УДК 004

К.Кузьмін, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ВІДДАЛЕНОГО КОНТРОЛЮ НА ОСНОВІ ТЕХНОЛОГІЇ INTEL ME

У статті розроблено програмне забезпечення, яке призначено для системи віддаленого контролю на основі технології Intel ME. Метою розробки є дослідження та принципи побудови системи віддаленого контролю на основі технології Intel ME. Об'єктом дослідження є процес віддаленого контролю на основі технології Intel ME. Предметом дослідження є методи віддаленого контролю на основі технології Intel ME. Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи віддаленого контролю на основі технології Intel ME. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

система віддаленого контролю, Intel ME

Постановка проблеми. Технологія Intel ME (або AMT, Active Management Technology) є одним із самих загадкових і потужних елементів сучасних x 86-платформ. Інструмент споконвічно створювалося як рішення для віддаленого адміністрування. Однак він має настільки потужну функціональність і настільки непідконтрольний користувачам Intel-based пристроїв, що багато хто з них хотіли б відключити цю технологію, що зробити не так-те просто.

Підсистема Intel Management Engine (ME) являє собою додатковий «схований» процесор, що є присутнім у всіх пристроях на базі чипсетів Intel (не тільки в PC і ноутбуках, але й у серверах).

Середовище виконання ME ніколи не «спить» і працює навіть при виключеному комп'ютері (при наявності чергової напруги), а також має доступ до оперативної пам'яті, мережного інтерфейсу, USB контролера й убудованого графічного адаптера.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи віддаленого контролю на основі технології Intel ME.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи віддаленого контролю на основі технології Intel ME.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем віддаленого контролю на основі технології Intel ME.
– Дослідження системи віддаленого контролю на основі технології Intel ME.
– Програмна реалізація системи віддаленого контролю на основі технології Intel ME.

Об'єктом дослідження є процес віддаленого контролю на основі технології Intel ME.

Предметом дослідження є методи віддаленого контролю на основі технології Intel ME.

Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Незважаючи на настільки великі можливості Intel Management Engine (ME), існують питання до рівня захищеності ME – раніше дослідники вже знаходили серйозні уразливості й вектори атак. Крім того, підсистема

містить потенційно небезпечні функції – віддалене керування, NFC, схований сервісний розділ (hidden service partition). Інтерфейси підсистеми ME недокументовані, а реалізація закрита.

Всі ці причини приводять до того, що багато хто розглядають технологію ME у якості «апаратної закладки». Ситуацію збільшує той факт, що з однієї сторони в користувача пристрою немає можливостей по відключенню цієї функціональності, а з інший виробник устаткування може допустити помилки в конфігурації ME.

Гарна новина полягає в тому, що способи відключення ME все-таки існують.

Техніки відключення Intel ME

Фахівці описали трохи технік відключення даної підсистеми:

– Засновані на збої ініціалізації ME.
– Через механізм відновлення мікропрограми ME.
– Недокументовані команди.
– Недокументований механізм, призначений для розроблювачів апаратури – Manufacture Mode.

Дослідники встановили, що розроблювачі апаратних платформ часто забувають виключати режим Manufacture Mode, що дозволяє використовувати останній метод на великій кількості комп'ютерів без яких або додаткових витрат у режимі «реального часу».

Більшість методів відключення використовують убудовані механізми ME, розроблені для вендорів пристроїв на платформі Intel.

І проте, виникає резонне питання: « чиДійсно ME перестає працювати в повному обсязі при використанні її убудованих механізмів відключення?» Як доказ факту відключення ME дослідники приводять наступний аргумент: ME працює у двох режимах використання пам'яті: тільки SRAM (убудований в ME) і SRAM + UMA. UMA – це частина пам'яті хоста, що використовується пам'ять, що підкачується як (swap). Після ініціалізації DRAM-контролера хостом ME завжди перемикається в режим SRAM + UMA.

Таким чином, якщо ME дійсно виключена, то при відключенні на апаратному рівні доступу ME до UMA-Пам'яті в довільний момент (засобами каналу VCm), у ME не буде відбуватися апаратних збоїв, пов'язаних з відсутністю даних і коду, які були витиснуті в UMA пам'ять (такі апаратні збої приводять до аварійного відключення живлення з основних апаратних компонентів платформи). З іншої сторони застосування цих методів дозволяє здійснити DoS-атаки на технологію AMT у випадку її застосування для віддаленого керування.

В 2005 році компанія Intel представила Active Management Technology (AMT) версії 1.0 – рішення для віддаленого адміністрування (керування, інвентаризація, відновлення, діагностика, усунення неполадок і т.д.) і захисту десктопних комп'ютерних систем, свого роду аналог технології Intelligent Platform Management Interface (IPMI), що використовується в серверах.

Архітектура AMT 1.0 ґрунтується на інтегрованому в чипсет мікроконтролері (Management Engine), наділеному досить вражаючими можливостями, наприклад:

– позаполосний (out-of-band) доступ до мережного інтерфейсу (Ethernet), що він розділяє з основним CPU, але, маючи власний контролер канального рівня, здійснює моніторинг усього вхідного мережного трафіку, з якого «вирізує» (за допомогою Packet Filter) пакети, призначені для нього. Для ОС (наявність і стан якої, до речі, на роботу AMT ніяк не впливає) цей трафік уже не видний;
– внутрішній веб-сервер з TLS-шифруванням;
– доступ до периферійного встаткування, одержання й зберігання в енергонезалежній пам'яті (там же, де і його прошивання) інформації про нього.

А ще цей мікроконтролер починає працювати при подачі живлення на материнську плату комп'ютерної системи (тобто при підключенні комп'ютера до електричної мережі, ще до того, як користувач натисне кнопку Power).

Отже, Management Engine завжди включений, але використання можливостей AMT вимагає активації (має на увазі завдання пароля, мережних параметрів,...) в BIOS setup, а точніше в MEBx setup.

Похвально, що дефолтний пароль («admin») при першому вході обов'язково потрібно змінити на новим, задовольняючим певним вимогам: мінімум 8 символів, серед яких повинні бути присутнім хоча б одна цифра, одна заголовна буква й один спец. символ.

Після налаштування AMT-сумісної комп'ютерної системи, віддаленому адміністраторові стають доступними мережні функції (для їхнього використання потрібен уведення логіна й пароля):

– інвентаризація апаратного забезпечення;
– веб-інтерфейс (по HTTP через порт 16992);
– Serial Over LAN (SOL) – віртуальний COM-Порт через мережу, що дозволяє включати / перезавантажувати / виключати комп'ютер, одержувати доступ до меню BIOS setup;
– IDE-Redirection (IDE-R) – опція перенапрямку завантаження з локального завантажувального пристрою на віддалене (попередньо підготовлений образ системи).

AMT 1.0 була реалізована на інтегрованому в південний міст чипсета (Input / Output Controller Hub, ICH) мережному модулі Intel 82573E series Gigabit Ethernet Controller.

Потім, в 2006 році, починаючи з AMT версії 2.0, мікроконтролер перенесли в північний міст чипсета (Graphics and Memory Controller Hub, GMCH). Саме тоді підсистему найменували в Intel Management Engine (ME) версії 2.0.

Одночасно із цим з'явився бренд Intel vPro, що позначав комплекс реалізованих на основі Intel ME технологій: AMT, Trusted Execution Technology (TXT) і Virtualization Technology (VT). Пізніше в цей список увійшли Identity Protection Technology (IPT) і Anti-Theft (AT).

Тоді ж Intel ME наділили ще більшою кількістю вражаючих можливостей, серед яких – повний доступ до всього вмісту оперативної пам'яті комп'ютера через внутрішній DMA-контролер, а надалі з'явилася можливість моніторингу відеопотоку, що виводиться на монітор (правда, тільки у випадку використання убудованого графічного ядра).

Поступово на цю підсистему стали навішувати усе більше різних системних функцій (деякими раніше займався BIOS) для забезпечення працездатності комп'ютерної платформи:

– частина функцій Advanced Control and Power Interface (ACPI) і Alert Standard Format (ASF);
– Quiet System Technology (QST);
– Integrated Clock Control (ICC);
– Trusted Platform Module (TPM);
– і інших технологій.

AMT теж не стояла на місці й активно розвивалася: змінювався состав використовуваних протоколів (наприклад, додалася підтримка HTTPS через порт 16993), у версії 6.0 для віддаленого адміністратора з'явилася фіча Remote Desktop, вона ж KVM (Keyboard Video Mouse), та інше.

Проте, через високу вартість реалізації, ця підсистема була присутня, за декількома виключеннями, тільки на материнських платах із чипсетами Intel лінійки Q.

Тоді до чого вся ця специфіка заліза із шильдиком vPro, що мало хто здобував через високу вартість (ну й інших причин)?

Справа в тому, що, починаючи з 2010 року, разом з переносом частини функціональних блоків північного мосту (графічне ядро, контролер пам'яті, ...) у корпус CPU, підсистему Intel ME стали вбудовувати в усі чипсети виробництва Intel. При цьому ME-контролер залишився в корпусі чипсета – в Platform Controller Hub (PCH). Це чипсети 5 серії й вище.

Функціональність AMT донині залишається доступною тільки на чипсетах лінійки Q, тобто тільки на встаткуванні із шильдиком vPro.

Думаєте тільки десктопи й ноутбуки? Ні, Intel-а відповідь!

Та ж доля осягла й серверні платформи від Intel: підсистема убудована в них, але під іншим ім'ям – Intel Server Platform Services (SPS). Відбулася поява й в SoC (on-a-Chip) під ім'ям Intel Trusted Execution Engine (TXE).

У підсумку архітектура кожної сучасної мобільної / лаптопної / дескопної / серверної комп'ютерної платформи із чипсетом / SoC від Intel містить у собі саму потайливу (від користувача системи) і привілейоване середовище виконання – підсистему Intel ME. Не дивно, що розробляючи цю архітектуру, компанія Intel була змушена серйозно попрацювати над її захистом від компрометації.

Розглянемо архітектуру цієї підсистеми, щоб розібратися в застосованій моделі безпеки.

Архітектура Intel ME

Intel Management Engine (ME) – убудована в комп'ютерні платформи підсистема, що забезпечує апаратно-програмну підтримку різних технологій Intel.

Як уже було сказано, перші версії цієї підсистеми були засновані на двокорпусних чипсетах Intel. Тоді як базова модель ME-контролера використовувався ARCtangent-A4 зі стандартною системою команд ARC32.

В однокорпусних чипсетах уже використовувалися ARCtangent-A5 / ARC600 з компактною системою команд ARCompact (ARC16/32).

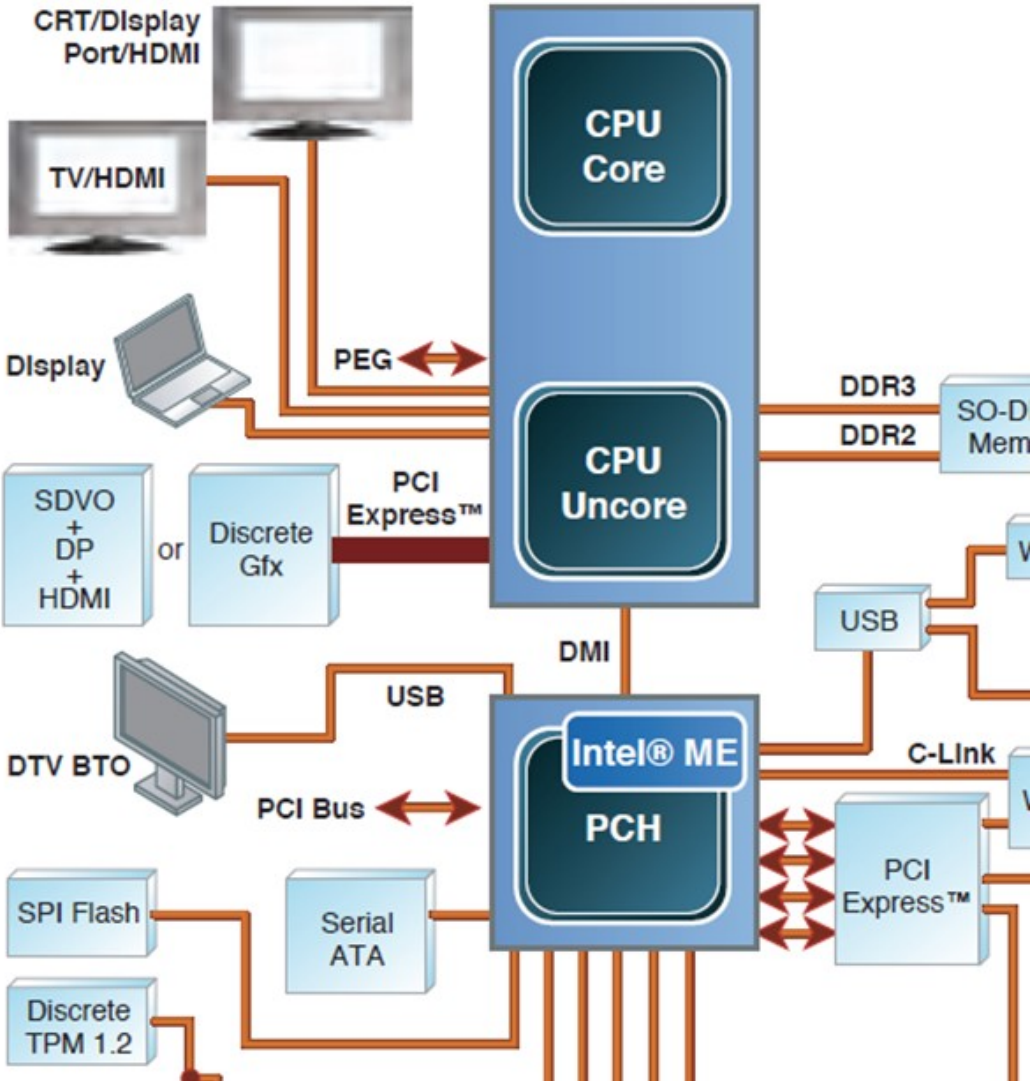

Рисунок 1 – Структурна схема системи

В Intel SoC (там де ця підсистема називається Intel TXE) як базова модель для ME-контролера використовується SPARC.

Нічого страшного, в Intel про це подбали: у самих останніх платформах (Skylake, чипсети 100 серії, Intel ME 11.x) ME-контролер має архітектуру... x86! У чипсетах тепер живе ще один x86.

Втім, состав компонентів підсистеми Intel ME (з версії 2.0) не змінювався. Це:

1. **ME-контролер** – убудований у чипсет 32-розрядний мікроконтролер типу RISC, що має внутрішні ROM і SRAM.

2. **Регіон ME в SPI флеш-пам'яті**, у якому зберігається розроблена й підписана компанією Intel прошивання ME-контролера (тому, саме Intel ME firmware).

3. **ME UMA** – схована від усіх, крім ME-контролера, область (16 – 32 МБ) в оперативній пам'яті комп'ютера, який він користується в якості runtime-memory для розміщення й запуску прошивання.

4. **Management Engine Interface (MEI)**, раніше відомий як **Host Embedded Controller Interface (HECI)**, – набір регістрів у конфігураційному просторі PCI і область в MMIO, що представляють собою інтерфейс для обміну інформацією з ME-контролером (по суті, єдиний канал зв'язку софта, що виконується на CPU, з підсистемою Intel ME).

5. **Окремий MAC** – контролер канального рівня, що надає ME-контролеру out-of-band доступ до загального фізичного мережного інтерфейсу для віддаленого адміністрування комп'ютерною системою.

6. **Деякі модулі в BIOS**, відповідальні за ініціалізацію платформи й, що повідомляють про результати своєї роботи ME-контролеру через MEI.

У випадку наявності шильдика Intel vPro, до складу підсистеми Intel ME додатково входить BIOS-модуль ME **BIOS Extenstion (MEBx)**, що надає графічний інтерфейс (показаний вище), а також здійснююче включення й конфігурування AMT через MEI.

Таким чином, у нас є середовище виконання ring -3 (так її умовно називають) – 1 штука. Її привілейованість обумовлює здатностями, якими наділений ME-контролер (про їх написане вище), а скритність – повною відсутністю можливості контролювати програмними (і навіть апаратними, в production-версіях плат) засобами.

Архітектура ME-контролера

Усередині ME-контролера, крім мікропроцесора ARC / SPARC / x86:

– ME ROM – енергонезалежна неперезаписувати^ся память, що, у якій зберігається стартовий код ME-контролера;

– ME SRAM – оперативна пам'ять використовувана ME-контролером при неприступності ME UMA, наприклад, на ранніх етапах роботи;

– кеш коду й кеш даних, для підвищення продуктивності при роботі з пам'яттю;

– C-Link (Controller Link) – шина, що дозволяє ME-контролеру взаємодіяти з периферійним апаратним забезпеченням у режимах S5 (System shutdown) / S3 (Sleep mode);

Різні апаратні блоки:

– високоточний таймер і WDT;
– контролер переривань;
– контролери пам'яті й DMA;
– інтерфейс HECI / MEI;
– RNG, акселлератор криптографічних функцій і функцій стиску.

Самий час розібратися в тому, як від модифікацій захищений код, що управляє всім цим багатством.

Прошивання Intel ME

Intel ME firmware, залежно від наповнення, розрізняють двох типів:

– 1.5 МБ, урізані версії;
– 5 МБ, повні версії.

Тип прошивання визначає состав прикладних модулів, у яких реалізовані певні технології (наприклад, AMT, IPT і т.д.). Хоча є й базова частина, однакова для різних прошивань:

– Bring Up, перший запускати^ся модуль, що, із прошивання.
– Kernel, ядро OCPB Thread.
– Деякі драйвери й служби.

В SPI флеш-пам'яті є кілька регіонів:

– Flash Descriptors, у якому зберігаються покажчики на всі інші регіони, а також read / write привілею для користувачів цієї пам'яті. Відзначимо, що звичайно цими дескрипторами забороняється перезапис ME регіону всім, за винятком самого ME-контролера;
– Gb (Gigabit Ethernet);
– ME, тут зберігається прошивання ME-контролера;
– BIOS;
– 3PDS (Third Party Data Storage), опціональний регіон.

Тепер глянемо на сам регіон ME. Це Flash Partition Table (FPT) – таблиця розділів ME firmware. У ній зберігаються покажчики на різного типу (код, дані, віртуальна область, ...) розділи і їхні параметри. Цілісність цієї таблиці контролюється одним байтом чексумми по зсуву 1Bh.

Нас цікавлять executable-розділи, тобто ті, що зберігають здійсненний код. Їх звичайно трохи, розглянемо один з них.

На початку кодового розділу розташовується маніфест, що складається із заголовка (зі службовими даними й ЕЦП) і таблиці модулів.

У наведеному дампі можна побачити 2048-бітний відкритий RSA ключ (модуль за зсувом 80h відносно початку розділу й експонента за зсувом 180h). Далі треба 256 байт сигнатури.

Своїм закритим ключем компанія Intel підписує частина заголовка маніфесту й таблицю модулів, прикладаючи отриманий підпис і відкритий ключ для перевірки.

А от і фрагмент таблиці модулів розглянутого розділу. Ця таблиця містить заголовки модулів, де зазначені деякі параметри й хеш-сума SHA256 (за зсувом 14h усередині заголовка).

Згенерувати власну пару ключів RSA-2048 і підписати ними розділ не вийде через те, що цілісність прикладеного відкритого ключа перевіряється стартовим кодом в ME ROM, у якому зберігається хеш-сума SHA256 відкритого ключа компанії Intel.

Цього цілком достатньо для захисту прошивання від підроблення. Програмно перезаписати ME регіон SPI флеш-пам'яті не можна (пам'ятаємо про дозволи в Flash Descriptors), апаратні засоби, звичайно дозволять обійти це обмеження, але контроль дійсності не виключити.

Подивимося убік захисту від бінарних уразливостей.

Ми побачили, що весь здійсненний код ME firmware розбитий на модулі різного призначення.

В ME-контролера є два режими роботи: привілейовані й користувальницький (аналоги kernel mode і user mode для CPU). Привілейований режим відрізняє, насамперед, можливість доступу до апаратних ресурсів і можливість обігу по адресах поза відведеним цим модулем діапазону пам'яті.

Кожний модуль запускається й працює в заданому (у заголовку цього модуля) режимі.

Распарсив весь ME регіон можна побачити, що привілейований режим використовується ядром OCPB і деякими драверами. Службам і прикладними модулям, як і покладено, приділяється тільки користувальницький режим.

Ми показали, що підсистема Intel ME є невід'ємною частиною архітектури сучасних комп'ютерних платформ (на основі чипсетів / SoC Intel). Очевидно, що її компрометація надає потенційному зловмисникові безмежні можливості контролю над платформою: доступ

до всього вмісту оперативної пам'яті (системна пам'ять, пам'ять гіпервізора, SMRAM, ACRAM, виділювана пам'ять для графічного ядра – GFX UMA), out-of-band доступ до мережного інтерфейсу (моніторинг усього мережного трафіку), віддалений контроль як частина штатної функціональності AMT, перезапис будь-яких регіонів SPI флеш-пам'яті. Бонусом до цього є повна відсутність можливостей виявлення.

Це є вагомою причиною для наявності в Intel ME серйозного захисту. Ми вважаємо, що вендори будь-якого мережного встаткування, що вбудовується, повинні прагнути до описаної моделі безпеки. Її характеризують наступні принципи:

– заборона на використання дефолтного пароля, примус до установки сильного пароля (відповідного певним вимогам);

– використання функцій шифрування в мережних протоколах;

– контроль цілісності й дійсності всього здійсненного коду прошивання;

– механізми захисту від експлуатації бінарних уразливостей.

Заздалегідь прокоментую можливі заклики використовувати комп'ютерні платформи на основі CPU і чипсетів від AMD: у них є дуже схожа технологія, називається Platform Security Processor (PSP). Представлена не дуже давно, в 2013 році.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів віддаленого контролю на основі технології Intel ME. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем віддаленого контролю на основі технології Intel ME.

– Досліджена система віддаленого контролю на основі технології Intel ME.

– На основі отриманих результатів досліджень створена програмна реалізація системи віддаленого контролю на основі технології Intel ME. Розроблені алгоритми дозволяють успішно вирішувати завдання віддаленого контролю на основі технології Intel ME. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». Cybersecurity Defensive Walls in Edge Computing, 2025. pp. 21-61.
2. Вінтенко, Б.Ю., Миронець, І.В., Смірнов, О.А., Коваленко, О.В., Усік, П.С., Буравченко, К.О., Лисенко, І.А. «Логіко-структурна модель комп'ютерно-орієнтованої процедури системи підтримки оперативного персоналу АЕС». Кібербезпека: освіта, наука, техніка. 2025. Том 2 № 30. С. 413-427, 2025.
3. Смірнова, Т.В. «Дослідження методів, моделей та сучасних ІТ-рішень для підтримки технологічних процесів у критичній інфраструктурі держави». Кібербезпека: освіта, наука, техніка. 2025. Том 2 № 30. С.195-208, 2025.
4. Вінтенко Б., Смірнов О., Миронець І., Смірнова Т., Смірнов С. «Імітаційна модель шляхів вхідних даних комп'ютерної інтелектуальної системи підтримки оператора енергоблоку АЕС». Комбінаторні конфігурації та їхні застосування: Матеріали XXVII Міжнародного науково-практичного семінару, присвяченого 125-річчю Національного університету «Запорізька політехніка» (Запоріжжя-Кропивницький-Київ, 4-6 червня 2025 р.). Запоріжжя: НУ «Запорізька політехніка», 2025. С.82-91.
5. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details». International Review on Modelling and Simulations 18 (1), 2025. pp. 32-42.
6. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В., Коваленко О.В., Мацуй А.М. «Модель шляхів отримання вхідних даних комп'ютерної інтелектуальної системи підтримки оперативного персоналу АЕС». Центральноукраїнський науковий вісник. Технічні науки. 2025. Вип. 11(42), ч. II. С.52-62.
7. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В. «Методи забезпечення відмовостійкості інтелектуальних систем підтримки оператора». VIII міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології", м. Кропивницький. 24-25 квітня 2025 р. – Кропивницький: ЦНТУ. – 2025. – С. 44-46.
8. Смірнов, О.А., Константинова, Л.В., Конопліцька-Слободенюк, О.К., Козірова, Н.В, Якименко, Н.М., Доренський, О.П., Буравченко, К.О. «Дослідження інструментів штучного інтелекту для роботи з базами

даних та аналізу даних». Кібербезпека: освіта, наука, техніка. 2025. №3(27), С. 429–448.)
9. Smirnov O., Fedorov E., Neskorodieva A., Neskorodieva T. «Intellectual Classification method of Gymnastic Elements Based on Combinations of Descriptive and Generative Approache». CEUR Workshop Proceedings Volume 3664, 2024, Pages 11-23.
10. Вінтенко, Б., Миронець, І., Смірнов, О., Коваленко, А., Конопліцька-Слободенюк, О., Смірнова, Т., Константинова, Л. «Дослідження застосування систем підтримки оперативного персоналу об'єкту критичної інфраструктури при керуванні енергоблоком АЕС з реактором типу ВВЕР-1000». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 6-26.
11. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
12. Kuznetsov O., Ilchenko O., Kryvinska N., Buravchenko K., Smirnov O., Savchenko Iu. «An Empirical Assessment of Leading Blockchain Financial Services». 2023 IEEE 1st Ukrainian Distributed Ledger Technology Forum (UADLTF), Kyiv, Ukraine, 2023, pp. 1-6,
13. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.
14. Malyukov V., Bebeshko B., Lakhno V., Smirnov O., Malyukova I., Mohylnyi H. «Managing the Purchase-Sale Process of Digital Currencies Under Fuzzy Conditions». Lecture Notes in Networks and Systems, 2023, 729 LNNS, pp. 104–112.
15. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
16. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
17. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
18. Вінтенко Б.Ю., Смірнов О.А., Коваленко А.С., Смірнов С.А., Буравченко К.О. «Дослідження вимог міжнародних стандартів IEC60880 та IEC62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 3(73), С. 155-166.
19. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
20. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 2(72), С. 170-178.
21. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
22. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А. «Дослідження нормативної документації та стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». VI міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології", м. Кропивницький. 20-21 квітня 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 35-36.
23. Smirnov, O., Karapetyan, A., Fedorov, E., «Creating Neural Network and Single Solution Human-Based Metaheuristic Methods of Solving the Traveling Salesman Problem». CEUR Workshop Proceedings, Volume 3312, 2022, pp. 47-58.
24. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. https://doi.org/10.1007/s42979-021-00739-w.
25. Smirnov O., Kovalenko O., Kovalenko A., Kavun S. «Quantitative Risk Assessment Method Development in the Context of the SDLC-model». 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 203-208, doi: 10.1109/PICST54195.2021.9772143
26. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
27. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
28. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
29. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based

pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.

30. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». International Journal of Computer Network and Information Security (IJCNIS). Vol. 12, No. 3, 2020. PP.33-43.
31. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.