ISSN 1727-7337 (print)
ISSN 2663-2217 (online)

УДК 004.75:004.274

doi: 10.32620/aktt.2024.6.09

А. Г. ТЕЦЬКИЙ, А. Є. ПЕРЕПЕЛИЦИН

Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

МОЖЛИВОСТІ ВИКОРИСТАННЯ АПАРАТНИХ ПРИСКОРЮВАЧІВ У СИСТЕМАХ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕННЯМ

Предметом *вивчення в даній статті є можливості технології FPGA (Field Programmable Gate Array) для рішень безпеки із прискорювачами мережевих інтерфейсів SmartNIC (Smart Network Interface Card), а також технології для побудови, розгортання, підтримки і прискорення систем виявлення вторгнень IDS (Intrusion Detection System) та систем запобігання вторгненням IPS (Intrusion Prevention System).* ***Метою*** *роботи є підвищення продуктивності компонентів мережевого захисту сучасних датацентрів з використанням апаратних карт прискорювачів мережевих інтерфейсів на основі технології FPGA.* ***Завдання****: провести аналіз класифікації кіберзагроз, проаналізувати методи виявлення кіберзагроз, проаналізувати можливості сучасних карт прискорювачів FPGA для створення SmartNIC, запропонувати архітектуру апаратної реалізації системи запобігання вторгненням на базі карт прискорювачів FPGA, запропонувати послідовність кроків для створення апаратної реалізації системи запобігання вторгненням на основі FPGA прискорення. Відповідно до поставлених завдань, були отримані наступні* ***результати****. Виконано аналіз основних категорій поширених кіберзагроз, які мають бути взяті до уваги під час створення систем. Проаналізовано два основні принципи виявлення вторгнень, включаючи сигнатурний метод і метод виявлення аномалій. Проведено аналіз можливостей застосування карт прискорювачів FPGA для апаратного прискорення роботи мережевих інтерфейсів та створення SmartNIC. Запропоновано архітектуру апаратної реалізації компонентів мережевого інтерфейсу для системи запобігання вторгненням на основі карт прискорювачів FPGA у складі датацентрів. Запропоновано послідовність кроків для створення реалізації системи запобігання вторгненням на базі FPGA.* ***Висновки.*** *Наукова новизна отриманих результатів полягає в тому, що проведений аналіз специфіки кіберзагроз датацентрів та карт прискорювачів FPGA з підтримкою високошвидкісних мережевих інтерфейсів дозволив запропонувати набір рекомендацій щодо створення систем виявлення вторгнень та систем запобігання вторгненням із перенесенням роботи до апаратної реалізації, що дасть змогу розвантажити обчислювальні ресурси серверу та цим підвищити його продуктивність. Програмна частина рішення передбачає можливість розширення та безперервного оновлення профілю роботи апаратної складової такої системи виявлення та запобігання вторгненням безпосередньо у системі.*

Ключові слова: *система виявлення вторгнень; система запобігання вторгненням; IDS; IPS; SmartNIC; FPGA як сервіс; розвантаження ресурсів датацентрів.*

Вступ

Хмарні обчислення набули поширення для підтримки процесів розроблення складних систем, у тому числі в аерокосмічній галузі. Дедалі більше даних зберігається й обробляється на хмарних серверах. Зі зростанням кількості кібератак захист серверів став одним із найбільш пріоритетних завдань для організацій. Ключовими інструментами в цій галузі є системи виявлення вторгнень і системи запобігання вторгненням [1].

Як випливає з назв систем IDS та IPS, їхніми основними завданнями є оперативне оповіщення персоналу про кіберінцидент, що трапився, і недопущення шкідливих дій, виконання яких може призвести до кіберінциденту [2].

Основними функціями IDS і IPS є моніторинг мережевого трафіку або дій на сервері в реальному часі, аналіз трафіку і виконуваних дій, виконання останньої дії у вигляді сповіщення для адміністратора системи в разі IDS або блокування шкідливого трафіку чи запобігання виконанню підозрілих команд у разі IPS [3]. Системи виявлення та запобігання вторгненням [4] є частиною комплексної системи безпеки серверів [5], впровадження таких систем дає можливість підвищити рівень захищеності систем, що сприятливо позначається на рівні довіри клієнтів до таких серверів.

Для датацентрів реалізація завдань оброблення набору даних з мережевого обміну з використанням засобів CPU (Central Processor Unit) займає значну частину ресурсу його обчислень і забирає цей ресурс в основних споживачів, зокрема віртуальних машин [6].

Використання прискорення обчислень за допомогою FPGA [7] та сучасних плат прискорення з потужними мережевими можливостями та інтерфейсами дозволяє реалізувати SmartNIC [8].

Компанії AMD [9] та Intel [10] випускають FPGA з інтерфейсами PCIe та підтримують інших виробників при виробництві плат прискорення на їх основі.

SmartNIC можуть бути задіяні в процесі виявлення вторгнень [11, 12], але це вимагає значних обчислювальних ресурсів, які можна порівняти з потужністю встановлених у сервері процесорів [13].

Використання FPGA для прискорення виявлення вторгнень на базі SmartNIC дозволяє розвантажити основні ресурси сервера для задач його користувачів [14].

Для виконання не тільки виявлення вторгнень, але й запобігання вторгненням з використанням переваг апаратного прискорення сучасних плат FPGA-прискорювачів, необхідно дослідити таку можливість та запропонувати рішення для впровадження.

Метою даної роботи є підвищення продуктивності компонентів мережевого захисту сучасних датацентрів з використанням FPGA-прискорювачів.

Для досягнення поставленої мети необхідно виконати наступні **завдання**:

1) провести аналіз класифікації кіберзагроз;

2) проаналізувати методи виявлення кіберзагроз;

3) проаналізувати можливості сучасних карт прискорювачів FPGA для створення SmartNIC;

4) запропонувати структуру апаратної реалізації системи запобігання вторгненням на основі карт прискорювачів FPGA;

5) запропонувати послідовність кроків для створення апаратної реалізації системи запобігання вторгненням на основі карт прискорювачів FPGA.

Структура цієї статті включає п'ять основних розділів. У розділі 1 та 2 наведено результати аналізу кіберзагроз та методів їх виявлення для визначення можливостей запобігання вторгненням на апаратному рівні. У розділі 3 наведено аналіз сучасних плат FPGA-прискорювачів для створення SmartNIC. У розділі 4 запропоновано структуру апаратної реалізації системи запобігання вторгненням з використанням FPGA. У розділі 5 запропоновано етапи створення програмної реалізації системи захисту від вторгнень на FPGA.

1. Аналіз класифікації кіберзагроз

У загальному випадку кіберзагрози можна розділити на кілька основних категорій, включно зі шкідливим програмним забезпеченням (ПЗ), атаками на мережеву інфраструктуру, атаками на кінцеві додатки, а також загрозами, пов'язаними з фізичним доступом до пристроїв.

Не варто забувати про методи соціальної інженерії, які можуть бути застосовані в будь-якій з вищезазначених категорій.

Шкідливе ПЗ вражає своєю різноманітністю, прикладами можуть бути віруси, трояни, шифрувальники та інші програми-вимагачі, які можуть заражати системи і порушувати їхню роботу [1]. Можуть поширюватися і мережею, якщо заражені пристрої з'єднані в загальну мережу.

Атаки на мережеву інфраструктуру можуть включати в себе атаки, що викликають відмову в обслуговуванні, які перевантажують сервіс і роблять його недоступним. Сюди ж можна віднести атаки, пов'язані з перехопленням трафіку, у цьому разі порушується конфіденційність інформації. В інших випадках найчастіше порушується доступність інформації.

Атаки на кінцеві додатки можуть бути спрямовані на вразливості в програмному забезпеченні. У цьому випадку основними цілями є виконання несанкціонованих команд, а також несанкціонований доступ до інформації, що захищається.

Фізичні загрози включають у себе можливості підключення несанкціонованих пристроїв у мережу, а також можливості підключення носіїв інформації, що може призвести до виконання і поширення шкідливого ПЗ.

Використання методів соціальної інженерії може мати велику кількість варіантів використання. У контексті згаданих загроз можна розглянути варіанти зараження комп'ютерів за допомогою розсилок і введення користувачів в оману. Облікові дані привілейованого користувача можуть бути отримані шляхом використання фішингу.

2. Аналіз методів виявлення вторгнень

Слід виділити два основні принципи функціонування систем виявлення вторгнень і систем запобігання вторгненням – це сигнатурний метод і метод виявлення аномалій.

При використанні сигнатурного методу виявлення відбувається на основі заздалегідь відомих сигнатур атак. Метод виявлення аномалій базується на виявленні аномальних патернів у мережевому трафіку або діях користувача.

ISSN 1727-7337 (print)
ISSN 2663-2217 (online)

Сигнатурний метод забезпечує високу точність за відомих атак, що дає змогу точно ідентифікувати загрозу і мінімізувати кількість помилкових спрацьовувань. Також цей метод відрізняється простотою впровадження і мінімальними налаштуваннями, що дає змогу легко впровадити його в наявну систему забезпечення безпеки. Недоліками такого методу є обмеженість у виявленні нових атак (немає відомих сигнатур) і можливість модифікації атак таким чином, щоб не були використані відомі сигнатури.

Потрібен час на додавання нових сигнатур у загальну базу, потім за допомогою регулярних оновлень база сигнатур буде актуалізована в конкретній інсталяції.

Сигнатурний метод добре підходить для захисту від відомих загроз і простий у впровадженні, проте малоефективний в умовах динамічних атак. Одним із найвідоміших рішень для виявлення та запобігання вторгненням із відкритим вихідним кодом, де використовується сигнатурний метод виявлення, є система Snort [15].

Метод виявлення аномалій можна назвати протилежним сигнатурному методу, оскільки він може виявляти нові та модифіковані атаки. При цьому є низка проблем, серед яких висока кількість помилкових спрацьовувань, складність у налаштуванні та впровадженні, оскільки необхідний період навчання, щоб визначити, що вважається нормальною поведінкою системи. Метод виявлення аномалій надає потужний інструмент для виявлення нових і складних атак, особливо тих, які не покриті сигнатурними методами.

Однак його висока ймовірність помилкових спрацьовувань і складність налаштування можуть стати суттєвими перешкодами для його ефективного використання. Прикладом рішення з виявленням аномалій є система Darktrace [16].

Кожен тип системи має свої сильні та слабкі сторони, і оптимальний захист досягається шляхом їхньої комбінації та інтеграції з новими технологіями, такими як машинне навчання. Поліпшення наявних систем та їхня адаптація під нові загрози дадуть змогу ефективніше захищати сервери та мінімізувати ризики кібератак.

3. Аналіз можливостей апаратного прискорення FPGA для створення SmartNIC

Дослідження технологій центрів обробки даних та плат для створення систем обробки даних, включаючи FPGA як сервіс, показує, що вони перебувають у стані безперервної трансформації [17].

AMD спільно з Alveo пропонує різні плати FPGA-прискорювачів з різними ресурсами. Вони можуть бути згруповані в одному шасі для встановлення в центрах обробки даних з якісним централізованим охолодженням. Одна хост-машина може містити велику кількість слотів з картами. Вони можуть бути запрограмовані незалежно або для виконання одного завдання в межах датацентру.

Ці плати, як правило, виконані у вигляді плати з підключенням через PCIe, часто включають додаткові джерела живлення, активне охолодження і додаткові зовнішні комунікаційні інтерфейси. Також доступні простіші варіанти реалізації, які слугують економічно ефективними варіантами за рахунок мінімізації додаткових апаратних периферійних пристроїв і ресурсів (наприклад, доступний обсяг пам'яті, тип інтерфейсу взаємодії користувача і хост-системи).

У даний час існує велика кількість альтернатив FPGA-плат. Одним з яскравих прикладів є VCU1525, потужна плата для розробки без HBM (High Bandwidth Memory), призначена для різних класичних задач обробки, таких як перетворення відео. З'явилися й інші плати, такі як U200 та U250, що дозволяють інтегруватися з динамічно розширюваною пам'яттю DDR4.

U25 – карта для мережевих завдань. U50 [18] та U280 [19] – карти з 8 ГБ HBM. U55C – одна з найпотужніших плат FPGA-прискорювачів у цьому форматі з 16 ГБ динамічної пам'яті.

Однак недоліком цієї плати U55C є те, що кількість незалежних каналів пам'яті, які дозволяють підключити частину проєкту до конкретного блоку пам'яті, є такою ж, як і в U280 та U50.

Плата VHK158 також містить пам'ять HBM2E об'ємом 32 ГБ, але цей оціночний набір призначений для машинного навчання і реалізований в дещо іншому вигляді [20].

Плата прискорювача UL3524 розроблена без HBM і призначена для реалізації власних алгоритмів і торгових стратегій з підтримкою ШІ [21].

Виробники FPGA-прискорювачів пропонують набір інструментів для створення проєктів [22].

Компанія Intel випускає плати SmartNIC з використанням FPGA Stratix 10 DX2100 [23] та Agilex AGF014 [24]. Компанія AMD виробляє чіпи для створення плат типу Xilinx Virtex UltraScale+ [25], в тому числі XCU26 [26].

Можливим варіантом побудови рішень при використанні набору прискорювачів на базі FPGA сімейства Xilinx компанії AMD є застосування фреймворку Xilinx Runtime у складі уніфікованої програмної платформи AMD Vitis Unified Software Platform [27].

Узагальнюючі результати аналізу та порівняння плат SmartNIC від Intel та AMD наведені в таблиці 1.

Таблиця 1

Порівняння апаратних карт прискорювачів на основі FPGA для створення рішень SmartNIC

Карта прискорювача	Інтерфейси	FPGA
FPGA SmartNIC FB2CDG1@AGM39D-2	2x QSFPDD56	Agilex AGMF039
Silicom SmartNIC N5013/N5014	4x QSFP28	Stratix 10 DX 2100
Intel FPGA SmartNIC N6000-PL Plat-form	2x QSFP28	Agilex AGF014
AMD Alveo SN1000 SmartNIC	2x QSFP28	UltraScale+ XCU26
NT200A02 200G SmartNIC	2x QSFP28	UltraScale+ VU5P

4. Запропонована архітектура апаратної реалізації системи запобігання вторгненням з використанням FPGA

Під час побудови таких систем необхідно визначитися з набором кіберзагроз, які, зокрема, можуть бути представлені відомими особливостями самої реалізації окремих компонентів. Необхідно сформувати такий список. Під загрозами розуміються потенційні можливості вчинення протиправної дії проти об'єкта. Такі загрози можуть здійснюватися через вразливості, якими може скористатися зловмисник для реалізації загрози.

Профіль загроз. Під час формування набору вимог, які будуть використані під час побудови таких систем, можуть використовуватися загальні закономірності таких загроз. Під час деталізації закономірностей груп загроз здійснюється заповнення їхнього профілю з використанням підключених баз даних загроз. Частина профілів можуть бути досить широкими з можливими елементами евристики для можливості прийняття рішення в динаміці безпосередньо під час роботи системи. До складу профілів має увійти пропонована класифікація кіберзагроз як параметр. Це може бути набір профілів: шкідливе ПЗ, розподілена відмова в обслуговуванні, атаки людини посередині, фішинг, інсайдерські загрози тощо.

Процес виявлення з використанням апаратної реалізації є можливістю не лише здійснювати фільтрації на підставі інформації з баз, а й брати участь у їх наповненні або зборі попередніх ознак, оброблення яких може бути виконано із залученням засобів різницевого аналізу. Після такого опрацювання система може надсилати запит на надання або додавання інформації до бази. Отже, застосування апаратної фільтрації та реалізації SmartNIC у FPGA дає змогу не тільки отримувати інформацію з баз, а й додавати її до відповідних баз.

Усе разом це може бути представлено архітектурно як набір контейнерів у складі інфраструктури, між якими здійснюватиметься обмін. Таке рішення за своєю суттю є розширенням базової версії інфраструктури датацентру (рисунок 1).

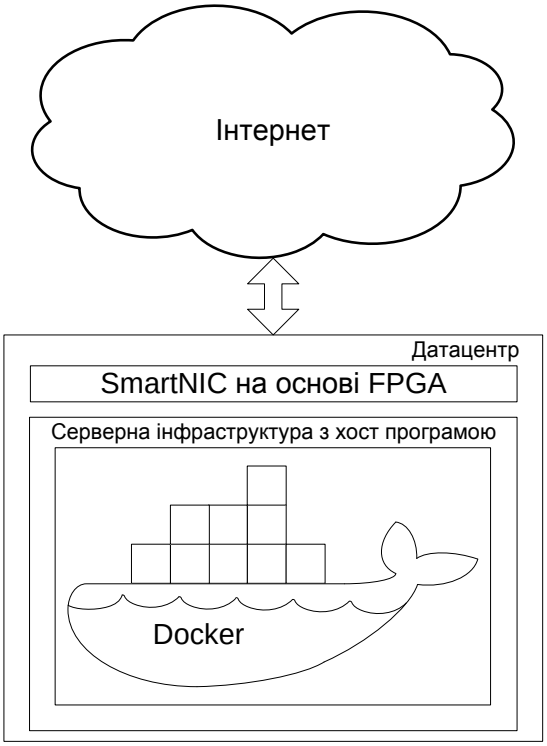

Рис. 1. Запропонована архітектура системи запобігання вторгнень на базі FPGA

У такому разі одним з елементів буде інтеграція того модуля, який здійснюватиме управління прискорювачами з SmartNIC у FPGA.

В архітектурі запропонованого рішення для роботи хост-додатка як складової частини апаратної реалізації SmartNIC у FPGA може підійти окремий контейнер у складі службових компонентів самої інфраструктури. У межах такого контейнера постійно відбуватиметься оновлення інформації з баз із відповідним оновленням поведінки апаратної реалізації SmartNIC у FPGA на підставі певних алгоритмів, закладених у їхню основу.

Одним з елементів є Server Infrastructure. Це окрема машина або окремий контейнер, де може бути зосереджена взаємодія засобів координації тих рішень, що безпосередньо виконуватимуть виявлення та конфігуруватимуть апаратні складові, для того, щоб доналаштовувати їх відповідно до нової інформації з актуалізованих баз.

Хост-додаток FPGA. Для безперервної роботи апаратної фільтрації в модулі FPGA SmartNIC необ-

ISSN 1727-7337 (print)
ISSN 2663-2217 (online)

хідне постійне їхнє доналаштування. Для підтримки такої взаємодії необхідний хост-додаток для роботи SmartNIC. Такий хост-додаток має бути розташований у складі поточної інфраструктури для можливості розміщення у складі датацентру. Мінімальною реалізацією може бути об'єднання хост-додатку для FPGA та інших контейнерів сервера.

Зв'язаність компонентів при розташуванні такої системи дає змогу підвищити продуктивність апаратної частини SmartNIC. Система пропонується як частина інфраструктури для датацентрів для забезпечення захисту.

Робота самого датацентру. При цьому немає необхідності додавання компонентів до складу користувацьких машин або контейнерів, оскільки процес фільтрації реалізовано на апаратному рівні завдяки обробці в складі FPGA SmartNIC. Це впливає на оцінку такого сервісу. Чим більше сторонніх компонентів від розробника або провайдера з'являється у складі користувацьких рішень, тим вищий ризик додавання вразливостей. Тому в межах запропонованих рішень кожен користувач такого сервісу отримує власний незалежний віртуальний простір, а механізми апаратної фільтрації та SmartNIC надаються на рівні інфраструктури.

5. Запропонована послідовність створення реалізації системи запобігання вторгненням на базі FPGA

Базуючись на розглянутих можливостях FPGA прискорювачів, потребах виконання завдань виявлення та запобігання вторгненням, а також необхідності забезпечення можливості налаштування таких рішень для конкретного екземпляра сервісу, є можливим запропонувати такі кроки побудови рішень з використанням FPGA для прискорення реалізації:

1) формування вимог і списку елементів мережевого обміну, обробка яких дасть змогу виявляти та запобігати вторгненням;

2) ухвалення рішень про вибір набору апаратних FPGA карт прискорювачів, їхнього виробника та інструментальних засобів для побудови рішень спільно з іншим обладнанням серверів;

3) ухвалення рішення про побудову такої системи з композиції наявних рішень для SmartNICs або про її розроблення на основі інструментальних засобів обраного виробника FPGA;

4) інтеграція хост-додатку для FPGA прискорювача до складу контейнера службової частини сервера для забезпечення можливості налаштування та управління;

5) налаштування зв'язків компонентів інфраструктури з хост-додатком SmartNIC і налаштування конекторів для роботи сервера.

Дискусія

У роботі проаналізовано інструменти, технології та методи запобігання вторгненням з використанням прискорення FPGA.

Висока якість роботи систем виявлення та запобігання вторгненням може бути підтверджена в процесі верифікації вимог, після чого може бути видано документ про відповідність вимогам щодо захисту даних.

Серед основних переваг сигнатурного методу виявлення вторгнень слід відзначити його високу точність у тих випадках, коли загроза вже відома. Цей метод легко впроваджується в наявні системи безпеки завдяки простоті налаштування.

Недоліком такого методу є обмеженість у виявленні нових атак. Швидкість оновлення бази даних сигнатур може також вплинути на якість виявлення нових загроз.

Метод виявлення аномалій більш перспективний для виявлення нових атак, оскільки він не обмежений заздалегідь визначеними сигнатурами. Однак його використання часто ускладнене високим рівнем помилкових спрацьовувань, що вимагає ретельного налаштування і навчання системи. Це може виявитися суттєвим бар'єром для його ефективного застосування в реальних умовах.

Процес створення таких рішень може спиратися на інструментальні засоби розроблення від виробників окремих компонентів, включаючи FPGA, карти прискорювачів та виробників програмного забезпечення. Такий підхід дає змогу знизити трудовитрати завдяки довіреним інструментам і при цьому гарантувати відсутність закладних елементів або троянів у складі самого рішення.

Серед запропонованого набору кроків слід виділити визначення набору кіберзагроз, які можуть бути, зокрема, представлені відомими особливостями самої реалізації окремих компонентів. Необхідно сформувати такий список і побудувати профіль загроз. Розширення та оновлення такого профілю дозволяє виконувати оновлення під час роботи такої системи без встановлення обладнання.

Практична реалізація та використання описаних елементів, зокрема прискорювачів SmartNIC у FPGA для реалізації запобігання вторгненням, дають змогу підвищити швидкодію роботи датацентрів, а також підвищити захищеність їхніх користувачів від відомих кіберзагроз.

Додавання до запропонованої послідовності моделі побудови профілю загроз дасть змогу отримати метод створення систем з апаратним прискоренням для запобігання вторгненням з використанням FPGA.

Висновки

Основним результатом даного дослідження в рамках поточної публікації є аналіз і запропонована послідовність створення систем з апаратним прискоренням процесів запобігання вторгненням у систему з використанням FPGA.

Проаналізовано два основні методи виявлення вторгнень. Наведені результати аналізу переваг і недоліків кожного методу показують, що деякі специфічні особливості систем виявлення та запобігання вторгнень становлять науковий інтерес.

Проведено аналіз можливих інструментів для запобігання кіберзагрозам. Проведено аналіз апаратних прискорювачів на основі FPGA.

Запропоновано структуру системи для запобігання вторгнень для відомих кіберзагроз із використанням FPGA. Запропоновано послідовність кроків створення рішень з апаратним прискоренням для запобігання вторгненням з використанням FPGA.

До напрямів подальших досліджень належить побудова та практичне дослідження чисельних показників діючої системи на основі власного рішення, яке частково організовано з готових компонентів або складатиметься повністю з авторських рішень.

Внесок авторів: формулювання мети і завдань дослідження – **А. Г. Тецький**, **А. Є. Перепелицин**, аналіз основних методів виявлення – **А. Г. Тецький**, аналіз карт прискорювачів – **А. Є. Перепелицин**, аналіз особливостей SmartNIC – **А. Г. Тецький**, **А. Є. Перепелицин**, створення структури апаратної реалізації – **А. Г. Тецький**, **А. Є. Перепелицин**, запропоновані рекомендації створення реалізації системи запобігання вторгненням та написання тексту статті – **А. Г. Тецький, А. Є. Перепелицин**.

Конфлікт інтересів

Автори заявляють, що немає конфлікту інтересів щодо цього дослідження, фінансового, особистого, авторського чи іншого, який міг би вплинути на дослідження та результати, представлені в статті.

Фінансування

Дослідження проведено без фінансової підтримки.

Доступність даних

Рукопис не має пов'язаних даних.

Використання засобів штучного інтелекту

Автори підтверджують, що не використовували генеративних технологій штучного інтелекту при створенні представленої роботи та дослідженні.

Автори прочитали та погодилися з опублікованою версією рукопису.

Література

1. Tetskyi, A. Intrusion detection and prevention systems as a component of ensuring compliance with regulatory documents [Text] / A. Tetskyi, & D. Uzun // Radioelectronic and Computer Systems. – 2024. – № 3. – P. 166-174. DOI: 10.32620/reks.2024.3.11.

2. Amoud, M. Dynamic adaptation and reconfiguration of security in mobile devices [Text] / M. Amoud, & O. Roudies // Proceedings of 2017 International Conference On Cyber Incident Response, Coordination, Containment & Control (Cyber Incident) . – 2017. – 6 p. DOI: 10.1109/CYBERINCIDENT.2017.8054639.

3. Shanthi, K. A Comparative Study of Intrusion Detection and Prevention Systems for Cloud Environment [Text] / K. Shanthi, & R. Maruthi // Proceedings of 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC 2023). – 2023. – P. 493-496. DOI: 10.1109/ICESC57686.2023.10193694.

4. K, P. A Comprehensive Survey: Exploring Current Trends and Challenges in Intrusion Detection and Prevention Systems in the Cloud Computing Paradigm [Text] / P. K, & P. Sudhakar // Proceedings of 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT 2024). – 2024. – P. 351-358. DOI: 10.1109/IDCIoT59759.2024.10467700.

5. Ghumman, S. A Comparative Evaluation of network Attack Detection and Prevention Strategies in multi model Cloud servers [Text] / S. Ghumman // Proceedings of 2023 4th IEEE Global Conference for Advancement in Technology (GCAT 2023). – 2023. – 6 p. DOI: 10.1109/GCAT59970.2023.10353441.

6. Tayyebi, Y. Security solutions in Cloud through customized IDS configuration at VM level [Text] / Y. Tayyebi, & D. S. Bhilare // Proceedings of 2018 International Conference on Advanced Computation and Telecommunication (ICACAT 2018). – 2018. – 5 p. DOI: 10.1109/ICACAT.2018.8933581.

7. Технології реалізації штучного інтелекту як сервісу на основі апаратних прискорювачів [Текст] / А. Є. Перепелицин, Є. В. Касапєн, Г. В. Фесенко, В. С. Харченко // Авіаційно-космічна техніка і технологія. – 2022. – № 6. – С. 57-65. DOI: 10.32620/aktt.2022.6.07.

8. Roy, A. A Novel Network On Chip Architecture For FPGA Smart NIC [Text] / A. Roy, V. Kapila, A. Gupta, & R. Pal // Proceedings of 2023 IEEE Women in Technology Conference (WINTECHCON 2023). – 2023. – 5 p. DOI: 10.1109/WINTECHCON58518.2023.10276404.

9. Alveo Product Selection Guide, Data Center Accelerator Cards, Xilinx. – Available at: https://www.xilinx.com/content/dam/xilinx/support/documents/selection-guides/alveo-product-selection-guide.pdf. – 24.07.2024.

ISSN 1727-7337 (print)
ISSN 2663-2217 (online)

10. Altera® FPGA AI NICs and SmartNICs, Accelerate Data from Edge to Cloud, Intel. – Available at: https://www.intel.com/content/www/us/en/products/details/fpga/platforms/smartnic.html. – 08.09.2024.

11. Wu, M. ONLAD-IDS: ONLAD-Based Intrusion Detection System Using SmartNIC [Text] / M. Wu, H. Matsutani, & M. Kondo // Proceedings of 2022 IEEE 24th Int Conf on High Performance Computing & Communications; 8th Int Conf on Data Science & Systems; 20th Int Conf on Smart City; 8th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys 2022). – 2022. – P. 546-553. DOI: 10.1109/HPCC-DSS-SmartCity-DependSys57074.2022.00100.

12. Pacífico, R. D. G. Function as a Service Offloaded to a SmartNIC [Text] / R. D. G. Pacífico, M. A. M. Vieira, L. F. S. Duarte, & J. A. M. Nacif // Proceedings of 2022 IEEE Latin-American Conference on Communications (LATINCOM 2022). – 2022. – 6 p. DOI: 10.1109/LATINCOM56090.2022.10000473.

13. Miano, S. Introducing SmartNICs in Server-Based Data Plane Processing: The DDoS Mitigation Use Case [Text] / S. Miano, R. Doriguzzi-Corin, F. Risso, D. Siracusa, & R. Sommese // in IEEE Access. – 2019. vol. 7. – P. 107161-107170. DOI: 10.1109/ACCESS.2019.2933491.

14. Sheeraz, M. Advancing Snort IPS to Achieve Line Rate Traffic Processing for Effective Network Security Monitoring [Text] / M. Sheeraz, M. Hanif Durad, S. Tahir, H. Tahir, S. Saeed, & A. M. Almuhaideb // in IEEE Access. – 2024. vol. 12. – P. 61848-61859. DOI: 10.1109/ACCESS.2024.3395123.

15. Shah, S. A. R. Performance comparison of intrusion detection systems and application of machine learning to Snort system [Text] / S. A. R. Shah, & B. Issac // Future Generation Computer Systems. – 2018. vol. 80. – P. 157-170. DOI: 10.1016/j.future.2017.10.016.

16. Vähäkainu, P. Use of Artificial Intelligence in a Cybersecurity Environment [Text] / P. Vähäkainu, & M. Lehto // Artificial Intelligence and Cybersecurity. Springer, Cham. – 2023. – P. 3–27. DOI: 10.1007/978-3-031-15030-2_1.

17. Тецький, А. Г. Тестування на проникнення компонентів FPGA як сервісу для забезпечення кібербезпеки [Текст] / А. Г. Тецький // Авіаційно-космічна техніка і технологія. – 2023. – № 6. – С. 95-101. DOI: 10.32620/aktt.2023.6.11.

18. Alveo U50 Data Center Accelerator Card Data Sheet, DS965 (v1.8) June 23, 2023. – Available at: https://docs.amd.com/r/en-US/ds965-u50 – 08.09.2024.

19. Alveo U280 Data Center Accelerator Card, UG1314 (v1.1) June 15, 2023. – Available at: https://docs.amd.com/r/en-US/ug1314-alveo-u280-reconfig-accel – 08.09.2024.

20. VHK158 Evaluation Board User Guide, AMD, UG1611 (v1.0). – Available at: https://docs.xilinx.com/r/en-US/ug1611-vhk158-eval-bd – 08.09.2024.

21. Alveo UL3524 Ultra Low Latency Trading Data Sheet, AMD, DS1009 (v1.1). – Available at: https://docs.xilinx.com/r/en-US/ds1009-ul3524 – 08.09.2024.

22. Alveo Portfolio Product Selection Guide, AMD, XMP451 (v2.1). – Available at: https://docs.amd.com/v/u/en-US/alveo-product-selection-guide – 08.09.2024.

23. Silicom FPGA SmartNIC N5014, Silicom Ltd. Connectivity Solutions. – Available at: https://www.silicom.dk/wp-content/uploads/2023/08/PB_Silicom_FPGA_SmartNIC_N5014_v1.4.pdf– 08.09.2024.

24. A SmartNIC for Accelerating Communications and Networking Workloads. Intel. – Available at: https://www.intel.com/content/www/us/en/content-details/779620/a-smartnic-for-accelerating-communications-and-networking-workloads.html – 08.09.2024.

25. NT200A02 200G SmartNIC, Xilinx. – Available at: https://www.xilinx.com/products/boards-and-kits/1-18tmaxd.html – 08.09.2024.

26. Alveo SN1000 SmartNIC, Xilinx. – Available at: https://www.xilinx.com/publications/technology-briefs/xilinx-alveo-sn1000-technical-brief.pdf – 08.09.2024.

27. Vitis Unified Software Platform Documentation: Embedded Software Development, AMD, UG1400 (v2024.1). – Available at: https://docs.amd.com/r/en-US/ug1400-vitis-embedded/Migrating-from-the-Classic-Vitis-IDE-to-Vitis-Unified-IDE – 08.09.2024.

References

1. Tetskyi, A., & Uzun, D. Intrusion detection and prevention systems as a component of ensuring compliance with regulatory documents. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2024, no. 3, pp. 166-174. DOI: 10.32620/reks.2024.3.11.

2. Amoud, M., & Roudies, O. Dynamic adaptation and reconfiguration of security in mobile devices. *Proceedings of 2017 International Conference On Cyber Incident Response, Coordination, Containment & Control (Cyber Incident)*, 2017, pp. 1-6. DOI: 10.1109/CYBERINCIDENT.2017.8054639.

3. Shanthi, K., & Maruthi, R. A Comparative Study of Intrusion Detection and Prevention Systems for Cloud Environment. *Proceedings of 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC 2023)*, 2023, pp. 493-496. DOI: 10.1109/ICESC57686.2023.10193694.

4. K, P., & Sudhakar, P. A Comprehensive Survey: Exploring Current Trends and Challenges in Intrusion Detection and Prevention Systems in the Cloud Computing Paradigm. *Proceedings of 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT 2024)*, 2024, pp. 351-358. DOI: 10.1109/IDCIoT59759.2024.10467700.

5. Ghumman, S. A Comparative Evaluation of network Attack Detection and Prevention Strategies in multi model Cloud servers. *Proceedings of 2023 4th IEEE Global Conference for Advancement in Technology (GCAT 2023)*, 2023, pp. 1-6. DOI: 10.1109/GCAT59970.2023.10353441.

6. Tayyebi, Y., & Bhilare, D. S. Security solutions in Cloud through customized IDS configuration at VM level. *Proceedings of 2018 International Conference on Advanced Computation and Telecommunication (ICACAT 2018)*, 2018, pp. 1-5. DOI: 10.1109/ICACAT.2018.8933581.

7. Perepelitsyn, A., Kasapien, Y., Fesenko, H., & Kharchenko, V. Technologies for Implementing of Artificial Intelligence as a Service based on Hardware Accelerators. *Aviacijno-kosmicna tehnika i tehnologia – Aerospace technic and technology*, 2022, no. 6, pp. 57-65. DOI: 10.32620/aktt.2022.6.07.

8. Roy, A., Kapila, V., Gupta, A., & Pal, R. A Novel Network On Chip Architecture For FPGA Smart NIC. *Proceedings of 2023 IEEE Women in Technology Conference (WINTECHCON 2023)*, 2023, pp. 1-5. DOI: 10.1109/WINTECHCON58518.2023.10276404.

9. *Alveo Product Selection Guide, Data Center Accelerator Cards, Xilinx*. Available at: https://www.xilinx.com/content/dam/xilinx/support/documents/selection-guides/alveo-product-selection-guide.pdf. (accessed July 24, 2024).

10. *Altera® FPGA AI NICs and SmartNICs, Accelerate Data from Edge to Cloud, Intel*. Available at: https://www.intel.com/content/www/us/en/products/details/fpga/platforms/smartnic.html. (accessed September 08, 2024).

11. Wu, M., Matsutani, H., & Kondo, M. ONLAD-IDS: ONLAD-Based Intrusion Detection System Using SmartNIC. *Proceedings of 2022 IEEE 24th Int Conf on High Performance Computing & Communications; 8th Int Conf on Data Science & Systems; 20th Int Conf on Smart City; 8th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys 2022)*, 2022, pp. 546-553. DOI: 10.1109/HPCC-DSS-SmartCity-DependSys57074.2022.00100.

12. Pacífico, R. D. G., Vieira, M. A. M., Duarte, L. F. S., & Nacif, J. A. M. Function as a Service Offloaded to a SmartNIC. *Proceedings of 2022 IEEE Latin-American Conference on Communications (LATINCOM 2022)*, 2022, pp. 1-6. DOI: 10.1109/LATINCOM56090.2022.10000473.

13. Miano, S., Doriguzzi-Corin, R., Risso, F., Siracusa, D., & Sommese, R. Introducing SmartNICs in Server-Based Data Plane Processing: The DDoS Mitigation Use Case. *in IEEE Access*, 2019, vol. 7, pp. 107161-107170. DOI: 10.1109/ACCESS.2019.2933491.

14. Sheeraz, M., Hanif Durad, M., Tahir, S., Tahir, H., Saeed, S., & Almuhaideb, A. M. Advancing Snort IPS to Achieve Line Rate Traffic Processing for Effective Network Security Monitoring. *in IEEE Access*, 2024, vol. 12, pp. 61848-61859. DOI: 10.1109/ACCESS.2024.3395123.

15. Shah, S. A. R., & Issac, B. Performance comparison of intrusion detection systems and application of machine learning to Snort system. *Future Generation Computer Systems*, 2018, vol. 80, pp. 157-170. DOI: 10.1016/j.future.2017.10.016.

16. Vähäkainu, P., & Lehto, M. Use of Artificial Intelligence in a Cybersecurity Environment. *In: Sipola, T., Kokkonen, T., Karjalainen, M. (eds) Artificial Intelligence and Cybersecurity*. *Springer, Cham*, 2023. pp. 3-27. DOI: 10.1007/978-3-031-15030-2_1.

17. Tetskyi, A. Testuvannia na pronyknennia komponentiv FPGA yak servisu dlia zabezpechennia kiberbezpeky [Penetration testing of FPGA as a Service components for ensuring cybersecurity]. *Aviacijno-kosmicna tehnika i tehnologia – Aerospace technic and technology*, 2023, no. 6, pp. 95–101. DOI: 10.32620/aktt.2023.6.11. (In Ukrainian).

18. *Alveo U50 Data Center Accelerator Card Data Sheet, DS965 (v1.8) June 23, 2023*. Available at: https://docs.amd.com/r/en-US/ds965-u50 (accessed September 08, 2024).

19. *Alveo U280 Data Center Accelerator Card, UG1314 (v1.1) June 15, 2023*. Available at: https://docs.amd.com/r/en-US/ug1314-alveo-u280-reconfig-accel (accessed September 08, 2024).

20. *VHK158 Evaluation Board User Guide, AMD, UG1611 (v1.0)*. Available at: https://docs.xilinx.com/r/en-US/ug1611-vhk158-eval-bd (accessed September 08, 2024).

21. *Alveo UL3524 Ultra Low Latency Trading Data Sheet, AMD, DS1009 (v1.1)*. Available at: https://docs.xilinx.com/r/en-US/ds1009-ul3524 (accessed September 08, 2024).

22. *Alveo Portfolio Product Selection Guide, AMD, XMP451 (v2.1)*. Available at: https://docs.amd.com/v/u/en-US/alveo-product-selection-guide (accessed September 08, 2024).

23. *Silicom FPGA SmartNIC N5014, Silicom Ltd. Connectivity Solutions*. Available at: https://www.silicom.dk/wp-content/uploads/2023/08/PB_Silicom_FPGA_SmartNIC_N5014_v1.4.pdf (accessed September 08, 2024).

ISSN 1727-7337 (print)
ISSN 2663-2217 (online)

24. *A SmartNIC for Accelerating Communications and Networking Workloads. Intel*. Available at: https://www.intel.com/content/www/us/en/content-details/779620/a-smartnic-for-accelerating-communications-and-networking-workloads.html (accessed September 08, 2024).

25. *NT200A02 200G SmartNIC, Xilinx*. Available at: https://www.xilinx.com/products/boards-and-kits/1-18tmaxd.html (accessed September 08, 2024).

26. *Alveo SN1000 SmartNIC, Xilinx*. Available at: https://www.xilinx.com/publications/technology-briefs/xilinx-alveo-sn1000-technical-brief.pdf (accessed September 08, 2024).

27. *Vitis Unified Software Platform Documentation: Embedded Software Development, AMD, UG1400 (v2024.1)*. Available at: https://docs.amd.com/r/en-US/ug1400-vitis-embedded/Migrating-from-the-Classic-Vitis-IDE-to-Vitis-Unified-IDE (accessed September 08, 2024).

Надійшла до редакції 10.10.2024, розглянута на редколегії 18.11.2024

POSSIBILITIES OF USING OF HARDWARE ACCELERATORS FOR INTRUSION DETECTION AND PREVENTION SYSTEMS

Artem Tetskyi, Artem Perepelitsyn

The subject of this study is the capabilities of FPGA technology for cybersecurity solutions with the network interface accelerators of SmartNIC, as well as the technologies for building, deploying, supporting, and accelerating intrusion detection systems and intrusion prevention systems. The **goal** of this work is to increase the performance of the network protection components of modern datacenters using hardware network interface accelerator cards based on FPGA technology. The **task** is to analyze the classification of cyber threats, to analyze methods of detecting cyber threats, to analyze the capabilities of modern FPGA accelerator cards for the creation of SmartNICs, to propose the architecture for hardware implementation of intrusion prevention system based on FPGA accelerator cards, and to propose the sequence of steps for creation of hardware implementation of intrusion prevention system based on FPGA acceleration. According to the tasks, the following **results** were obtained. The analysis of the main categories of common cyberthreats that should be considered when creating systems is performed. Two main principles of intrusion detection including the signature method and the anomaly detection method are analyzed. The analysis of the possibilities of using FPGA accelerator cards for hardware acceleration of network interfaces and the creation of SmartNICs is performed. The architecture of hardware implementation of network interface components for intrusion prevention system based on FPGA accelerator cards in data centers is proposed. The sequence of steps for creation of FPGA-based implementation of intrusion prevention system is proposed. **Conclusions.** The scientific novelty of the obtained results is in the fact that the analysis of the specifics of cyberthreats of datacenters and capabilities of FPGA accelerator cards with support of high-speed network interfaces allows to propose the set of recommendations for the creation of intrusion detection systems and intrusion prevention systems with the transfer of work to hardware implementation, which will make it possible to offload the computing resources of server and thereby increase its performance. The software component of the solution provides the possibility of improvements and continuously updating the operating profile of the hardware component of such intrusion detection and intrusion prevention systems directly in the system.

Keywords: Intrusion Detection System; Intrusion Prevention System; IDS; IPS; FPGA as a Service; SmartNIC; offloading datacenter resources.

Тецький Артем Григорович – канд. техн. наук, доц. каф. комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Перепелицин Артем Євгенович – канд. техн. наук, доц., доц. каф. комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Artem Tetskyi – PhD, Associate Professor at the Computer Systems, Networks and Cybersecurity Department, National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine,
e-mail: a.tetskiy@csn.khai.edu, ORCID: 0000-0003-1745-2452, Scopus Author ID: 57202894656.

Artem Perepelitsyn – PhD, Associate Professor at the Computer Systems, Networks and Cybersecurity Department, National Aerospace University «Kharkiv Aviation Institute», Kharkiv, Ukraine,
e-mail: a.perepelitsyn@csn.khai.edu, ORCID: 0000-0002-5463-7889, Scopus Author ID: 56332607800.