УДК 004.8/681.5 DOI: https://doi.org/10.32515/2414-3820.2024.54.117-125

Р.М. Минайленко, доц., канд. техн. наук, **Л.І. Поліщук,** ст. викл.
Центральноукраїнський національний технічний університет, Кропивницький, Україна
e-mail: aron70@ukr.net

Особливості проектування архітектури довіри нульового рівня

В статті проведено аналіз особливостей архітектури довіри нульового рівня (АДНР), яка є відносно новою концепцією інформаційної безпеки, враховуючою віддалений формат доступу співробітників до інформації, яка є власністю підприємства, де вони працюють. Показано, що традиційні моделі забезпечення інформаційної безпеки, засновані на периметрі безпеки, не дозволяють забезпечити потрібний рівень захисту від можливих загроз.

АДНР є визначеним набором принципів керування для організації заходів, які доцільно використовувати з метою вдосконалення інформаційної безпеки підприємств і підвищення рівня їх захищеності. Основним завданням АДНР є зведення до мінімуму ризиків інформаційної безпеки від впливу зовнішніх вторгнень зловмисників на інформаційні активи підприємства і забезпечення його нормального функціонування.

архітектура, нульовий рівень довіри, безпека, комп'ютер

Постановка проблеми. З розвитком мережевих технологій і появою можливості віддаленої роботи виникла необхідність забезпечити безпечний доступ користувачів з власних домашніх комп'ютерів до інформаційних сервісів і корпоративних баз даних підприємств. В результаті виникають ускладнення в архітектурі інформаційних систем і систем безпеки підприємств [1–3].

Архітектура довіри нульового рівня (АДНР) є відносно новою концепцією в області інформаційної безпеки і стала відображенням напрямків розвитку архітектури систем інформаційної безпеки підприємств. Основною метою впровадження АДНР є зниження ризиків інформаційної безпеки на підприємстві від можливих наслідків зовнішніх вторгнень зловмисників та забезпечення нормальної роботи підприємства.

При використанні моделі АДНР передбачається, що зловмисник, який найчастіше знаходиться ззовні, також може перебувати всередині підприємства, і між ними немає різниці. Виходячи з цього, при використанні моделі АДНР компанія повинна відмовитися від беззаперечної довіри до власних співробітників і постійно контролювати свої активи. При цьому заходи безпеки інформації повинні проводитися постійно [4–6,7].

Аналіз останніх досліджень і публікацій. При використанні моделі АДНР під час доступу до активів або облікових записів користувачів необхідно постійно перевіряти їх місцезнаходження, ідентифікувати пристрої, тип операційної системи та специфіку інформації, що використовується. Тобто при доступі до даних, які належать певному підприємству, враховується велика кількість інформації про користувача. Крім того, кількість цієї інформації може змінюватися відповідно до алгоритму, заданого системою безпеки [7, 8].

На рисунку 1 представлена узагальнена архітектура системи захисту інформації з використанням АДНР:

Архітектура АДНР складається з двох основних рівнів:

1. Рівень доступу користувача.
2. Рівень підприємства з його інформаційними активами.

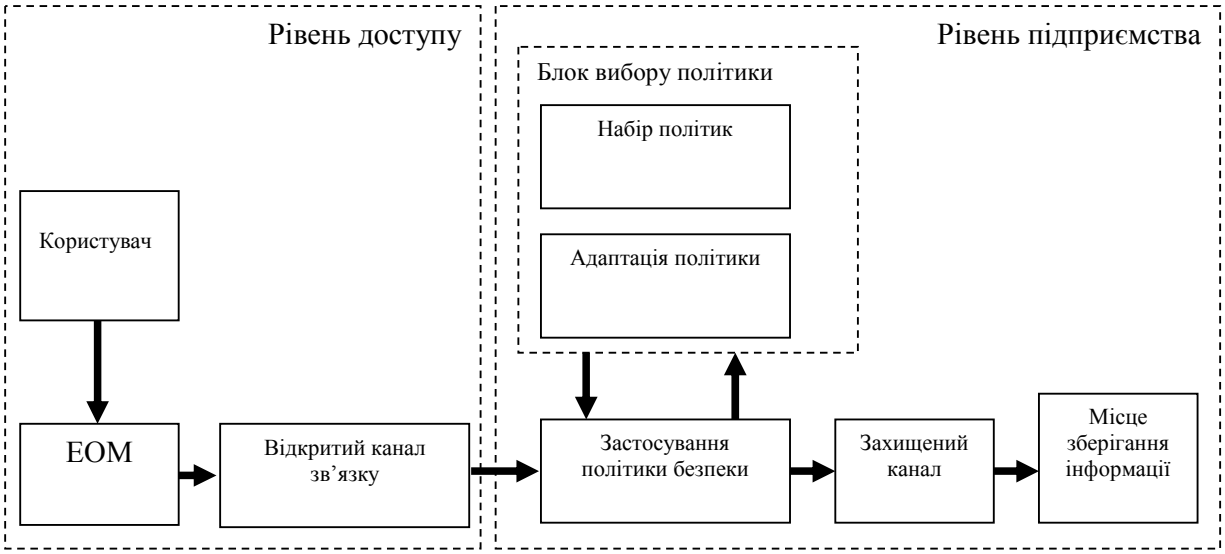

Рисунок 1 – Схема доступу до інформації підприємства з використанням АДНР
Джерело: розроблено авторами

Користувач може сформувати запит на дозвіл входу в інформаційну систему підприємства та надіслати його через відкритий інформаційний канал. Далі запит надходить до блоку застосування політики безпеки, де формується вибір політики безпеки. Вся інформація про активність користувачів аналізується блоком вибору політики безпеки, і, при необхідності, коригується блоком адаптації політики. Після отримання дозволу користувач отримує доступ до конфіденційної інформації підприємства через захищений канал [7,9–12].

АДНР – це модель безпеки та комплекс технологій, які використовують принцип нульового рівня довіри, тобто «нікому не довіряй, усіх перевіряй». А традиційні моделі безпеки припускають, що коли інформація вже потрапила в середину корпоративної мережі, вона безпечна. АДНР базується на принципі, що всі пристрої та користувачі є потенційною загрозою, незалежно від того, чи знаходяться вони всередині периметра мережі, чи працюють віддалено. Тому дозвіл на використання ресурсів компанії надається лише після перевірки та постійного моніторингу користувачів і стану безпеки пристроїв.

Метою впровадження АДНР є забезпечення безпечного віддаленого доступу до програм і даних, зниження ризику витоку даних та інших видів кіберзагроз, надання доступу до ресурсів мережі лише перевіреним і авторизованим користувачам і пристроям [7, 13].

Для успішного впровадження та отримання всіх переваг цього підходу, навіть за умови придбання спеціалізованих програмних продуктів, необхідно забезпечити певне навчання персоналу перед початком роботи та застосування передових політик безпеки та безпечного доступу.

Постановка завдання. Інформаційні системи вирішують важливе завдання забезпечення безпечного доступу до інформації підприємства та його віддалених філій. Від ефективності вирішення цієї проблеми залежить не тільки виконання

поточних завдань підприємства, а й, власне, існування самого підприємства в реаліях сьогодення [14, 15].

Концепція підтримки життєвого циклу складної виробничої системи та її системи безпеки багато в чому залежать від архітектури підприємства. Основні компоненти архітектури підприємства показані на рисунку 2:

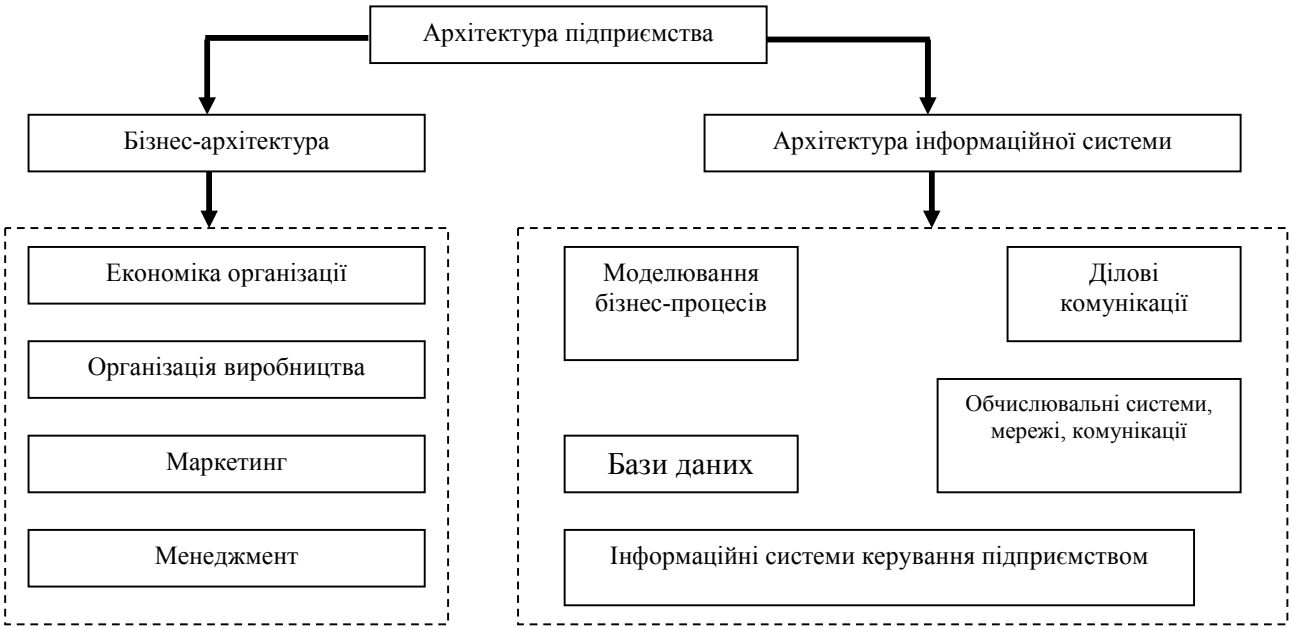

Рисунок 2 – Основні складові архітектури підприємства

Джерело: розроблено авторами

Складовими архітектури підприємства є бізнес-архітектура та архітектура інформаційної системи, які тісно пов'язані між собою. Слід зазначити, що розподілені інформаційні системи більш вразливі з точки зору забезпечення інформаційної безпеки.

Крім того, інтеграція офісної та віддаленої домашньої інформаційних систем значно ускладнює архітектуру системи захисту інформації.

Завдання проектування інформаційних систем і систем безпеки підприємства складні і залежать від специфіки того чи іншого підприємства.

В загальному випадку АДНР має базуватися на семи основних принципах:

1. Підприємству або організації слід захищати всі свої дані, послуги та пристрої. При умові, якщо користувачі мережі можуть отримувати доступ до ресурсів організації з власних пристроїв, то такі гаджети теж мають враховуватись при проектуванні системи захисту підприємства

2. Комунікації. Всі комунікації, як внутрішні, так і за межами мережі, мають однаково оброблятися та захищатися найбезпечнішим із наявних методів.

3. Посесійний доступ. Кожне звертання до критично важливого ресурсу організації повинно встановлюватись відокремлено для кожного сеансу.

4. Динамічні політики. Доступ до ресурсів організації повинен надаватися згідно зі встановленими правилами політики організації та керуватись принципом найменших привілеїв. Ця політика має визначати:

– ресурси організації;

– користувачів;

– права доступу для користувачів.

5. Моніторинг. Для забезпечення належного захисту даних та корпоративних ресурсів організації повинні моніторити ці ресурси і все, що з ними відбувається.

6. Перевірка. Перед тим, як надавати доступу до будь-якого корпоративного ресурсу організація має забезпечити динамічну перевірку користувачів.

7. Безперервне покращення системи безпеки. Організація має збирати інформацію про поточний стан мережних активів, інфраструктуру та з'єднання для поліпшення стану безпеки.

Ці принципи проектування архітектури нульової довіри можуть одночасно і не застосовуватись. Можете обмежитись реалізацією лише декількох із них, тих які найбільше відповідають конкретним потребам. Причому АДНР не потребує повної заміни існуючої мережевої архітектури на основі периметра, а пропонує розширення існуючої мережі завдяки додаванню сегментів мережі, захищених шлюзами, що значно покращить політику безпеки та правила доступу для користувачів.

Принципи проектування архітектури нульової довіри представлені на рисунку 3:

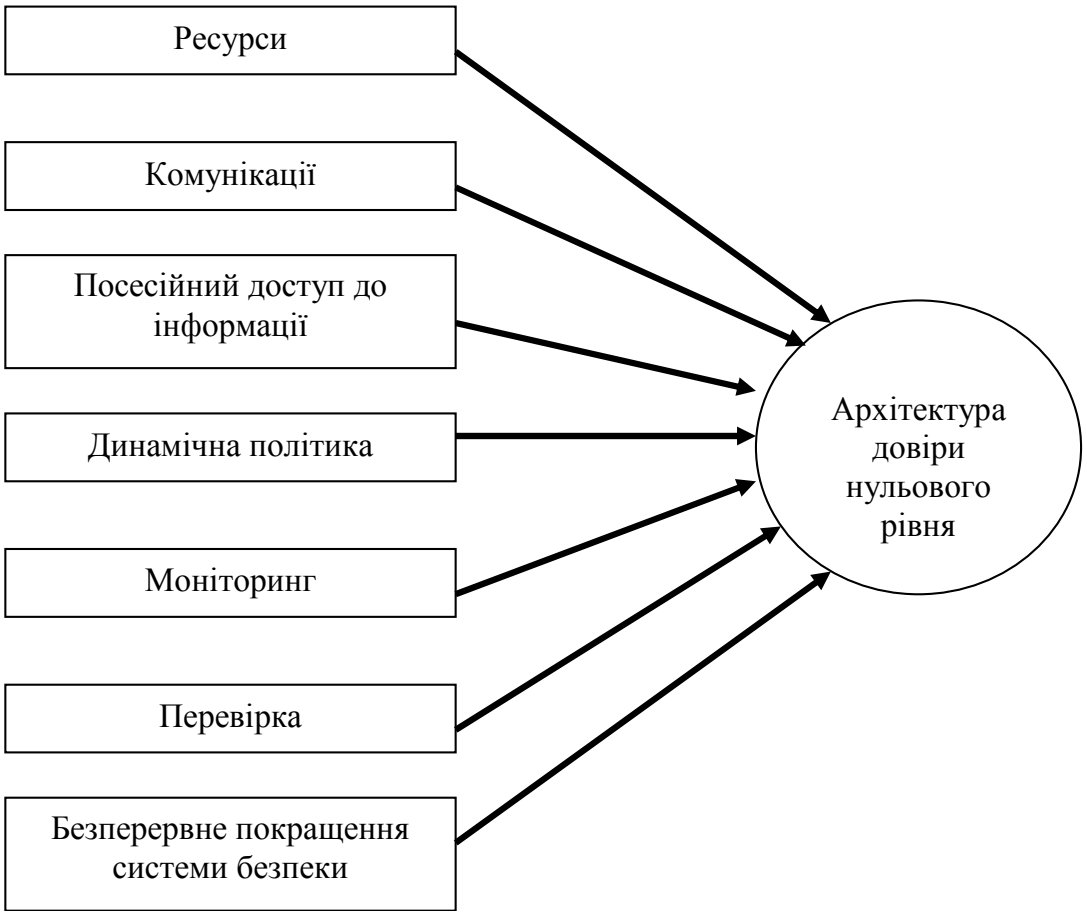

Рисунок 3 – Принципи проектування архітектури нульової довіри

Джерело: розроблено авторами

Виклад основного матеріалу. За результатами аналізу можна виділити наступні особливості проектування систем захисту інформації на базі АДНР:

1. Обсяг інформації, що обробляється в інформаційних системах, постійно зростає.

2. Використовуються різні внутрішні комп'ютерні мережі з власними інформаційними системами.

3. Методи забезпечення інформаційної безпеки мережі не забезпечують необхідного рівня інформаційної безпеки, оскільки немає чітко встановлених меж інформаційної безпеки для розподілених підприємств. Тобто, якщо зловмисник перетнув охоронний периметр, то подальший горизонтальний рух комп'ютерною мережею буде досить простим. У цьому випадку доцільно використовувати АДНР.

Архітектура нульового рівня довіри орієнтована, перш за все, на захист даних і послуг, але має можливість розширення на всі компоненти підприємства і кінцевих користувачів послуг. Але доступ буде дозволено лише тим користувачам, які визначені як такі, що потребують цього доступу, і при цьому забезпечується постійна перевірка та авторизація особи. Також виконується аналіз безпеки кожного звертання до системи.

При проектуванні систем безпеки підприємств на базі АДНР значну увагу слід приділяти політиці безпеки [7, 16, 17].

Формування політики безпеки для кожного конкретного об'єкта потребує обробки великих масивів даних, на основі яких за допомогою алгоритмів класифікації приймається те чи інше рішення щодо зміни алгоритмів безпеки та адаптації політик під конкретний об'єкт. Реалізація динамічного формування набору політик безпеки вимагає збору та аналізу даних, обробки інформації та адаптації політик безпеки доступу до інформації.

При проектуванні систем захисту програмного забезпечення використовуються різноманітні шаблони, які відображають досвід, накопичений розробниками інформаційних систем, що призводить до скорочення часу та ресурсів на їх створення та впровадження.

Але провадження АДНР має не тільки переваги, але і певні недоліки, що показано на рисунку 4.

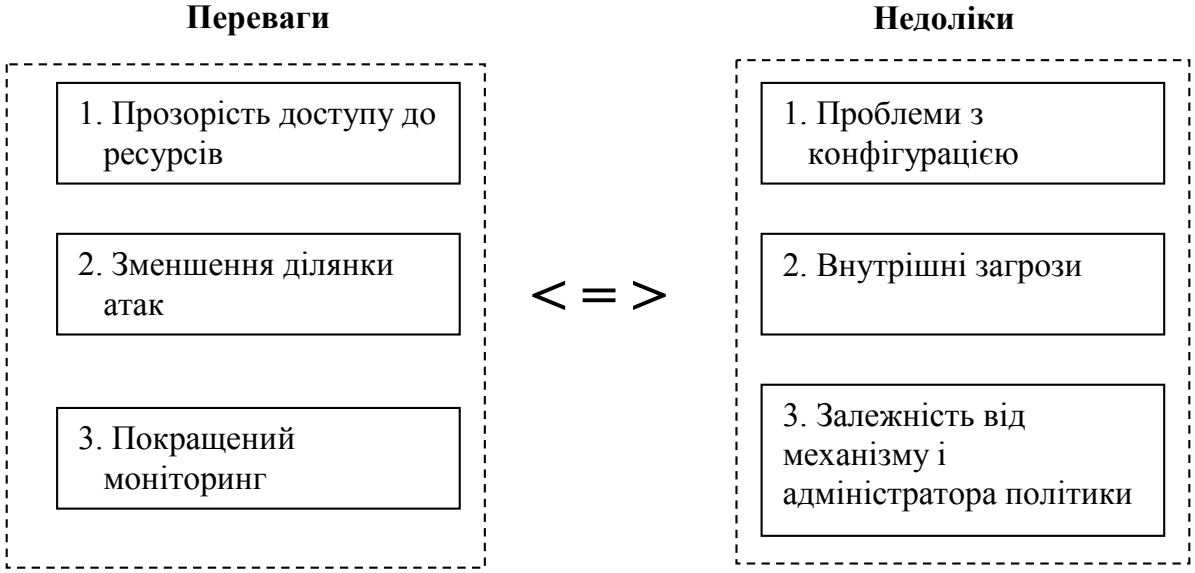

Рисунок 4 – Переваги та недоліки впровадження АДНР

Джерело: розроблено авторами

Охарактеризуємо спочатку переваги впровадження АДНР:

1. Застосування АДНР вимагатиме визначення і класифікації всіх ресурсів мережі, що дозволятиме бачити, хто із співробітників отримав доступ до ресурсів, і розуміти, які заходи потрібно застосувати для захисту ресурсів.

2. При збільшенні уваги на безпеку окремих визначених ресурсів організації, які реалізують принци нульової довіри, зменшуються ризики атак зловмисників, направлених на периметр мережі.

3. Концепція безпеки з нульовою довірою передбачає впровадження додаткових рішень, що дозволяє організаціям простіше виявляти потенційні загрози та своєчасно реагувати на них.

Недоліками від провадження АДНР є:

1. Виникнення проблем з конфігурацією. АДНР не створюється за допомогою єдиного рішення, тому виникатимуть труднощі з некоректним налаштуванням вже використовуваного обладнання.

2. Впровадження архітектури з нульовою довірою значно покращує захист від зовнішніх атак, але коли зловмисник знаходиться всередині периметра і використовує свій статус з корисливою метою, то виникає загроза витоку конфіденційної інформації. Цю проблему в певній мірі можна усунути шляхом використання розширених заходів: керування привілейованим доступом, багатофакторна перевірка та ручне підтвердження запитів на доступ.

3. Архітектура з нульовою довірою залежить від механізму та адміністратора політики і потребує їхнього дозволу на користування корпоративними ресурсами. Тому продуктивність мережі в цілому є залежною від правильної конфігурації та обслуговування.

Висновки. На теперішній час працівники підприємств можуть працювати віддалено та отримувати доступ до активів компанії. Традиційні моделі забезпечення інформаційної безпеки, які базуються на моделі зовнішнього периметра безпеки, не дозволяють забезпечити належний рівень захисту від можливих загроз.

Використання АДНР, основним елементом якого є динамічна зміна персоналізованої політики безпеки користувачів, дозволяє вирішити цю проблему та дозволяє забезпечити постійний контроль доступу до конфіденційної інформації компанії.

АДНР – це визначений набір принципів управління організацією діяльності, які повинні використовуватися з метою покращення інформаційної безпеки підприємств та підвищення рівня їх безпеки.

Основним завданням АДНР є мінімізація ризиків інформаційної безпеки від впливу зовнішніх вторгнень зловмисників на інформаційні активи компанії та забезпечення їх нормального функціонування.

Список літератури

1. Sosnin O. (2020). *Digitization as a new reality of Ukraine.* URL: https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny/ (Accessed: 15 March 2024).
2. Fleck A. (2024, February 22). Cybercrime Expected To Skyrocket in Coming Years. Retrieved from https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027 (Accessed: 26 February 2024).
3. Ashwini Kumari M. and Nandini Prasad K. S. A Behavioral Study of Advanced Security Attacks in Enterprise Networks, 2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bangalore, India, 2021, pp. 1–5. DOI: 10.1109/CSITSS54238.2021.9682903

4. Anjum I., Kostecki D., Leba E., Sokal J., Bharambe R., Enck W., Nita-Rotaru C., & Reaves B. (2022). Removing the Reliance on Perimeters for Security using Network Views. Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies. pp. 151–162, https://doi.org/10.1145/3532105.3535029
5. Sheikh N., Pawar M., & Lawrence V. (2021). Zero trust using Network Micro Segmentation. IEEE INFOCOM 2021 – IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 1–6. https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484645
6. Wu Y. G., Yan W. H. and Wang J. Z. Real identity based access control technology under zero trust architecture, 2021 International Conference on Wireless Communications and Smart Grid (ICWCSG), Hangzhou, China, 2021, pp. 18–22, doi: 10.1109/ICWCSG53609.2021.00011
7. Nair Anita (2021). The Why and How of adopting Zero Trust Model in Organizations. TechRxiv. Preprint. pp. 1–6, https://doi.org/10.36227/techrxiv.14184671.v1
8. Hines C. D. and Chowdhury M. M. Uncover Security Weakness Before the Attacker Through Penetration Testing, 2022 IEEE International Conference on Electro Information Technology (eIT), Mankato, MN, USA, 2022, pp. 492–497, doi: 10.1109/eIT53891.2022.9813950 164
9. Abhishek Arote, Umakant Mandawkar. Android Hacking in Kali Linux Using Metasploit Framework, International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7, Issue 3, pp. 497–504, May–June-2021. Available at doi: https://doi.org/10.32628/CSEIT2173111
10. What are the main challenges and benefits of implementing a zero trust network architecture? (2023, October 6). Retrieved from https://www.linkedin.com/advice/1/what-main-challenges-benefits-implementing-4e (Accessed: 26 February 2024).
11. Tyshyk I. (2023). Vybir tekhnolohii viddalenoho dostupu dlia efektyvnoi orhanizatsii zakhystu merezhevykh ziednan. Elektronne fakhove naukove vydannia “Kiberbezpeka: osvita, nauka, tekhnika”, 3(19), pp. 34–45. DOI: 10.28925/2663-4023.2023.19.3445
12. Yuanhang He, Daochao Huang, Lei Chen, Yi Ni, Xiangjie Ma. A Survey on Zero Trust Architecture: Challenges and Future Trends, Wireless Communications and Mobile Computing, vol. 2022, Article ID 6476274, 13 pages, 2022. https://doi.org/10.1155/2022/6476274
13. Rose S., Borchert O., Mitchell S., & Connelly S. (2020). Zero Trust Architecture. NIST Special Publication 800–207. *National Institute of Standards and Technology*. pp. 1–50, DOI: 10.6028/NIST.SP.800-207
14. Koeppen D., MacDonald N., Watts J. (2022, October 3). 7 Effective Steps for Implementing Zero Trust Network Access. URL: https://emt.gartnerweb.com/ngw/eventassets/ en/conferences/hub/identity-accessmanagement/documents/gartner-iam-implementing-zero-trust-network-access.pdf (Accessed: 26 February 2024).
15. Deloitte Cybersecurity Threat Trends Report 2023. (n.d.). URL: https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-threat-trends-report-2023.html (Accessed: 26 February 2024).
16. M-Trends 2023: Cybersecurity Insights From the Frontlines, Mandiant. Report. URL: https://www.mandiant.com/resources/blog/m-trends-2023 (Accessed: 26 February 2024).
17. The 2024 SonicWall Cyber Threat Report, SonicWall, 2024, URL: https://www.sonicwall.com/medialibrary/en/white-paper/2024-cyber-threat-report.pdf (Accessed: 26 February 2024).

References

1. Sosnin, O. (2020). *Digitization as a new reality of Ukraine* . https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny/ [In Ukrainian] (Accessed: 15 March 2024). [In Ukrainian]
2. Fleck, A. (2024, February 22). Cybercrime Expected To Skyrocket in Coming Years. https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027 [in English].
3. Ashwini Kumari, M. & Nandini Prasad, K. S. (2021). A Behavioral Study of Advanced Security Attacks in Enterprise Networks. *2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions* (CSITSS), Bangalore, India, pp. 1–5. [in English]. DOI: 10.1109/CSITSS54238.2021.9682903
4. Anjum, I., Kostecki, D., Leba, E., Sokal, J., Bharambe, R., Enck, W., Nita-Rotaru, C., & Reaves, B. (2022). Removing the Reliance on Perimeters for Security using Network Views. *Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies*. pp. 151–162, [in English]. https://doi.org/10.1145/3532105.3535029

5. Sheikh, N., Pawar, M., & Lawrence, V. (2021). Zero trust using Network Micro Segmentation. IEEE INFOCOM 2021 – IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 1–6. [in English]. https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484645
6. Wu, Y. G., Yan, W. H. & Wang, J. Z. (2021). Real identity based access control technology under zero trust architecture, 2021 International Conference on Wireless Communications and Smart Grid (ICWCSG), Hangzhou, China, 2021, pp. 18–22, [in English]. doi: 10.1109/ICWCSG53609.2021.00011
7. Nair Anita (2021). The Why and How of adopting Zero Trust Model in Organizations. TechRxiv. Preprint. pp. 1–6, https://doi.org/10.36227/techrxiv.14184671.v1
8. Hines, C. D. & Chowdhury, M. M. (2022). Uncover Security Weakness Before the Attacker Through Penetration Testing. *2022 IEEE International Conference on Electro Information Technology (eIT)*, Mankato, MN, USA, 2022, pp. 492–497 [in English]. doi: 10.1109/eIT53891.2022.9813950 164
9. Abhishek Arote, & Umakant Mandawkar. (2021). Android Hacking in Kali Linux Using Metasploit Framework, International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Vol.7, Issue 3, pp. 497–504, May–June-2021. [in English]. doi: https://doi.org/10.32628/CSEIT2173111
10. What are the main challenges and benefits of implementing a zero trust network architecture? (2023, October 6). https://www.linkedin.com/advice/1/what-main-challenges-benefits-implementing-4e [in English].
11. Tyshyk, I. (2023). Vybir tekhnolohii viddalenoho dostupu dlia efektyvnoi orhanizatsii zakhystu merezhevykh ziednan. Elektronne fakhove naukove vydannia "Kiberbezpeka: osvita, nauka, tekhnika", 3(19), pp. 34–45. [in English]. DOI: 10.28925/2663-4023.2023.19.3445
12. Yuanhang, He, Daochao, Huang, Le,i Chen, Yi, Ni, & Xiangjie, Ma. (2022). A Survey on Zero Trust Architecture: Challenges and Future Trends, Wireless Communications and Mobile Computing, vol. 2022, Article ID 6476274, 13 pages, [in English]. https://doi.org/10.1155/2022/6476274
13. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800–207. National Institute of Standards and Technology. pp. 1–50. [in English]. DOI: 10.6028/NIST.SP.800-207
14. Koeppen, D., MacDonald, N. & Watts, J. (2022, October 3). 7 Effective Steps for Implementing Zero Trust Network Access. https://emt.gartnerweb.com/ngw/eventassets/ en/conferences/hub/identity-accessmanagement/documents/gartner-iam-implementing-zero-trust-network-access.pdf [in English].
15. Deloitte Cybersecurity Threat Trends Report (2023). (n.d.). Retrieved from https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-threat-trends-report-2023.html [in English].
16. M-Trends (2023). Cybersecurity Insights From the Frontlines, Mandiant. Report. Retrieved from: https://www.mandiant.com/resources/blog/m-trends-2023 [in English].
17. The 2024 SonicWall Cyber Threat Report, SonicWall, (2024). https://www.sonicwall.com/medialibrary/en/white-paper/2024-cyber-threat-report.pdf [in English].

Roman Minailenko, Assoc. Prof., PhD tech. sci., **Liudmyla Polishchuk,** Senior Lecturer
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine

Analysis of Features of Zero-level Trust Architecture

The article provides an overview and analysis of modern BIOS interfaces. It is shown that due to the large The article analyzes the features of the zero-level trust architecture (ZTR), which exists. a relatively new concept of information security, taking into account the remote format of employee access to information that is the property of the enterprise where they work.

It is shown that traditional models of ensuring information security, based on the security perimeter, do not allow to provide the required level of protection against possible threats.

ADNR is a defined set of management principles for the organization of activities that should be used in order to improve the information security of enterprises and increase the level of their security.

The main task of ADNR is to minimize information security risks from the impact of external intrusions by intruders on the company's information assets and ensure its normal functioning.

With the development of network technologies and the emergence of the possibility of remote work, there was a need to provide employees with secure access from their home computers to information services and corporate databases of enterprises. As a result, the architecture of information systems and security systems became more complicated. With the development of network technologies and the emergence of the possibility of remote work, there was a need to provide employees with secure access from their home computers to information services and corporate databases of enterprises. The result was the complication of information systems and security systems of enterprises.

When using the ADNR model, it is assumed that the attacker, who is most often from the outside, can also be inside the enterprise, and there is no difference between them. Based on this, when using the ADNR model, the company must abandon unquestioning trust in its own employees and constantly monitor its assets. At the same time, information security measures must be carried out constantly.
architecture, zero trust, security, computer

Одержано (Received) 14.09.2024 *Прорецензовано (Reviewed) 25.11.2024*
Прийнято до друку (Approved) 02.12.2024