планують зробити це найближчим часом. Ще 26% планують перейти з локального PAM на хмарне рішення [22]. І компанії, які швидко переходять на PAM у хмарі, розуміють такі його переваги:

- *нижча вартість*. Фонд Енні Е. Кейсі виявив, що з переходом у хмару було скорочено кількість серверів на 85% [22];
- *мінімізація порушень*. Університет Сан Дієго і його студенти очікують 100% безвідмовної роботи, що вважають синонімом до слова хмара [22];
- *швидкий перехід*. Університет Лойоли налаштовував хмарне середовище приблизно за тиждень і здійснив міграцію лише за день [22];
- *висока доступність і географічне резервування*. Впевненість у тому, що привілейований доступ буде завжди доступним [25].

PAM для хмари. Керування та захист доступу до систем і служб у хмарі не можливий без відповідних інструментів, оскільки наслідки використання некерованих привілейованих облікових записів, прив'язаних до хмарних ресурсів, доволі помітні. Відповідно до звітів McAfee [22]:

- 27% організацій, які використовують платформу як послугу — PaaS, стикаються з крадіжкою даних зі своєї хмарної інфраструктури;
- 92% компаній продають хмарні облікові дані в DsrkWeb;
- компанії, які використовують AWS і/або Azure, мають 14 неправильних конфігурацій інфраструктури як послуги — IaaS, що мають погане керування привілеями.

За даними IDG 2020 року 90% компаній мали певну частину своєї інфраструктури у хмарі. Такий вибух хмарних сервісів призвів до поширення привілейованих облікових записів, що зумовило потребу в переході до хмари і PAM, оскільки рішення для контролю доступу вже сприймаються як необхідне та належне [24].

PAM для хмари дає змогу контролювати те, що користувачі можуть бачити і робити на хмарних платформах — 52% організацій, службах — 65% організацій та в програмах — 70% бізнес-застосунків хмарні, щоб посилити поверхню для атак і розв'язати проблеми безпеки хмар [25]. PAM для IaaS і PaaS захищає облікові дані і записи, пов'язані з платформами AWS, Azure та Google Cloud [25]. PAM для SaaS і вебзастосунків усуває людський фактор, оскільки замість ненадійних паролів інструмент здатен контролювати один секрет у безпечному сховищі [25].

Саме тому хмарне рішення PAM є найкращим способом для керування і захисту привілейованих облікових даних, оскільки більшість помилок спричинено клієнтом, а не постачальниками хмарних послуг. Про що свідчить звіт IDC за 2021 рік [23], де 88% компаній зазнали принаймні одного зламу за півтора роки порівняно з 79% у попередній період. І як попереджає Gartner [25]: проблема полягає не в безпеці самої хмари, а в політиках і технологіях безпеки та контролю над ними.

Отже, хмара — це подальша перспективна стратегія розвитку для PAM.

Інтеграція PAM/IAM

Ручні процеси керування привілейованим доступом стають складними, особливо в разі використання гібридних хмар та виявлення певних типів атак у розосередженій мережі з одним набором привілеїв до різних бізнес-активів [28]. Тож динамічний характер хмар вимагає розуміння працівниками наданих їм ролей та мінімально необхідних для виконання службових завдань доступів, і видалення останніх, коли вони стають непотрібними.

Саме так ключовим компонентом для хмарних PAM-рішень є аналітика ідентифікації, що дає змогу виявляти та повідомляти про порушення і реагувати на потенційні проблеми [28] у керуванні привілейованим доступом. Адже розширені привілеї — це зростаюча відповідальність, а отже, і підвищені доступи, а також фінансові і репутаційні втрати компанії в разі злому. Оскільки привілейовані облікові записи виходять за межі локальної чи хмарної корпоративної інфраструктури і містять облікові записи різних відділів і їх працівників [29], тож процес керування обліковими привілейованими записами має бути ефективним.

Модель віддалених і гібридних робочих місць потребують об'єднання рішень PAM та IAM — розмиття меж, оскільки вони значно спрощують керування доступом [26]. На ринку рішень керування привілейованим доступом зазначена технологія презентується як платформа ідентифікації та керування доступом [27], що дає можливість IT-організаціям здійснювати перехід до хмарних ресурсів і постає новим стандартом у сфері телекомунікацій.

Ідентичність стосується людей, тому IAM мають одну єдину цифрову ідентичність для кожної особи, після чого потрібні підтримання, зміна та контроль цієї ідентичності [29]. Тож IAM допомагають керувати як окремими користувачами, так і спільними обліковими записами — групами користувачів з однаковими правами та дозволами. Інструменти ж PAM здійснюють захист та керування всіма типами привілейованих облікових записів, що робить таке рішення більш специфічним, цілеспрямованим та добре інтегрованим у загальну стратегію керування ідентифікацією та доступом [29].

У хмарних моделях керування привілейованим доступом та в дотриманні правил контролю цього доступу відповідальність покладається саме на замовника та користувача послуги. За даними Gartner до 2023 року 99% збоїв у хмарній безпеці відбуватимуться з вини клієнта, де 50% проблем пов'язуватимуть саме з неправильною конфігурацією привілейованих облікових записів та наданими їм доступами. Отже, стратегія керування привілейованим доступом уже зараз вимагає захисту привілейованих облікових даних, які використовуватимуться для доступу та керування хмарними ресурсами [29].

І найкращим розвитком стратегії є рішення, що надаватиме доступ усім користувачам через єдину консоль керування — рішення SaaS, яке централізуватиме надання доступу, здійснюватиме аудит та змінюватиме тимчасово потрібний привілейований доступ на доступ для всіх [30]. Цінність такої консолі вагома для 58% компаній, що мають гібридну модель хмари [30], і необхідність у керуванні привілейованим доступом для всієї інфраструктури без потреби у використанні різнорідних PAM.

Тож адаптація до сучасного робочого процесу та мінімізація впливу на безпеку під час компрометації привілейованих облікових записів є новим та необхідним напрямком розвитку в керуванні привілейованим доступом [31].

ВИСНОВКИ

Наукова новизна здобутих результатів дослідження ринку свідчить про те, що зацікавленість PAM-рішеннями з боку замовників, котрі усвідомлюватимуть потребу у засобах керування паролями і контролю доступу адміністраторів, визначає подальший розвиток та конкурентоспроможність даних систем, а сучасні хмарні середовища вимагають нових підходів до керування привілейованим доступом.

Збільшення площ атак, підвищені ризики безпеки, необхідність відповідати сучасним робочим бізнес-процесам — усе це вимагає впровадження нових рішень PAM із підвищеним рівнем безпеки, автоматизацією, а також інтеграцією у хмарне середовище.

Отже, рух у бік конвергенції PAM/IAM дасть можливість подолати традиційні бар'єри, що з'являються у процесі впровадження традиційних PAM у хмару, і стати динамічними вирішеннями безпеки, що зможуть налаштовуватись на основі передбачуваних загроз та здійснювати інтелектуальну автентифікацію [33]. А також автоматизувати керування привілеями, регулярно змінюючи паролі та встановлюючи безпечні рівні доступу [33].

Список використаної літератури

*1. **OWASP** Top Ten [Електронний ресурс]. URL: https://owasp.org/www-project-top-ten/*

*2. **Sager T.** CIS Controls. Auditing, Assessing, Analyzing: A Prioritized Approach using the Pareto Principle [Електронний ресурс]. URL: https://www.cisecurity.org/wp-content/uploads/2018/01/Pareto-Principle.pdf*

*3. **What** Is Privileged Access Management (PAM)? [Електронний ресурс]. URL:*

https://heimdalsecurity.com/blog/privileged-access-management-pam/

4. **2021** IBM Security X-Force Insider Threat Report [Електронний ресурс]. URL:
https://www.ibm.com/downloads/cas/YNAPDA6B.

5. **The Cost** of Insider Threats 2020 [Електронний ресурс]. URL:
https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#/

6. **Privileged** Access Management Solutions Market [Електронний ресурс]. URL:
https://www.alliedmarketresearch.com/privileged-access-management-solutions-market-A12403.

7. **Privileged** Access Management: Essential and Advanced Practices [Електронний ресурс]. URL:
https://www.ekransystem.com/en/blog/pam_best_practices.

8. **Привілейований** доступ. Облікові записи [Електронний ресурс]. URL:
https://docs.microsoft.com/ru-ru/security/compass/privileged-access-accounts.

9. **Привілейований** доступ: стратегія [Електронний ресурс]. URL:
https://docs.microsoft.com/ru-ru/security/compass/privileged-access-strategy.

10. **Why** and How to Prioritize Privileged Access Management [Електронний ресурс]. URL:
https://www.gartner.com/en/articles/why-and-how-to-prioritize-privileged-access-management.

11. **Телеграм-канал** Державної служби спеціального зв'язку та захисту інформації України [Електронний ресурс]. URL:
https://t.me/dsszzi_official.

12. **Державна** служба спеціального зв'язку та захисту інформації України [Електронний ресурс]. URL:
https://cip.gov.ua/ua.

13. **Державна** служба спеціального зв'язку та захисту інформації України [Електронний ресурс]. URL:
https://instagram.com/dsszzi?utm_medium=copy_link.

14. **Практика** використання, нові функції і сценарії роботи PAM [Електронний ресурс]. URL:
https://www.anti-malware.ru/analytics/Technology_Analysis/PAM-using-new-Features-and-Scenarios#part3.

15. **Контроль** привілейованих користувачів. Що таке PAM-система? [Електронний ресурс]. URL:
https://www.it-world.ru/cionews/security/147451.html

16. **Microsoft** is a 5-time Leader in the Gartner Magic Quadrant for Access Management. [Електронний ресурс]. URL:
https://www.microsoft.com/security/blog/2021/11/09/microsoft-is-a-5-time-leader-in-the-gartner-magic-quadrant-for-access-management/?culture=uk-ua&country=UA.

17. **Access** Management 2022 [Електронний ресурс]. URL:
https://www.kuppingercole.com/reprints/62c08b4d46f70b1c19245b8f09011f5e?culture=uk-ua&country=UA.

18. **Identity** and Access Management solutions (PAM)? [Електронний ресурс]. URL:
https://nordlayer.com/identity-access-management/?gclid=Cj0KCQjwvZCZBhCiARIsAPXbajs0eT4TOD5IHthwSDwFj-Yn6wQ0Oj3DHV6-2qlvt-NUQXiXi8K2aZ7YaAnhiEALw_wcB

19. **9 Identity** and Access Management best practices [Електронний ресурс]. URL:
https://nordlayer.com/blog/iam-best-practices/

20. **Privileged** Access Manager (PAM) [Електронний ресурс]. URL:
https://softprom.com/ru/vendor/cyberark/product/pam.

21. **Privileged** Access Management [Електронний ресурс]. URL:
https://oneidentity.bakotech.com/privileged-access-management.

22. **PAM** in the cloud vs. PAM for the cloud. What's the difference? [Електронний ресурс]. URL:
https://delinea.com/blog/pam-privileged-access-management-in-vs-for-the-cloud.

23. **PAM** for the Cloud [Електронний ресурс]. URL:
https://delinea.com/resources/pam-for-cloud-security-whitepaper.

24. **Privileged** Access for Cloud-Native Workloads (Cloud PAM): Securing Identities in dynamic environments; on-premise, hybrid & public cloud [Електронний ресурс]. URL:
https://delinea.com/blog/cloud-pam-privileged-access-for-cloud-native-workloads.

25. **Privileged** Access Management for the Cloud [Електронний ресурс]. URL:
https://thycotic.com/solutions/privileged-access-management-for-the-cloud/

26. **Your** Guide to Privileged Access Management (PAM) [Електронний ресурс]. URL:
https://jumpcloud.com/blog/privileged-access-management.

27. **What** is a Cloud Directory? [Електронний ресурс]. URL:
https://jumpcloud.com/blog/what-cloud-directory.

28. **Why** Privileged Access Management Is So Hard in the Cloud [Електронний ресурс]. URL:
https://securityintelligence.com/articles/privileged-access-management-hard-cloud/

29. **Privileged** Access Management (PAM) What is Privileged Access Management? [Електронний ресурс]. URL:

https://delinea.com/what-is/privileged-access-management-pam.

30. ***Migrating*** *Your Privileged Access Management (PAM) to the Cloud [Електронний ресурс]. URL:*

https://www.strongdm.com/blog/privileged-access-management-pam-cloud-migration.

31. ***Rethinking*** *Privileged Access Management for Cloud and Cloud-Native Environments. [Електронний ресурс]. URL:*

https://goteleport.com/blog/rethink-modern-pam-for-cloud-environments/

32. ***Applying*** *Privileged Access Management to Cloud Environments [Електронний ресурс]. URL:*

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-1/applying-privileged-access-management-to-cloud-environments.

33. ***Privileged*** *Access Management (PAM) in the Cloud [Електронний ресурс]. URL:*

https://www.ssh.com/academy/iam/privileged-access-management-in-the-cloud.

H. I. Haidur, S. O. Gakhov, V. E. Dmitriiev, M. I. Hanchenko

RELEVANCE AND PROSPECTS OF THE DEVELOPMENT OF PRIVILEGED ACCESS MANAGEMENT SOLUTIONS

The subject matter of the article is cyber security incidents related to the violation of the rights of privileged users and the development of the market of PAM solutions over the past five years — 2017–2022. And there is also a process of safe and secure granting of access permissions to the organization's information systems with the provision and tracking of secure user activity in the company's business network and cloud environment. The goal and tasks are: determining the relevance and need for management and administrator access control tools, as well as studying the growth trends of the PAM service market. Determination of prospects for the development of a strategy for the implementation of PAM solutions for or in cloud environments. The methods used are: forecasting methods based on market analysis and conclusions from the presented reports of international companies regarding the development of PAM solutions and increasing demand for system data in the future, as well as observing trends in the transition of organizations' activities to the cloud environment with the development of cloud services: IaaS, PaaS, SaaS. The following results were obtained: the reports of CIS Controls, OWASP, Balabit, Gartner, Allied Marked Research and studies of global vendors: Heimdal security, Microsoft, IBM were considered, which made it possible to draw the necessary conclusions and prove the feasibility of using and increasing demand for PAM systems in the next ten years and prove the prospects and the need to implement a new PAM development strategy in the cloud through integration and blurring the boundaries with IAM. Conclusions. The scientific novelty of the obtained market research results indicates that the interest of PAM solutions on the part of customers, who will be aware of the need for access control tools for administrators, determines the further development and competitiveness of these systems. Increasing attack surfaces, increased security risks, the need to keep up with modern business processes — all this requires the implementation of new PAM solutions with an increased level of security, automation, as well as integration to ensure comprehensive information protection, which will become an integral part of the overall strategy information and cyber security of both enterprises and state institutions.

Keywords: vulnerability; incident; access control; PAM; privileged access; privileged accounts; information security; cloud environment; cloud services; IaaS; PaaS; SaaS; IAM.