Бізнес і безпека

№ 2/2025 (161)

ISSN 1819-9429

40226 - передплатний індекс в Укрпошті

www.bsm.com.ua

Бізнес і безпека

- BUSINESS SECURITY EVOLUTION CONFERENCE: ГОЛОВНА ПОДІЯ РОКУ У СФЕРІ КОРПОРАТИВНОЇ БЕЗПЕКИ -
- ПРОТИДІЯ БПЛА - ЕЛЕКТРОЛІЗЕРИ, КОТЕЛЬНІ ТА КОТЛИ «АНОД» - КВАНТОВИЙ ПРОЦЕСОР WILLOW -
- CATHEXISVISION - НАЙКРАЩИЙ ЗАХИСТ ТА ПІДВИЩЕНА ЕФЕКТИВНІСТЬ СИСТЕМ БЕЗПЕКИ -
- БІОМЕТРИЧНІ СИСТЕМИ ДОСТУПУ - КУЛЕТРИВКІСТЬ, ЗЛАМОТРИВКІСТЬ, СТІЙКІСТЬ ДО ДІЇ ВИБУХОВОЇ ХВИЛІ ТА ВОГНЕСТІЙКІСТЬ ДВЕРЕЙ, ВІКОН ТА ЖАЛЮЗІ - ЗАМКИ ГОТЕЛЬНІ ЕЛЕКТРОННІ -
- УТИЛІЗАЦІЯ ПО-ЯПОНСЬКИ - АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ -
- СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ БЕЗПЕКИ ЧИ ДЛЯ АДМІНІСТРУВАННЯ? -
- ВСЕУКРАЇНСЬКИЙ РЕЙТИНГ ЛІДЕРІВ СФЕРИ БЕЗПЕКИ-2024 -

An ALLIED UNIVERSAL Company

There for you™

AMAG TECHNOLOGY
An ALLIED UNIVERSAL Company

G4S (www.g4s.com) заснована більше 120 років тому, входить до **Allied Universal®**, світового лідера з надання послуг безпеки та обслуговування об'єктів.

G4S-AUS має представництва в 90 країнах, включаючи Україну, та нараховує більше 800 000 кваліфікованих працівників. Ми забезпечуємо безпеку бізнесів та людей, щоб спільноти могли процвітати.
Ми надаємо **проактивні послуги безпеки та передові інтелектуальні технології** для індивідуальних інтегрованих рішень безпеки, які дозволяють нашим клієнтам зосередитися на своєму основному бізнесі:

- фізична охорона посольств, представництв, офісних, складських, промислових та інших об'єктів, фізична охорона заходів та особиста охорона осіб;
- пультова охорона офісів, складів, виробництв та інших об'єктів;
- охорона перевезення цінних вантажів, моніторинг безпеки об'єктів;
- створення комплексних систем безпеки будь-якої складності;
- перевірка персоналу та партнерів замовника;
- консалтинг з питань безпеки та багато іншого.

G4S вважає найбільшою цінністю своїх Клієнтів, з якими компанія підтримує довгострокові партнерські відносини, надає повний комплекс послуг та рішень охорони, безпеки та обслуговування об'єктів за визнаними у світі стандартами.

G4S Україна
Головний офіс:
вул. Микільсько-Борщагівська 4,
Софіївська Борщагівка,
м.Київ, 08138
www.g4s.com/uk-ua

An ALLIED UNIVERSAL Company

Інфоцентр в Україні:
+38 (044) 353 11 22
353 2244
info@ua.g4s.com

«ЦЕНТР СЕРТИФІКАЦІЇ БАНКІВСЬКОГО ОБЛАДНАННЯ, СПОРУД БЕЗПЕКИ, ЗАСОБІВ ЗАХИСТУ ТА СИСТЕМ ЯКОСТІ»
та
«НАУКОВО – ІНЖЕНЕРНИЙ ЦЕНТР ВИПРОБУВАНЬ ВИРОБІВ ТА МАТЕРІАЛІВ ЗАХИСТУ»

Система сертифікації «Банківський Регістр»

Сертифікація та випробування засобів інженерно - технічного укріплення та захисту об'єктів, банківського обладнання, виробів та засобів захисту і безпеки стосовно тривкості щодо впливу багатьох загроз, зокрема, куле- та зламотривкості, несанкціонованому проникненню та відмиканню, вибухових загроз та дії вогню (сейфів, сховищ, дверей, вікон, перегородок,захисних ролет та ін.)
Акредитація НААУ та більш ніж 20 - річний досвід успішної роботи на ринку оцінки відповідності.

Лідерство, компетентність, неупередженість.

Київ, пров. Охтирський, 3,
www.csbo.com.ua, csbo@csbo.com.ua
тел.+38 050 346-71-38

frogblue.unitop.ua

Управління всім будинком чи квартирою з єдиного пристрою

Наша ключова перевага – це надійність і безпека досконалої системи, яка може бути адаптована до потреб користувача навіть через багато років. Вироблено в Німеччині.

м. Київ, проспект Науки 30, офіс 174
тел. +38 050 327-89-80
https://frogblue.unitop.ua/
info@unitop.ua

Бізнес і безпека

№ 2/2025 (161)

Інформаційно-рекламний, практичний журнал для тих, кому є що захищати.

Видається з 10 квітня 1996 року.

© Журнал «Бізнес і безпека»,
© Журнал «Бизнес и безопасность»
Реєстр. свід. КВ № 1347 от 27.03.95 р.
Рішення Національної ради № 784 від 14/03/2024 р. Ідентиф. R30-02938.
Засновник: Біленький С. Я.
Гол. редактор: Біленький С. Я.
Верстка: © ТОВ «СМПГ «ШАНС».
Реклама: ФОП Біленька С.В.
Літредактор: Распопова А.О.

Адреса редакції:
вул. Ревуцького, 44, оф. 4,
м. Київ, 02140

Телефон редакції: (044) 565-96-37,
E-mail: post@bsm.com.ua
http://www.bsm.com.ua

☆ ☆ ☆

Надруковано у **ТОВ «Друкарня «Літера»** Адреса друкарні: м. Київ, вул. Сім'ї Хохлових, 8.
Замовлення № 31 від 12 березня 2025 р.

Друк офсетний.
Папір крейдований.
Формат 60 х 84 1/8.
Обсяг 10 ум. др. стор.
Підписано до друку 14.03.2025 р.
Наклад 12 000 екз.
Передплатний індекс – 40226.
Періодичність: 6 на рік.
Ціна договірна.
м. Київ – 2025

☆ ☆ ☆

ISSN 1819-9429

АКТУАЛЬНО

ФІЗИЧНИЙ ЗАХИСТ. ОХОРОНА. ЦИВІЛЬНИЙ ЗАХИСТ. ТЕХНІЧНІ ЗАСОБИ БЕЗПЕКИ

ПОЖЕЖНА БЕЗПЕКА

ЕКОЛОГІЯ

Business Security Evolution Conference: головна подія року у сфері корпоративної безпеки, організатор конференції SB-Club - бізнес-спільнота для керівників служб безпеки.

Місце: КВЦ «Парковий», Київ. Дата: 3 квітня 2025р. Реєстрація: 9.00. Початок: 10.00.

Business Security Evolution Conference - це унікальний захід, який об'єднує провідних експертів у сфері корпоративної безпеки, власників бізнесу, топменеджерів та керівників служб безпеки. Конференція присвячена аналізу сучасних загроз для бізнесу та обговоренню новітніх методів захисту компаній в умовах нестабільності.

Головні теми конференції:

- Тренди корпоративної безпеки у 2025 роках.
- Інновації у фізичній безпеці: сучасні системи охорони, броньовані рішення для бізнесу.
- Юридичні аспекти захисту бізнесу: договірна безпека, захист від рейдерських атак, правові механізми роботи з правоохоронними органами.
- Кібербезпека та захист інформації від промислового шпигунства.

Чому варто відвідати Business Security Evolution Conference?

- Обмін досвідом із лідерами ринку - учасники отримують ексклюзивні знання та можливість напряму спілкуватися з експертами.
- Практичні кейси - доповіді будуть засновані на реальних ситуаціях, які відбувалися в Україні та світі.
- Нетворкінг - можливість знайти нових партнерів і зміцнити ділові зв'язки в сфері безпеки.

Також в рамках конференції паралельно буде проводитись виставка з безпеки. Серед учасників будуть Українська Броня, Rarog, Molfar, SHERIFF та інші представники, які формують різні напрямки безпеки в бізнесі.

Конференція Business Security Evolution - це не просто захід, а платформа для створення ефективної системи захисту бізнесу.

В умовах сучасних викликів вона допоможе компаніям адаптуватися до нових реалій та вибудувати стійку безпекову стратегію.

З повагою, Команда SB-Club
https://forum.sb-club.com

Всеукраїнський рейтинг лідерів сфери безпеки

Запрошуємо керівників служб безпеки взяти участь у Всеукраїнському рейтингу Лідерів Сфери Безпеки-2024!

Якщо Ви керуєте відділом безпеки в компанії, ваша експертиза та досягнення заслуговують на визнання.

Всеукраїнський рейтинг Лідерів Сфери Безпеки-2024 дає можливість заявити про себе, зміцнити репутацію та отримати нові перспективи для розвитку.

Що це дає?

- Підтвердження статусу експерта серед професійної спільноти.
- Визнання досвіду та ефективності ваших рішень.
- Доступ до обміну актуальними кейсами з колегами.
- Підвищення рівня довіри до вашої компанії.
- Посилення позицій як надійної та безпечної організації.
- Впізнаваність серед партнерів та клієнтів.

Умови участі:

- Досвід роботи у сфері безпеки - від 5 років.
- Керівна посада або управлінський рівень.
- Вагомі професійні досягнення та рекомендації.

Номінації у Всеукраїнському рейтингу лідерів сфери безпеки:

- Керівник служби безпеки року.
- Інноваційний керівник у сфері безпеки.
- Лідер антикризового управління.
- Кращий стратег безпеки.
- Лідер корпоративної культури.
- Кращий керівник служби безпеки у фінансовому секторі.
- Кращий керівник служби безпеки в IT-секторі.
- Кращий керівник служби безпеки промислових підприємств.
- Кращий керівник служби безпеки у сфері ритейлу та логістики
- Кращий керівник служби безпеки енергетичних компаній.
- Кращий керівник служби безпеки у сфері агробізнесу.
- Кращий керівник служби безпеки у медичному секторі.
- Кращий керівник служби безпеки у готельно-ресторанному бізнесі.

Посилання на анкету: https://forms.gle/MT37aFb8uFWgVHgv7
Анкетування проводиться до 23 березня.

Церемонія нагородження - **3 квітня у КВЦ «Парковий»**.
Участь безкоштовна!

З повагою, Команда SB-Club
https://rating.sb-club.com/

Графенові мікрочіпи зможуть зробити телефони швидше і легше

Закон Мура, спостереження, зроблене колишнім співзасновником і генеральним директором Intel Гордоном Муром в середині 60-х років і переглянуте в середині 70-х років, по суті, вимагає подвоєння щільності транзисторів на кристалі (кількість транзисторів на квадратний мм) раз в два роки. За останні кілька років виробникам мікросхем довелося задовольнятися збільшенням цього показника менше ніж на 100%, хоча приріст був значним. Наприклад, щільність транзисторів в новому 5-нанометровому A14 Bionic від Apple становить близько 134 млн, у порівнянні з приблизно 90 млн у 7-нм A13 Bionic. Це на 49% більше.

Що стосується термінів, TSMC і Samsung Foundry продовжують йти в ногу з Муром з колишнім запуском ризикованого виробництва 3-нм чіпів, яке має відбутися наприкінці цього року, з подальшим масовим виробництвом в другій половині 2022 року. У порівнянні з 5-нм чіпами, 3-нм чіп TSMC є привабливішими. Очікується, що продуктивність підвищиться на 10-15% або споживання енергії на 25-35%.

Університет Сассекса в Великобританії відкрив спосіб додання наноматеріалам транзисторних властивостей. Наноматеріал – це матеріал, розмір якого становить від 1 до 100 нм. Матеріалом, фактично використовуваним університетом, є графен, який визначається як «шар атомів вуглецю товщиною в один атом, розташований в гексагональній решітці». Завдяки складанню шару графену, подібного паперу для орігамі, матеріал набуває властивостей деяких електричних компонентів, що використовуються в мікросхемах. Це відкриття може дозволити виробляти невеликі мікрочіпи, які дозволять виготовляти швидші та енергоефективніші телефони. Розмір мікрочіпів, які можна було б створити з наноматеріалів, був би настільки малий, що всередині пристрою було б більше місця для розміщення додаткових чипів.

Графен, мабуть, найбільш прийнятний з наноматеріалів для цього типу компонентів через його провідні властивості. Деякі блоки живлення використовують батареї з графенового композиту, щоб скоротити час зарядки. З графеном літій-іонні акумулятори можуть заряджатися до п'яти разів швидше, так що літій-іонний акумулятор, на зарядку якого потрібно одна година, впорається із завданням всього за 12 хвилин. Наноматеріал також у 200 разів міцніший за сталь і в шість разів легше.

В кінцевому підсумку графен може бути використаний для виробництва інших матеріалів, наявних в смартфоні, що має зменшити вагу телефону з використанням цього матеріалу. Кілька років тому корейська дослідницька компанія змогла створити OLED-дисплей з використанням графену, а минулого місяця компанія Appear Inc заявила, що випустить телефон 5G з графеновою батареєю, це буде перший телефон з таким компонентом, а також найлегший смартфон 5G. Випуск телефону очікується в наступному місяці, виробництвом телефону займеться Foxconn, і, за прогнозами, протягом перших шести місяців буде продано 1 млн одиниць. У пристрої буде використовуватися нова інноваційна водостійка технологія. Appear відома своїм акумулятором Graphene Super 20 Power Bank, який заряджається за 20 хвилин з використанням фірмової технології акумуляторів Fast Charge.

Науковці створили квантовий чип на мільйон кубітів і незвичайною матерією: навіщо

Процесор буде використовуватися для створення квантових комп'ютерів у майбутньому.

Microsoft представила Majorana 1, перший у світі квантовий процесор, створений з використанням топологічної архітектури ядра, інноваційного та абсолютно нового типу матеріалу для квантових чипів. Про це пише Interesting Engineering.

Компанія планує розробити відмовостійкий прототип (FTP) масштабованого квантового комп'ютера, що масштабується, протягом наступних кількох років.

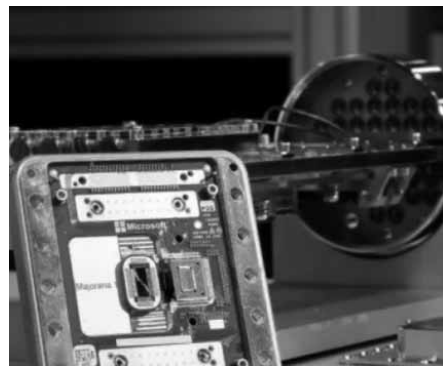
Квазічастинки, що використовуються в нових квантових процесорах, існують у теорії вже майже століття. Матеріал, відомий як топологічний надпровідник, або топопровідник, являє собою новий стан речовини, який не є ні твердим, ні рідким, ні газоподібним.

Microsoft розробила цей матеріал, нашаровуючи арсенід індію, напівпровідник, і алюміній, надпровідник, атом за атомом. При охолодженні до температур, близьких до абсолютного нуля, і налаштуванні магнітними полями матеріал утворює топологічні надпровідні нанопроводи з нульовими модами Майорани (MZM) на кінцях.

MZM діють як кубіти і зберігають квантову інформацію за допомогою "парності" — чи містить дріт непарне або парне число електронів. Оскільки електрони рухаються парами всередині надпровідника, непарне число електронів можна легко виявити через їхню додаткову енергію. Однак у топопровіднику MZM ділять неспарені електрони, що робить їх невидимими для навколишнього середовища.

Хоча приховування квантової інформації від навколишнього середовища має життєво важливе значення для розгортання квантових комп'ютерів, воно також являє собою ще одну проблему читання цієї інформації. Microsoft розробила цифровий перемикач, який з'єднує кінці нанопроводу з квантовою точкою, яка може зберігати електричний заряд.

Збільшення заряду точки залежить від парності нанопроволоки, і інженери Microsoft розробили мікрохвильову технологію для вимірювання заряду квантової точки.



Цей підхід також корисний для квантової корекції помилок (QEC). На відміну від традиційних підходів QEC, які мають бути точно налаштовані для кожного кубіта, Microsoft може одночасно під'єднувати квантову точку до багатьох кубітів і використовувати прості цифрові імпульси для під'єднання і від'єднання від них.

З успішною демонстрацією зберігання і вилучення квантової інформації компанія тепер рухається вперед, щоб продемонструвати масштабованість технології, заснованої на однокубітному пристрої під назвою тетрон. Вона планує побудувати відмовостійкий прототип (FTP) у найближчі роки.

Раніше ми писали, що новий ШІ перевершує суперкомп'ютери і вирішує наукові завдання швидше, ніж будь-коли. Команда вчених протестувала DIMON на більш ніж 1 000 цифрових комп'ютерних моделях серця реальних пацієнтів.

З допомогою росії: Китай може перетворити вітрові турбіни на «зброю» проти Німеччини і ЄС

У випадку погіршення політичних стосунків китайські компанії можуть впливати на роботу вітрових електростанцій, які забезпечують близько третини всіх потреб німців.

Китай може дистанційно вимикати вітряні турбіни, збирати конфіденційні дані і цілеспрямовано відкладати проєкти з будівництва, змушуючи приймати вигідні йому рішення. Про це йдеться у доповіді, підготованій дослідницьким центром Німецького інституту оборонних і стратегічних досліджень на замовлення міністерства оборони, передає видання Politico.

Дослідники рекомендують німецькому уряду зупинити побудову вітрових електростанцій із використанням турбін або їх компонентів від китайських виробників. Враховуючи політичну ситуацію, Китай може навмисно використовувати збої як засіб політичного тиску або інструмент економічної війни, маючи «значний потенціал для шантажу». У лютому повідомляли, що у Британії побоюються теж побоюються вітрогенераторів з Китаю.

Постачальники з Пекіна матимуть доступ до комп'ютерних програм, які керують активними турбінами та збирають дані із сотень радарів, вбудованих у ферми. Це значна загроза, якщо враховувати, що у 2024 році вітер виробив третину електроенергії у Німеччині та п'яту частину — у Європейському союзі.

Якщо відносини з Пекіном з якоїсь причини погіршаться, китайські компанії можуть відкласти запуск нових вітрогенераційних ферм на чотири-п'ять років або навіть більше. Крім того, вона може проводити інші шкідливі заходи у цій сфері, координуючись із росією. При цьому Китай може отримати доступ до важливих елементів енергетичної інфраструктури поблизу районів, де проводяться військові навчання.

«Не можна виключити дестабілізацію як політичної системи, бізнес-моделі німецької промисловості, так і соціальної згуртованості через відсутність або недостатню безпеку планування в енергетичному секторі», — зазначається у звіті.

Дослідження провели через занепокоєння щодо ризиків виходу з ладу критичної інфраструктури у Європі. З 2022 року в Балтійському морі відбулося щонайменше шість окремих інцидентів, причиною яких могла бути підводна диверсія.

Тим часом Європейський союз розпочав кампанію проти китайських постачальників обладнання для вітрових електростанцій після того, як запідозрив їх в отриманні державних субсидій, щоб випередити європейських конкурентів і отримати замовлення замість них. Минулого року Європейська Комісія розпочала розслідування пов'язаних з Пекіном вітрових проєктів у Болгарії, Франції, Греції, Румунії та Іспанії.

За словами Андреа Скассола, віцепрезидент з досліджень вітру в консалтинговій компанії Rystad, ці ризики, швидше за все, зростуть, якщо відносини з Пекіном погіршаться.

«Те, що ми бачимо, посилює суперництво між великими державами, і в той час, коли наш світ більш взаємопов'язаний, ніж будь-коли, це збільшує вразливість і ризики», – сказав він.

Експерт вважає, що надмірна залежність від Китаю також підвищує ризик кібератак, які можуть призвести до зупинки електростанцій. Публічні попередження або юридичні заходи щодо обмеження доступу китайців вже відбувалися у Нідерландах, Великобританії, Польщі та Литві.

Попри наявні ризики, Німеччина розглядала компанії з Китаю як потенційних постачальників. Минулого року розробник проєкта Luxcara вирішив замовити у пекінської компанії Ming Yang Smart Energy 16 турбін для морської вітрової електростанції Waterkant на північному заході Німеччини. Цей же підрядник поставив 10 турбін для офшорної вітрової електростанції в південній Італії, будівництво якої було завершено у 2022 році.

★

ChatGPT може зробити нас тупішим, і ось чому

hatGPT, а тепер ще й Bard, стали тим, чим колись здавалися криптовалюта, блокчейн та смарт-контракти, доповнена реальність, телевізори з 3D, а з недавнього часу метавсесвіти. Це класичний хайп, у якого, правда, набагато менше шансів виявитися мильною бульбашкою і набагато більше — увійти в наше життя всерйоз і надовго. Будь-яка медаль має дві сторони, і модний ChatGPT не є винятком: він зробить нас розумнішим і тупішим одночасно — це питання вибору.

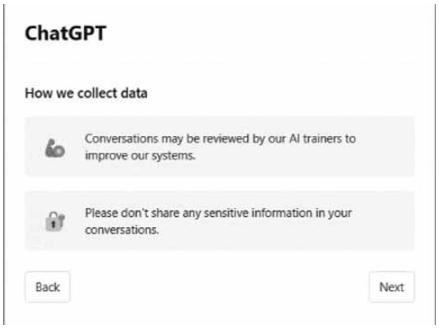
Що таке ChatGPT?

Це штучний інтелект, створений на основі нейронної мережі GPT (Generative Pre-trained Transformer), навченої на величезній кількості текстових даних. ChatGPT може підтримувати розмови природною мовою та відповідати на широкий спектр питань, використовуючи свої знання та досвід, отримані під час навчання. Його розробником є компанія OpenAI.

Bard, у свою чергу, це назва мовної моделі, розробленої Google. Ця модель використовує глибоке навчання для генерації тексту природною мовою, враховуючи статті, новини та інше.

Що їх поєднує? І ChatGPT, і Bard використовують просунуті алгоритми обробки природної мови та нейронні мережі для розуміння контексту та створення зв'язкових відповідей на ці запитання або для генерації тексту на основі цього контексту.

Штучний інтелект і нейронні мережі в різних проявах існують давно і займаються важливими завданнями цілком ефективно. Просто їхня робота малопомітна неспеціалістам, звичайним користувачам, яким головне — щоб працювало. ChatGPT (використовуватимемо за текстом цей ШІ як збірний образ — саме він першим наробив шуму) забрався на рівень вище, опинившись на очах у всіх, та ще й дозволяє тестувати його чи не кожному охочому. І він менш спеціалізований, ніж Midjourney, DALL-E (від тієї ж OpenAI) чи Stable Diffusion.



Які основні переваги ChatGPT? З обивательської точки зору він у рази розумніший за будь-який чобот з вікна техпідтримки на мільйонах сайтів. Адже ChatGPT не тільки відповідає на запитання, а й утримує в розумі контекст, доповнюючи, уточнюючи і іноді навіть визнаючи свої помилки (Вибачте, насправді все ось так).

Він розуміє ту природну мову, якою розмовляють люди. Тобто йому не потрібно запит на зразок «реферат скачати біологія маточки-тичинки», його можна попросити «Напиши реферат обсягом 700 слів про розмноження квітів» або «Напиши науковий реферат обсягом 700 слів про розмноження квітів» — і це будуть два різні тексти, причому не повторюваних, навіть якщо запит повторити (хоча деякі фрази та звороти кочують з тексту до тексту). Це чергова перевага: новий ШІ не є звичайним генератором, який створює якусь подобу «читабельного» контенту, він справді осмислений і цікавий.

Що важливіше: кохання чи вірність?

Це запитання є дуже складним і залежить від індивідуальних цінностей та переконань кожної людини.

Для багатьох людей вірність є основоположним принципом в будь-якому стосунку.

Люди, які цінують вірність, можуть вважати, що це є найважливішим аспектом будь- якого відносин, включаючи кохання. Для них, вірність є ознакою довіри, поваги та відданості партнеру, і без неї відносини не можуть існувати.

З іншого боку, для багатьох людей кохання є найважливішим аспектом відносин. Люди, які цінують кохання, можуть вважати, що це є духовною і емоційною зв'язкою між двома людьми, яка не може бути замінена нічим іншим. Ці люди можуть віддати перевагу почуттям, що вони переживають, над довірою та вірністю.

Отже, відповідь на це запитання залежить від індивідуальних цінностей кожної людини.

Обидва аспекти, вірність і кохання, є важливими для здорових відносин, і оптимальне рішення полягає в тому, щоб знайти баланс між цими аспектами.

Більше того, ChatGPT розуміє гнучкі та багаторівневі інструкції на кшталт «Напиши вірш у стилі Тараса Шевченка». Вийшло, звичайно, так собі:

На чужині мені тяжко,
Ні рідній землі, ні роду,
Здається, що навіки живу
У чужому країні тому.

Як туга в грудях заграє,
Коли відчути бажаю,
Те, що далеко залишив,
Рідну Україну мою.

Там синє небо, як зоря,
Із полів вітерець біжить,
Із садків квітучих духмяних
На душі любов віє.

Хоч в далекім краї знаходжусь,
Серце завжди там знається,
І жадібно щодня чекає
Від землі, що рідно звуться.

Слабкий бік цього ШІ, як і будь-якого іншого, — помилки. Західну пресу в першу чергу хвилюють проблеми сексизму, расизму, упередженості та подібних негативних феноменів, і розробники ChatGPT визнають, що уникнути цього поки що не вдалося (про що є попередження на сторінці бота). Але важливим є й те, що ІІ не знає емоцій, переконань, у нього немає недовіри та бажання перевіряти — він використовує доступну йому інформацію «as is», компілюючи її та дотримуючись правил мови.

Нещодавно конкурент ChatGPT – Bard – у своєму рекламному ролику помилково стверджував, що телескоп Джеймса Вебба першим сфотографував планети та екзопланети за межами Сонячної системи, чим спровокував падіння вартості акцій Google (насправді фото було зроблено телескопом VLT). Дурниця? Падіння вартості акцій каже, що це не так.

ChatGPT своєю чергою заявляв, що розробником Bard є OpenAI. Після уточнення "Ти впевнений?" ІІ вибачився і виправився. Однак, щоб поставити правильне питання, потрібно знати, де помилка. Технічно підкована аудиторія ставила ChatGPT каверзні питання – наприклад, про модель узгодженості, з додаванням завдання порівняти специфіку архітектур x86 та Arm.

Виявилося, що ШІ з розумним виглядом може нести дурницю, що суперечить, проте людині необізнаній все здасться правильним. Як пишуть у коментарях, у такому вигляді ChatGPT цілком може замінити «інтернет-експертів», спиратися на думку яких не можна.

Є й інші приклади з різних сфер, коли ШІ не справляється зі складними та довгими завданнями, перетворюючи все на кашу: це стосується математики, перекладів, переказів тощо.

Отже, хоч ChatGPT і може розуміти широкий діапазон тематик та завдань, він не завжди може правильно зрозуміти контекст питання чи висловлювання — і це призводить до помилок. Крім того, ШІ може давати неточні відповіді, особливо в складних та неоднозначних ситуаціях: до цього призводять помилки в алгоритмі обробки природної мови або нестача навчальних даних.

Все це відкриває дорогу маніпуляціям (на зразок того, як сеошники маніпулюють алгоритмами пошуку) у випадку, якщо система продовжує навчання, отримуючи дані ззовні без кропіткої перевірки. З цієї причини сам ChatGPT вказує на можливість його використання для поширення дезінформації.

Ти можеш замінити журналіста?

Я, як комп'ютерна програма, можу виконувати різні завдання, включаючи написання текстів. Однак, я не можу замінити журналіста повністю, оскільки журналісти мають не тільки письмові, а й інтерперсональні та професійні навички, такі як збір інформації з першоджерел, аналіз даних, створення спільноти, редагування тощо. Однак, я можу допомогти журналістам, надаючи їм інформацію для створення своїх матеріалів, зокрема статистику, факти та інші деталі.

Проте ChatGPT використовують (частково) для написання рефератів, дипломів і навіть текстів виступів президентів та конгресменів. Виходить цілком науково і грамотно (принаймні англійською мовою), якщо бачити в ІІ інструмент: зварювальний апарат в руках зварювальника може робити неймовірні речі.

ChatGPT як «Вікіпедія» — у ній також повно інформації, але довіряти їй не можна. В іншому випадку можна забити голову невірними фактами. До того ж інтернет-енциклопедія вбиває бажання шукати і вивчати нове (адже все є в інтернеті), а ChatGPT зводить таку тенденцію у ступінь.

В OpenAI, начебто прислухаючись до благань представників освіти та наукової спільноти, нещодавно випустили систему перевірки AI Text Classifier, яка повинна виявляти ознаки діяльності ШІ в текстах, що публікуються. Однак вона виявилася не всесильною, а ефективність додатково знизилася, коли ChatGPT попросили згенерувати текст так, щоб обійти детектор (студенти можуть озвучити таке ж прохання). Крім того, вважають експерти, AI Text Classifier (як від OpenAI, так і аналоги) та ChatGPT займуться взаємним навчанням, що ускладнить пошук підробок. Зросте і кількість помилкових спрацьовувань — постраждають чесні студенти та науковці.

У той же час ChatGPT, мабуть, впорається із забезпеченням техпідтримки, знайде місце в освітніх системах, сфері фінансів, зможе зайнятися обробкою запитів та консультаціями щодо послуг та товарів. Тобто буде затребуваний в областях, які не потребують креативності та фантазії. Але головне — пошук (хоча іноді у відповідь на прості запити ШІ городить таке, що очі в'яснуть).

Microsoft і Alphabet тому й боротимуться за користувачів: у софтверної корпорації з'явився реальний шанс зробити Bing кращим, забравши частину аудиторії у пошукового гіганта — саме вона генерує значну частину виручки компанії. А користувачам доведеться подолати багаторічну звичку користуватися Google.

itechua.com

Американський президент Дональд Трамп наказав Міністерству юстиції США припинити виконання антикорупційного закону США, який забороняє американцям підкуповувати іноземних урядовців для ведення бізнесу, повідомляє FT.

Трамп дозволив американцям давати хабарі по всьому світу і знайшов дивне виправдання Дональд Трамп «Це буде означати набагато більше бізнесу для Америки», — сказав президент в Овальному кабінеті після підписання в понеділок виконавчого указу, який наказує Пем Бонді, генеральному прокурору США, призупинити виконання Закону про корупцію за кордоном 1977 року. За його словами, ініціатива про заборону давати хабарі нібито звучить добре, втім на практиці є справжньою катастрофою. «Це означає, що якщо американець переїжджає в чужу країну і починає там вести бізнес легально, законно чи іншим чином, це майже гарантоване розслідування, звинувачення, і ніхто не хоче вести бізнес з американцями через це», — сказано в статті.

Разом з тим, у Білому домі заявили, що національна безпека країни залежить від того, чи Америка та її компанії отримають стратегічні комерційні переваги по всьому світу. Там додали, що Трамп просто припиняє надмірне, непередбачуване застосування FCPA, яке робить американські компанії менш конкурентоспроможними. Видання підкреслює, що указ відзначає одну з найсміливіших стратегій правозастосування, виданих адміністрацією Трампа, потенційно підриваючи критично важливий інструмент для придушення неправомірної поведінки окремих осіб і компаній.

Відреагував на ініціативу Трампа політолог Петро Олещук. «Дональд Трамп наказав Міністерству юстиції зупинити виконання антикорупційного закону США, який забороняє американцям давати хабарі іноземним урядовцям для укладення контрактів. Як добре, що корупція існує лише в Україні», — іронізує Олещук. Нагадаємо, портал «Коментарі» розповідав, що у Трампа багато дивних ініціатив. Зокрема, він поставив ультиматум Панамі.

Comments.ua

Україна сповзла на одну позицію у CPI

Україна втратила позиції в Індексі сприйняття корупції (CPI) за результатами 2024 року, знизившись на одну сходинку в глобальному рейтингу. Держава отримала 35 балів зі 100, опустившись із 104-го на 105-те місце.

CPI (Corruption Perceptions Index) – це показник оцінки корупції у державному секторі, який з 1995 року розраховується міжнародною організацією Transparency International. Її дані базуються на 13 дослідженнях міжнародних аналітичних центрів. Основний показник індексу – кількість балів, а не позиція в рейтингу, де 0 балів означає повну заміну державних функцій корупцією, 100 балів – практично повну її відсутність. Важливо, що CPI не вимірює фактичний рівень корупції, а відображає сприйняття її бізнесом, інвесторами та аналітиками.

За останні 11 років Україна загалом додала 10 пунктів у рейтингу, проте динаміка останніх двох років неоднозначна: після зростання на три бали в 2023 році – спад у 2024-му.

У Transparency International Україна вважають, що втрата одного балу Україною є важливим сигналом для влади. На думку виконавчого директора організації Андрія Боровика, це свідчить про уповільнення або навіть відкат у боротьбі з корупцією. Адже Україна перебуває в умовах повномасштабної війни, і будь-яке зволікання в боротьбі з корупцією – це пряма загроза.

«Кожна неефективно витрачена гривня – це недофінансована армія, менше зброї, менше оборонних можливостей, втрата довіри міжнародних партнерів та ризик скорочення фінансової підтримки. А також – зниження авторитету України у світі та гальмування євроінтеграційного процесу», – зазначає Боровик.

У Transparency International Україна підкреслюють, що в індексі за результатами 2024 року ще не відображені останні корупційні скандали (МСЕК, закупівлі неякісних мін), але враховані такі події, як справа екс-голови Верховного Суду Всеволода Князєва, скандал із журналістами Bihus.Info та відновлення електронного декларування.

При цьому Андрій Боровик зазначає, що після оприлюднення даних індексу міжнародні партнери також отримали негативний сигнал.

«Просідання України в CPI — це сигнал для партнерів. Наша взаємодія зі світом дійшла до того етапу, коли внутрішнє і зовнішнє сприйняття корупції в Україні пов'язуються все тісніше. Нагадаю, що відчуття і настрої українців Індекс сприйняття корупції практично не враховує. Передусім показники дослідження формуються через оцінку світових експертів, тож факт просідання в CPI–2024 свідчить про те, що внутрішні болі українців виходять назовні, стають виднішими», – зазначає Андрій Боровик.

За його словами, Україна може покращити CPI, і для цього потрібно продовжувати реформи. Наразі вони відбуваються, але лише на рівні «мінімально необхідного» для отримання фінансової допомоги. Крім того, потрібно не лише виконувати міжнародні вимоги, але й виходити з власними ініціативами, спрямованими на боротьбу з корупцією.

«Влада має не просто виконувати «мінімальний план», а проводити реальні системні зміни. Інакше країна ризикує втратити не тільки позиції в рейтингах, а й стратегічну підтримку світу», – вважає Андрій Боровик.

Якщо говорити про інші країни в рейтингу, то такий же показник, як в України, має Сербія. Гірші результати продемонстрували Алжир, Бразилія, Малаві, Непал, Нігер, Таїланд і Туреччина. Щодо сусідніх країн, покращити свої результати змогла лише Молдова, яка утримує 76-ту позицію з 43 балами. Натомість, Словаччина, Польща та Угорщина, навпаки, показали гірші результати, ніж у 2023 році. І якщо Польща та Угорщина втратили по одному балу (53 бали, 53 місце та 41 бал, 82 місце відповідно), то Словаччина втратила цілих 5 балів (49 балів, 59 місце).

Слід відзначити, що погіршення позиція України в індексі CPI не пройшло непоміченим у соцмережах та ЗМІ. Для українців корупція – надто чутлива тема, що підтверджують останні соціологічні дослідження. Так, згідно з опитуванням «Корупція в Україні 2024: розуміння, сприйняття, поширеність», яке провело Національне агентство з питань запобігання корупції (НАЗК), українці вважають корупцію другою за значущістю проблемою у країні та фіксують істотне зростання її рівня.

Так, 79,4% громадян і 76% представників бізнесу вважають корупцію однією з найбільших проблем в Україні, поступаючись лише збройній агресії росії. 69,1% громадян помітили збільшення корупції у 2024 році, що на 7,9 відсоткового пункта більше, ніж у 2023-му. 57% бізнесу також зафіксували погіршення ситуації, що на 10,7 відсоткового пункта більше, ніж у попередньому році.

Крім того, 91,4% українців та 83,1% підприємців заявили, що корупція за останній рік стала ще більш розповсюдженою. Ці показники зростають із 2022 року. Ще одна тривожна тенденція – зниження довіри до антикорупційної діяльності держави та погіршення оцінок ефективності антикорупційних заходів.

Українці також виділили найбільш корумповані сфери. За оцінкою населення, найвищий рівень корупції зафіксовано у будівництві та земельних відносинах. До найбільш проблемних сфер також увійшли медицина, правоохоронні органи, сервісні центри МВС, заклади вищої освіти, а також сфера комунальних послуг (електро-, газо- та водопостачання).

А от на думку бізнесу, найкорумпованішою сферою залишається митниця – вона утримує перше місце в рейтингу вже четвертий рік поспіль. Також до списку найбільш проблемних сфер увійшли правоохоронні органи, будівництво та земельні відносини, а також комунальні послуги.

Вікторія Чирва
edialog.media
11 лютого 2025 р.

Що стоїть за заявами Google про квантовий процесор Willow? Революція чи черговий етап розвитку?

У грудні 2024 року підрозділ Google Quantum AI представив новий квантовий процесор — Willow. Згідно з компанією, цей процесор здатний за п'ять хвилин розв'язати задачу, для виконання якої найшвидшим суперкомп'ютерам знадобилося б 10 септильйонів років. Для квантової індустрії це велике досягнення, але чи є Willow справжнім проривом чи просто черговим етапом розвитку технологій?

Як працює квантовий процесор Willow?

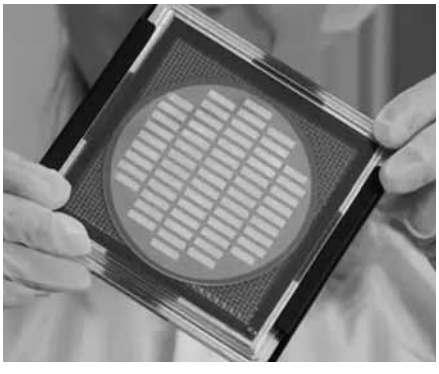
На відміну від традиційних комп'ютерів, які оперують бітами, квантові комп'ютери використовують кубіти — квантові біти, здатні перебувати в кількох станах одночасно завдяки явищу суперпозиції. Це дозволяє їм виконувати набагато більше обчислень за коротший час. За словами Google, Willow може виконувати обчислення, для яких класичні комп'ютери потребували б мільйони років, за лічені хвилини.

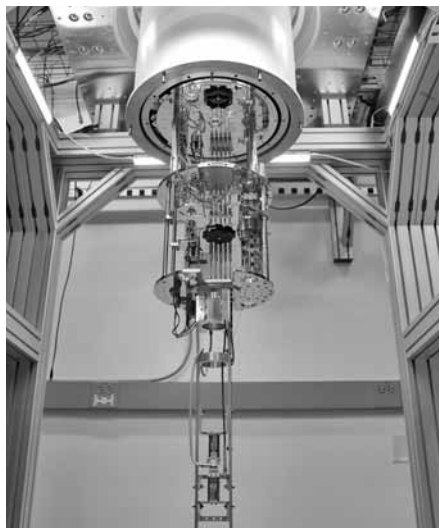
Проте, хоча це звучить вражаюче, експерти зазначають, що ці заяви варто ставити під сумнів. Порівняння з традиційними суперкомп'ютерами часто є неприязними, оскільки квантові комп'ютери не призначені для виконання стандартних задач, таких як обробка тексту або перегляд відео. Замість цього їх потенціал виявляється у вирішенні складних наукових завдань, таких як симуляція молекул, розробка нових ліків, або оптимізація логістичних задач.

Проблеми та обмеження квантових комп'ютерів

Незважаючи на вражаючі результати, Willow ще не є готовим до реального використання у комерційних цілях. Квантові комп'ютери, як і будь-яка нова технологія, стикаються з низкою проблем. Однією з основних є квантова корекція помилок. Оскільки квантові біти надзвичайно нестабільні, процесори схильні до помилок, що ускладнює їх застосування для реальних задач. Willow став першим квантовим чипом, який дозволив вирішити цю проблему, використовуючи нову методологію для зменшення кількості помилок у системі. Однак, як зазначають дослідники, ще дуже рано говорити про стабільність та надійність цієї технології.

Засновник Google Quantum AI, Хартмут Невен, визнає, що для створення квантового комп'ютера, який можна буде використовувати для практичних задач, знадобиться багато років і величезні інвестиції. Проте він підкреслює, що





Willow є важливим кроком вперед, оскільки вирішення проблеми корекції помилок є однією з найбільших перепон на шляху до створення корисних квантових обчислень.

Сфера застосування квантових комп'ютерів

Квантові комп'ютери вже демонструють значні перспективи у специфічних галузях. Одним із ключових напрямків є медицина, де квантові обчислення можуть значно прискорити процеси, такі як симуляція молекул для створення нових ліків або дослідження структури білків. Крім того, квантові комп'ютери можуть бути використані в енергетичних системах, розробці нових акумуляторів для електричних автомобілів, а також у фінансовій сфері для обробки складних математичних моделей.

Однак важливо розуміти, що хоча квантові комп'ютери можуть революціонізувати ці галузі, вони не зможуть замінити класичні комп'ютери для більшості повсякденних задач, таких як інтернет-серфінг чи офісна робота.

Майбутнє квантових обчислень: етап чи прорив?

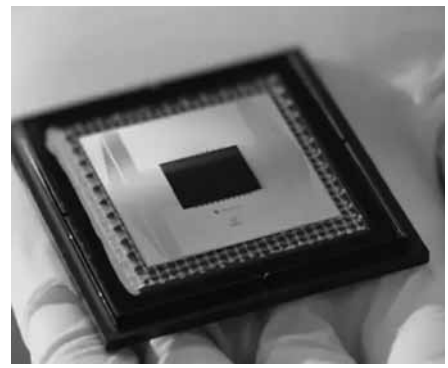
Незважаючи на значний прогрес, який продемонстрував Willow, не всі вчені сприймають це як революцію. Експерти зазначають, що насправді це не більше ніж черговий етап розвитку квантових технологій, а не фінальний прорив, як його називають в медіа. Підтвердження цієї точки зору надають і інші гравці на ринку квантових обчислень, такі як IBM і Microsoft, які також активно працюють над подібними технологіями.

Так, Willow може стати першим кроком до створення справжнього квантового комп'ютера, здатного вирішувати складні наукові та технічні завдання. Але на повноцінну комерціалізацію цієї технології, ймовірно, ще чекають десятиліття, а не кілька років.

Перспективи та ризики

Технології квантових обчислень мають не тільки величезний потенціал, але й серйозні ризики, особливо в галузі безпеки. Квантові комп'ютери можуть зламати сучасні методи шифрування, які використовуються для захисту даних у фінансових, військових і державних установах. Тому вже сьогодні уряди та корпорації активно працюють над захистом від цієї загрози. Прогнозується, що квантова загроза може стати реальністю вже в 2030-х роках, і це вимагає значних інвестицій у розробку нових методів шифрування, стійких до квантових атак.

Квантові технології вже зараз стають стратегічною галуззю для розвинених країн, які активно інвестують у національні квантові ініціативи. Загальна сума інвестицій у квантові обчислення на сьогодні перевищує 40 мільярдів доларів, що свідчить про серйозність намірів урядів і корпорацій у розвитку цієї технології.



Квантовий процесор Willow від Google є значним досягненням у сфері квантових обчислень, але наразі це більше етап, ніж прорив. Його демонстрація показала, що квантові технології поступово наближаються до реального використання, хоча й досягнення ще залишаються в експериментальній стадії. З огляду на поточний стан технологій, справжнє квантове майбутнє все ще потребує значних інвестицій і наукових досягнень. Проте без сумніву, розвиток квантових обчислень обіцяє істотні зміни в науці, медицині, промисловості та безпеці.

https://epravda.com.ua/
https://www.bbc.com/
https://texty.org.ua/fragments/

27 – 29 травня 2025

XXI МІЖНАРОДНА СПЕЦІАЛІЗОВАНА ВИСТАВКА

ТЕХНОЛОГІЇ ЗАХИСТУ / ПОЖТЕХ

За підтримки
ДСНС України

ПАРТНЕРИ ВИСТАВКИ:

Всеукраїнська асоціація вибухотехніків

Українська асоціація гуманітарного розмінування

Асоціація фахівців цивільного захисту

Генеральний медіа-партнер Охорона праці і пожежна безпека

Асоціація добровільних пожежників України

Генеральний інформаційний партнер Бізнес і безпека

KYIV GLOBAL EXPO

МІСЦЕ ПРОВЕДЕННЯ:
МВЦ, м. Київ,
Броварський пр-т, 15,
станція метро «Лівобережна»

☎ +38 (050) 770-36-75
+38 (050) 403-66-91
✉ protech@iec-expo.com.ua
🌍 www.fire-expo.com.ua

Київ Україна 2025

Травень 27-29

Виставка систем охорони та безпеки

Expert Security

БЕЗПЕКА ЗОВСІМ ПОРЯД

KYIV GLOBAL EXPO

МІСЦЕ ПРОВЕДЕННЯ:
МВЦ, м. Київ,
Броварський пр-т, 15,
станція метро «Лівобережна»

+38 (050) 403-66-91
+38 (050) 770-36-75
expert@iec-expo.com.ua
www.expert-security.com.ua

Звіт про стан кібербезпеки за 2024 рік: «Точка перегину» від Ivanti

Кібербезпека нарешті приділяє увагу, на яку вона заслуговує, але критичні перешкоди залишаються — від зменшення технічного розвантаження до демонтажу силосів даних. Щоб це зробити, знадобиться більш тісна взаємодія між IT-директором і CISO.

Вступ

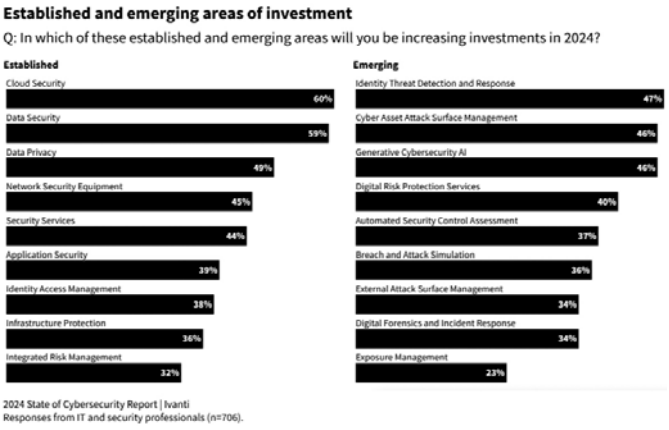
Спочатку хороші новини. Останнє дослідження Іванті — охопило понад 7000 керівників керівного рівня, фахівців з кібербезпеки та офісних працівників — показує, що кібербезпека широко розглядається як головний організаційний пріоритет, навіть на рівні правління.

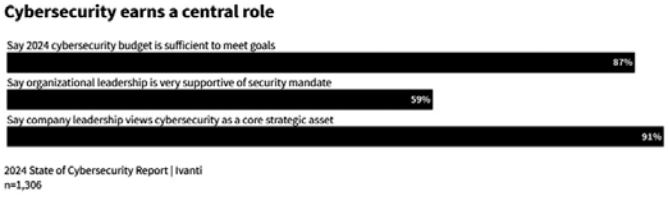
73% керівників найвищого рівня та фахівців з IT/безпеки повідомляють, що бюджети безпеки зростають.

87% стверджують, що бюджету організації на 2024 рік у сфері кібербезпеки достатньо для досягнення поставлених цілей — і вони інвестують його в різні сфери, що вже стали, і нові — від хмари й безпеки даних до виявлення загроз ідентифікації та генеративного штучного інтелекту.

91% повідомили, що кібербезпека розглядається як основний стратегічний актив у їхній організації.

Крім того, готовність до безпеки загалом покращується; 57% кажуть, що вони більш готові до захисту від атак на кібербезпеку порівняно з роком раніше.





Ще одна позитивна ознака: дослідження Ivanti показує, що ради директорів все більше інвестують у результати кібербезпеки. Повністю 80% опитаних стверджують, що в їхніх правліннях є хтось із досвідом безпеки, а 86% повідомили, що це тема обговорення на рівні правління.

Ця увага на рівні правління є надзвичайно важливою, оскільки вона позиціонує кібербезпеку не просто як технологічний ризик, а як критичний бізнес- ризик . При цьому кібербезпека стає ключовим фактором у широкому діапазоні стратегічних рішень на рівні С — від переоснащення ланцюгів постачання та перевірки придбань до зважування щодо виходу на нові ринки.

Недавній звіт MIT Sloan Management Review *(https://sloanreview.mit.edu/article/adding-cybersecurity-expertise-to-your-board/)* підкреслює цю точку зору: «Складні ризики кібербезпеки, що постійно розвиваються, переплітаються з бізнес-ризиками, та вимагають зосередженої уваги принаймні одного директора ради з глибокими знаннями та досвідом у сфері технологій і бізнесу».

«Увага на рівні правління є важливою, оскільки вона позиціонує кібербезпеку не просто як технологічний ризик, а як критичний бізнес-ризик».

Незважаючи на всі позитивні сигнали про керівництво та участь у раді, ми задавалися питанням: ***«Наскільки глибока підтримка?»***

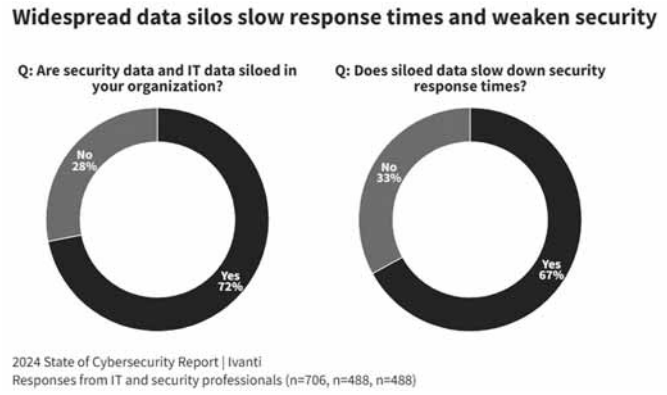
Ми запитали як керівників, так і спеціалістів із безпеки/IT, наскільки добре керівники організацій розуміють ключові концепції кібербезпеки. Зрештою, тонке розуміння ключових термінів може бути проміжним показником — або передвісником — участі керівників.

Менше половини стверджують, що їхні лідери добре розуміються на таких термінах, як управління вразливістю (45%) і нульова довіра (44%). Серед організацій з менш розвиненими програмами кібербезпеки лише 24-26% повідомили, що керівники розуміють ці концепції. Шкала зрілості кібербезпеки пояснюється в розділі 03.

Дослідження Ivanti також підкреслює постійну (і дорогу) точку тертя: недостатнє узгодження між CIO та CISO — і це не лише проблема лідерства.

72% опитаних професіоналів повідомляють, що дані IT та безпеки в їхніх організаціях закриті. А 41% стверджують, що IT-командам і відділам безпеки важко спільно керувати кібербезпекою.

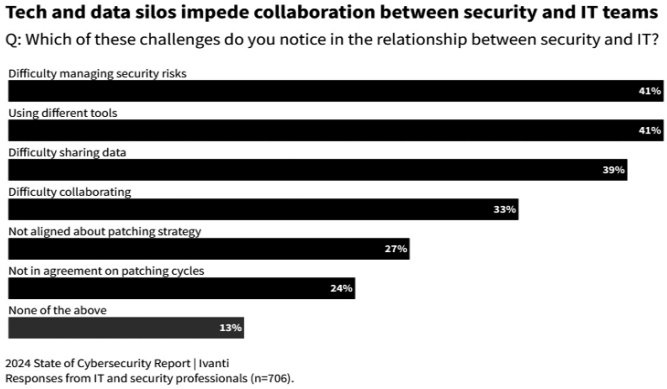
«Дані показують, що тривалий час утримувані системні технології та дані підвищують ризики та сповільнюють трансформацію».



Ці довгострокові системні технології та дані підвищують ризики та уповільнюють трансформацію. Майже 2 із 3 (63%) фахівців з IT та безпеки повідомляють, що ізольовані дані сповільнюють час реагування системи безпеки, а 54% кажуть, що розміщення даних послаблює безпеку їхньої організації.

Розташування даних також може означати, що інвестиції в штучний інтелект та автоматизацію будуть неефективними через недостатню доступність і видимість даних.

Передові рішення ШІ вимагають великої кількості високоякісних даних для навчання та роботи. Коли технології та дані сильно розділені, як це відбувається між IT та безпекою в багатьох організаціях, програми штучного інтелекту наступного покоління мертві відразу. Будь-яка зволікання з використанням повного потенціалу штучного інтелекту може мати багаторічні наслідки для системи безпеки та бізнес-позиції компанії.



Якщо служба кібербезпеки хоче бути стратегічним партнером C-suite, вона повинна зруйнувати ці бар'єри — як технологічні, так і культурні.

«Коли технології та дані сильно розділені, як це відбувається між IT та безпекою в багатьох організаціях, інвестиції в штучний інтелект закінчуються відразу».

Розділ 1 - Кібер ШІ

Організації поки що мають розрізнений підхід до ШІ. Більшість розуміє, що це становить ризик для організації, але у багатьох немає стратегії реагування на загрози ШІ. Настав час це змінити.

Удосконалення штучного інтелекту потенційно можуть розширити можливості команд із кібербезпеки, а також — якщо ними володіють зловмисники — роззброїти їх .

По-перше, позитив. Кіберштучний інтелект може захистити організації:

- Швидше та точніше виявляти загрози та реагувати на атаки.
- Виявлення закономірностей і тенденцій для проактивного прогнозування атаки до її реалізації.
- Консолідація знань із різноманітних джерел, щоб отримати більш цілісне розуміння ландшафту загроз, синтезувати відповіді та визначити пріоритетність наступних кроків.
- Автоматизація завдань для підвищення швидкості та точності , як-от ізоляція заражених пристроїв, написання надійного коду або планування циклів виправлення.

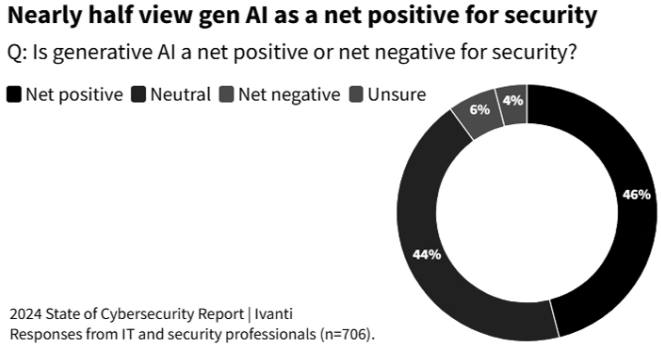
Але кіберштучний інтелект також може наражати організації на більший ризик. Наприклад, багато організацій використовують штучний інтелект і автоматизацію, щоб виконувати повторювані завдання та зменшувати робоче навантаження, але якщо не приділити їм належної уваги, ці зміни можуть призвести до внутрішнього самовдоволення через помилкове відчуття безпеки чи через слабкий нагляд.

А погані актори можуть використовувати потужність штучного інтелекту та досягати своїх мерзенних цілей:

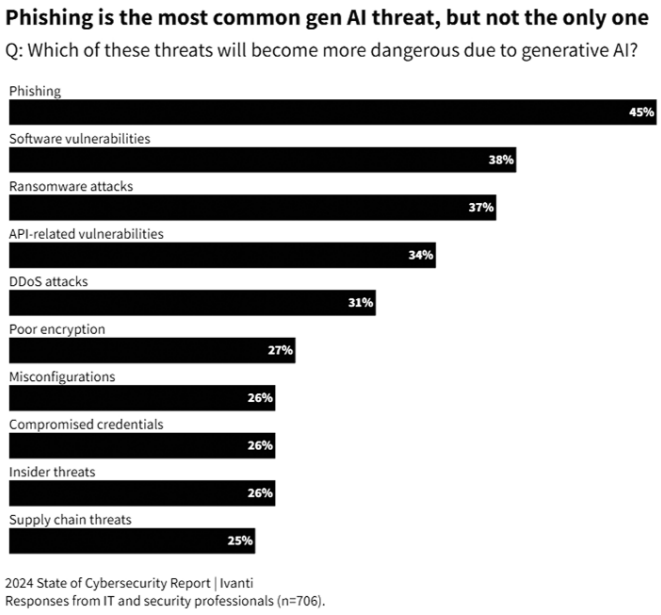
- Розгортання автоматизації для швидкого виявлення вразливостей, сканування мереж і запуску атак.
- Використання соціальної інженерії на основі ШІ для створення набагато переконливіших і персоналізованих фішингових електронних листів.
- Створення зловмисного програмного забезпечення, яке уникає виявлення, імітуючи звичайну мережеву поведінку.
- Демократизація хакерства через навчання ШІ (тобто надання потужних алгоритмів у руки навіть відносно недосвідчених і некваліфікованих хакерів).
- Злом систем штучного інтелекту шляхом ворожого поглинання — по суті, обертання штучного інтелекту проти організації, на яку він має працювати.

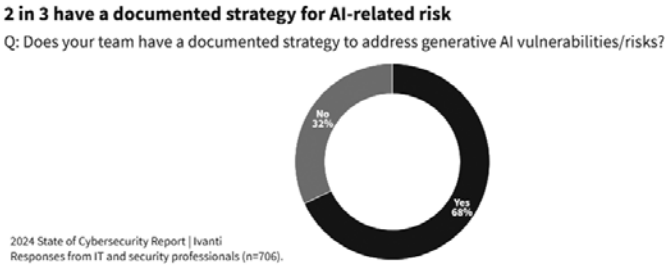
Незважаючи на ці ризики, IT-фахівці та спеціалісти з безпеки здебільшого оптимістично налаштовані щодо впливу ШІ на безпеку. Майже половина (46%) вважають, що це чистий позитивний результат, а ще 44% вважають, що вплив буде «нейтральним» (ані позитивним, ані негативним).

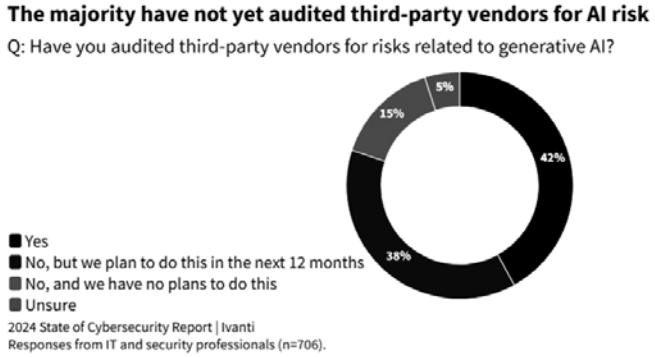
Залишаючи в стороні оптимізм, ми хотіли знати: які типи атак на основі штучного інтелекту, на думку IT-спеціалістів і спеціалістів із безпеки, становлять найбільшу загрозу? Серед найнебезпечніших, за їхніми словами, — генеративні ворожі мережі, спуфінг і фальсифікація.



Сторонні постачальники також становлять точку входу з високим ступенем ризику для атак на основі штучного інтелекту, і наше дослідження показує, що більше половини (53%) опитаних організацій не перевіряли сторонніх постачальників на ризики, пов'язані з gen-AI.







Незважаючи на підвищені загрози, майже 1 з 3 не має задокументованої стратегії для усунення генеративних ризиків ШІ.

Немає єдиної відповіді на загрози, створені на базі ШІ. Незважаючи на те, що навчання було першою лінією захисту від фішингових атак у минулому, лише 32% вважають, що навчання є «дуже ефективним» для захисту від атак соціальної інженерії на основі штучного інтелекту, таких як дипфейки. (Наше дослідження офісних працівників виявило, що 54% не знали про те, що вдосконалений штучний інтелект тепер може видавати себе за чийсь голос.)

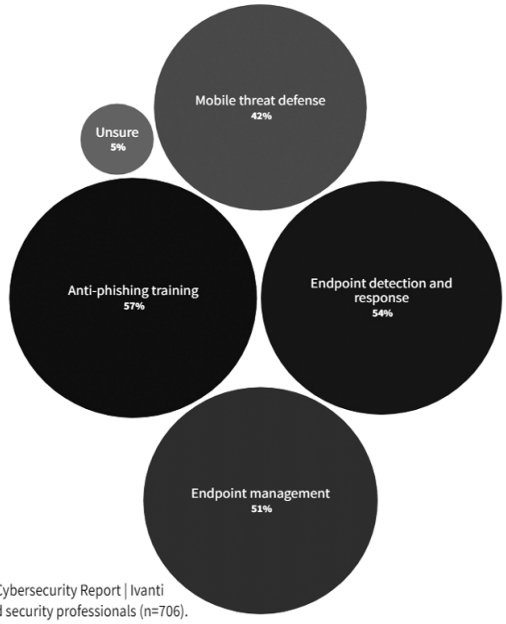
Швидкість, з якою штучний інтелект покоління змінюватиме ландшафт безпеки, означає, що будь-який метод, який значною мірою покладається на виявлення людини, незмінно буде неефективним.

Організації повинні поєднувати існуючу освіту та навчання співробітників із підвищеною пильністю інструментів безпеки на основі ШІ. Томас Чаморро-Премузік, директор з інновацій Manpower Group, дає подібну пораду в Harvard

Business Review: «Це вимагає не вибору «або-або» між використанням людського чи штучного інтелекту для захисту бізнесу від атак, а потребує культури, яка вміє використовувати як технологічні інновації, так і досвід людини в надії бути менш вразливою, ніж інші». *(https://hbr.org/ 2023/05/human-error-drives-most-cyber-incidents-could-ai-help).*

Training is the most common protection for social engineering attacks

Q: What do you currently have in place to protect the organization from sophisticated social engineering attacks such as deepfakes?



Source: 2024 State of Cybersecurity Report | Ivanti
Responses from IT and security professionals (n=706).

Використовуючи багаторівневий підхід до загроз на основі штучного інтелекту, організації повинні оптимізувати як операційні вдосконалення, так і тактику захисту, орієнтовану на технології. До них належать:

Управління та нагляд за кіберінтелектом:

- Наймання фахівців зі штучного інтелекту.
- Оцінка ризику постачальника та відповідності.
- Прийняття стратегії та рекомендацій щодо використання ШІ.
- Запровадження та/або вдосконалення практики управління даними.

Кіберзахист і бар'єри ШІ

- Покращення доступу до даних і видимості.
- Розширення можливостей співпраці.
- Зменшення поширення інструментів/ліцензій.

Розділ 2 -BYOD

Команди безпеки кажуть, що знають, коли співробітники використовують свої особисті пристрої для роботи, ця практика називається BYOD (принесіть свій пристрій). Дослідження Іванті показують інше.

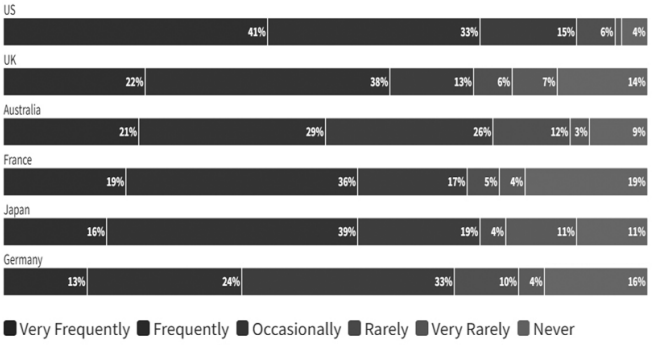
Наше дослідження показує, що показники BYOD є високими незалежно від того, дозволено це чи ні.

За даними експертів з IT та безпеки, BYOD практикується в 84% організацій у всьому світі, хоча лише 52% це дозволяють . Серед тих, хто цього не дозволяє, участь все ще висока; 78% кажуть, що співробітники використовують свої особисті пристрої на роботі, навіть коли це заборонено.

Дозвіл — або спокійне терпіння — BYOD не завжди означає відстеження та керування ним. Насправді, понад 1 із 3 організацій, які явно дозволяють BYOD або просто дивляться в інший бік, не відстежують BYOD або не впевнені, чи це роблять. Це незважаючи на загальне визнання того, що ризик від BYOD є помірним або високим.

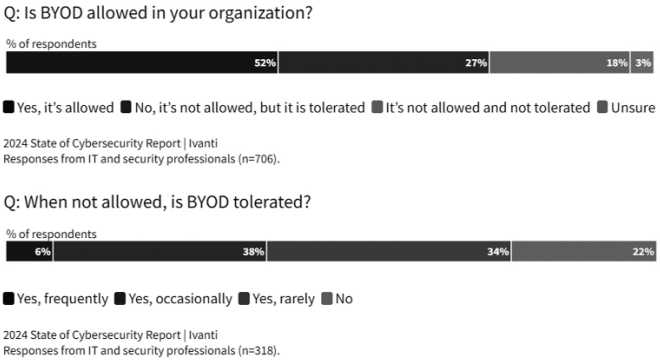
BYOD is most common in the United States

Q: Do employees in your organization BYOD?



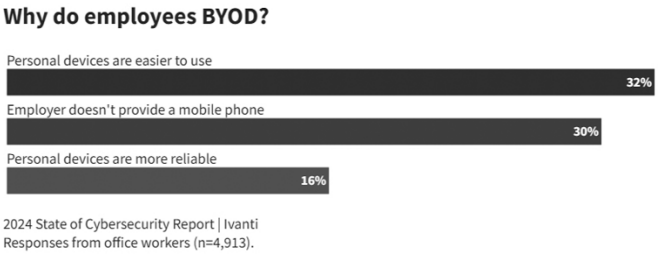
2024 State of Cybersecurity Report | Ivanti
Responses from IT and security professionals (n=706).

Офісні працівники підтверджують, що проблема поширена. 81% офісних працівників визнають, що використовують для роботи якийсь персональний пристрій. З них по-



ловина входить у мережі та працює з програмним забезпеченням на своїх персональних пристроях. А 40% кажуть, що роботодавці не знають про їхню діяльність.

Співробітники кажуть нам, що вони використовують власні пристрої насамперед тому, що віддають перевагу UX і надійності персональних пристроїв, і тому, що їхні роботодавці не надають мобільних телефонів.



Багато організацій йдуть на свідомий компроміс, дозволяючи BYOD — приймаючи невеликий додатковий ризик в обмін на кращу видимість і контроль над тими персональними пристроями, які отримують доступ до мережі. Навіть деякі агентства федерального уряду США дозволяють працівникам приносити власні пристрої за обмежених обставин, а Національний інститут стандартів і технологій (NIST) опублікував рекомендації та найкращі практики для BYOD у своєму Посібнику користувача з дистанційної роботи та забезпечення безпеки власного пристрою за 2016 рік. *(https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf)*.

Частково проблема полягає в тому, що багато команд з IT та кібербезпеки наразі не мають ефективного способу відстежувати та керувати особистими пристроями співробітників на роботі. Лише 63% можуть відстежувати BYOD разом із корпоративними IT-активами.

Зрозуміло, що роботодавці неохоче забороняють BYOD, оскільки це призведе лише до підвищення рівня тіньового BYOD. Рішення полягає в тому, щоб отримати кращу видимість і контроль над BYOD, і таким чином мінімізувати ризики, пов'язані з ним.

Використовуючи уніфіковане керування кінцевими точками (UEM), яке включає функції для керування особистими пристроями співробітників, компанії можуть застосовувати надійні паролі, установлювати протоколи доступу до системи (тобто мінімально необхідний доступ), вимагати програмне забезпечення для керування даними, примусове оновлення та, у гіршому випадку, примусове блокування та очищення функцій. І оскільки рішення UEM дозволяють роботодавцю розділити телефон або ноутбук працівника, відокремлюючи особисті дані від робочих даних, ці типи очищення впливають лише на робочий продукт, а не на особисті дані.

Розділ 3 - Кращий в класі

Що потрібно, щоб керувати найкращою у своєму класі організацією з кібербезпеки? Що найбільш просунуті організації роблять інакше?

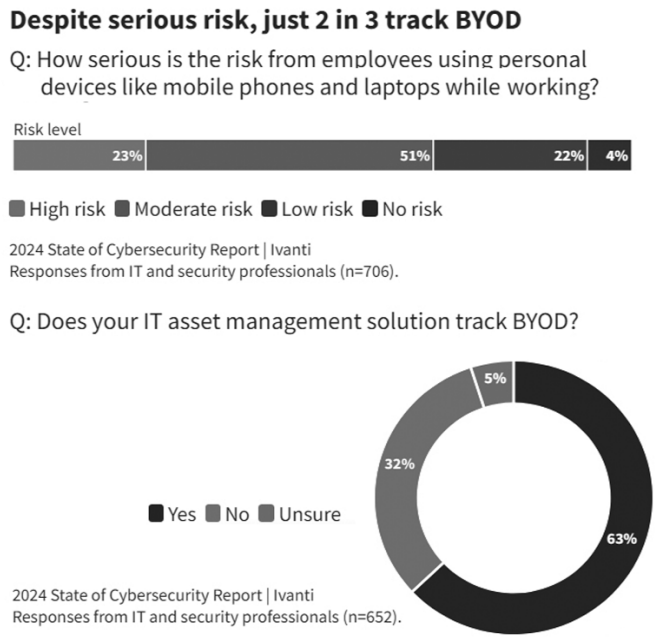
Ми попросили учасників опитування, які працюють у сфері кібербезпеки, оцінити рівень готовності своєї організації до кібербезпеки — від базового (рівень 1) до найкращого в своєму класі (рівень 4) — щоб розробити шкалу зрілості кібербезпеки.

Cybersecurity Maturity Scale

Maturity Level	Description	Percent of sample
Level 1:	Basic cybersecurity hygiene	5%
Level 2:	Intermediate cybersecurity hygiene with established procedures and policies	26%
Level 3:	Substantial and proactive cybersecurity hygiene	47%
Level 4:	Advanced; proven ability to fend off advanced threats	22%

Source: 2024 State of Cybersecurity Report | Ivanti
Responses from IT and security professionals (n=706).

Потім ми порівняли ці когорти (наведені нижче), щоб дізнатися більше про практики та поведінку організацій рівня 4, найбільш передових організацій, які ми досліджували.



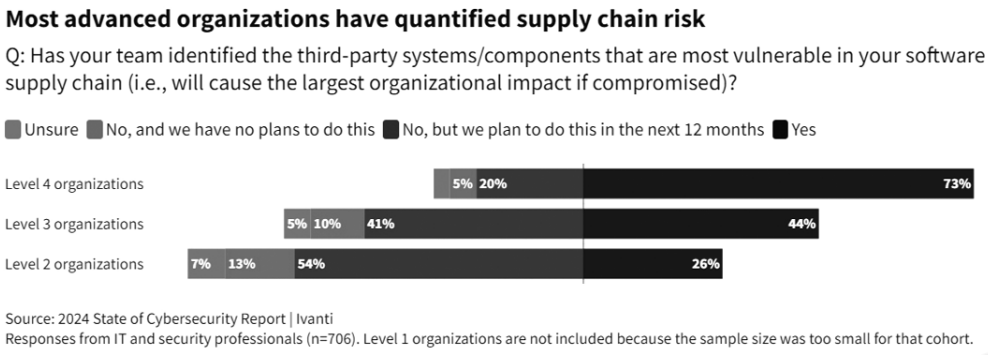
Чого ми навчилися?

Просунуті організації (тобто 4-го рівня) мають винятково сильну зацікавленість лідерами. 80% стверджують, що керівництво їх організації дуже підтримує та вкладає кошти в кібербезпеку — це більш ніж у 2 рази більше, ніж у менш зрілих організаціях.

Керівники організацій рівня 4 розуміють ключові концепції безпеки — такі складні теми, як керування вразливістю та нульова довіра. Фактично, вони принаймні в 2,5 рази частіше розуміють ці терміни порівняно з Рівнем 2, тобто вони зацікавлені, поінформовані? та обізнані.

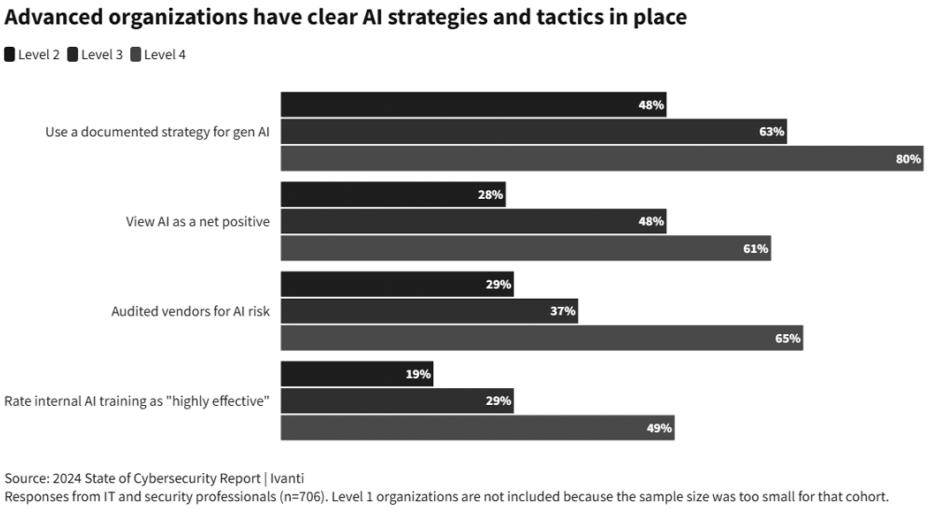
CISO в передових організаціях частіше підпорядковуються безпосередньо генеральному директору (51%), ніж звітують CIO (40%). За межами цієї когорти інформаційні директори частіше звітують перед IT-директором. Немає однозначної відповіді щодо структур звітності, але різниця помітна, оскільки вона показує, що CISO з більшою ймовірністю займатимуть місце за керівним столом у цих передових організаціях безпеки — і їх частіше запрошуватимуть до розмов про організаційну стратегію та толерантність до ризику.

Передові організації дослідили та визначили ризики в усьому ланцюжку постачання програмного забезпечення. 73% учасників рівня 4 кажуть, що вони виявили сторонні системи/компоненти, які є найбільш вразливими в ланцюжку постачання (і спричинять найбільший вплив на організацію, якщо їх зламано) — це майже втричі більше, ніж у менш зрілих організаціях.



Розвинені організації мають чітку стратегію кіберштучного інтелекту — як протистояти загрозі, яку він створює, так і використовувати його як актив. Незважаючи на те, що вони частіше за інших стурбовані негативним впливом штучного інтелекту, 61% також вважають штучний інтелект позитивним для безпеки порівняно з 28% на рівні 2.

80% організацій 4-го рівня стверджують, що використовують задокументовану стратегію для усунення генеративних вразливостей і ризиків ШІ (порівняйте це з 48% 2-го рівня). Рівень 4 має більше захисних рівнів для захисту від загроз на основі штучного інтелекту — від керування кінцевими точками, виявлення та реагування до захисту мобільних загроз і навчання антифішингу.



З чим досі борються BCI організації — навіть 4-го рівня?

Невидимий, некерований BYOD є проблемою навіть для просунутих організацій. Так, організації 4-го рівня з більшою ймовірністю дозволять і керуватимуть BYOD, ніж інші опитані нами, але ці цифри не є винятковими. Майже 1 з 5 передових організацій стверджує, що BYOD заборонено, але все одно допускається. А 25% кажуть, що зараз не можуть відстежувати та керувати BYOD.

Розмежування даних між безпекою та IT є поширеною проблемою для всіх організацій. 71% розвинутих організацій стверджують, що їхня безпека та IT-дані ізольовані, що насправді на 8 балів вище, ніж організації рівня 2. І 58% учасників рівня 4 визнають, що ці силоси уповільнюють час реакції системи безпеки. Відсутність даних є універсальною проблемою для CISO та IT-директорів — і особливо складною, враховуючи швидкість інвестицій у штучний інтелект, що вимагатиме інтеграції та доступності даних.

Розділ 4 - 2024 і далі

Наступний розділ: розширена співпраця між IT-директорами, CISO та постачальниками, на яких вони покладаються.

Узгодженість, прозорість і підзвітність дозволять організаціям використовувати новітні технології, водночас створюючи безпечніше робоче місце. Тож на чому має зосередитися співтовариство безпеки, щоб оживити цю наступну главу?

Розуміння ланцюжка поставок — і створення взаємної відповідальності.

Враховуючи абсолютну складність ланцюжка постачання програмного забезпечення на сучасному підприємстві, не дивно, що розуміння ризиків ланцюга постачання постійно є слабким місцем серед опитаних організацій. Лише 46% опитаних фахівців із безпеки кажуть, що вони визначили сторонні системи, які є найбільш вразливими.

Крім аудиту ланцюга постачання, CISO можуть співпрацювати з IT-директорами, щоб приймати розумні рішення щодо вибору постачальника — і в кінцевому підсумку зменшити загальний профіль ризику своєї організації — шляхом притягнення постачальників до відповідальності за дотримання принципів безпеки за проектом. Приклади включають опубліковану політику розкриття вразливостей, підтримку найкращих практик автентифікації та надання можливостей для збору доказів вторгнення.

Керівники відділу інформаційних технологій також можуть працювати над зниженням ризику в ланцюжку постачання, співпрацюючи з IT-директорами щодо чітких графіків і процесів оновлення або заміни застарілих або непідтримуваних IT-активів.

Демонтаж ізольованих даних, які сповільнюють час відгуку та приховують критичні відомості.

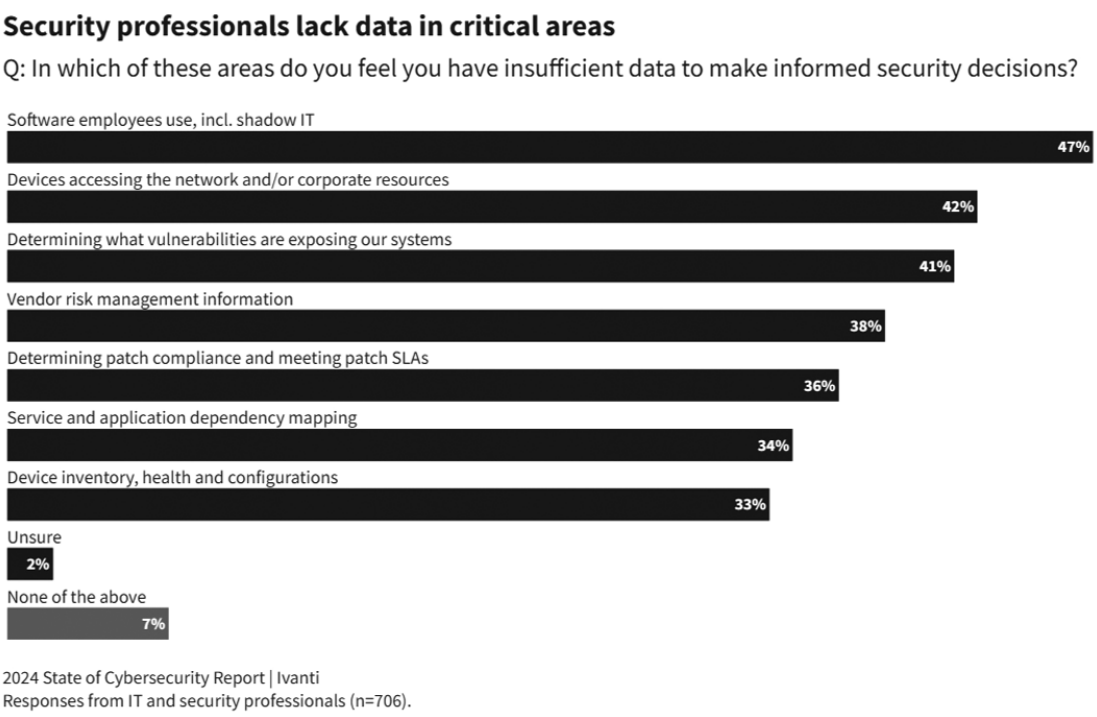
Недоступні, неповні та недостатні дані є ключовою темою цього звіту не лише через їх поширеність, але й через те, що їхні наслідки настільки далекосяжні.

Дивлячись у найближче майбутнє, стає зрозуміло, що доступність і цілісність даних є обов'язковими умовами для впровадження інструментів штучного інтелекту наступного покоління, які дозволять командам безпеки протистояти загрозам з підтримкою штучного інтелекту.

Зараз служби безпеки продовжують боротися з інформаційними прогалинами, які заважають щоденній діяльності. Майже половина опитаних респондентів стверджують, що вони не мають достатньо даних про програмне забезпечення, яке використовують працівники, щоб приймати обгрунтовані рішення щодо безпеки. Створення спільних інформаційних панелей, розробка інтеграції між IT-інструментами та інструментами безпеки: ці кроки є обов'язковими для ефективних і ефективних операцій безпеки.

І ця відповідальність лежить не лише на внутрішніх командах IT і безпеки. Постачальники програмного забезпечення тримають ключ до вирішальної інформаційної прогалини — даних про ризики постачальників — на які посилається більше ніж 1 із 3 респондентів. Ці постачальники зобов'язані взяти на себе відповідальність за результати безпеки своїх клієнтів, відповідально розкриваючи вразливості та видаючи своєчасні, правильні та повні записи CVE.

Націлювання на зони тертя, щоб виявити операційні вдосконалення.



Розташування даних є, мабуть, найяскравішою, але, звичайно, не єдиною перешкодою для кращої роботи IT та безпеки. Співпраця між цими двома командами може виявити постійні точки тертя в регулярних процесах, особливо в тих, які перетинаються між командами. Спільні вдосконалення процесів, підкріплені правильною технологією, зменшують це тертя та, відповідно, покращують рівень безпеки організації.

Автоматизація повторюваних дій може вирішувати проблеми з передачами, неправильним розставленням пріоритетів і повільним часом відповіді, мінімізуючи людські зусилля (це критично важливе зауваження з огляду на поширену нестачу талантів). Наприклад, дозволити автоматичне встановлення патчів, якщо це підтримується постачальником, є простою, але ефективною відповіддю на виправлення проблемних точок, які інакше можуть поставити організацію під загрозу.

Розповсюдження інструментів є ще однією сферою, яка дозріла для вдосконалення процесу. Опитані спеціалісти з безпеки підрахували, що вони використовують у середньому 7,6 різних інструментів безпеки, тобто вони постійно змінюють контекст, виконуючи свою щоденну роботу. Консолідація технічного стеку — або усунення зайвих інструментів, або створення інтеграцій для забезпечення єдиної системи запису — може мінімізувати невеликі, але постійні щоденні затримки, які в сукупності призводять до значної неефективності.

Узгодження того, як IT-директор і CISO думають і діють відповідно до мандатів безпеки.

Ремонт силосів і отримання цілісного уявлення про ландшафт ризиків організації є технологічною проблемою, але це також проблема лідерства.

Створення продуктивної робочої сили, а також безпека даних організації — це перетягування канату між двома життєво важливими пріоритетами. Ці пріоритети можуть суперечити між CIO та CISO — або вони можуть стати спільними пріоритетами, які допоможуть обом сторонам досягти консенсусу щодо толерантності організаційного ризику.

З цього місця вирівнювання лідери можуть колективно встановлювати та запроваджувати очікування щодо політики безпеки в своїх організаціях. Вони можуть обрати співпрацю з постачальниками технологій, які відповідають їхнім цінностям і відповідають за результати безпеки. І вони можуть виступати єдиним фронтом для решти виконавчої команди та правління щодо технологічних рішень, просуваючи порядок денний, який однаково підтримує робочу силу та захищає організацію.

Методологія дослідження

У жовтні 2023 року Ivanti опитав понад 7300 керівників, спеціалістів із IT та кібербезпеки, та офісних працівників. Наша мета: зрозуміти найактуальніші сучасні загрози кібербезпеці, а також нові тенденції, можливості та бізнес-стратегії.

У рамках дослідження ми розробили шкалу зрілості кібербезпеки. Додаткову інформацію див. у розділі 03. Збір інформації за допомогою самозвіту має обмеження, оскільки люди можуть бути упередженими при оцінці власних зусиль; однак ми вважаємо, що результати, засновані на цій моделі зрілості, надають корисні сигнали для сфери кібербезпеки. Ми просимо читачів пам'ятати про ці обмеження.

Це дослідження було проведено компанією Ravn Research, а експертів було набрано MSI Advanced Customer Insights. Результати опитування не зважені. Додаткова інформація по країнах доступна за запитом.

ivanti.com

ЕФЕКТИВНЕ ОПАЛЕННЯ БУДІВЕЛЬ БУДЬ-ЯКОЇ ПЛОЩІ ТА ПРИЗНАЧЕННЯ!

МОДУЛЬНІ КОТЕЛЬНІ компанії «АНОД»

- ВИСОКА ЕФЕКТИВНІСТЬ
- АДАПТИВНІСТЬ
- ЕКОЛОГІЧНА ЧИСТОТА

Модульний підхід дозволяє задовольнити потреби споживачів у надійному опаленні, незалежно від масштабу будівлі. Котельні можуть бути встановлені як в житлових будинках, так і в комерційних або індустріальних спорудах.

Однією з головних переваг модульних електричних котелень «ANOD» є їх ефективність. Вони розроблені з використанням передових технологій, що підвищують продуктивність опалювання.

Пропонуємо модульні котельні різної потужності – від 100кВт до 600кВт.
Котельні більш великої потужності виробляються під індивідуальне замовлення.

ЕЛЕКТРИЧНІ КОТЛИ «АНОД»

- КОНКУРЕНТНА ЦІНА
- ЛЕГКИЙ МОНТАЖ
- СУЧАСНА АВТОМАТИКА

Електричні котли «АНОД» виробляються двох типів: **тенові та електродні в корпусі**. Підходять для встановлення у квартирах, офісах, будинках – під різну площу опалення.

ЕЛЕКТРОДНІ КОТЛИ «АНОД»

- МАЛИЙ РОЗМІР
- ТОЧКОВЕ ЗАСТОСУВАННЯ
- СТИЛЬНИЙ ДИЗАЙН

Однофазні та трифазні моделі різної потужності для економного опалення квартир, офісів, будинків тощо.

АВТОМАТИКА «АНОД ДІДЖИТАЛ»

- ІНОВАЦІЙНІ РІШЕННЯ
- ШИРОКИЙ СПЕКТР ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ
- МОЖЛИВІСТЬ ЗОВНІШНЬОГО УПРАВЛІННЯ ДВОМА СИСТЕМАМИ

Контроль та регулювання параметрів систем електричного опалення. Сучасне мікропроцесорне обладнання може дистанційно керувати та підтримувати необхідний температурний режим, відстежувати споживання електроенергії, забезпечувати безпечну експлуатацію для всіх видів тенових та електродних котлів незалежно від виробника.

Плавне регулювання потужності – забезпечує використання саме тільки енергії, рівноцінної тепловтраті приміщення.

Має **вмонтований добовий програматор**, за допомогою якого можна перекинути основне споживання електричної енергії на опалення по нічному тарифу.

Виставки у галузі безпеки - 2025 р.

Security & Counter Terror Expo (SCTX) 2025

Лондон, Великобританія, 25–26 березня 2025

Виставка, яка зосереджена на контртерористичних технологіях та рішеннях для національної безпеки. Вона збирає урядових експертів, правоохоронців та постачальників технологій, що спеціалізуються на боротьбі з тероризмом, кібербезпеці, розвідці та антитерористичному захисті.

https://www.sctx.co.uk

ISC West 2025

Лас-Вегас, США, 26–29 березня 2025

Одна з найбільших виставок безпеки в Північній Америці, що охоплює всі аспекти фізичної безпеки, включаючи відеоспостереження, контроль доступу, системи сигналізації та інші передові рішення для захисту підприємств, будівель і інфраструктури.

https://www.iscwest.com

IFSEC International 2025

Лондон, Великобританія,
19–21 травня 2025

Провідна міжнародна виставка, що зосереджена на рішеннях для фізичної безпеки, відеоспостереження, контролю доступу та новітніх технологіях у галузі безпеки. Це місце для зустрічей професіоналів у галузі безпеки з усього світу.

https://www.ifsec.co.uk

The International Security Expo 2025

Лондон, Великобританія, 2–3 жовтня 2025

Виставка, яка охоплює всі аспекти безпеки, від кіберзахисту до фізичної охорони, а також інновації у галузі управління ризиками, систем протипожежної безпеки та інших важливих аспектів захисту.

https://www.internationalsecurityexpo.com

SecuTech Expo 2025

Тайбей, Тайвань, 22–24 квітня 2025

Виставка з фокусом на технологіях безпеки для Азійського ринку. Подія охоплює відеоспостереження, контроль доступу, інтелектуальні будівлі та технології для забезпечення кібербезпеки.

https://www.secutech.com

Milipol Paris 2025

Париж, Франція, 18–21 листопада 2025

Глобальна виставка та конференція з оборонних і безпекових технологій, що об'єднує урядові організації, військових і постачальників з усього світу. Виставка охоплює широкий спектр рішень для фізичної безпеки, технологій для боротьби з тероризмом та інші аспекти національної безпеки.

https://www.milipol.com

7. Cyber Security Expo 2025

Нью-Йорк, США, 23–24 червня 2025

Спеціалізована виставка, присвячена кібербезпеці, де представлені новітні технології для захисту від кіберзагроз, а також рішення для захисту інфраструктур та корпоративних даних.

https://www.cybersecurityexpo.com

Asia Security Expo 2025

Сінгапур, 22–24 вересня 2025

Велика виставка безпеки в Азії, що охоплює фізичну та кібербезпеку, а також інноваційні рішення для охорони підприємств, з особливим фокусом на потреби та тенденції в азійському регіоні.

https://www.asiasecurityexpo.com

Global Security Exchange (GSX) 2025

Даллас, США, 10–12 вересня 2025

Конференція і виставка, що охоплює всі напрямки безпеки, включаючи управління ризиками, охорону, фізичну та кібербезпеку. Це важлива подія для професіоналів у сфері корпоративної та урядової безпеки.

https://www.gsx.org

Intersec Dubai 2025

Дубай, ОАЕ, 18–20 січня 2025

Одна з найбільших міжнародних виставок безпеки на Близькому Сході, яка охоплює усі аспекти безпеки, від відеоспостереження до протипожежних та інженерних рішень, а також кібербезпеки та управління кризами.

https://www.intersecexpo.com

SAFETY & SECURITY EXPO 2025

Франкфурт, Німеччина, 2–4 вересня 2025

Виставка, що об'єднує технології для забезпечення безпеки, включаючи системи спостереження, охорону, виявлення загроз, а також інтелектуальні системи для управління безпекою в підприємствах.

https://www.security-expo.com

Smart Security Expo 2025

Шанхай, Китай, 10–12 червня 2025

Виставка технологій безпеки для "розумних міст", зокрема в галузі відеоспостереження, контролю доступу, автоматизації та інших інтелектуальних систем для забезпечення безпеки в урбанізованих зонах.

https://www.smartsecurityexpo.com

DEFSEC International 2025

Велінгтон, Нова Зеландія,
17–19 червня 2025

Виставка з акцентом на оборонні технології та національну безпеку в Океанії, з особливим фокусом на військові технології, збройні сили та державні структури.

https://www.defsec.co.nz

Tactical & Survival Show 2025

Мельбурн, Австралія, 23–25 травня 2025

Виставка, яка зібирає провідних виробників та постачальників тактичного спорядження, інноваційних технологій для особистої безпеки та виживання. Це подія, де учасники можуть ознайомитися з новітніми рішеннями для підвищення безпеки на рівні індивідуального користувача, зокрема для військових, поліцейських, охоронців та активних мандрівників. Окрім демонстрацій продукції, будуть проведені семінари та тренінги з практичного використання спорядження у критичних ситуаціях.

GISEC Global 2025

Дубай, ОАЕ, 2–4 червня 2025

Одна з найбільших виставок кібербезпеки на Близькому Сході. Тут представлені найновіші рішення для захисту від кіберзагроз, інфраструктурної безпеки та управління ризиками в цифровому середовищі.

https://www.gisec.ae

European Cyber Security Conference 2025

Брюссель, Бельгія, 13–15 травня 2025

Конференція, що зосереджена на кібербезпеці, включаючи новітні тенденції, рішення для захисту інфраструктури та безпеки даних. Вона збирає провідних європейських експертів та компанії в галузі кіберзахисту.

https://www.europeancybersecurityconference.com

FIME (Future of International Mobility & Security Expo) 2025

Париж, Франція, 8–10 квітня 2025

Виставка, що зосереджена на інноваціях у галузі безпеки мобільності та транспортних систем. Включає в себе рішення для безпеки транспортних засобів, смарт-транспортних технологій та інфраструктури.

https://www.fime-expo.com

18. Secutech India 2025

Мумбаї, Індія, 11–13 вересня 2025

Індійська виставка, що охоплює всі аспекти безпеки, зокрема відеоспостереження, системи контролю доступу та кібербезпеку. Вона є важливим майданчиком для компаній, які працюють на ринку безпеки в Індії.

https://www.secutechindia.com

ASIS 2025

Орландо, США, 8–11 вересня 2025

Щорічна міжнародна конференція та виставка з корпоративної безпеки, охорони та ризик-менеджменту, що об'єднує лідерів галузі для обміну досвідом і презентації новітніх технологій та рішень у сфері безпеки.

https://www.asisonline.org

20. Smart Security Expo Asia 2025

Гонконг, 3–5 грудня 2025

Виставка інтелектуальних рішень для забезпечення безпеки, зокрема в галузі відеоспостереження, автоматизації будівель та управління доступом, з фокусом на азійський ринок.

https://www.smartsecurityexpoasia.com

World Security Congress 2025

Лісабон, Португалія, 21–23 жовтня 2025
https://www.worldsecuritycongress.com

Cyber Defense Summit 2025

Вашингтон, США, 7–9 жовтня 2025
https://www.cyberdefensesummit.com

National Homeland Security Conference 2025

Чикаго, США, 14–16 червня 2025
https://www.nationalhomelandsecurityconference.com

INTERNATIONAL
EXPO GROUP

UZ SECURE EXPO #14

2-3-4
APRIL
2025

Uzbekistan, Tashkent

SECURITY TECHNOLOGY
FIRE SAFETY
LABOUR AND ENVIRONMENTAL PROTECTION
IT SECURITY - INFORMATION PROTECTION

INTERNATIONAL EXPO GROUP

UZ SECURE EXPO #14

MAIN SECTORS OF THE EXHIBITION:

SAFETY TECHNOLOGIES

TECHNICAL SECURITY:

- Anti-terrorism and screening equipment
- Building Automation and Safety
- Intelligent Building Management Systems
- Night vision devices, optics and optronics
- Production of safes (locks, turnstiles) and the development of their encoding
- Burglar alarm and alarm systems
- Closed circuit television and surveillance systems
- Access control systems
- Chemical Remedies
- Personal safety equipment
- Border Guard Systems
- Products for the military and law enforcement agencies
- Communication facilities and their components
- Green technology, environmental protection and disposal

SYSTEMS AND MEANS OF FIRE SAFETY:

- Fire alarm systems
- Fire extinguishing systems and means
- Fire retardant materials and structures
- Equipment and accessories
- Fire fighting equipment and special units

RESCUE EQUIPMENT:

- Machinery, technology, equipment for the prevention of accidents, disasters and liquidation of their consequences
- Personal protective equipment, first aid equipment
- Outfit and equipment of firefighters and rescuers
- Rescue devices
- Mountain rescue equipment and gear
- Personal protection equipment for respiratory organs
- Life support equipment
- Special equipment

ECOLOGY

ENVIRONMENTAL PROTECTION AND SAFETY:

- Control and prevention of air pollution and air purification technologies; systems and equipment for air purification in production and in enclosed spaces
- Emissions from industrial enterprises, thermal power plants, and motor vehicles
- Cleaning and removal of exhaust gases
- Environmental monitoring
- Degassing , filters
- Forced air supply systems
- Air conditioning and cooling ventilation
- Water treatment equipment and materials
- Municipal and industrial waste
- Equipment and technologies for the collection, processing, disposal, neutralization and disposal of industrial waste
- Waste collection and disposal:
  -Presses, crushers, shredders
  -Waste disposal equipment
  -Waste incineration equipment
  -Tare acceptance machines

OCCUPATIONAL SAFETY

PRODUCTION AND REALIZATION OF INDIVIDUAL PROTECTION EQUIPMENT:

- Special clothing
- Special shoes
- Protective equipment for head, face, eyes, hands, respiratory and hearing safety belts
- Collective protection
- Safety equipment and technology
- Technical and fire safety
- Sanitary service
- Research and development on labour protection
- Occupational medicine. Occupational hygiene
- Rehabilitation means

IT SECURITY

THE PROTECTION OF INFORMATION. BANK EQUIPMENT:

- Banking equipment
- ATMs, terminals, readersInformation technologies and security Software
- Production, personalisation and engineering of bank cards
- Bank equipment
- Technical means of information protection
- Information technology and security
- Software

For participation in the exhibition please contact:
Olga Feofilaktova
Project Manager

(+998 93) 381-07-84
IEG_uz
(+998 71) 238-94-68
InternationalExpoGroup
sales@specieg.uz
www.ieg.uz
IEGuz

Покроковий посібник з протидії застосування безпілотних літальних апаратів (БПЛА)

Безпілотні літальні апарати (БПЛА), широко відомі як дрони, набувають все більшого поширення в різних секторах, починаючи від аматорського і закінчуючи комерційним застосуванням. Хоча дрони надають численні переваги, вони також створюють потенційні загрози безпеці, що потребують вирішення. Цей посібник має на меті надати огляд технологій протидії БПЛА, щоб допомогти зрозуміти і зорієнтуватися в мінливому ландшафті контрзаходів протидії безпілотникам.

Розуміння загроз БПЛА

Щоб отримати повне уявлення про загрози, пов'язані з БПЛА, важливо визначити потенційні ризики, які вони несуть. Безпілотники можуть бути використані у різні способи, наприклад, для втручання у приватне життя, для контрабанди нелегальних товарів, ведення несанкціонованого спостереження і навіть для застосування зброї.

Нещодавні інциденти підкреслюють потенційну небезпеку, яку становлять дрони. Наприклад, у травні 2023 року вхідні рейси в аеропорту Гатвік були призупинені майже на годину через повідомлення про безпілотник поблизу аеродрому. Це призвело до того, що 12 прибуваючих рейсів було перенаправлено в інші аеропорти. Цей інцидент не лише спричинив значні перебої в роботі, але й висвітлив потенціал дронів для втручання в роботу критично важливої інфраструктури.

В іншому інциденті у тому ж місяці росія звинуватила Україну у спробі замаху на російського президента владіміра путіна за допомогою безпілотника, який завдав удару по Кремлю. Хоча Україна заперечувала свою причетність до цього інциденту, він продемонстрував можливість використання безпілотників у політично вмотивованих атаках.

Ці епізоди викрили вразливі місця в системі безпеки, показавши, як дрони можуть проникати в охоронювані зони, не спрацьовуючи на традиційні заходи безпеки. Хоча жоден з дронів безпосередньо нікому не загрожував, той факт, що дрони потенційно можуть переносити шкідливі об'єкти або вести несанкціоноване спостереження, викликає значне занепокоєння. Більше того, здатність малих дронів уникати виявлення радарами ще більше посилює ці ризики. Це підкреслює нагальну потребу в жорсткому регулюванні та ефективних заходах безпеки для зменшення небезпеки, пов’язаної з несанкціонованим використанням дронів.

Поради читачеві

1. Будьте в курсі подій: Будьте в курсі останніх новин і тенденцій, що стосуються технології безпілотників та їх застосування. Розуміння мінливого потенціалу загроз, пов'язаних з БПЛА, може допомогти вам передбачити потенційні ризики.

2. Оцінюйте ризики: Регулярно оцінюйте вразливості вашої організації, пов'язані з використанням дронів.

Визначте сфери, де дрони можуть становити загрозу безпеці, та визначте пріоритетні заходи для зменшення цих ризиків.

3. Обирайте правильні технології: Інвестуйте в комбінацію технологій виявлення та ідентифікації, адаптованих до вашого конкретного середовища. Враховуйте такі фактори, як дальність виявлення, точність і простота інтеграції з існуючими системами.

4. Впроваджуйте системи виявлення: Використовуйте надійні системи виявлення, які поєднують різні технології (радари, радіочастотні детектори, оптику тощо) для забезпечення комплексного моніторингу та ідентифікації загроз.

5. Створюйте операційні процедури: Розробіть чіткі та ефективні операційні процедури, включаючи «зону тривоги» для визначення пріоритетності загроз, затвердіть план реагування на несанкціоновану діяльність безпілотників.

Огляд технологій з протидії БПЛА

Оскільки жодна з існуючих технологій не може забезпечити захист 100% без супутніх збитків або перешкод для інших сигналів зв'язку, протидія загрозам БПЛА вимагає багаторівневого підходу, який поєднує в собі виявлення, ідентифікацію, відстеження і різні рівні методів нейтралізації. Кожен рівень має слугувати певній меті та робити свій внесок в вашу стратегію протидії БПЛА.

Технології виявлення

Технології відіграють вирішальну роль у виявленні присутності несанкціонованих БПЛА в певній місцевості.

Ці технології включають:

- радіолокаційні системи;
- акустичні датчики;
- радіочастотні (РЧ) сканери;
- електрооптичні системи.

Кожна з цих технологій має свої переваги і недоліки. Їх оптимальне використання залежить від таких факторів, як умови навколишнього середовища та бажана дальність виявлення. Крім того, їхня ефективність у розрізненні санкціонованих і несанкціонованих дронів може бути не високою, що часто призводить до потенційних хибних тривог:

- недостатня точність створює хибні тривоги - це стосується виявлення інших об'єктів, окрім дронів (птахів, автомобілів тощо);

- нездатність відрізнити «свого» від «чужого» - це значна перешкода в галузях/місцях, де дрони інтенсивно використовуються на постійній основі.

Технології ідентифікації та відстеження

Після виявлення БПЛА для його ідентифікації та відстеження зазвичай застосовуються такі технології, як електрооптичні датчики, інфрачервоні камери і системи комп'ютерного зору. Вони надають операторам інформацію про БПЛА, включаючи його тип, траєкторію польоту і корисне навантаження. Незважаючи на свою ефективність, ці методи також мають притаманні їм недоліки, насамперед щодо точності та обчислювальної здатності.

Саме метод ефективного аналізу протоколів може дати найкращі результати. Саме аналіз протоколів дає можливість роз-

шифровувати сигнали зв'язку між дроном і його контролером, надаючи в режимі реального часу інформацію про унікальний ідентифікатор дрона, марку, модель, місцезнаходження, напрямок польоту і навіть місцезнаходження оператора.

Перехоплення і розшифровка сеансу зв'язку між дроном і пультом дистанційного керування, дають можливість отримувати дані для ефективної ідентифікації та відстеження літального апарату, а також допомагають оцінювати можливі потенційні загрози, що робить цей метод перспективним для забезпечення комплексної протидії.

Технології пом'якшення наслідків

У ситуаціях, коли безпілотні літальні апарати (БПЛА) становлять значну загрозу, можуть бути застосовані різні технології для її зменшення. Ці технології, спрямовані на виведення з ладу або нейтралізацію БПЛА. Вони охоплюють низку методів, таких як глушіння, спуфінг і кінетичне перехоплення. Глушіння порушує зв'язок між безпілотником і оператором, підробка надає БПЛА неправдиву інформацію, а кінетичні методи передбачають фізичне перехоплення або знищення безпілотника. Хоча ці методи здаються ефективними, вони часто мають суттєві недоліки. Вони, як правило, дорогі, можуть перешкоджати іншим операціям в умовах щільної міської забудови і створюють ризик виведення з ладу безпілотника над населеними пунктами, що може завдати шкоди пересічним громадянам.

З іншого боку, аналітика протоколів є більш життєздатним рішенням, особливо - але не тільки - в умовах щільної міської забудови. Вона функціонує шляхом аналізу сигналів зв'язку між дроном і його контролером, надаючи інформацію в режимі реального часу, що полегшує точну оцінку загрози. Аналітика протоколів не порушує повсякденну роботу, не викликає хибних тривог і дозволяє за необхідності обережно зменшити навантаження на дрон, безпечно приземливши його у визначеному місці. Це також дозволяє точно визначити місцезнаходження контролера у випадках, коли необхідно затримати оператора. У той час як інші методи часто створюють юридичні та етичні дилеми, аналітика протоколів обходить ці проблеми, що робить її перспективним підходом для комплексної безпеки безпілотників у міському середовищі.

Нормативно-правова база та юридичні аспекти

Використання технологій протидії БПЛА регулюється чинними нормативно-правовими актами в різних юрисдикціях. Балансування між інтересами безпеки та правами на приватність є складним завданням. Влада постійно працює над створенням всеосяжних рамок, які враховують ризики, пов'язані з безпілотними літальними апаратами, і водночас поважають індивідуальні права. Організаціям і приватним особам вкрай важливо розуміти і дотримуватися цих правил при впровадженні заходів з протидії БПЛА.

Використання дронів, або безпілотних літальних апаратів (БПЛА), регулюється різними органами по всьому світу:

Сполучені Штати

Федеральне управління цивільної авіації США (FAA) є органом, відповідальним за регулювання використання безпілотників у США. Воно запровадило низку правил використання безпілотників, зокрема правило Part 107 для комерційних дронів і правило дистанційної ідентифікації, яке зобов'язує безпілотники передавати в ефір свої ідентифікаційні дані та дані про місцезнаходження. FAA постійно працює над оновленням цих правил, щоб безпечно інтегрувати дрони в національну систему повітряного простору.

Європа

В Європі регулюванням використання безпілотників займається насамперед Агентство з авіаційної безпеки Європейського Союзу (EASA). Правила EASA поширюються на всі країни-члени ЄС і класифікують дрони на «відкриті», «спеціальні» та «сертифіковані» категорії залежно від ризику, який вони становлять. Регламент зосереджується на експлуатаційних характеристиках безпілотника, а не на самій платформі. Оператори дронів також зобов'язані реєструватися в країні, де вони проживають або мають основне місце діяльності.

Азія

В Азії регулювання безпілотників варіюється від країни до країни. Ось два приклади:

Китай

Адміністрація цивільної авіації Китаю (CAAC) регулює використання дронів. Станом на час мого останнього оновлення у вересні 2021 року, CAAC вимагає, щоб усі дрони вагою понад 250 грамів були зареєстровані під справжніми іменами.

Японія

Міністерство землі, інфраструктури, транспорту і туризму (MLIT) здійснює нагляд за регулюванням використання дронів. Японські правила використання дронів забороняють польоти в густонаселених районах і певному повітряному просторі поблизу аеропортів без дозволу MLIT.

Австралія

Управління з безпеки цивільної авіації (CASA) здійснює нагляд за регулюван-

ням використання безпілотників в Австралії. CASA вимагає, щоб оператори комерційних дронів мали ліцензію та сертифікат. Рекреаційні користувачі повинні дотримуватися певних стандартних умов експлуатації, наприклад, не літати вище 400 футів і тримати дрон на відстані щонайменше 30 метрів від інших людей.

Канада

У Канаді регулюванням використання дронів займається Міністерство транспорту Канади. Згідно з канадським законодавством, дрони поділяються на дві основні категорії: до 25 кілограмів і ті, що використовуються в межах візуальної видимості, а також на базові та просунуті операції. Для кожного типу операцій існує свій набір правил; наприклад, для просунутих операцій оператор повинен скласти іспит і мати модель дрона, схвалену Міністерством транспорту Канади.

Південна Африка

У Південній Африці використання дронів регулюється Південноафриканським управлінням цивільної авіації (SACAA). Комерційні оператори дронів повинні отримати ліцензію дистанційного пілотування та сертифікат оператора. Серед інших правил, дрони не повинні літати вище 400 футів над землею і не повинні літати вночі без дозволу директора цивільної авіації.

Індія

В Індії за регулювання безпілотників відповідає Генеральний директорат цивільної авіації (DGCA). Дрони поділяються на п'ять категорій залежно від максимальної злітної ваги: Нано-, мікро-, малі, середні та великі. Усі дрони (за винятком нанодронів, що літають нижче 50 футів, і тих, що належать NTRO, ARC і Центральним розвідувальним агентствам) повинні бути зареєстровані і мати унікальний ідентифікаційний номер (UIN).

Кожен з цих органів має на меті забезпечити безпечне використання безпілотників, повагу до приватного життя та безпеку. Вони постійно працюють над оновленням нормативно-правових актів у міру розвитку технології безпілотників і їх використання в комерційному, рекреаційному та державному секторах. Ці органи також співпрацюють на міжнародному рівні для гармонізації правил і стандартів використання безпілотників.

Безпілотні літальні апарати: майбутні тенденції та виклики

З розвитком технологій протидії безпілотникам зростають і виклики, пов'язані з протидією загрозам з боку БПЛА. Нові технології, такі як штучний інтелект, машинне навчання і вдосконалені датчики, пропонують потенційні рішення для боротьби з можливостями БПЛА, що розвиваються. Проте виникають і нові виклики, такі як поява ройових дронів і автономних систем. Постійні дослідження і розробки є життєво важливими для того, щоб випереджати ці нові загрози.

Кращі практики та рекомендації для безпілотних авіаційних систем

Впровадження ефективних заходів протидії БПЛА вимагає комплексного підходу:

1. Проведіть ретельну оцінку ризиків: Почніть з визначення потенційних вразливостей і ризиків, характерних для вашого середовища. Ця оцінка допоможе вам визначити пріоритети та ефективно розподілити ресурси.

2. Інвестуйте у відповідні технології виявлення та ідентифікації: Обирайте технології, які відповідають вашим конкретним потребам, і враховуйте такі фактори, як дальність виявлення, обмеження прямої видимості, точність і можливості інтеграції.

3. Забезпечте комплексне навчання: Переконайтеся, що персонал, відповідальний за протидію БПЛА, пройшов належну підготовку з експлуатації обладнання, розпізнавання загроз і протоколів реагування. Постійні тренінги допомагають командам бути готовими та володіти найсучаснішими методами.

4. Сприяйте співпраці: Налагоджуйте міцні партнерські стосунки з правоохоронними органами, регуляторними органами та іншими зацікавленими сторонами. Обмін інформацією та координація зусиль підвищує ефективність стратегій протидії БПЛА.

5. Впроваджуйте ефективні операційні процедури:

Створення «Зони тривоги» - визначення певної зони інтересу, що дозволяє визначити пріоритетність важливих подій та оптимізувати оперативну готовність.

- Розробіть план реагування: Наявність детального плану реагування має вирішальне значення при виявленні несанкціонованого або ворожого дрона. Цей план повинен включати способи інформування про загрозу всередині та за межами організації, кроки для оцінки серйозності загрози та дії, які необхідно вжити.

- Впроваджуйте системи виявлення: Ефективна боротьба з БПЛА починається з надійної системи виявлення, яка може включати радар, радіочастотні (РЧ) детектори, акустику, оптику, аналітику протоколів або їх комбінацію. Ці системи повинні регулярно тестуватися і оновлюватися, щоб гарантувати, що вони здатні виявляти найновіші моделі безпілотників.

- Встановіть процедури заборони: Після виявлення загрози ви повинні розробити процедури перехоплення, які можуть варіюватися від радіоелектронного глушіння до технології виведення з ладу безпілотників. Їх слід застосовувати обережно, щоб уникнути

будь-яких супутніх збитків або юридичних проблем.

- Проводьте регулярні тренування: Весь персонал, залучений до операцій з протидії БПЛА, повинен проходити регулярні тренінги. Це включає в себе розуміння загроз від безпілотників, роботу з обладнанням для їх виявлення та пом'якшення наслідків, а також ефективне виконання плану реагування.

- Регулярне тестування системи: Часте тестування ваших заходів з протидії БПЛА допоможе виявити будь-які потенційні слабкі місця або прогалини у вашому захисті. Ці тести повинні імітувати реалістичні загрози, щоб точно оцінити ваші процедури.

- Дотримання правових та нормативних вимог: Будь-які заходи протидії БПЛА повинні відповідати місцевим законам і правилам. Це може вплинути на те, які типи заходів протидії БПЛА вам дозволено використовувати.

- Післяопераційний аналіз: Після кожної операції з протидії БПЛА проводьте детальний аналіз, щоб оцінити ефективність ваших дій, вивчити отриманий досвід і відповідно вдосконалити процедури.

Дотримуючись цих найкращих практик і рекомендацій, ви зможете підвищити здатність вашої організації протидіяти загрозам БПЛА та краще захистити свої активи і громадську безпеку.

Висновок

Отже, протидія загрозам з боку БПЛА вимагає багатогранного підходу, що поєднує технології виявлення, ідентифікації, відстеження і нейтралізації. Оскільки протидія безпілотникам стає все більш поширеною, для організацій вкрай важливо залишатися в курсі змін у ландшафті БПЛА та інвестувати в ефективні контрзаходи. Sentrycs пропонує передові рішення для захисту важливих об'єктів та забезпечення громадської безпеки. Наш комплексний набір передових технологій забезпечує надійне виявлення, точну ідентифікацію та ефективну нейтралізацію загроз безпілотних літальних апаратів.

Шані Вайнштейн,
Серпень 6, 2023

фото ілюстративні

CATHEXISVision - найкращий захист та підвищена ефективність систем безпеки

Поряд з випробуваною протягом багатьох років VMS MOBOTIX (ми рахуємо її найкращою в секторі безкоштовних VMS для малих і середніх проектів) пропонуємо сьогодні розглянути в ваших проектах сучасну, функціональну VMS CATHEXIS. Більше 20 років на ринку, сотні складних, великих проектів в усіх областях індустрії по всьому світу, власна аналітика від периетральних задач до складних аналітичних модулів для проектів торгівлі, транспорту, безпечних міст, інтеграція зі всіма відомими виробниками камер, підтримка всіх існуючих кодеків і тд.

З липня 2020 року ми стали офіційним дистрибютором CATHEXIS в Україні з прямою підтримкою технічного офісу в Україні, якісна підтримка маркетингового відділу, локалізація VMS (українська мова), технологічне партнерство з MOBOTIX (на рівні пропрієтарного кодека MxPEG, метаданих, аналітики), Fibrenetix (оптимізовані для відеоспостереження сервери зберігання), інтеграція з відомими виробниками систем контролю доступу, систем сигналізації (наприклад, остання версія 2025 інтеграція з виробником українських систем Ajax), відкрите та швидке розуміння нових інтеграцій в нових проєктах конкретно під кожного замовника.

Партнерство CATHEXIS, FIBERNETIX та MOBOTIX дає змогу використати повний спектр інструментів для побудови будь-якої складності проектів з якісним обладнанням відео, зберігання даних та функціональним програмним забезпеченням і аналітикою. Це важливо, тому що ці виробники є технологічними партнерами між собою і періодично обмінюються технічною інформацією для побудови надійної та стабільної платформи безпеки. В 2018 році Cathexis отримав нагороду від **Benchmark Innovation Awards** як найбільш стабільну VMS в світі. В 2020 році Cathexis також був обраний у фінал у категорії Video Solutions. **Benchmark Innovation Awards** вважається однією з найпрестижніших нагород у міжнародному секторі безпеки. І знову це сталось у 2023 та 2024 році.

CathexisVision, був нагороджений престижною нагородою **Benchmark Innovation Award 2024**. Це визнання зміцнює позицію CathexisVision як глобального експерта з програмного забезпечення для управління відео, відомого своїми передовими можливостями в галузі безпеки, операційної ефективності та бізнес-аналітики.

Нагорода **Benchmark Innovation Awards** вшановує компанії, які забезпечують видатні технологічні досягнення, трансформуючи галузеві стандарти. CathexisVision вирізнявся своїм надійним набором інструментів відеоспостереження, включаючи аналітику на основі штучного інтелекту, бездоганну сторонню інтеграцію та автоматизоване управління сигналами тривоги.

CathexisVision користується довірою у всьому світі за його:

- Розширена відеоаналітика: Моделі глибокого навчання для розуміння, керованого штучним інтелектом.

- Ефективне управління сигналізацією: автоматизація відповідей на події для швидшого прийняття рішень.

- Масштабована інтеграція: робота зі сторонніми системами, такими як контроль доступу, панелі сигналізації тощо.

Новая версія, що щойно з'явилася, **CathexisVision 2025**, надає вам інструменти, які допоможуть вам прокласти чіткий шлях через конкурентні вимоги до управління безпекою. У швидкозмінному середовищі моніторингу та управління об'єктами та інсталяціями наші інтелектуальні рішення роблять ваше життя простішим і безпечнішим.

Цьогорічний реліз розроблений, щоб забезпечити цінність у всіх сферах управління безпекою, завдяки функціям, які базуються на стабільній, масштабованій і потужній платформі CathexisVision.

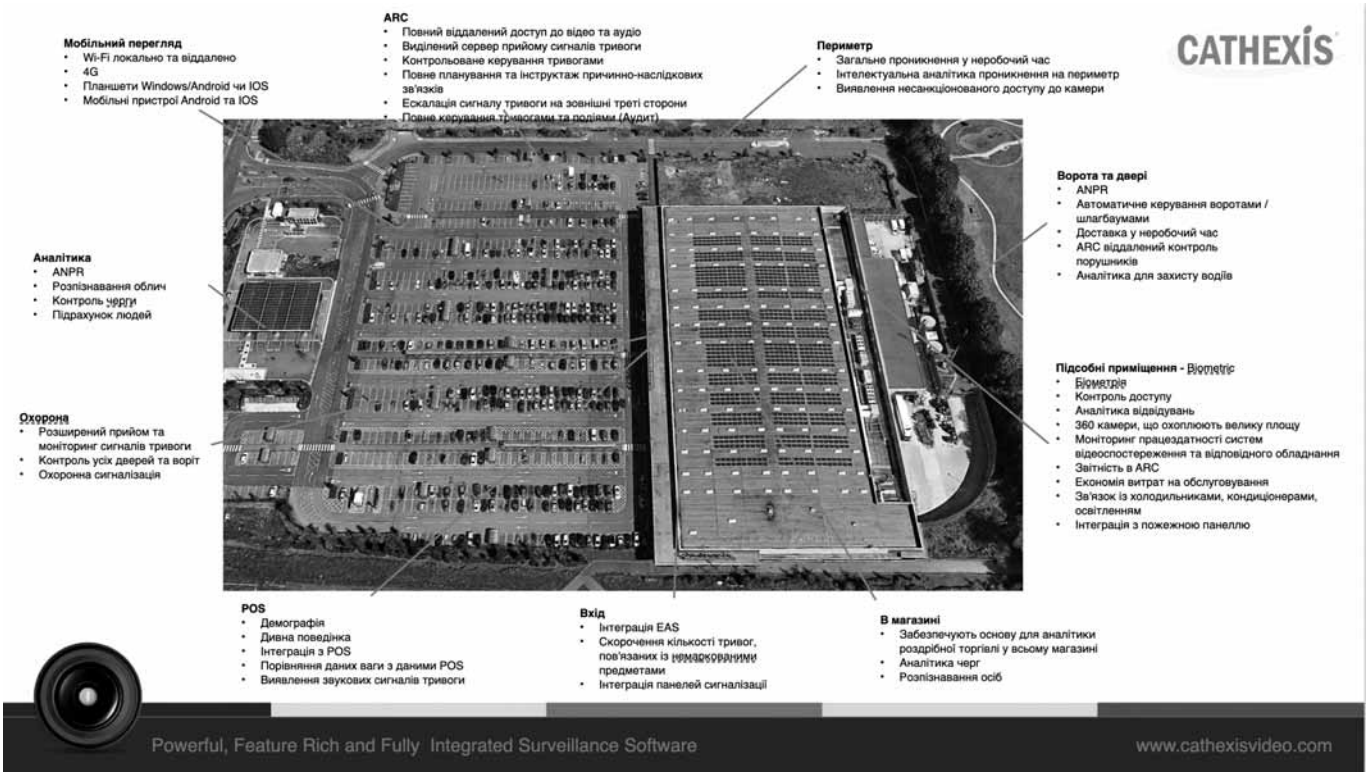
Розширений пошук функцій в Carbon (Клієнт/Оператор): Швидше знаходьте потрібний відеоматеріал, фільтруючи його на основі атрибутів - тепер з колірним фільтром.

CathexisVision Web: Спростіть віддалений доступ за допомогою браузерного клієнта, який усуває проблеми з установкою.

Тегування ресурсів у Carbon: Спростіть огляд і пошук певних ресурсів завдяки додаванню тегів ресурсів, що координуються за кольором.

Робочі процеси управління тривогами: Переконайтеся, що жодна деталь не буде пропущена в критичні моменти, за допомогою настроюваних інструментів управління тривогами.

ГІС-карти в Carbon: Візуалізуйте масштаби і зв'язки між об'єктами і ресурсами більш чітко, включивши геопросторові дані у ваші кастомізовані карти.



Нові інтеграції: Безперешкодна інтеграція з найсучаснішими системами, зокрема пожежними панелями Bosch та системами сигналізації Ajax.

Покращення налаштувань і моніторингу: Скористайтеся такими можливостями, як масове оновлення/імпорт камер в CathexisVision і сповіщення на робочому столі в Carbon, які покращують загальний користувацький досвід.

Перевага CathexisVision

CathexisVision - це система управління відео даними (VMS) з відкритою платформою, що поєднує гнучкість, багату функціональність та простоту використання. Він доступний у декількох варіантах, щоб відповідати конкретним вимогам системи на основі кількості підключених пристроїв, кількості необхідних серверів та сайтів та розширених функціональних можливостей. Це гарантує, що користувачі не платять за функції, які їм не потрібні.

CathexisVision пропонує прямі інтеграції, що підтримують більшість провідних брендів камер на ринку спостереження, а також ряд спеціальних варіантів, таких як панорамні камери та пристрої, що використовують Edge технології. Він також підтримує ONVIF. CathexisVision має широкий спектр функцій, які забезпечують доступ до складного та інтуїтивного програмного пакету VMS. Це різко знижує помилкові тривоги та надає точну інформацію для користувачів, які використовують тригери подій. Це досягається завдяки використанню алгоритмів класифікації об'єктів, які використовують складну технологію нейронної мережі. Ці алгоритми дозволяють використовувати додаткове правило в процесі прийняття рішень, ініціюючи події лише в тому випадку, якщо виявлений об'єкт заздалегідь визначений тип, наприклад людина або транспортний засіб.

Удосконалені алгоритми дозволяють користувачам точно ідентифікувати об'єкти та події в даній місцевості та діяти рішуче. Алгоритм AI класифікації об'єктів створює базу даних, яка дозволяє обшукувати записане відео, наприклад, пошук усіх червоних автомобілів у визначеному районі протягом попереднього тижня.

Система VMS також призначена для забезпечення кіберзахисту та надання функцій, що запобігають втраті критичних даних.

Існує як найменше 5 можливостей, що Cathexis відрізняється від великих виробників VMS.

1. Стабільність / надійність: програмне забезпечення дійсно супер стабільне, що гарантує клієнту час роботи. Чотири роки 2018, 2020, 2023 та 2024 CathexisVision займає перше місце в рейтингу найкращих VMS, як найбільш стабільна система VMS.

2. Відеоаналітика: великий набір рішень для задач відеоаналітики, включаючи класифікацію об'єктів за допомогою нейронних мереж. Розробка власних аналітичних модулів під «ключ» для Замовника.

3. Інтеграція із сторонніми системами: контроль доступу, сигнальні та пожежні системи, вторгнення, POS, ваги, системи огородження периметра тощо). Швидка інтеграція нових продуктів, наприклад, український виробник Ajax.

4. Ефективність роботи для операторів ControlRoom чи Ситуаційних Центрів: поліпшення середовища оператора за рахунок поліпшення простоти використання та використання програмного забезпечення для прийняття рішень для надання допомоги користувачу. Наприклад, суміжне відображення камер, яке дозволяє операторам легко стежити за людьми за кількома камерами та функціями розумного пошуку, щоб користувачі могли дуже швидко знаходити кадри, пов'язані з інцидентами, що в свою чергу поліпшує ситуаційну обізнаність.

5. Низька загальна вартість власності. Вимоги до апаратного забезпечення не є великими. Розумні витрати на ліцензію забезпечать для клієнтів низький ТСС.

Системи Cathexis Ви можете використовувати з різними камерами та апаратним забезпеченням будь якого виробника, або достатньо легко інтегрувати в існуючу систему. Якщо Ви розпочинаєте побудову системи безпеки з чистого аркуша, ми готові запропонувати Вам оптимальні рішення надійних камер, гігабітні (10/40Гб/с) комутатори 2 та 3 рівня, сервери та робочі місця для операторських кімнат з повним оснащенням, додаткові системи контролю доступу та сигнальні системи, аналітичні стандартні модулі чи розроблені індивідуально для Вас. Практично, ми пропонуємо ВСІ компоненти сучасної системи безпеки найвищого гатунку та необмежених можливостей, гарантійне обслуговування 3-8 років, сервісну підтримку, проведення аудиту та наш 30 річний досвід на цьому ринку. Ми працюємо майже зі всіма відомими системними інтеграторами і готуємо для них рішення систем безпеки, що базуються на наших компонентах.

ТОВ «ЮНІТОП»
http://www.unitop.ua
info@unitop.ua

Професійна бездротова електрична інсталяція.
Простота децентралізованого встановлення.
Високий рівень безпеки.
Можливість масштабування - від лофт до промислового об'єкту.

Це якщо в стисло.

Технологічний лідер frogblue

Усі продукти **frogblue** розробляються та виробляються на підприємстві в Кайзерслаутерні, Німеччина. Як засновники компанії MOBOTIX AG, FROGBLUE мають багаторічний досвід і перевірену репутацію в галузі технологічних інновацій.

Frogblue є піонером у виробництві бездротових електричних установок на базі Bluetooth® для професійного використання з 2016 року, сертифікованих VDE та ILAC, з виробництвом у Німеччині.

Значна перевага є можливість вільно налаштовувати функції вимикачів в будь-який час за допомогою додатку або адаптувати їх до нових вимог. Frogblue сумісний з будь-якою програмою для вимикачів, що дозволяє отримати доступ до багатьох функцій за допомогою стандартного вимикача. Інтерфейси користувача для смартфонів і дисплеїв автоматично генеруються на основі конфігурацій модулів.

Надійність та відмовостійкість досягається завдяки паралельній передачі повідомлень через тришарову комірчасту мережу. Завдяки вбудованій підтримці універсального стандарту SIP-телефонії наша професійна система відеодомофонів повністю здатна підтримувати багатокористувацькі і навіть багатоклієнтські вимоги.

У поєднанні з інтегрованим зчитувачем RFID і введенням PIN-коду через дисплей, вона забезпечує децентралізоване рішення для контролю доступу з 3-факторною автентифікацією за допомогою відео".

Основні переваги

- Frogblue пропонує професійне комплексне керування будівлею за допомогою одного додатку: освітлення, затінення, опалення, вентиляція, сигналізація, доступ і дверний зв'язок.
- Не потребує кабелів керування або розподільчих шаф, що дозволяє безперервно розширювати систему.
- Підтримує стандартні вимикачі світла від провідних постачальників.
- Сцени на основі часу керують освітленням, кольором і затіненням.
- Найвища надійність завдяки паралельному обміну повідомленнями через мережі Bluetooth®, Wi-Fi та Cellular-Mesh.
- Смартфон безпосередньо зв'язується з будівлею через Bluetooth® - ніякої мережі або IT-інфраструктури не потрібно.
- Миттєве відновлення до попереднього стану протягом 1 секунди після відключення живлення.
- Висока надмірність, оскільки не залежить від центрального комп'ютера/сервера.
- Високий рівень безпеки завдяки власному шифруванню та міткам часу.
- Безпека обслуговування завдяки автоматичному документуванню.
- Багатокористувацький SIP відеодомофон: Прямі глобальні дзвінки зі смартфонів і одночасне підключення декількох IP-телефонних систем.

Що робить frogblue?

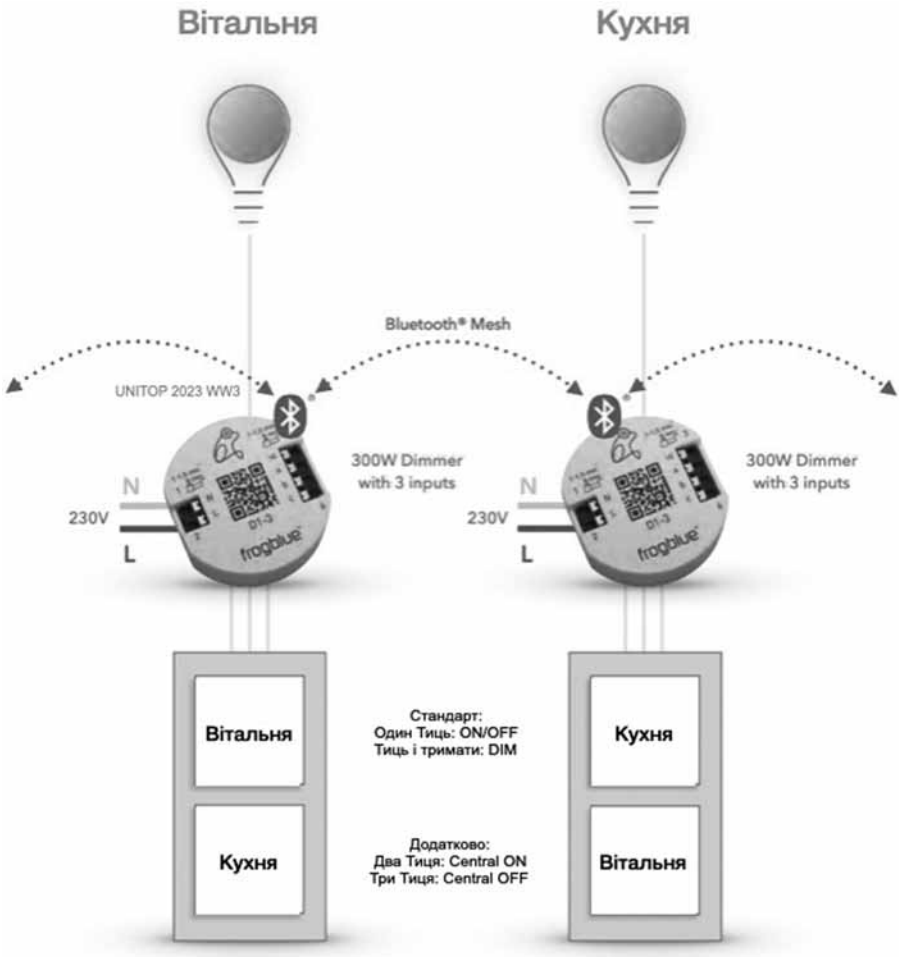
Frogblue пропонує системи освітлення, затінення, вентиляції, доступу, відеозв'язку, сигналізації та управління опаленням для професійного використання. Керує будівлями від односімейних будинків до промислових комплексів.

Здійснює моніторинг будівель, записує події та надсилає тривоги безпосередньо на смартфони. Відеодомофон SIP забезпечує децентралізований контроль доступу за допомогою карток і PIN-кодів для об'єктів з кількома орендарями та великих об'єктів нерухомості.

Найбільші переваги - це надійність і безпека зрілої системи німецького виробництва, яка гнучко інтегрує дверний зв'язок, доступ і автоматизацію будівлі.

Автоматизація будівель

Frogblue пропонує широкий асортимент приводів і датчиків для керу-



вання будівлею. Вона підтримує децентралізовану установку за вимикачами світла без необхідності прокладання кабелів управління або встановлення розподільних шаф, що робить її надзвичайно ефективною і масштабованою в будь-який час.

Система **frogblue** може бути повністю прихованою, оскільки всі функції ініціюються за допомогою стандартних вимикачів і передаються бездротовим способом. Бажаючі можуть зберегти існуючу програму вимикачів. Для користувача візуально немає ніякої різниці між **frogblue** і традиційною електричною інсталяцією.

Передача даних за допомогою **Bluetooth MESH**, як високошифрованого бездротового зв'язку. Часткові відмови компонентів або збої не впливають на основний зв'язок системи.

Система **frogblue** самодокументується, забезпечуючи операційну чіткість і підзвітність на довгі роки.

Асортимент продукції

Frogs

Це серце frogblue. Без кабелів керування наші жабки бездротово з'єднують освітлення, жалюзі, вентилятори, вікна, двері, відкатні ворота, опалювальні системи, домофони та стандартні вимикачі світла через Bluetooth®. Вони встановлюються в коробки прихованого монтажу вимикачів і потребують лише підключення до електромережі 110-240 В.

Cubes

Мають компактний дизайн, плаский корпус з білого скла та розмір, як у вимикача. Встановлені в коробку прихованого монтажу та живляться від мережі 110...240 В, вони є енергоефективними, активуючись лише за необхідності завдяки вбудованому датчику наближення.

frogTerminal

це відео SIP-інтерком, який забезпечує децентралізовані рішення для контролю доступу за допомогою карток і PIN-кодів для будь-яких сценаріїв, від сценаріїв з декількома орендарями до великомасштабних проектів.

Нульова IT-інфраструктура

Система управління будівлею frogblue принципово не потребує мережевої інфраструктури або Wi-Fi в будівлі. Наші модулі також не потребують проводки для керування, лише мережевого живлення.

Це значно зменшує потребу в монтажних джгутах, кабельних лотках і свердлінні отворів. Окремі модулі вимикачів, дверні контакти або температурні датчики можуть працювати від батареї від трьох до п'яти років.

Frogblue не потребує розподільчої шафи та розподільчих модулів. Це не тільки економить простір, але й мінімізує витрати на робочу силу та електроенергію.

Крім того, менша кількість кабелів для встановлення означає мінімальні зусилля, необхідні для протипожежного захисту.

Бездротова, не радіо, не Wi-Fi

frogblue не є типовим рішенням для сигналізації, оскільки кожен модуль системи ретранслює вхідні повідомлення, поки всі модулі не будуть досягнуті, без обмеження радіусу дії в межах будівель.

frogblue Bluetooth Mesh пропонує безпрецедентну надійність і надзвичайно стійку до перешкод завдяки нашій передовій технології.

На відміну від радіо- або Wi-Fi систем, тут немає центральних компонентів для передачі повідомлень, які можуть вийти з ладу.

frogblue гарантує, що всі повідомлення надійно зашифровані та захищені від несанкціонованого втручання (атак повторного відтворення) завдяки використанню вбудованих міток часу.

CLOUD на вимогу

Хмарні сервіси або доступ до інтернету не є обов'язковою умовою для керування будівлею. Крім того, жодні дані не зберігаються поза межами вашої будівлі.

Для дистанційного керування оператори можуть активувати прямий і високозахищений VPN-доступ або скористатися безкоштовним і безпечним frogCloud.

frogCloud не вимагає облікового запису або адреси електронної пошти; він анонімний і безкоштовний.

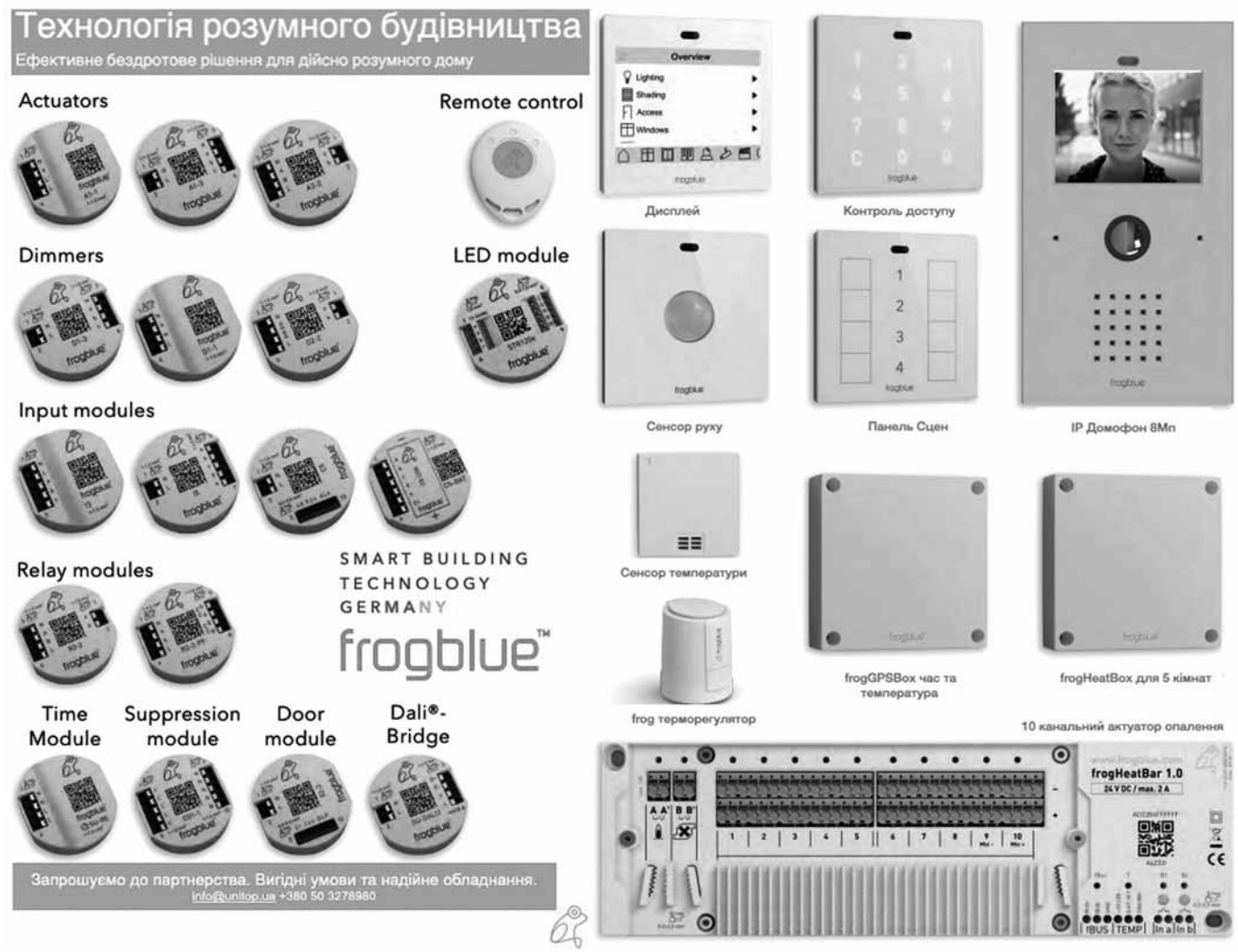
Помічник конфігурації автоматично і безпечно встановлює з'єднання з вашим смарт-пристроєм через QR-код, автоматично генеруючи користувацький інтерфейс і дозволи.

frogCloud використовує універсальний стандарт MQTT і управляється з датацентру в Німеччині.

Відеодомофон SIP

Відеодомофон **frogTerminal**, базується безпосередньо на інтегрованому універсальному стандарті SIP-телефонії, підтримуючи сценарії з декількома користувачами аж до великомасштабних розподілених розгортань. Найбільша перевага полягає в можливості одночасної інтеграції декількох SIP-телефонних систем і SIP-серверів від декількох клієнтів без використання додаткового обладнання.

Крім того, **frogblue** дозволяє здійснювати прямі SIP-дзвінки на будь-який IP-відеотелефон. Смартфони автоматично підключаються до інтеркому за допомогою дзвінка через нашу SIP-хмару.



8-мегапіксельна камера зі світлочутливою оптикою забезпечує повний панорамний огляд на 180°. Навіть у шумному середовищі мова залишається кришталево чистою. Відеожурнал записує як події дзвінка, так і доступ за допомогою PIN-коду або RFID-мітки. Неправильний вхід і спроби несанкціонованого доступу також фіксуються.

Децентралізований контроль доступу

frogTerminal дозволяє кожному учаснику багатокористувацької системи керувати власними PIN-кодами для доступу до дверей або для активації спеціальних функцій. Для підвищення безпеки від підбору PIN-коду дисплей клавіатури постійно змінює свою розкладку.

Вбудований RFID-зчитувач (DESFire EV2®) забезпечує 2-факторну автентифікацію. Додаткова перевірка дзвінків, наприклад, у неробочий час, забезпечує 3-факторну автентифікацію за допомогою відео.

Картки не потребують додаткового програмування; вони самоідентифікуються під час використання.

Інтеграційна архітектура frogblue RFID забезпечує децентралізоване рішення для контролю доступу, мережеве підключення до кожного frogTerminal не є необхідним.

Наближення до **frogTerminal,** дотик до дисплея або неправильне введення також можуть автоматично викликати дзвінки.

Відкритий для інтеграції

Підключення обладнання сторонніх виробників і додаткові функції, такі як керування зовнішнім освітленням через сторонню систему керування будівлею або запуск камери для запису, можуть бути легко інтегровані з frogTerminal через Bluetooth або IP-команди.

Ці дії можна запускати за допомогою PIN-коду та RFID-картки, а також за допомогою телефонного дзвінка. Наприклад, через IP можна керувати шлагбаумами або запитувати стан відкатних воріт.

Наш **frogLink-USB** слугує **SDK** або шлюзом для систем сторонніх виробників, таких як камери **MOBOTIX®** або система управління будівлею **EisBar®**.

frogblue підтримує універсальний стандарт відеотелефонії SIP та інтегрує системи сторонніх виробників, такі як BacNet®, KNX® тощо, за допомогою настроюваних IP-зв'язків.

Безпосередня генерація інтерфейсів

Всі графічні інтерфейси користувача для настінного дисплея і смартфона генеруються автоматично, безпосередньо відображаючи специфічну інформацію, призначену під час конфігурації кожного модуля.

Це включає в себе:

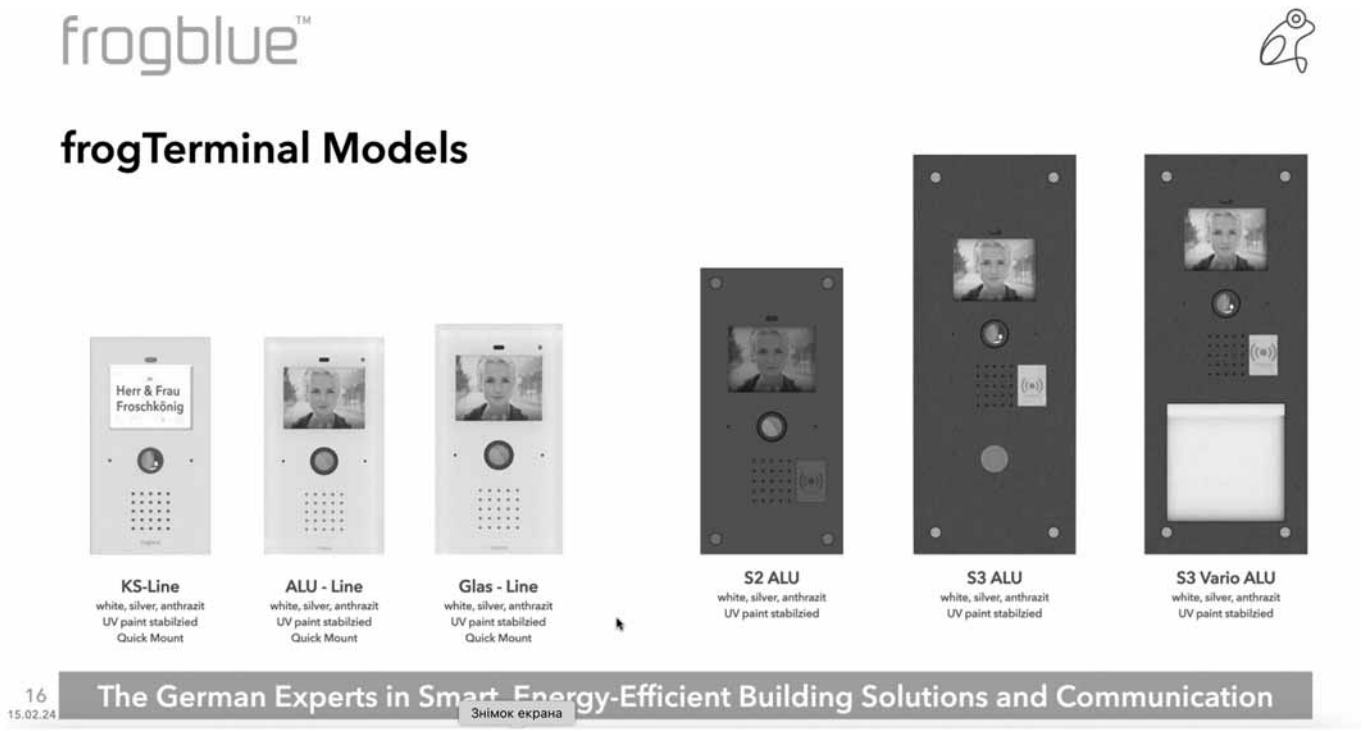
- розташування модуля в приміщенні (наприклад, будівля 13, перший поверх, відкритий майданчик, офіс 12, фойє);
- функції входів і виходів модуля (наприклад, світло, вентиляція, жалюзі, вимикач світла, віконний контакт);
- природні описові повідомлення на модулі (наприклад, Стельове світло, Стан вітру, Центральний дзвінок, Ніч, ЛР віконний контакт).

Значною додатковою перевагою є те, що такий підхід дозволяє інсталяторам чітко конфігурувати проект, забезпечуючи ефективне довгострокове обслуговування.

Автоматична генерація користувацьких інтерфейсів значно зменшує витрати на конфігурацію. Будь-які наступні зміни негайно інтегруються.

Проста конфігурація

Frogblue легко налаштовується - програмування не потрібне! Налаштування таких функцій, як перемикання ланцюгів або центральне вимкнення, здійснюється за допомогою реальних, описових назв, таких як «Світло у фойє», «Дзвінок біля воріт» або «Двері холу».



Знімок екрана

Кожному входу можна призначити кілька функцій за допомогою таких дій, як клацання, подвійне клацання, тривале натискання тощо, і він може керувати будь-якою функцією в проекті, включно з попередньо встановленими сценами.

Якщо виходи диммерів мають однакові назви, світло автоматично синхронізує яскравість і колір; при однакових назвах на входах модуля автоматично формується тумблер.

Такий підхід є зрозумілим, мінімізує помилки і підтримує довгострокову документацію. Просте налаштування освітлення, затінення, вентиляції, опалення, а також домофону можна виконати за півдня.

Frogblue бездротово з'єднуємо світло, жалюзі, вентилятори, вікна, двері, опалення, домофони та стандартні вимикачі за допомогою Bluetooth® MESH.

Контролери встановлюються за звичайними вимикачами/розетками і потребують лише мережі 110...240В. Не потрібно прокладати дроти керування, оскільки з'єднання здійснюється віртуально.

Єдиний додаток контролює весь будинок, локально через **Bluetooth®** або по всьому світу зі смартфона. **Frogblue** легко встановлюється без сервера або розподільчої шафи, а його налаштування - дитяча забавка.

Інтерком, **frogTerminal**, підтримує універсальний стандарт **SIP**-телефонії, що робить його повністю придатним для використання кількома орендарями.

Основні перевагами є надійність і безпека зрілої системи, яка може бути адаптована до потреб користувачів навіть через роки.

Більше інформації, презентації, демо оснащення, партнерство:

http://www.frogblue.unitop.ua
infomx@unitop.ua

Розумний дім: безпека, економія та зручність

Сьогодні технології «розумного дому» стали необхідністю, особливо в умовах війни. Вони забезпечують безпеку, економію ресурсів та зручність. Розумний будинок – це система, яка поєднує датчики, камери, розумні замки, освітлення та клімат-контроль у єдину екосистему, якою можна керувати через смартфон або голосові команди.

Чому розумний дім актуальний?

Під час війни безпека стає пріоритетом. Розумний будинок захищає від мародерів, пожеж та затоплень. Датчики відкриття дверей, вікон та руху миттєво повідомляють про загрози. Камери відеоспостереження дозволяють віддалено стежити за домом, що особливо важливо для тих, хто вимушено залишив житло.

Крім безпеки, система допомагає економити ресурси. Термостати та термоголовки оптимізують опалення, а розумні розетки дозволяють дистанційно керувати електроприладами, унеможливлюючи їхню роботу вхолосту.

З чого почати?

Безпека: Встановіть датчики руху, відкриття дверей та камери відеоспостереження.

Економія: Додайте термостати, термоголовки та розумні розетки.

Зручність: Налаштуйте автоматизацію освітлення та побутових приладів, наприклад, вмикання світла при вході в кімнату.

Найкорисніші пристрої

Датчики протікання води: Попереджають про затоплення.

Датчики диму та чадного газу: Захищають від пожеж та отруєння.

Розумні замки: Дозволяють віддалено контролювати доступ.

Камери відеоспостереження: Забезпечують візуальний контроль.

Термостати та термоголовки: Допомагають економити на опаленні.

Як працює розумний будинок?

Система базується на центральному шлюзі (хабі), який об'єднує всі пристрої. Через додаток на смартфоні можна керувати системою та налаштовувати автоматизації, наприклад, вмикання світла при виявленні руху.

Як обрати пристрої?

Вартість: Визначте бюджет.

Функціональність: Оберіть пристрої за потребами.

Сумісність: Переконайтеся, що всі пристрої працюють в одній системі.

Чому важливо звертатися до фахівців?

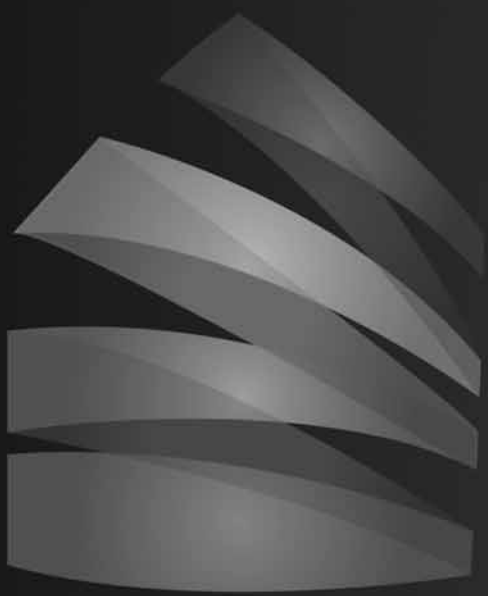
Створення розумного дому – складний процес. Фахівці допоможуть правильно підібрати та налаштувати пристрої, уникнути помилок і зайвих витрат.

Скільки коштує?

Вартість залежить від комплектації. Мінімальний набір (шлюз, датчики руху та відкриття дверей) коштує від кількох тисяч гривень. Систему можна розширювати поступово.

Розумний дім – це потужний інструмент для безпеки, економії та комфорту. Почніть з базових пристроїв і поступово розширюйте систему. Звертайтеся до фахівців, щоб отримати максимальну віддачу від інвестиції.

19-21 БЕРЕЗНЯ 2025



INTER BUILD EXPO

ІНТЕРБІЛДЕКСПО

МІЖНАРОДНА БУДІВЕЛЬНА ВИСТАВКА

Місце проведення:

МІЖНАРОДНИЙ ВИСТАВКОВИЙ ЦЕНТР

Київ, Броварський пр-т, 15
(метро Лівобережна)

ВІДБУДУЄМО РАЗОМ!

Біометричні системи доступу

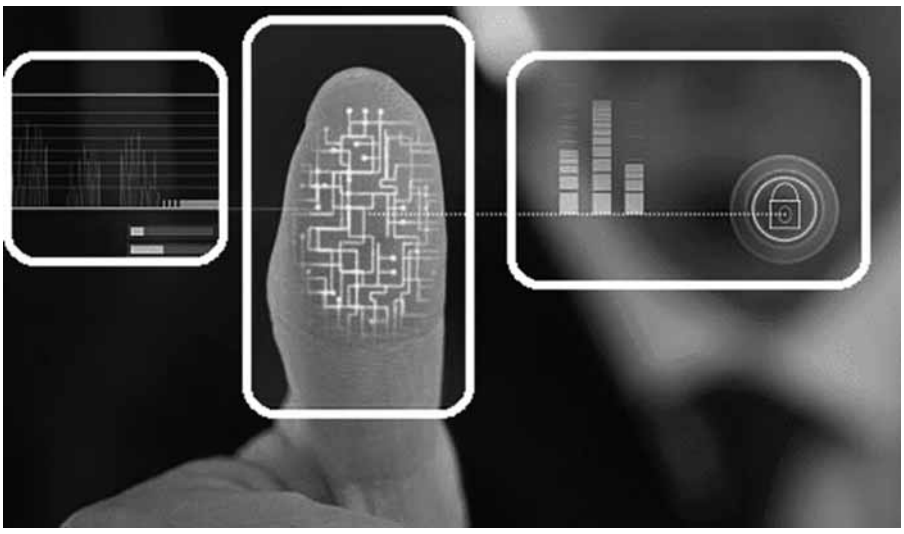
Біометричні системи стають поширеним способом захисту даних користувача. Але їх розробникам варто врахувати, що ідентифікація за унікальними фізіологічними параметрами не дає стовідоткового захисту від атак хакерів.

Існує три способи ідентифікації особи людини. По-перше, ми можемо переконатися, що він знає щось секретне (наприклад, кодове слово або PIN), – це найпоширеніший і найдешевший у реалізації механізм, який, однак, є найнезахищенішим. Дізнатися пароль нескладно, рідко хто дотримується правил вибору надійних поєднань символів. Другим способом перевірки є контроль володіння якоюсь неповторною річчю (наприклад, смарт-карткою, ключем або штрих-кодом). Це надійніший і дорожчий спосіб аутентифікації.

Нарешті, третій спосіб – це перевірити, що людина має якусь унікальну фізичну, біологічну, фізіологічну або поведінкову характеристику (наприклад, відбитками пальців або райдужною оболонкою ока). Саме цей метод сьогодні набирає популярності, оскільки вважається, що, крім зручності для користувача, він є і більш захищеним. Але це зовсім так.

Якщо у користувача вкрали пароль, це не смертельно, його можна замінити. Вкрадена карта або токен теж підлягають відновленню. А ось біометричний фактор унікальний – за жодних обставин ви не зможете змінити відбитки пальців, голос, очі або розташування вен на руці. Це найпопулярніші методи біометричної ідентифікації, з яких у банках застосовуватимуться поки що тільки голос та геометрія обличчя. Серед інших властивих людині особливостей можна назвати почерк, у тому числі клавіатурний, запах, електроенцефалограму мозку та електрокардіограму серця, ходу і навіть геометрію сідниць, яка, виявляється, теж унікальна.

У принципі біометрія справді вирішує багато класичних проблем. Традиційний варіант перевірки особи клієнта за кодовим словом тощо, давно вже перестав хоч якось боронити від шахраїв. За даними дослідження Opus Research A New Authentication Paradigm: Call Center Security without Compromising Customer Experience, 65% банківських клієнтів не задоволені перевіркою за паролем та кодовим словом при дзвінках до кол-центру. 49% клієнтів вважають, що перевірка надто довга (від 40 до 90 секунд). 74% хоча б раз не отримали доступу до своїх даних через те, що не пройшли перевірку і не змогли підтвердити свою особу стандартним способом. Чи може біометрія допомогти у цих випадках?



Вважаючи, що біометрія зробить життя зручнішим і безпечнішим, ми починаємо його активно впроваджувати, не зваживши все за і проти. Що може загрожувати біометричним системам? Проблема в тому, що «втрачені» голос або дані геометрії обличчя використовувати знову буде неможливо. Зрозуміло, «втратити» їх не так просто: вони спеціальним чином перетворюються і потім зберігаються у спеціальному сховищі.

У фантастичних фільмах погані хлопці відрізають пальці, записують голос, роблять 3D-маски обличчя або долоні муляжі. Ці варіанти атаки справді існують, але вони спрямовані лише на систему зчитування біометричних даних. Насправді векторів атак набагато більше. Наприклад, можна зламати сам зчитувач, і хоч би що йому пред'являли, він видаватиме помилку. Можна втрутитися у роботу системи верифікації та змінити рішення системи на потрібне зловмисникам. Можна зламати сховище біометричних профілів та внести нові, а також підмінити/знищити наявні дані щодо потрібних людей. І це, мабуть, найнебезпечніший варіант для будь-якої схеми біометрії.

Наразі існує не менше півтори десятки способів зламати систему біометричної ідентифікації, і вибір найзручніших із них залежить від конкретних завдань, що стоять перед хакерами. Якщо потрібно дискредитувати всю систему, атака буде спрямована на сховище біометричних профілів. Якщо потрібно змусити систему прийняти «правильне» рішення, ефективніше атакувати систему верифікації. Коли дії зловмисників спрямовані на конкретну людину, то логічніше синтезувати її голос та відео. Існуючі технології вже дозволяють, маючи запис голосу або відео будь-якої людини, синтезувати її мову або накласти її на інший відеозапис.

Наразі існує таке поняття як Big Data. Big Data – це термін, який використовується для опису великих обсягів даних, що важко обробити за допомогою традиційних методів та інструментів.

Ці дані мають три основні характеристики, відомі як «3V»: Volume (Обсяг), Variety (Різноманітність) і Velocity (Швидкість). Додатково, інколи розглядають також Veracity (Достовірність) та Value (Цінність). Ось більш детальний опис кожної з цих характеристик:

Volume (Обсяг): Величезна кількість даних, що генерується різними джерелами, такими як соціальні мережі, сенсори, транзакції, мобільні пристрої тощо.

Variety (Різноманітність): Дані можуть бути структурованими (таблиці, бази даних), неструктурованими (тексти, зображення, відео) або напівструктурованими (XML-файли, лог-файли).

Velocity (Швидкість): Дані генеруються та обробляються в режимі реального часу або близькому до нього.

Veracity (Достовірність): Якість та точність даних, що впливає на достовірність отриманих результатів.

Value (Цінність): Корисність даних для прийняття рішень, отримання нових знань та створення цінності для бізнесу чи інших сфер діяльності.

Обробка Big Data вимагає спеціалізованих технологій та інструментів, таких як Hadoop, Spark, NoSQL бази даних та інші платформи, що дозволяють ефективно зберігати, обробляти та аналізувати великі обсяги даних.

Почнемо з методу розпізнавання осіб у Big Data системи вуличного відеоспостереження. Існуючі алгоритми Machine Learning можуть успішно розпізнати людину навіть по 70% обличчя, наприклад, якщо вона частково його приховала під медичною маскою. Окуляри, головні убори, борода та вуса знижують точність розпізнавання приблизно з 95 до 92%. При цьому такі способи маскування підвищують ймовірність помилкового спрацьовування (помилка 1-го роду по confusion matrix) приблизно в 5 разів – до рівня 0,01%. Менш складні біометричні системи, встановлені на індивідуальних пристроях типу смартфона, можна обдурити навіть без використання спеціальних пристроїв. Відмічаються множинні випадки зламування Face ID від Apple за допомогою близнюків або візуально схожих людей. Наприклад, в'єтнамська фірма Bkav змогла зламати цей пристрій за допомогою недорогої маски лише за $200. А рухливі 3D-муляжі на основі випадкових фотографій із соцмережі Facebook допомогли вченим Університету Північної Каролiни обдурити 4 з 5 систем розпізнавання облич ще у 2016 році. Сценічний макіяж (грим), перуки та кольорове скло окулярів також підвищують ймовірність того, що алгоритм Machine Learning помилиться, зробивши хибне спрацьовування або помилкову відмову.

У 2017 році хакери змогли обдурити сканер райдужної оболонки ока смартфона Samsung Galaxy S8, підробивши райдужку за допомогою звичайної контактної лінзи, на яку було розміщено знімок чужого ока. Така імітація була зроблена за допомогою цифрового фото ока з високою роздільною здатністю в режимі нічної зйомки, коли вимкнено інфрачервоний фільтр. Роздрукувавши на лазерному принтері фото з попередньо відкоригованим налаштуванням яскравості та контрасту, зловмисники наклеїли його просту контактну лінзу і показали сканеру смартфона. Також подібним чином було дискредитовано дактилоскопічний сканер, який прийняв за справжній відбиток пальця підробку, роздруковану струмопровідним чорнилом на глянцевому папері. Таким чином дослідники cybersecurity з університету Мічігану США успішно обдурили вбудовані сканери смартфонів Samsung Galaxy S6 та Huawei Honor 7.

А інженери з Берлінського технічного університету продемонстрували, як можна обійти біометричну систему автентифікації за рисунком вен на долоні. Для цього вони розробили прототип приладу, який непомітно збирає ці біометричні дані за допомогою одноплатного комп'ютера Raspberry Pi та компактної цифрової камери без інфрачервоного фільтра. Отримані фото долонь було опрацьовано з метою чіткого виділення вен, на місці яких були намальовані однопіксельні лінії. Потім зображення було роздруковане та залите воском, що імітує поверхню шкіри. Працездатність цього способу була показана на реальному обладнанні Hitachi і Fujitsu в 2018.

У 2019 році стало відомо про можливість обдурити сканер відбитка пальців смартфона Samsung Galaxy S10 за допомогою моделі штучного пальця, роздрукованого на 3D-принтері. Тоді ж, у 2019 році, дактилоскопічний сканер смартфона OnePlus 7 Pro був введений в оману муляжем, зробленим із фольги та клею ПВА.

Вищеописані інциденти грунтувалися на точному копіюванні біометричних даних конкретної людини. Однак деякі фрагменти папілярних візерунків у багатьох людей є загальними. Тому ще у 2017 році було запропоновано спосіб обману біометрії за допомогою універсального «майстер-відбитка». Вчені Нью-Йоркського та Мічиганського університетів за допомогою технологій Big Data проаналізували 8,2 тисячі відбитків і виявили 92 універсальні фрагменти для кожної групи з 800 випадково відібраних зразків, який принаймні на 4% точно збігався з іншими. Дослідники відзначають, що основі такої фрагментації можна створити цілу низку «майстер-відбитків», здатних обдурити практично будь-яку систему дактилоскопічної біометрії.

Deep Fake – загроза для біометрії

У 2019 році світ охопила істерія під назвою Deep Fake, коли за допомогою технологій глибокого машинного навчання (Deep Learning) почали створюватися численні аудіо- та відео-підробки на реальних людей. При цьому використовується генеративно-змагальні мережі (GAN, Generative Adversarial Network), коли одна нейромережа генерує підробку, а інша розпізнає її. Таким чином, обидві мережі тренують одна одну, поступово доводячи результат до досконалості.

Штучний інтелект вже використовується різними типами загроз, а кількість кібератак із його застосуванням зростає з кожним роком. Найбільш небезпечною є загроза в контексті соціальної інженерії, де генеративний штучний інтелект може допомогти зловмисникам створювати досить переконливий аудіо та відео контент. Серед інших найпоширеніших схем із використанням такого контенту зловмисниками є:

Обхід аутентифікації: дипфейк-технологія допомагає шахраям видавати себе за користувачів під час перевірок на основі селфі та відео для створення нових облікових записів та отримання доступу до них.

Зламування корпоративної електронної пошти: штучний інтелект дозволяє обманом змусити жертву перевести кошти на аккаунт під контролем шахрая. Також можуть використовуватися аудіо та відео дипфейки для маскування під генеральних директорів та інших керівників під час телефонних дзвінків та онлайн-зустрічей.

Шахрайство з видачею себе за іншого: програми, створені на базі великих

мовних моделей (LLM), відкриють нові можливості для шахраїв. Завдяки даним, отриманим зі зламаних або загальнодоступних облікових записів у соцмережах, шахраї можуть видати себе за жертву віртуального крадіжки та інших афер, призначених для обману друзів та близьких.

Афери з впливовими особами: у 2025 році очікується використання шахраями технології штучного інтелекту для створення підроблених або дублюючих облікових записів знаменитостей, впливових осіб та інших відомих людей у соцмережах. Зокрема, зловмисники можуть опублікувати дипфейк-відео, щоб заманити передплатників поділитися особистою інформацією та грошима.

Шахраї зламують як звичайних користувачів, так і популярні Telegram-канали та відправляють шкідливі посилання: у першому випадку контактам від імені зламаного користувачам, у другому – від імені власника із закликом купувати якісь товари, за когось проголосувати та просто просять гроші на вигадані потреби. Свої повідомлення шахраї стали супроводжувати дипфейками відео або аудіо, які повинні переконати користувачів у їхній легітимності.

За даними поліції Гонконг, співробітницю фінансової служби міжнародної компанії обманом змусили виплатити 25 млн. доларів шахраям, які за допомогою технології «дипфейк» видавали себе за фінансового директора компанії під час відеоконференції.

Користувач соцмережі, досвідчений розробник, використовував технологію дипфейків, щоб допомогти другу влаштуватися на роботу, замінивши свою особу на особу друга під час відеоспівбесіди. Для підготовки до інтерв'ю використовувалася програма, навчена на датасеті із 10 тис. фото друга. Після того, як на першій співбесіді хлопців розкусили через збій синхронізації дипфейка, вони навчили модель заново протягом тижня, і на другій співбесіді все пройшло успішно: другові запропонували роботу із зарплатою 4 тис. доларів на місяць.

Поступово дипфейки стали загрозою навіть судам, страхових компаній, дослідницьких інститутів, у яких справжність доказів і джерел особливо важлива.

Несумлінні компанії тепер можуть відмовити у задоволенні законних претензій, посилаючись на те, що представлені дані фейк. Так, у реального користувача заблокували гроші, оголосивши, що він дипфейк.

За допомогою штучного інтелекту можна створювати дипфейки на медичну тематику, наприклад, статистичні дані пацієнтів, медичні знімки (КТ, МРТ, рентгенівські зображення), відео з лікарями, наукові публікації та дослідження. Це несе серйозні ризики, якщо використовувати дипфейки зі злим наміром.

Шахраї опублікували фейковий відеоролик на YouTube, видавши його за офіційний виступ мільярдера Ілона Маска на конференції Bitcoin-2024, де він обіцяє безкоштовну роздачу різних крип-

товалютів. У фейковому ролику від користувачів потрібно надіслати на вказану адресу будь-яку суму. Аферистам вдалося зібрати з довірливих користувачів фінансових активів суму 28 586 доларів.

Дипфейки, як виявилося, завдають чимало клопоту. 72% опитаних щодня турбуються про можливість шахрайства з використанням дипфейків, що може призвести до крадіжки їхніх грошей чи особистої інформації. 45% компаній стурбовані здатністю генеративного штучного інтелекту створювати складніші синтетичні особистості. Очікується, що ринок дипфейк-технології на базі штучного інтелекту значно розшириться, збільшившись з 564 млн. доларів у 2024 р. до суттєвої суми в 5,13 млрд. доларів до 2030 р.

Дипфейки еволюціонують загрозливими темпами. Ще два роки тому підробки легко було відрізнити за низькою якістю передачі руху; крім того, люди в таких відео практично ніколи не моргали. Однак технології не стоять на місці, і дипфейки останнього покоління виконані помітно якісніше.

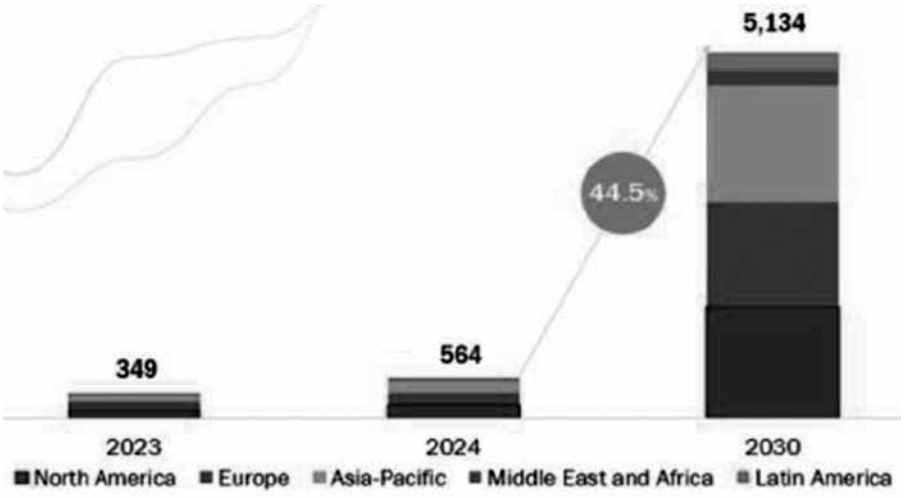
Група з безпеки штучного інтелекту Європейського інституту телекомунікаційних стандартів (European Telecommunications Standards Institute, ETSI) опублікувала звіт про ризики використання ІІ для маніпулювання «образами цифрової ідентичності»; у документі йдеться про атаки на системи дистанційної біометричної ідентифікації та аутентифікації за допомогою дипфейків.

«Найнадійнішим методом протистояння ризикам для компаній і організацій може стати розробка ретельно опрацьованих процесів, де важливі рішення і транзакції схвалюються не на основі внутрішньої біометричної аутентифікації, але завжди підтверджуються за стандартною процедурою, що включає мультифакторну аутентифікацію», – резюмують автори звіту.

В ухваленому ЄС законі про регулювання штучного інтелекту міститься вимога про обов'язкове маркування дипфейків водяними знаками.

Як захистити біометричні дані від крадіжки та злому

Держструктури, банки, виробники гаджетів та розробники мобільних додатків все частіше використовують біометрію, щоб ідентифікувати користувачів. Аутентифікація по обличчю чи відбитку пальця для багатьох стала вже звичною справою. Здавалося б, «вкрасти обличчя» зараз навіть простіше, ніж вкрасти пароль: наші фото та відео є у соціальних мережах, на записах камер відеоспостереження. Зрештою, сфотографувати нас може будь-який перехожий у метро чи на вулиці. На практиці відбитки пальців теж вкрасти не так складно зі скляної поверхні і навіть по відеозапису. Але сила біометричних даних над їх секретності, а способах захисту від підробок.



Види атак на біометричні дані користувачів

Біометричні дані використовують державні служби, банки, виробники гаджетів і розробники додатків, які зберігають важливу інформацію користувача або гроші. Аутентифікація з біометрії допомагає переконатися, що до облікового запису входить саме та людина, на яку він зареєстрований. Адже пароль може ввести будь-хто - підглянувши, підслухавши або підібравши його за допомогою хакерської програми, а ваші обличчя, руки і голос є тільки у вас.

Але чи надійний цей спосіб насправді і що буде, якщо шахраї вкрадуть біометричні дані? Скомпрометований пароль можна змінити, а ось з індивідуальними характеристиками такий фокус вже не пройде.

Атаки на біометричні системи бувають трьох видів. Зловмисники можуть:

– ***Змусити користувача авторизуватись у системі.*** Так само як у випадку з паролем, за допомогою методів соціальної інженерії або прямих погроз зловмисники можуть змусити користувача подивитися в камеру, вимовити потрібну фразу або прикласти палець до датчика, щоб отримати доступ до його облікового запису.

– ***Вкрасти дані користувача: у нього самого чи з бази.*** Насправді біометричні дані не такі секретні, як про них звикли думати. Особи є на фотографіях та відео в соціальних мережах, на записах із відеореєстраторів та камер відеоспостереження. Щоб отримати зразок голосу, можна просто зателефонувати людині та вивести її на розмову. А відбитки пальців можна зняти з будь-якої скляної поверхні навіть по фотографії. Компанія Cisco Talos, яка спеціалізується на кібербезпеці, ще 2020 року опублікувала звіт про те, як фахівцям вдалося відновити відбитки пальців із більшості дзеркальних поверхонь із точністю близько 80%. Ще одне підтвердження: у 2021 році силовики змогли вирахувати та посадити наркоторговця, який виклав у Мережу фотографію із сиром у руках. На фотографії читалися його відбитки, які допомогли співробітникам правопорядку ідентифікувати злочинця. Щоб отримати біометричні дані, сьогодні не потрібно навіть зламувати базу – все є у відкритому доступі.

– ***Зламати систему біометричної автентифікації.*** Зловмисники можуть зламати сховище та підмінити дані користувачів, щоб входити до їхніх облі-

кових записів за своїми відбитками пальців, обличчям або голосом. Або втрутитись у роботу системи верифікації та вплинути на її вирішення, щоб будь-які дані зі сканера вона вважала коректними. Але зазвичай злочинці намагаються піти найпростішим шляхом, а влаштовувати атаки на банківські чи державні біометричні системи для них надто складно та дорого. Крім того, якщо система захищена настільки погано, що її можна легко зламати, то неважливо, як влаштовано автентифікацію користувачів, – за допомогою біометрії, пароля або коду перевірки.

У першому та третьому випадку, якщо користувач сам пройшов верифікацію або зловмисники зламали систему автентифікації, взагалі не має значення, які дані вона запитувала на вході – пароль, відбиток пальця чи ще щось. Хоча і в цих випадках біометрія забезпечує більший захист, ніж секретний пароль. А ось із другим типом атак та способами захисту від них розглянемо докладніше.

Захист бази

По-перше, зламати державне чи банківське сховище, щоб вкрасти біометричні дані користувачів, – справа дуже клопітна та ризикована. Це не те саме, що обманом змусити довірливих користувачів авторизуватися в системі та перевести всі гроші на підставний рахунок.

А по-друге, самі біометричні дані, які використовуються для входу в систему, ніде не зберігаються лише їх хеш. Розглянемо, як це працює, на конкретному прикладі.

Щоб входити до банківської програми за допомогою відбитка, користувач спочатку надає банку зразок. Коли він вперше прикладає палець до сканера, система отримує унікальний малюнок і за допомогою хеш-функції перетворює його на рядок із певним набором символів.

Саме цей рядок і зберігається в базі, а не сам відбиток. На відміну від фотографії, такий запис займає набагато менше місця.

Коли наступного разу користувач спробує увійти до програми з відбитком, система знову перетворює дані зі сканера на хеш і шукатиме аналогічний запис у базі. Порівнювати записи набагато швидше, ніж зображення та фотографії, тому для користувача верифікація відбувається миттєво.

Але головне – хеш-запис неможливо перетворити назад на відбиток пальця, який потрібен для аутентифікації. Тобто навіть якщо зловмисники зламають базу та вкрадуть дані, вони не зможуть відтворити відбитки користувачів та використовувати їх для входу – хеш до сканера не додаси.

Те саме відбувається з будь-якими іншими біометричними даними. До речі, навіть паролі вже більше 20 років не зберігаються у відкритому вигляді – тільки в хеш-записах, щоб сисадмін, який обслуговує базу, не міг непомітно увійти в обліковий запис від імені користувача.

Захист від підробок та імітації

За 10 років біометрія зробила крок далеко вперед: у 2013–2014 роках банки тільки починали впроваджувати розпізнавання голосу по телефону, щоб скоротити кількість додаткових перевірок для користувачів, а сьогодні ми вже обговорюємо оплату проїзду в метро та аутентифікацію в банкоматах за унікальними рисами особи.

В умовах, коли біометричні дані знаходяться буквально у відкритому доступі, головним захистом залишається здатність систем автентифікації відрізнити дані живої людини від підробки, створеної зловмисниками. Liveness, або так звана перевірка на жвавість. Адже сила біометричних даних над секретності, а їх неповторності.

Голос

Найпростіший спосіб біометрії – за голосом. Ще до того, як банківські програми з входом по відбитку пальця

набули широкого поширення, банки почали впроваджувати розпізнавання голосу.

Коли клієнт дзвонив до банку з якимось питанням, система визначала, наскільки його голос схожий на зразок, що є в базі. І якщо не схожий, йому ставили додаткові запитання. Наприклад, просили назвати останні операції на карті. Чим більше було сумнівів у тому, що телефонував власник картки, тим більше етапів перевірки потрібно було пройти.

З ускладненням атак почали з'являтися нові способи захисту.

Можливі атаки

Усі вони базуються на тому, що зловмисники мають зразок голосу користувача.

– Відтворити запис голосу на момент автентифікації.

– Використовувати штучний інтелект, який говоритиме голосом користувача.

– За допомогою спеціальної програми зробити так, щоб зловмисник говорив голосом користувача.

Способи захисту

– Задавати раптові нетипові питання, яких зловмисники не могли б передбачити. Наприклад, назвіть поточну дату або скажіть, який курс гривни до долара.

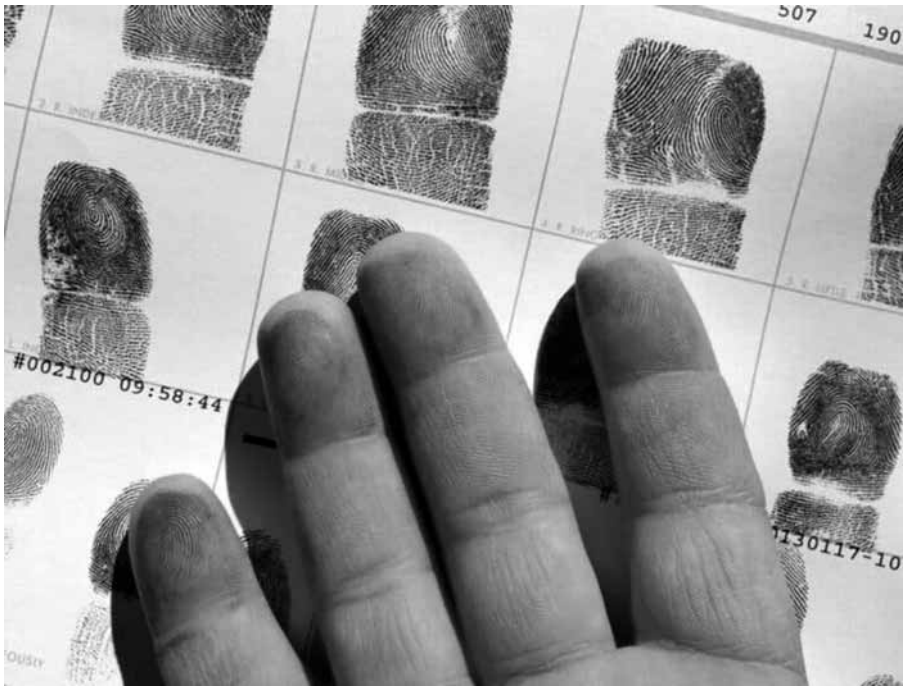
– Враховувати час відповіді. Щоб штучний інтелект обробив запит і видав потрібну відповідь, потрібно більше часу, ніж відповідь живої людини.

– Паралельно використовувати інші способи верифікації користувача: відеокамеру, пароль, SMS-код.

– Використовувати методи визначення синтезованої мови, деталі яких не наводяться їх розробниками з метою безпеки.

Відбитки пальців

Отриманий зразок відбитка пальця потрібного користувача можна зімітувати під час автентифікації. Наприклад, наклеїти на свій палець підробку із желатину. Для цього можна взяти відбиток, зробити його рельєфним за допомогою фотошопу та надрукувати на принтері форму для заливки. Залити цю форму желатином, а після застигання наклеїти на палець. Також зловмисники



можуть використати глину, стоматологічний гіпс і навіть пластилін. Але й від таких атак є захист.

Можливі атаки

– Відтворити відбиток пальця за допомогою гіпсу, пластиліну, желатину чи глини.

Способи захисту

Перевіряти за допомогою датчиків:

– температуру тіла в момент аутентифікації – виготовлені зразки завжди будуть холоднішими;

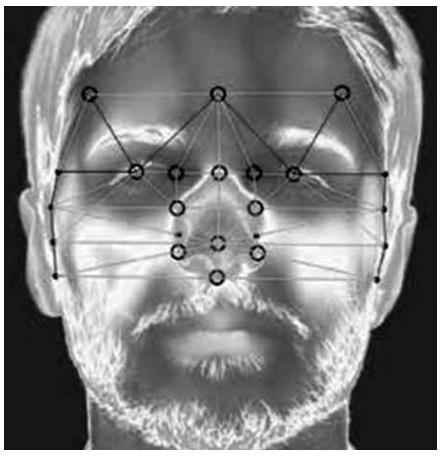
– електропровідність пальця;

– пульс – за допомогою оптичних або ультразвукових датчиків.

Сама по собі підробка відбитків пальців – надто складне та накладне заняття для шахраїв. Їм набагато простіше працювати з банками, які взагалі нічого не перевіряють, ніж добувати та відтворювати відбитки користувачів без гарантії, що у них на рахунках взагалі є гроші.

Обличчя

Щоб провести аутентифікацію, зловмисникам потрібні фотографії або відео, на яких добре читається обличчя користувача.



Можливі атаки

Щоб увійти до системи, зловмисники можуть використати:

– фото чи відео користувача;

– маску;

– грим;

– синтезовану за допомогою штучного інтелекту модель користувача.

Способи захисту

– Попросити користувача посміхнутися, моргнути чи зробити інший рух обличчям – заздалегідь заготовлені фото та відео не пройдуть такої перевірки.

– Попросити користувача піднести до обличчя паспорт, щоб порівняти зображення – шахраї можуть зімітувати обличчя, але не паспорт.

– Використовувати інфрачервоні камери, які здатні зчитувати рельєф обличчя – фото- та відео будуть плоскими.

– Перевірити температуру за допомогою інфрачервоної камери – фото, відео, зліпки та маски будуть холодними.

– Визначити за допомогою камери картину кровоносних судин обличчя, яка відрізняється навіть у близнюків. Наприклад, така функція вже є у камерах iPhone.

– Контролювати датчики зчитування та стежити за підключенням шкідливого ПЗ у момент аутентифікації, яке може імітувати особу користувача.

– У момент аутентифікації за допомогою камери відстежувати мимовільний рух зіниць, щоб переконатися, що око живе, а не імітація.

– У складних випадках підключити до перевірки живого модератора.

Проблеми з точністю ідентифікації користувачів по обличчю виникають зазвичай через те, що система перевірки налаштована погано. На конференції з безпеки Offzone-2018 презентували дослідження, у якому згадувався цікавий спосіб обходу «перевірки на жвавість». В одному випадку для ідентифікації потрібно було подивитися в камеру та зробити певний рух обличчям. Дослідники взяли фотографію користувача, згорнули навпіл і доклали до половини свого обличчя. Коли система попросила посміхнутися, усміхнулася лише частина особи, але цього виявилося достатньо. Тобто половина фото допомогла пройти перевірку на рисах обличчя, а половина живої особи – перевірку на міміку. В іншому випадку сервіс виконував перевірку із затримкою, тобто можна було спочатку показати камері фотографію користувача, а потім усміхнутися «іншою особою», і перевірка вважалася пройденою.

Висновок

Ідентифікація користувача за допомогою пароля тримається на тому, що його знає лише одна людина. Тут вкрай важливий чинник секретності: якщо хтось дізнається пароль, його доведеться міняти. Біометричні дані не можна скомпрометувати в такий спосіб. Навіть якщо всі фотографії або всі відбитки пальців всіх людей на планеті будуть доступні для зловмисників, це не вплине на надійність аутентифікації. Головний захист цієї системи в тому, що живу людину неможливо зімітувати повністю. Навіть коли йдеться про близнюків, відбитки пальців, риси обличчя та розташування судин у них різні. Якщо шахраї навчаться обходити один тип перевірки, розробники біометричних систем вигадають інший.

Зловмисники можуть підібрати пароль від облікового запису або змусити користувача ввести його самостійно і навіть надіслати їм SMS-код. Але автентифікація за допомогою біометрії переводить протистояння на новий рівень: це вже не боротьба шахраїв із простою людиною, це боротьба шахраїв із системою, і перемогти в ній буде набагато складніше.

Д. Мусієнко

https://vaiti.io/kak-zashhitit-biometricheskie-dannye-ot-krazhi-i-vzloma/

https://lukatsky.blogspot.com/2016/12/blog-post.html

https://www.forbes.ru/tehnologii/367261-obmani-menya-kak-hakery-obhodyat-sistemy-biometricheskoy-zashchity

https://bigdataschool.ru/blog/biometrics-hacks-use-cases.html

https://www.secuteck.ru/articles/dipfejki-uzhasy-iskusstvennogo-intellekta

https://www.eset.com/ua-ru/about/newsroom/blog/smart-technologies/budushcheye-tekhnologiy-ili-kiberugroza-chto-ozhidat-ot-iskusstvennogo-intellekta-v-2025-godu/

https://d-russia.ru/dipfejki-kak-sredstvo-vzloma-sistem-biometricheskoj-identifikacii-otchjot-evropejsko--instituta.html

Системи відеоспостереження для безпеки чи для адміністрування?

У будь-якого ринку, незалежно від його призначення, є лише три корпоративні цілі – прибуток, зростання та подальша діяльність. Ринок технічних засобів безпеки (ТЗБ) не виняток. І жодної безпеки свого клієнта з його метою не значиться. Його завдання – лише виконати вимоги замовника. А для правильної постановки завдання споживач повинен сам мати хоча б базові знання, а простіше кажучи, чітко сформулювати, що він хоче зрештою отримати. Зовсім небезпечно сліпо йти керуючись пропозиціями ринку, оскільки такі пропозиції цілком будуть спрямовані на вирішення виключно ринкових завдань – прибуток, зростання, подальша діяльність – а не на кінцеву потребу замовника.

Ще кілька десятків років тому між ринком ТЗБ і кінцевим споживачем стояла якась структура або окремі фахівці від імені власне безпеки, що володіла всім комплексом питань і розглядала технічну систему не більше як інструмент, що дозволяє знизити витрати для вирішення кінцевої задачі. Сьогодні через абсолютно невиправдану економію з боку споживача, і суто з ініціативи самого ринку в більшості випадків у питаннях безпеки замовник почав спілкуватися з ринком ТЗБ безпосередньо. Ну, а якщо так, то безпекою в повному обсязі доведеться займатися саме клієнту. Сьогодні практично будь-яка встановлена десь, кимось і якось відеокамера у масовій свідомості асоціюється із підвищенням заходів безпеки. Камера стала мало не синонімом безпеки. А якщо таких камер сотні – це вже «безпрецедентні заходи безпеки». Зрозуміло, що ринок при цьому швидко розвивається. Це можна назвати перемогою ринку над безпекою.

З іншого боку, не всіх споживачів цієї безпеки, такий стан справ влаштовує. Ще момент, що заслуговує на дуже пильну увагу. Практично вся електронна апаратура з моменту становлення ринку подешевшала на порядок. Але, з іншого боку, порядки зросли вартості технічних систем. А все, що стосується відео, насамперед. І причина зовсім не у стрімкому зростанні зарплат монтажників, проектувальників чи відсотка прибутку. Просто сьогодні замовник масово платить за величезну кількість незатребуваних функцій та можливостей. У пошуку конкурентних переваг виробник вигадує нові і нові опції для свого обладнання просто тому, що відрізнятися від продукції конкурентів – це його життєва необхідність. А оскільки конкурентна перевага стає такою за умови його значущості для споживача, переконує свого клієнта, що нова властивість йому конче необхідна. Причому часто зовсім щиро, оскільки сам не володіє в належному обсязі кінцевим споживчим результатом, будучи фахівцем зовсім іншої галузі.

«Відеореєстрація сьогодні є найголовнішою функцією систем відеоспостереження!» – це гасло взяте дослівно зі ЗМІ ринку технічних засобів безпеки. А насправді можна сказати, що відеореєстрація має опосередковане відношення до безпеки, на відміну від відеоспостереження. Ось і розставимо усі крапки над «і».

Будь-який виробник термін «безпека» намагатиметься приліпити до своїх товарів та/або послуг на будь-якому ринку, якщо є хоч якийсь привід. Оскільки знаходиться безпека на найнижчих рівнях ієрархії потреб, а, значить, товар матиме максимальну купівельну привабливість. Але споживачеві важливо не те, що декларується, а що він отримає насправді. Тому має сенс дати конкретне визначення, що особисто ми під цим розумітимемо.

Отже: безпека – це умови середовища, у яких потенційно можлива небезпека не може бути реалізована.

Цілком логічним буде вислів: безпека, тобто без небезпеки. Небезпеки просто не повинно бути.

Перший важливий момент – безпека завжди відноситься до конкретної потенційної загрози. Не буває безпеки взагалі від усього. Потрібно спочатку уявляти, від яких загроз ми збираємося захиститися і, відповідно, будувати всю схему. Таким чином, починається будь-яка безпека з аналізу загроз. Цей момент зараз масово ігнорується. А спочатку на ринку були навіть фірми, в діяльність яких входили аналіз загроз, і побудова моделей реагування.

Другий момент – це умови середовища, тобто цілий комплекс організаційно-технічних заходів, спрямований на своєчасну та адекватну реакцію потенційні загрози.

І третій момент – потенційно можлива небезпека не може бути реалізована. Тобто своєчасна та адекватна реакція має бути в обов'язковому порядку успішною. Просто деякі зусилля, незалежно від вкладень у них, але які досягли мети, до безпеки не відносяться.

Будь-які технічні засоби безпосередньо у визначенні не фігурують і власне ніякої безпеки не несуть. Це лише інструмент, покликаний, як і будь-який інструмент, знизити собівартість рішення кінцевого завдання. Розставте по периметру озброєних бійців із інтервалом 5 метрів, і жодна відеосистема вам у принципі не знадобиться. Але це дуже дорого та далеко не всім доступно.

Відеореєстрація має зареєструвати певну подію. Тобто сама подія вже трапилася, і через визначення безпеки ніяк не може відноситися до такої в принципі, оскільки безпека покликана сама подію не допустити. Хоча зменшувати роль відеореєстрації у вирішенні величезного переліку питань не варто. Насамперед, це, звичайно, розшук і слідство. Звичайно, лиходія, якщо він з'явився таким, треба неодмінно знайти та знешкодити. Тільки небезпека в цьому випадку вже відбулася, а безпеки не сталося. Реєстрація будь-якого роду, в тому числі і відео, застосовується повсюдно і в багатьох галузях. Тільки до безпеки її відносять виключно на нашому ринку ТЗБ. У кожному літаку є чорні скриньки. Без увімкненої «чорної скриньки» не погасне табло біля пілота «До зльоту не готовий». Але ніхто не відносить «чорну скриньку» до системи безпеки польоту. Парашут відносять, а «чорна скриньку» – ні. І навряд чи пасажир відчує себе безпечніше, якщо дізнається, що на авіалайнері, на якому він летить, найкраща у світі «чорна скринька». Або, скажімо, відеореєстратор в автомобілі – всім очевидно, що знадобиться саме тоді, коли небезпека вже трапилася. Сам собою цей

ISSN 1819-9429 00153>

№ 4/2024 (157)

ISSN 1819-9429 00157>

9 771819 942003

40226 - передплатний індекс в Укрпошті

www.bsm.com.ua

Бізнес і безпека

більш детально, читайте на стор. <None>

чудовий пристрій ніякої безпеки не додає і до такої ніяк не відноситься.

Камери контролю швидкісного режиму, всупереч численним заявам влади всіх рівнів, до безпеки не належать відповідно до нашого визначення. Вони лише зафіксували факт порушення швидкісного режиму, що відбувся, який може являти собою дійсну небезпеку, але далі за прийнятою стандартною схемою ніяких дій щодо його припинення не сталося. Причини порушення не встановлені – водій міг перебувати у неадекватному стані та рухатись далі, становлячи небезпеку для оточуючих. Або навпаки, порушення швидкісного режиму було вимушеним і пов'язане із запобіганням потенційній аварії. З точки зору безпеки «живий поліцейський» з радаром є більш ефективним рішенням. Але знову ж таки, у таких масштабах це суттєво дорожче.

Щоб принципово розділити технічні системи за їх споживчими функціями віднесемо всі завдання, що стосуються фіксації подій, до систем адміністративних, незалежно від їх важливості, включаючи і розшук, і слідство, і просто адміністративний контроль чогось.

Отже, якщо система покликана запобігти якійсь події, тобто події не має статися, це система безпеки. Якщо покликана зафіксувати подію, що відбулася, для наступних дій, це система адміністрування. У межах того самого об'єкта, зазвичай, існують обидві системи. Але біда нашого ринку в тому, що два абсолютно різні завдання – безпека та адміністрування – найчастіше намагаються вирішити в рамках єдиної технічної системи без урахування об'єктивних можливостей та обмежень. І з величезними переплатами за незатребувані функції.

Якщо якийсь приватний об'єкт може бути оснащений відповідно до власних індивідуальних вимог, з урахуванням конкретних умов та можливостей, то при побудові систем для державних установ як головна вимога виступає виконання якихось кимось розроблених та затверджених приписів, наказів абсолютно безвідносно реальних умов та можливостей.

Мірилом ефективності є запевнення саме ринку щодо технічних параметрів обладнання. А наскільки вони можуть бути реалізовані у конкретній системі, цього часто просто не знають. У тому числі й ті, хто розробляв такі керівні документи.

Ринок породив (свідомо) у споживачі впевненість у тому, що чим камер у системі більше, параметри їх досконаліші, тим вся система ефективніша.

Цілком виправдано з позиції ринку – чим більше продано, чим продано дорожче, тим краще. І споживач (а то й сам ринок) часто просто не знає про ті об'єктивні обмеження, які здатні зробити навіть саму «навернену» систему і неефективною, і не виправдано дорогою через переплату за явно не потрібні функції.

Тому що система оцінюється не за кінцевим споживчим завданням, не більше ніж інструмент для його вирішення, а сама по собі, за суто технічними параметрами.

Перше дуже важливе обмеження – обсяг візуальної інформації, яку може повноцінно сприймати оператор. Так, чим більше інформації, якою володіє оператор для своєчасного оголошення тривоги, тим, безперечно, краще. Однак, цей обсяг об'єктивно обмежений нашими фізіологічними можливостями. І якщо обсяг інформації, що надходить, перевищує той, який може обробити мозок оператора, значить, якась інформація пройде зовсім непоміченою. А наскільки такі пропуски будуть актуальними для безпеки, ніхто заздалегідь сказати не може.

За дослідженнями ще початку 90-х років минулого століття, один підготовлений оператор може контролювати одночасно 6-8 зображень. Це насправді так. Причому, 8 зображень були в змозі відстежувати небагато операторів. У більшості при такому навантаженні виявлялися явні провали в оцінці інформації, що надійшла. У всіх казино, які доводилося оснащувати відеоспостереженням, на одного підготовленого оператора ніколи не припадало більше шести зображень. Причому це був не один монітор, поділений на 6 картинок з різних камер, а шість моніторів, на кожен з яких на повний екран було виведено зображення з однієї камери. При цьому мінялися оператори кожні 2:00. Маючи крісло, оператори все одно працювали стоячи через дуже високу напругу уваги. Ну, і заробляли оператори, немало. А тепер, шановний споживач, порівняйте ці умови з тими, які ви маєте в реальності. Якщо перед вашим оператором (він же сторож, він же вахтер, він ще й ключі видає і протипожежні обходи здійснює) сяють на одному або парі моніторів 9 зображень від найсучасніших 3-мегапіксельних камер, можете вважати, що він не бачить нічого. І додаткові камери, які встановлюються в рамках підвищення заходів безпеки, насправді безпеку лише знижують.

Тепер поговоримо про «мегапіксельність». Або про високу роздільну здатність відеокамер. Це наступний, ініційований ринком момент введення споживача в оману. Точніше, ринок не спромігся дати роз'яснення з цього питання. Тому що треба було повсюдно впроваджувати IP-відеоспостереження, а далі на його основі створювати всілякі програмні продукти, «хмарні послуги» тощо. А IP-камера може «похвалитися» лише високою роздільною здатністю. І більше нічим. І у споживача при мовчанні ринку (і навмисно, і з власного незнання) почала формуватися дуже невірна і небезпечна помилка: чим вища роздільна здатність, тим більше можна побачити. Все те саме, як і з кількістю камер – наш мозок може сприйняти стільки інформації, скільки здатний обробити, а наше око здатне побачити те, що дозволяє людський зір.

Ми ніколи не розглянемо мишу на полі з висоти 50 метрів. А сова – запросто. Так у неї зір влаштований, сітківки двох очей майже весь розмір голови займають. Тому й бачить. А ми побачимо те,

що нам дано природою. Не випадково батьки телебачення зупинилися на частотному спектрі в 6 МГц (для стандарту PAL) і горизонтальному дозволі в 550 телевізійних ліній. Тому що на максимальних розмірах екранів того часу все одно око більше не розгляне. Могли б і 7 МГц зробити. Напружилися б і 8 МГц подужали. Але сенсу в цьому не було.

Можливості нашого зору визначаються полем зору сцени, яка відображається на екрані певної величини. А поле зору камери визначається фокусною відстанню об'єктива та форматом матриці камери. За дослідженнями отримано такі результати для діагоналі зображення 12":

- щоб помітити людину, поле зору по горизонталі має становити 20 м;
- читати номер автомобіля - 2 м;
- упізнати незнайому людину - 2 м;
- упізнати знайому людину - 5 м.

Слід сказати, що дані, схоже, враховують реальну ситуацію на реальному посту спостереження – з відволіканнями на іншу інформацію, перегляд одночасно кількох зображень тощо. Якщо уважно дивитися в монітор, то людину помітите при полі зору і в 50 метрів.

Принагідно – дані щодо настільки популярних нині дозволів Full HD і 4K. Роздільна здатність Full HD починає бути видною при діагоналі екрану 27", а 4K починається від 39". Подивіться, які телевізори продаються – ні в кого на ринку телевізорів не вистачає нахабства оголосити дозвіл 4K на діагоналях менше 39" хоч і могли б – покупець однаково не помітить різниці. Натомість на ринку ТЗБ вже пропонують відеодомофони з дозволом 4K. А щоб продемонструвати дозвіл 8K на виставці в Лос-Анжелесі, фірма Samsung привезла із собою екран із діагоналлю 12 метрів.

А тепер заміряйте діагональ не ваших моніторів на посту спостереження, а зображень, які реально спостерігає оператор. Особливо вражає пропозиція перегляду камер високої роздільної здатності на екрані смартфона. За таких реальних умов формату екрану 720 х 576 більш ніж достатньо.

Зрештою, ейфорія високої роздільної здатності і незнання базових моментів призводять до того, що споживач встановлює ширококутну камеру високої роздільної здатності в надії, що він побачить всю площу, що охоплюється, у всіх нюансах. В результаті подія може бути помічена лише поблизу безпосередньої установки та в останній момент.

Зазвичай в рекламних проспектах дилерів по продажах камер відеоспостереження знайдеться картинка, схожа на наведену, яка може ввести в оману людину не фахівця в галузі відеоспостереження. Якщо розглядати цю картину на форматі екрану 3840 х 2160 то зображення 640 х 480 дійсно матиме орієнтовну площу вказану на картинці. Але ж за допомогою відповідних об'єктивів ми можемо весь об'єкт, який ми бачимо на картині 3840 х 2160 побачити і на картині 640 х 480, правда роздільна здатність буде гіршою.

Зрозуміло, що спостерігати мегапіксельні зображення можна тільки на екрані, що підтримує цю роздільну здатність, а також око людини повинно розрізняти ці пікселі. Особливо це стосується сучасних смартфонів.

Звичайно, висока роздільна здатність – це безперечне досягнення ринку і більш ніж виправдано.

Проте нашого ринку безпосередньо стосуються широкі можливості електронного збільшення. При високій роздільній здатності всього зображення з'являється можливість збільшити масштаб з тим розрахунком, щоб на заданому розмірі екрана отримати саме поле зору, яке необхідне для розпізнавання об'єкта. Загальна роздільна здатність фрагмента, звичайно, буде зменшуватися в міру збільшення масштабу (висока роздільна здатність поширюється на весь кадр, відповідно, яку частину від усього зображення ми отримаємо на екрані, така ж частина від загального дозволу залишиться для фрагмента), однак дозвіл, що залишився, цілком можливо, виявиться в межах допустимого для розпізнаваності.

Найпростіший досвід, доступний кожному.

Зробіть фотографію вулиці з автомобілями з максимально можливою роздільною здатністю (навіть не 3 Мріх, як для відеокамери високої роздільної здатності, а 10-20 Мріх) і широким кутом захоплення. Швидше за все, жоден із номерів машин вам на екрані комп'ютерного монітора з діагоналлю 17 дюймів прочитати не вдасться. І почніть робити електронне збільшення. Коли номер почне читатися, ви побачите, що поле зору на екрані відповідає ширині смуги близько 2 метрів на місцевості, яку ви фотографували.

Так само можна на екрані розглядати не всі зображення, а лише його фрагмент, що забезпечує необхідне розпізнавання.

Тільки слід врахувати два основні моменти. Перший – це завжди втрата дорогоцінного часу для ухвалення рішення про необхідні дії для запобігання небажаній події, яка обчислюється в кращому разі хвилинами. На окремих об'єктах, які доводилося оснащувати, і де сили фізичного реагування були безпосередньо на об'єкті, такий час обчислювався секундами. А якщо згадати раніше наведені приклади казино, то, за словами керуючих, гарний шулер встигає пересмикнути колоду карт за 0,1 с.

Другий, а може, й головний момент. Подібні дії повністю відволікають увагу оператора на єдине зображення, з яким він починає працювати предметно. Решту відеоінформації на період таких дій буде втрачено. Навіть якщо це «тривожне» зображення виведено на окремий екран. Багато варіантів апаратури прийому та обробки зображень дозволяють виводити одне зображення на окремий монітор, як за сигналом тривоги (за вбудованим відеодетектором, інтеграції з окремою системою сигналізації або за бажанням оператора), проте, у цьому випадку всі питання деталізації зображення повинні виконуватися окремим оператором, без втрати постійної мінімально необхідної відеоінформації. Це стосується і керованих камер на поворотних пристроях, і трансфокаторами об'єктивів. Хибна тривога на одній частині об'єкта та проникнення на об'єкт в іншій його частині – це стандартна схема подібних дій.

А ось для відеозапису, коли подія вже відбулася (а безпека в силу нашого визначення не відбулася) висока роздільна здатність корисна прямо пропорційно – чим вища роздільна здатність, тим більше інформації ми з цього зображення зможемо отримати. Саме з допомогою електронного збільшення. Бо поспішати вже нема куди. Але це до безпеки стосунку не має, а стосується виключно адміністрування. У силу тих самих раніше прийнятих термінів.

Можна запропонувати такі рекомендації.

Розмір матриці та мегапікселі

Матриці, на яких розміщені мегапікселі – це прямокутний пристрій за об'єктивом. На ній фокусується зображення. Розмір матриці в характеристиках камер записується як діагональ у дюймах: 1/4", 1/3", 2/3", 1/2". Чим більше матриця, тим більше на неї потрапляє світла, тим детальніше картинка і потенційно ширший огляд. Тому якщо перед вами дві камери на 2Мрх, 1/3" і 1/4", то якщо дозволяє бюджет, 1/3" краще.

Якщо камера використовується в слабоосвітленому приміщенні, є сенс пожертвувати мегапікселями на користь більшої матриці, а значить більш високої чутливості.

Поради щодо вибору камер

Наші рекомендації щодо вибору камери: не женіться за цифрами. Щоб без спотворень показувати відео з роздільною здатністю 1920 х 1080 (формат Full-HD) вистачить 2Мрх, але без запасу. «Запас» стане в нагоді, щоб зумувати , наблизити об'єкт і розглянути фрагмент краще. Якщо потрібно, можна підібрати іншу оптику або додати ще одну камеру з вищою роздільною здатністю.

Без необхідності встановлювати камери 4МРх і вище не потрібно. По-перше, у доступних за ціною камер з високою роздільною здатністю нижче світлочутливість – вони швидше ніж камери на 1,3 і 2Мрх сліпнуть при поганому освітленні. Сучасні моделі нівелюють проблему: коли мало світла, вони переходять у монохромний режим з інфрачервоним підсвічуванням, але через якість бюджетних матриць картинку спотворюють шуми.

По-друге, висока роздільна здатність з'їдає більше місця в архіві. Внаслідок цього доводиться чимось жертвувати: зменшувати частоту кадрів, збільшувати розмір сховища або скорочувати час зберігання записів. З практики проектування та монтажу відеоспостереження, а також досвіду клієнтів скажемо, що не варто зменшувати частоту кадрів. На смиканому запису з 10 кадрами на секунду у разі злочину важче виявити правопорушника та довести провину. Ми рекомендуємо такий вихід: зберігати менше за часом і писати за рухом зі швидкістю в 20 кадрів/сек.

Наведемо реальні приклади зображень із відеокамер з різною роздільною здатністю на фото нижче.

Висновки:

1. У переважній більшості випадків досить 1-, 2-х мегапіксельних IP камер. А якщо потрібна найкраща деталізація віддалених об'єктів, то вирішувати таке завдання потрібно не бездумним збільшенням мегапікселів, а зменшенням кута огляду за допомогою варіофокального об'єктива. Цим ми «наблизимо» картинку до себе і зможемо розглянути, що нам треба.

2. Збільшення кількості відеокамер. Можливо таке рішення буде трохи дорожчим, зате воно вирішить ваше завдання напевно. А можливо ціна пари 2-х мегапіксельних камер з кутом огляду в 50° буде меншою, ніж ціна однієї 5- або навіть 4-х мегапіксельної з кутом в 100°. Але інформації про територію вони нам дадуть набагато більше.

3. Потрібно враховувати, що зі збільшенням кількості пікселів без збільшення фізичного розміру матриці лише погіршує чутливість відеокамери, тому, що площа пікселя стає меншою, і на його поверхню потрапляє менше світла.

4. Ну і останнє, що потрібно пам'ятати - зі збільшенням «мегапіксельності» ви додатково переплачуватимете за процесорну потужність записуваних пристроїв, накопичувачі (HDD), пропускну здатність мережі і трафік, при перегляді через Інтернет.

Різні автоматизовані системи, звичайно, можуть значно полегшити роботу оператора, але зовсім не замінювати її.

Рішення щодо активній протидії потенційній небезпеці приймає конкретна

1 МП IP камера: Space Technology ST-120 IP Home, роздільна здатність 1280x720, матриця 1/4, об'єктив 3,6 мм

4 МП IP камера: Dahua IPC-HFW-4421EP-0360B, роздільна здатність 2560x1440, матриця 1/3, об'єктив 3,6 мм

особа. Вона і відповідає за вжиття чи неприйняття заходів. До того ж жодна автоматична система не позбавлена ймовірності хибних спрацьовувань.

Окремо варто зупинитися на функції розпізнавання облич відеокамерами. Це сьогодні заявляється багатьма фірмами-виробниками/постачальниками на перших рядках рекламних текстів. По-перше, слід враховувати, що подібна функція в більшості випадків працює тільки спільно з приймальною апаратурою цього виробника або його програмним забезпеченням. А по-друге, завжди варто проаналізувати, як саме ця опція виявиться корисною саме на вашому об'єкті. Занести в базу особи всіх своїх і пропускати їх автоматично? А що робити з відвідувачами збоку? А якщо перед об'єктивом представлена фізіономія «свого», а в мертвій чи тіньовій зоні поруч із цим «своїм» стоїть група озброєних лиходіїв, а «свій» перебуває під дулом пістолета? Чи ви надішлете запит до бази МВС щодо даних осіб усіх потенційних лиходіїв, щоб не допустити нікого з них на свій об'єкт? Так ця база змінюється щодня по кілька разів, та й навряд чи вам її взагалі дадуть. Чи набагато важливіше не розглядати у деталях фізіономію відвідувача, а загальну ситуацію на вході? Скільки людей, чоловіків чи жінок присутні і чи зможе охорона перешкодити небажаним діям з їх сторони? Загалом, будь-яку «автоматику» варто докладно проаналізувати з погляду її реальної користі для кінцевого завдання, оскільки будь-яка додаткова опція коштує додаткових грошей, а незатребувані функції означають невиправдані витрати.

Якщо розібратися, до питань безпеки, тобто той мінімум відеоінформації, яка достатня для вжиття заходів щодо запобігання небезпечній ситуації, детальна ідентифікація не стосується. Все набагато простіше. Лізе людина через паркан – зовсім неважливо, у що він одягнений, як виглядає і що в нього в руках. Нормальний відвідувач піде через офіційний пропускний пункт. Це однозначно тривога. Достатньо було б найпростішої чорно-білої камери.

Те саме, якщо хтось намагається проникнути через вікна. Важливо заздалегідь продумати всі можливі варіанти інформації для прийняття активних дій та вирішити, як таку інформацію отримати у найкоротші терміни з мінімальними витратами. І, звісно, опрацювати модель цих активних дій. Без них жодна безпека не відбудеться, незалежно від наявності та якості технічної системи відеоспостереження.

Необхідний та достатній функціонал систем відеоспостереження

Так, система відеоспостереження асоціюється у більшості споживачів з відеокамерою. Але якщо ви візьмете вартість хоч скільки серйозної системи і розділите її на кількість камер, у вас вийде цифра, що мінімум, на порядок перевищує вартість однієї камери. При кілометрових довжинах магістралей сума буде більшою на 2, а то й на три порядки. Саме магістральне та приймальне обладнання, а також монтажні та пусконалагоджувальні роботи складають основну вартість системи. І, мабуть, лише на ринку ТЗБ така побудова системи реєстрації є типовою.

Найдоступніший і зрозуміліший для всіх приклад – автомобільні відеореєстратори, які здійснюють запис відео та звуку на встановлену в них карту пам'яті і дуже часто вбудовану пам'ять. Пристрій повністю автономний. Потрібна лише подача на нього живлення. Зображення на екран виводиться, як правило, на короткий період для налаштування та перевірки працездатності, а у штатному робочому режимі екран гасне, щоб не створювати водію перешкод. Є просто вид через лобове скло. І нікому не спадає на думку збирати інформацію з усіх відеореєстраторів до якогось центру моніторингу і зберігати в гігантських архівах. Насамперед тому, що у звичайному штатному режимі інформація це нікому не потрібна. Є водії, котрі жодного разу не переглядали запис зі своїх реєстраторів. Тому що безпека водіння у них на висоті.

Ще наочніший приклад із «чорними скриньками» літаків. У штатному режимі немає можливості зняти записану інформацію. Тільки за аварії, у складі комісії з обов'язковою присутністю представника заводу-виробника. Чи можна було б організувати передачу всієї інформації з усіх літаків до єдиного центру? Звісно. З допомогою супутникових каналів зв'язку, з передачею великих масивів даних. І, звісно, з величезними витратами. І це буде в чистому вигляді незатребувана функція, оскільки всі рішення на борту повітряного судна приймає командир, а ніхто ззовні ніяк не може вплинути на ситуацію на борту. Більше того, через різні причини подібна інформація могла б стати доступною тим, для кого вона є закритою. Натомість можна було б запровадити унікальні програмні продукти, наприклад, пошуку по архіву, що широко пропонує, зокрема, ринок ТЗБ.

Отже, якщо відеоінформація потрібна лише за подією, що відбулася, і не становить жодної цінності в штатному режимі, немає жодної необхідності її безперервно транслювати на єдиний пост і безпосередньо спостерігати.

І категорично не можна транслювати її на пост відеоспостереження задля безпеки. Як було зазначено вище, там обсяг відеоінформації вже знаходиться на межі можливостей обробки, і будь-яка додаткова лише знижуватиме ефективність роботи системи. До того ж інформація, яка безпосередньо до безпеки не відноситься. Крім того, у різній записаній відеоінформації можуть бути зацікавлені абсолютно різні структури одного і того ж об'єкта, і інформація для однієї структури може бути закритою для іншої. При побудові системи з єдиним для всіх джерел відеореєстрації сховищем, обсяг архіву з урахуванням часу зберігання виявляється колосальним, а пошук за таким архіву часто-густо вимагає застосування окремих спеціальних програмних продуктів.

Передача відеоінформації в будь-який віддалений пост вимагає окремого обладнання, проектно-монтажних і пусконалагоджувальних робіт, що незрівнянно за ціною з вартістю власне камери, нерідко пов'язана з обмеженнями, що накладаються самим каналом зв'язку, схильна до зовнішніх перешкод і можливих небезпечних впливів як технічного, так і навмисного характеру.

І завжди небезпечно «складати всі яйця в один кошик». Якщо є єдине місце з встановленим багатоканальним реєстратором або сервером, зі сховищем усіх даних, воно і представлятиме головний інтерес для того, хто зацікавлений у знищенні записаної інформації. Реалізувати таке цілком реально. Від банального механічного руйнування до подачі високої напруги руйнівного значення в лінії зв'язку та/або живлення.

Якщо кількість відеокамер для цілей безпеки завжди і суттєво обмежена наявним людським фактором, то відеореєстрація для цілей адміністрування обмежена лише бажаннями замовника та, звичайно, його фінансовими можливостями. На відміну від систем безпеки ефективність систем адміністрування прямо пропорційна кількості відеокамер, задіяних для цих цілей.

Перехід від схеми відеозапису, що широко пропагується ринком ТЗБ, у групових центрах із загальними сховищами даних до автономних відеореєстраторів на порядки б знизили вартості систем за рахунок відмови від найдорожчого елемента систем – каналів передачі з усім супутнім обладнанням. А, значить, суттєво розширилося б застосування відео для завдань адміністрування, оскільки об'єктивна потреба таких завдань практично повсюдна, і зупиняє замовника, як правило, виключно ціновий фактор.

Ринок, звичайно, всіляко цьому противитиметься, оскільки неминуче в рази скоротяться продажі в цілих сегментах обладнання – від кабелів, до мережних комутаторів, багатоканальних відеореєстраторів, пристроїв захисту від небезпечних наведених напруг, сховищ даних, програмних продуктів пошуку по архіву тощо. Але напрями розвитку ринок повинен визначати, виходячи з потреб свого клієнта, а не нав'язувати власне бачення завдання, яке має суто ринкові інтереси.

Слід зазначити, що автономні реєстратори вже застосовуються деякими структурами на вирішення завдань адміністрування. Наприклад, на шоломах бійців усіляких силових структур передбачено штатне місце для кріплення камери-реєстратора. Ціну таких камер цілком можна порівняти з вартістю автовідеореєстратора, доступного будь-якому автомобілісту. Принципово подібні камери нічим не відрізняються від будь-якої іншої, що має функцію запису на борту. Що ж до часу запису, то на сьогодні доступні SD-картки ємністю до 2 терабайт. Для більшості випадків цього досить. Якщо комусь і цього мало, можна встановити жорсткий диск будь-якого необхідного об'єму – або в корпус самої камери, якщо йдеться про зовнішні камери, або розмістити в безпосередній близькості від неї.

Що стосується роздільної здатності автономних відеокамер-реєстраторів, ось тут вона себе може проявити у всій красі. Чим більше мегапікселів, тим більша можлива деталізація зображення, тим ширшим може бути кут огляду об'єктива, оскільки розширюється діапазон електронного збільшення для віддалених об'єктів. І жодних обмежень, пов'язаних із пропускною можливістю каналу передачі, оскільки такого просто немає.

Все, що потрібно для працездатності подібного автономного відеореєстратора – подати на нього живлення та встановити бажане місце. Така найпростіша операція доступна безпосередньо користувачеві, а, отже, він сам може конфігурувати систему на власний розсуд, змінювати місця установки і зони контролю в будь-який момент.

Якщо мова йде про внутрішні камери, при необхідності перегляду записаної інформації достатньо вийняти з камери картку пам'яті та відкрити її на комп'ютері. За бажання можна застосувати будь-які програми обробки, що є в арсеналі користувача: перегляд заданого інтервалу часу, пошук архіву, ідентифікація осіб тощо. Так, щоб отримати доступ до записаної інформації, доведеться йти щоразу до місця встановлення камери, а не працювати з єдиним сервером. Але трапляються події, які потребують розслідування чи іншого адміністративного втручання, не так часто одному об'єкті. А якщо виділити на подібні дії хоча б десяту частину заощаджених коштів, певно ніхто не відмовиться від такого підробітку. Якщо ж говорити про державні правоохоронні органи, їхній прямий обов'язок – зібрати доказову базу незалежно від того, де вона фізично перебуває. Ну, і ще важливий момент – низька вартість подібного рішення дозволяє багаторазово резервувати особливо актуальну відеоінформацію, встановлюючи не одну, а кілька камер у різних місцях для запису однієї сцени з різних напрямків. У цьому випадку знищення відеозапису з будь-яких причин видається практично неможливим.

Єдине питання, яке вимагає сьогодні досконального опрацювання – це автономні відеореєстратори, що встановлюються на зовнішніх територіях. Можливо, має сенс оснастити такі камери Wi-Fi модулями, забезпечивши дистанційне завантаження інформації по каналу Wi-Fi . Можливо, комусь буде достатньо мати доступ до комунікаційного роз'єму для завантаження по кабелю, звісно якщо є доступ безпосередньо до камери.

Як правило, відеокамери з функцією відеозапису на борту мають одночасно зовнішній вихід в одному або декількох стандартах, серед яких є аналоговий стандарт PAL. Якщо необхідний відеозапис з камери, задіяної для системи безпеки, найбільш вигідним рішенням є організація запису саме на борту в максимально можливій роздільній здатності, а передачу сигналу для прямого спостереження можна здійснювати саме в стандарті PAL, особливо якщо камера віддалена від поста спостереження не більш ніж на 100 метрів.

По-перше, дозволів для прямого спостереження на реальному моніторі буде достатньо. По-друге, не буде затримки в 1-2 секунди, порівняно з передачею сигналу по лінії Ethernet. А по-третє, економія при великих довжинах ліній буде дуже відчутною. А на якість запису жодним чином не вплине пропускна спроможність каналу передачі.

Вирішення абсолютної більшості споживчих завдань залежить виключно від людського чинника. Навіть завдань, пов'язаних із штучним інтелектом, оскільки споживачем виступає саме людина. Питання успіху таких рішень – це питання сумлінності та компетентності цього самого людського чинника. Навіть не постійний чи періодичний контроль із безумовною доказовою базою у формі відеозапису, але навіть просто можливість такого контролю, про що сам людський фактор має бути поінформований, завжди позитивно позначиться на всьому процесі виконання посадових обов'язків. Сфера застосування такого технічного рішення поширюється далеко за межі галузі безпеки.

Наведемо приклад, що стосується дитячих садочків. Питання сумлінної роботи вихователів у групах, харчування, дотримання порядку денного, знаходження персоналу на робочих місцях абсолютно не стосуються питань зовнішньої безпеки об'єкта. І зовсім не логічно навіть у формі відеозапису змішувати інформацію з цих питань із питаннями безпеки. Займатися безперервним контролем діяльності персоналу є абсурдним. А ось можливість контролю в будь-який момент часу не вимагатиме жодних поточних витрат, тільки разове вкладення в обладнання. І позитивно позначиться на діяльності персоналу.

Вимагають окремого адміністрування і безпосередньо питання безпеки. В даному випадку мається на увазі не запис з камер безперервного відеоконтролю, що доводить сам факт події, якщо така була пропущена оператором системи. Ціла низка завдань безпеки, що пов'язана з використанням спеціальних технічних засобів, має на увазі не тотальну, а вибіркову перевірку можливих джерел небезпеки. Питання успішності подібних завдань визначається виключно сумлінністю та компетентністю особи, яка приймає рішення. Найбільш очевидні приклади – перевірка людських потоків при допуску на об'єкти транспортної структури, у місця проведення спортивних і культурних заходів щодо проносу заборонених предметів. Буває, що такий контроль просто неможливо зробити тотальним, як, наприклад, у вестибюлях метро, і вибірковість визначається виключно на розсуд персоналу охорони. Найчастіше такий контроль може мати суто формальний характер. За відсутності будь-якого об'єктивного контролю у персоналу, що визначає допуск на об'єкт, завжди є можливість послатися на недосконаліть оглядового обладнання, якщо все ж таки заборонені предмети опинилися на самому об'єкті. Повноцінний віддалений відеоконтроль не буде хоч скільки-небудь ефективним з суто технічних міркувань, не кажучи вже про невиправдано високі витрати на подібне рішення. Але якщо кожен співробітник усвідомлюватиме, що, незважаючи на відсутність безперервного зовнішнього контролю його роботи, у разі будь-якого інциденту винну особу неодмінно буде встановлено, цього виявиться більш ніж достатньо для ефективної роботи такого контрольно-пропускного пункту. А для цього потрібно відносно незначне та разове вкладення коштів.

Ю.Дмитренко

http://www.tzmagazine.ru/
https://ittell.ru/
http://kb-sb.ru/pub/10/918/

Сучасні загрози для дверей вікон та жалюзі. Кулетривкість зламотривкість стійкість до дії вибухової хвилі та вогнестійкість

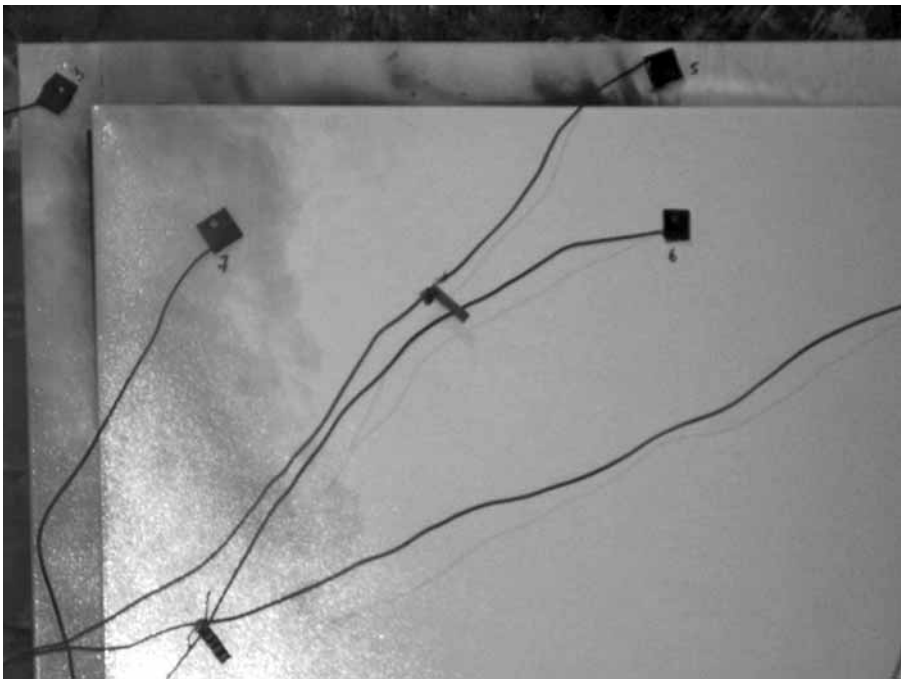
З першого дня повномасштабного вторгнення ми фактично живемо від однієї повітряної тривоги до іншої. Звуки оповіщення про небезпеку з повітря стали дещо звичними, але все одно змушують нас хвилюватися.

Під час вибуху уламки скла та уламки дверних конструкцій можуть бути так само небезпечними, як і сама вибухова хвиля. Кулі стрілецької зброї, яка також буває задіяна під час відбиття атак з повітря, також можуть спричинити пошкодження наших дверей та вікон. Пожежа, яка може виникнути під час атаки, також несе значні загрози як для нашого життя, так й для майна. Несанкціоноване проникнення у домівку, коли ми прямуємо до укриття або просто у справах, це пряма загроза втрати майна та усього, що нажито упродовж років.

Саме так, у сучасному світі вікна, двері, ролети чи жалюзі наших домівок або квартир повинні захищати не лише від холоду чи шуму, а й від більш серйозних загроз – куль, зламу, вибухових хвиль та пожежі. Розуміння реальної здатності наших домівок, їх вікон, дверей, захисних ролет або жалюзі протистояти загрозам дії вибухової хвилі, куль, вогню, можуть значно підвищити шанси на порятунок життя людей та збереження майна.

Єдине незалежне документування рівня здатності вікон, дверей, ролет чи жалюзі протидіяти впливу таких загроз - це їх випробування та сертифікація в акредитованих лабораторії та органі з сертифікації. І це не бюрократична формальність, а реальна перевірка їхньої здатності рятувати життя, підстава для вибору надійних захисних конструкцій споживачем та підстава для пропозиції надійних захисних конструкцій від виробника.

Давайте, трохи розберемо, що саме стоїть за випробуваннями та сертифікацією вікон, дверей, захисних ролет та жалюзі стосовно здатності протистояти загрозам дії вибухової хвилі, куль, спробам зламування, вогню.



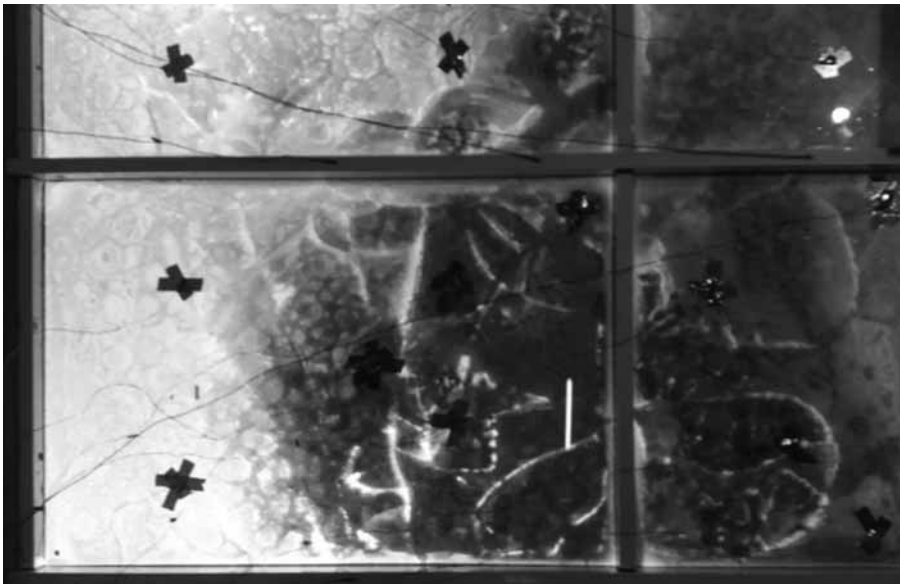
Зразок двері під час випробувань на вогнестійкість

Тривкість до дії вибухової хвилі оцінюється відповідно до вимог ДСТУ EN 13123-2:2006 «Вікна, двері та жалюзі. Стійкість до вибуху. Класифікація та технічні вимоги. Частина 2. Діапазон випробування», який є гармонізованим зі європейським стандартом EN 13123-2:2004. При випробуваннях, які проводять на спеціалізованих полігонах, моделюють вплив вибухової хвилі, яка генерується при використанні контрольованих тротилових зарядів масою від 3 до 20 кг, залежно від заявленого класу тривкості, на визначених відстанях. Це дозволяє перевірити, чи витримає конструкція ударну хвилю та чи збереже цілісність для захисту людей. Оцінювання результатів базується на наявності або відсутності уламків зі зворотного боку зразка (тобто протилежному ударній хвилі), ступеню руйнування та здатності відчиняння механічним способом після впливу ударної хвилі. Класи тривкості від EXR1 до EXR5 характеризують здатність конструкції витримати певний тиск ударної хвилі.

Фото зразка після випробувань на тривкість до дії ударної хвилі

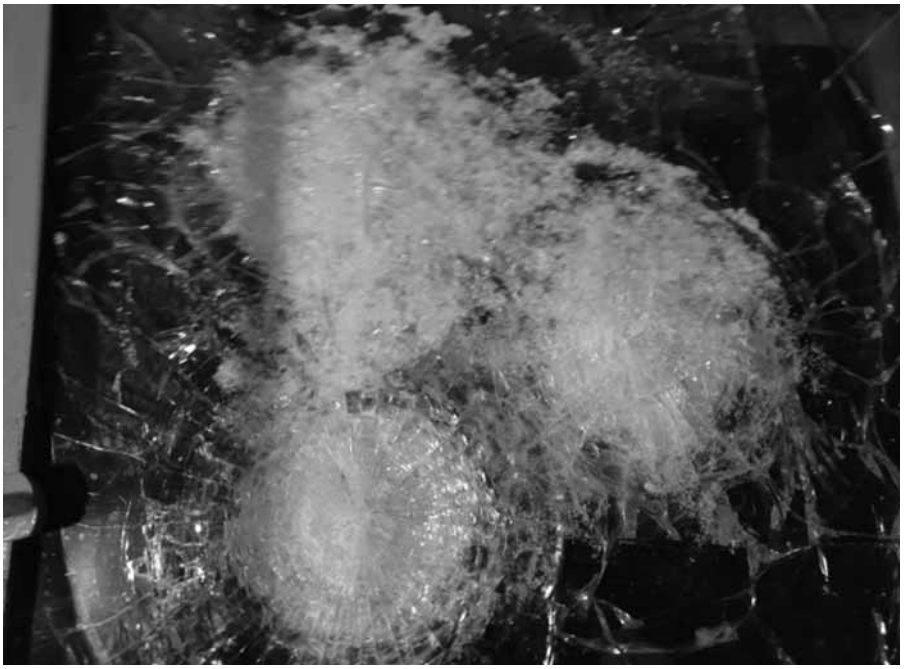
Кулетривкість визначається здатністю вікон, дверей, ролет або жалюзі витримувати влучання куль стрілецької зброї. В Україні використовується стандарт ДСТУ 4547:2006 «Вікна, двері та жалюзі. Кулетривкість. Вимоги та класифікація» (національна версія загальноєвропейського стандарту EN 1522:1998), який класифікує класи тривкості залежно від типу зброї та боєприпасів. Спеціалізоване обладнання лабораторії дозволяє моделювати вплив куль стрілецької зброї зі скрупулезною фіксацією швидкостей, дистанції, результату влучань, ризику утворення осколків.

Якщо казати про зламотривкість, то чи знали ви, що більшість спроб пограбування відбувається через вікна або двері? Саме тому оцінка рівня стійкості дверей



Зразок вікна під час випробувань на вогнестійкість

Зразок вікна під час випробувань на зламотривкість



Зразок скла під час випробувань на кулетривкість

і вікон до злому відповідно до ДСТУ EN 1627:2014 «Вікна, двері та жалюзі. Тривкість щодо зламування. Класифікація та технічні вимоги (EN 1627:2011, IDT)» може бути базисом для вибору того рівня захисту, якого ви заслуговуєте.

При випробуваннях відповідно до ДСТУ EN 1627 моделюють атаки ломами, кувалдами, ножівками, механічними та електричними інструментами, такими як болгарки та дрилі. Вони імітують різні рівні злому – від спроб фізичної сили до використання спеціалізованого обладнання, що дозволяє визначити реальну здатність конструкції до протидії спробі незаконного проникнення. Оцінка зламотривкості базується на проміжку часу, упродовж якого конструкція опирається зламу при використанні певного набору інструментів.

Якщо казати про пожежу, то це одна з найпоширеніших загроз для житла. Випробування на вогнестійкість відповідно до ДСТУ EN 1363-1:2023 «Випробування на вогнестійкість. Частина 1. Основні вимоги» та ДСТУ EN 1364-1:2022 «Випробування не несучих будівельних конструкцій на вогнестійкість. Частина 1 Стіни» проходять у спеціальних печах при температурах понад 1000°C. Процес триває від десятків хвилин до кількох годин залежно від класу вогнестійкості конструкції. Оцінюються такі критерії, як збереження цілісності та теплоізоляційних властивостей під впливом екстремальних температур. Важливо оцінити, скільки часу конструкція зможе утримувати вогонь, не руйнуючись і не поширюючи полум'я.

За більш ніж 20-річний досвід надання послуг з оцінки відповідності на ринку безпеки, ЦСБО та НІЦВВМЗ вже впевнились, що якщо виробники прагнуть виробляти не просто двері, вікна чи жалюзі, а надійні засоби захисту для людей, то скоріше рано, ніж пізно, ми обов'язково зустрінемось.

Усі вже розуміють, що шлях сертифікації на підставі результатів випробувань - це не тільки про якісний продукт, не тільки про виконання нормативних вимог, а й про репутацію та реальну турботу про людей, їх життя та майно.

Замки готельні від провідних виробників

Серед фірм, що традиційно виробляють замки електронні готельні, ми зупинились на двох-трьох виробниках. Наводимо зовнішній вигляд запропонованої продукції.

939SS-33-DMF1 (Ш-38мм)

930SS-5-DMF1 (Ш-75мм)

029SS-5-DMF1 (Ш-68мм)

939SS-DMF1 (Ш-44мм)

M1-130

939SS-8-DMF1 (Ш-50мм)

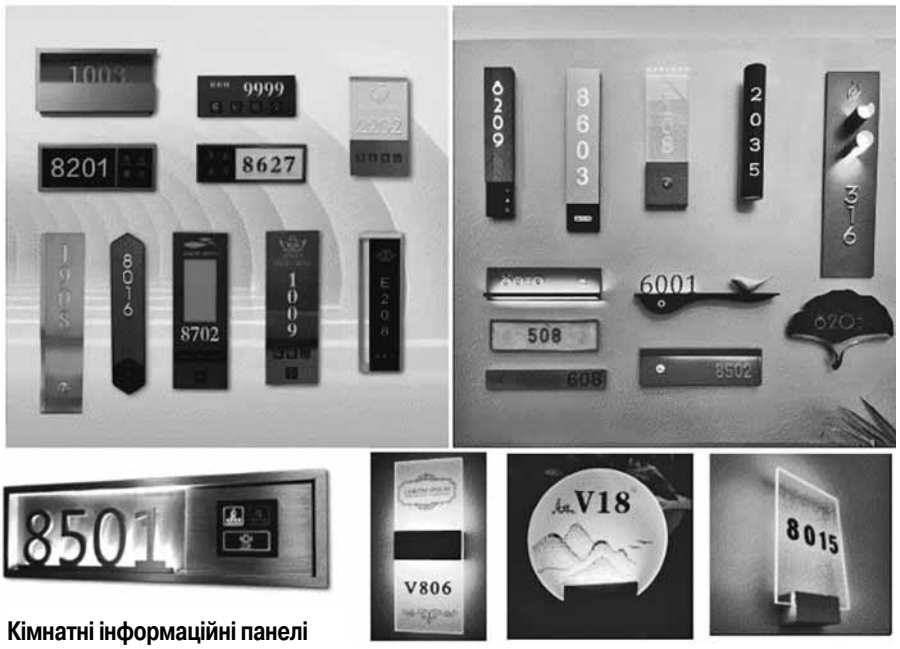
R6

Електронний замок на вхідні двері

Огани управління електронного замка

Замки на вхідні двері

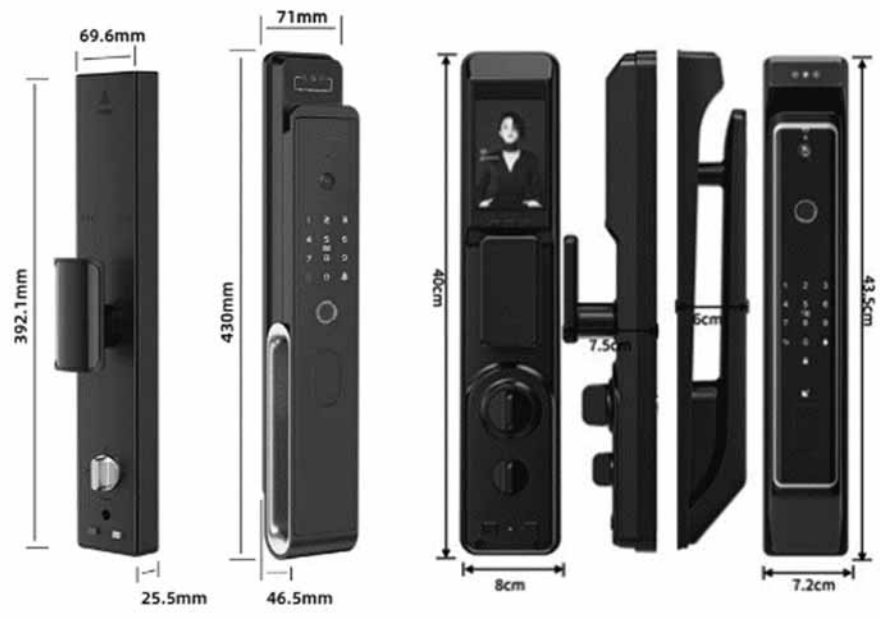
Фіксований доступ



Кімнатні інформаційні панелі

Комбінований доступ

Програмний доступ



Замки на вхідні двері

Tavex

ТОВ ТАВЕКС ПЛЮС
050-5772076
Олександр Столяренко

Електронні замки -2024

Ми звикли, що двері обладнуються замками. Стандартний замок має защіпку та запираючий ригель. Зазвичай, защіпка керується за допомогою ручки, а ригель керується за допомогою циліндра із механічним циліндровим ключем або пласким ключем. Так ми жили роками. Все змінюється.

Раніше люди стояли в чергах на отримання провідного телефону, а тепер в будь який момент можна придбати смартфон, який також надає послуги мовного зв'язку, але крім того багато додаткового сервісу.

Подібна ситуація складається на замковому ринку. Як кажуть охоронці, важливо не лише запобігти проникненню через двері, але і вчасно повідомити власника квартири про намагання та результат проникнення. В додаток не забудемо про таку прозаїчну річ як втрата ключів та порив кишеней ключами.

Почнемо із замків на вхідні двері

На дверях стандартно встановлюється два замки. Один повсякденний і другий для допоміжного застосування. (під час відпустки, відрядження, канікул і т.п. Повсякденний має циліндр під ключ і ручку відкривання дверей. Сучасні виробники замків додають новітні сервіси: доступ через безконтактну картку, за кодом, по відбитку пальця. за формою обличчя, за венозною картину судин пальця, через смартфон локально або дистанційно.

На сьогодні продано дуже багато вхідних дверей, які стандартно встановлюються на квартири в багатоповерхових будинках. Користувачам необхідно запропонувати шляхи модернізації.

Варіант 1. Смарт-циліндр

Ці циліндри мають доступ по безконтактній картці, коду, смартфону, відбитку пальця, мають механічний ключ екстреного доступу.

Недоліки. Для підгонки замка під реально існуючі двері, треба переробляти циліндровий механізм. Головне: замки працюють за принципом механічного ключа. При відкритті, після розпізнавання коду, необхідно обертати ручку для відкриття. При закритті – знову необхідно ввести код і повертати ручку для закриття. Це зветься напівавтоматика. Багатьом також не подобається сильно виступаюча фасадна частина замка. Виникає бажання її зламати. В цілому гарно естетично. Живлення від батарей.

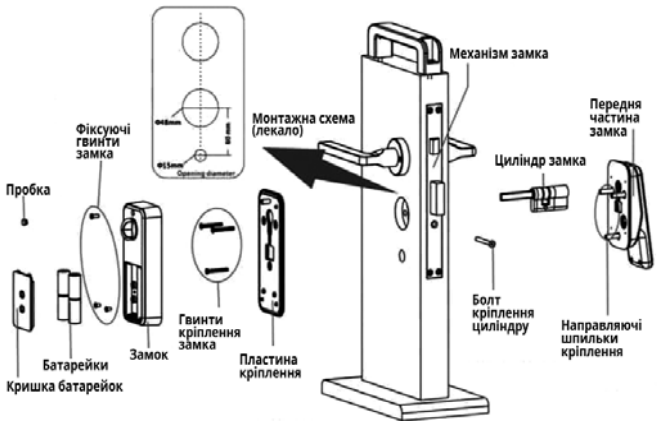
Варіант 2. Смарт накладки

Смарт накладки встановлюються на існуючий замок, але на відміну від попереднього варіанту: відкриття та закриття замка реалізується у автоматичному режимі за допомогою вбудованого електромотора із редуктором.

Цей варіант є найбільш оптимальним для встановлення на існуючий замковий механізм.

Варіант 3. Розглянемо Смарт-замки.

Смарт замки на вхідні двері забезпечують автоматичне відкривання за закривання дверей за допомогою моторного приводу замкового циліндра, мають зручну фіксовану ручку для переміщення полотна дверей, а також мають додаткові сенсорні можливості. Головне – це відеоідентифікація – доступ за формою обличчя і ще одна особливість – вбудований відеодомофон, який дозволяє дистанційно спілкува-



Меблеві електронні замки: для шаф фітнес-залів, басейнів, хостелів

тися із клієнтом, що стоїть перед дверима. Запуск відеодомофона реалізується відвідувачем при натиску на кнопку «дзвоник», самостійно власником замка або самостійно замком, якщо відвідувач знаходиться перед дверима більше встановленого часу і не викликає власників квартири. Такий замок працює під управлінням одного із замкових смартфонних додатків і спілкується із смартфоном через додатки TTLock, TUYA, WisHome. Особливість зазначених смарт замків полягає в тому, що вони базуються на китайських замкових механізмах 6068. В Україні головним чином застосовуються замкові механізми 6085. Із китайськими смарт накладками двері із українськими замковими механізмами не сумісні.

Представляємо запропоновані варіанти смарт замків на вхідні двері.

Варіант 4. Розширення можливостей варіанта 2 шляхом встановлення СМАРТ ДЗВОНИКА.

До смарт накладок із Варіанта 2 можна додати СМАРТ ДЗВОНИК і ми отримаємо функціонально смарт замок, запропонований у Варіанті 3.

Є багато варіантів форми СМАРТ ДЗВОНИКА. Наведемо найбільш популярні.

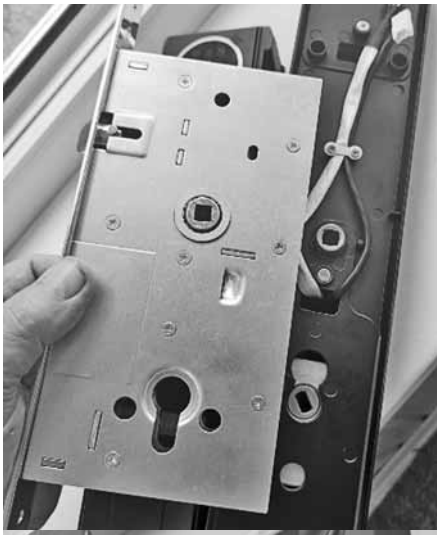
Дзвоник має автономне живлення від вбудованого акумулятора. Підзарядка рекомендується через кожних 3 місяці в залежності від частоти спілкування. Зображення та звук надходять і генеруються тільки через смартфон декількох

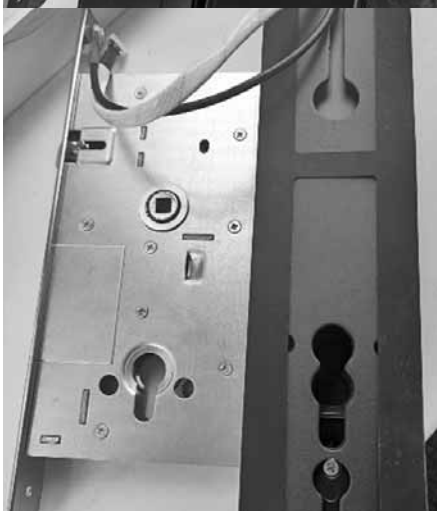
власників. Всередині помешкання встановлюється в розетку дзвоник, який із дверним смарт дзвоником обмінюється інформацією по радіоканалу.

Варіант 5. Сучасний багатофункціональний смарт замок у конструктиві тягни/штовхай із адаптацією під широко встановлені в Україні виробниками вхідних дверей замкові механізми 6085 Турецького та Євпропейського походження.

Ніхто із виробників не робить замок унікальним тільки під замкові механізми 6085. Замки робляться багатофункціональними під замкові механізми 6068 (Китайський стандарт, та 6085 (Європейський стандарт). Представляємо такий замок FANTOM.

Особливість цього замка видно, якщо дивитись на внутрішні поверхні замка.





На цих фото представлені частини накладок замка разом із 6085 замковим механізмом. На лівому фото представлена задня панель із розташованим проти замкового циліндра – моторним приводом відкривання / закривання замка. На середньому фото представлено внутрішній вигляд фасадної панелі із отвором для механічного ключа екстреного доступу. На третьому фото представлені лицьові сторони фасадної та внутрішньої накладок разом із замковим механізмом 6085.

Замок забезпечує доступ через код, безконтактну картку, відбиток пальця, форму лиця та через смартфонний додаток TUYA із можливостю спостереження через вбудовану у фасадну панель – відеокамеру.

Термін поставки – 4 тижні після замовлення.

Tavex

ТОВ ТАВЕКС ПЛЮС
050-5772076
Олександр Столяренко

Як знешкодити «майнера» на компютері

Випадки прихованого майнінгу ростуть у геометричній прогресії. За даними антивірусної компанії Symantec, за минулий рік вони почастішали у 340 разів.

У той же час, відзначають дослідники, на 35% знизилося число атак за участю вірусів-вимагачів. Хоча ще недавно такі атаки були найбільш популярними.

За даними Національного центру кібербезпеки Великобританії, прихований майнінг буде головною загрозою для інтернет-користувачів, як мінімум, у найближчі два роки.

Що це таке

Прихований майнер – stealth miner, майнер-бот, ботнет – програма, яка в автоматичному режимі веде майнінг непомітно для користувача. Це додаткове програмне забезпечення, яке встановлюється на комп'ютер, використовує його ресурси і переказує заробіток на гаманець розробника.

Робота майнера дуже схожа на дію вірусу. Він теж маскується під системний файл, робить певні операції і вантажить систему, але є одне "але".

Вірус — це програма, яка шкодить системі. Прихований майнер діє за іншою схемою. Він просто використовує ресурси процесора гаджета, щоб добувати криптовалюту і переказувати її в гаманець свого творця.

На відміну від класичних вірусів, які крадуть і пересилають дані з комп'ютера, віруси-майнери використовують його технічні потужності.

Хто може стати жертвою

Жертвою прихованого майнера може стати кожен користувач. Під загрозою – не тільки сервери великих компаній, а й домашні комп'ютери, особливо ігрові. Майнери працюють на всіх платформах, пристроях, операційних системах і браузерах. Таким чином, від них не захищений ніхто.

Свою роль у цьому відіграла поява монет, для видобування яких не потрібні майнінг-ферми. Для них достатньо середніх за потужністю пристроїв. Найпопулярнішими криптовалютами у шахраїв є Monero і Zcash.[L]

За даними ESET, програми-майнери поширюються кількома шляхами.

Перший – коли користувач шукає інформацію і потрапляє на скомпрометований сайт, куди зловмисники помістили шкідливий код, або на сайт, адміністратори якого додали в код частину інфікованого коду для заробітку на відвідувачах.

При відвідуванні такого сайту спрацьовує скрипт, який починає використовувати ресурси пристрою. Цей метод найбільш поширений і працює майже на всіх пристроях та операційних системах.

Другий – соціальні мережі або файлообмінники.

Користувачеві можуть приходити повідомлення від інших користувачів або підроблених акаунтів-ботів про те, що він нібито став переможцем в акції або конкурсі. Для отримання призу користувачеві пропонується перейти за посиланням, яке завантажує небезпечне програмне забезпечення.

Залежно від пристрою відбувається завантаження шкідливих програм. Для комп'ютера або ноутбука це файл .exe, для мобільного пристрою – .apk.

Також шкідливе програмне забезпечення може поширюватися на ігрових форумах. Користувачеві пропонують завантажити вірус під виглядом оновлення до гри або неліцензійної версії для безкоштовного користування.

Як виявити

Згідно з рекомендаціями ISSP, слід перевірити «Диспетчер завдань». При наявності майнера там буде відображатися великий відсоток завантаження центрального або графічного процесорів — у межах від 70% до 100%.

Перші симптоми присутності майнера — збої в роботі інформаційної системи, швидка розрядка акумулятора, перегрівання пристрою, наявність запущених підозрілих процесів, нетипове підвищення гучності роботи відеокарти, високий рівень використання електроенергії.

Чому це небезпечно

Якщо у пристрої «селиться» майнер, це може призвести до зростання споживання електроенергії і поломки гаджета, адже його ресурси буде використовувати шкідливе ПЗ. Також стануть набагато повільніше запускатися програми.

Ще менш приємною знахідкою, ніж сам майнер, може стати несанкціоноване використання паролів, у тому числі для отримання фінансової вигоди.

Крім того, якщо ботнет отримав доступ до пристрою, це може загрожувати змінами у роботі гаджета. Наприклад, деякі майнери блокують панель управління пристрою, через що користувач не може їх позбутися.

Як знешкодити

Фахівці ESET радять використовувати актуальні версії антивірусів, які блокують загрози на етапі завантаження. Якщо комп'ютер інфіковано, слід виконати його повне сканування і видалити небажані та потенційно небезпечні програми.

При потраплянні на інфікований сайт його потрібно закрити й очистити кеш браузера. Якщо вказаний сайт був доданий у закладки, його слід видалити. Якщо користувач зіткнувся з ботнетом, який не піддається цим заходам, краще звернутися до фахівця, щоб не погіршити ситуацію.

Цілющі сервіси

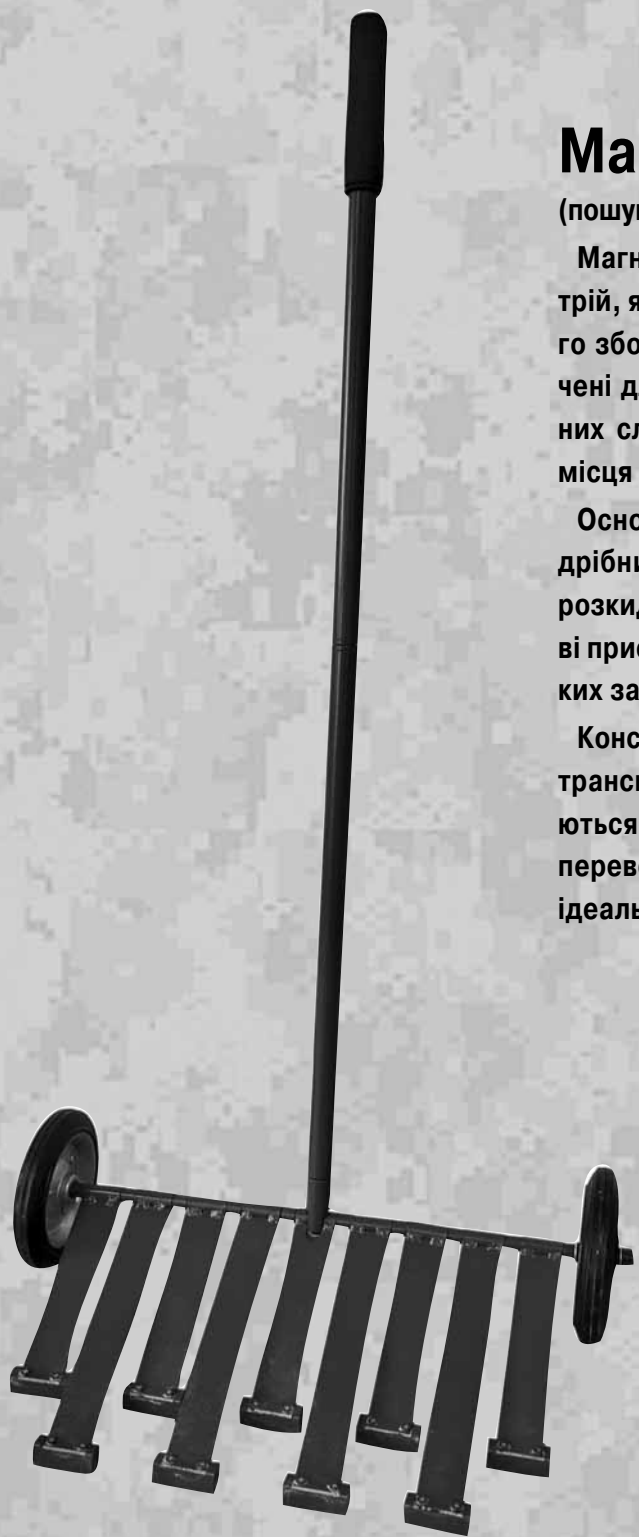
Для сканування пристрою на наявність шкідливого ПЗ можна використовувати безкоштовну утиліту Malwarebytes та її доповнення AdwCleaner.

Перший додаток перевіряє жорсткий диск та оперативну пам'ять на наявність вірусів, другий — на рекламні програми. Регулярне сканування з великою імовірністю убезпечить гаджети від прихованого майнінгу.

У браузері можна використовувати розширення ScriptBlock, NoCoin і MinerBlock, які блокують піратські скрипти і зупиняють потенційно небезпечні алгоритми. ★

Магнітні граблі МГ-2

(пошукове магнітне пристосування)



Магнітні граблі МГ-2

(пошуковий магнітний пристрій)

Магнітні граблі МГ-2 — це спеціальний пошуковий пристрій, який використовується для швидкого та ефективного збору металевих осколків після вибуху. Вони призначені для експертів-криміналістів, фахівців вибухотехнічних служб та саперних груп, які проводять обстеження місця події, пов'язаного з вибухом.

Основне завдання МГ-2 — полегшити пошук та збір дрібних металевих фрагментів вибухового пристрою, розкиданих на великій території. Завдяки магнітній основі пристрій є значно ефективнішим за інші засоби для таких завдань.

Конструкція МГ-2 проста та зручна у використанні. Для транспортування граблі легко розбираються та складаються, що дозволяє переносити їх у спеціальній сумці та перевозити будь-яким видом транспорту. Це робить їх ідеальним інструментом для роботи в польових умовах.

Технічні характеристики:

1. Ширина поля обстеження, мм . . . . . - 450;
2. Вага, кг, не більше . . . . . - 7,5;
3. Габарити виробу, мм, в транспортному положенні . . . . . - 550x300x150;
4. Габарити виробу, мм, в робочому положенні . . . . . - 150x550x1400.

Комплектація:

1. Рухливі магніти на осі . . . . . - 9;
2. Колесо . . . . . - 2.
3. Штанги збірної ручки . . . . . - 3;
4. Сумка спеціальна з планшетами . . . . . - 1.

ТОВ «ДАМІНЕР», Україна, 16610, Чернігівська обл., м. Ніжин, вул. Геологів, 30,
Тел. +38 (050) 381-17-23, +38(096) 855-82-14, E-mail: daminer23@ukr.net,сайт: www.daminer.com.ua

Апаратне забезпечення інформаційної безпеки держави

(Коротка історія створення спеціальної апаратури магнитного запису в Україні)

Апаратура магнітного запису, зберігання, відтворення та обробки спеціальних радіосигналів

Як відомо з попередніх публікацій («Бізнес і безпека». №№5, 6 2024; №1, 2025) пристрої точного магнітного запису (ТМЗ) знайшли широке застосування в різних галузях науки і техніки та відрізняються великою різноманітністю конструкцій. У більшості АТМЗ, які створював НДІ ЕМП, входили до складу великих радіокомплексів отримання, передачі та обробки розвідувальної інформації. Оскільки ці комплекси були складні, містили багато складових частин – радіоприймачів, антенної техніки, різноманітної апаратури перетворення та обробки інформації і т. п. з плином часу замовники запропонували для спрощення роботи та експлуатації зазначених комплексів первинну обробку та перетворення інформації включити в склад АТМЗ. Це дозволяло б оптимізувати структуру комплексу, зменшити кількість складових частин Вимоги до апаратів ТМЗ випливають із вимог до всього радіокомплексу загалом і функції первинної обробки інформації покласти надати до складу вже наявних функцій реєстрації, зберігання та аналізу інформації.

Досягнення мікроелектроніки та пов'язаний з ними у 70-х – 80-х рр. минулого сторіччя майже повсюдний перехід до цифрових методів обробки та передачі сигналів з'явилися поштовхом до широкого впровадження цифрової техніки в спеціальні види апаратури точного магнітного запису. Завдяки ним підвищилась оперативність керування, з'явилась можливість реалізації достатньо швидких аналізу та обробки перехоплених сигналів з визначення їх параметрів та навіть змісту, за рахунок виключення стрічкопротягувальних механізмів з відповідною електронікою їх управління, суттєво зменшились споживана потужність від джерел електроживлення, габарити та маса АТМЗ, у підсумку підвищилась її надійність. Іншими словами відбулась заміна магнітної стрічки з усіма її недоліками як елемента пам'яті АТМЗ на твердотільну (напівпровідникову) пам'ять.

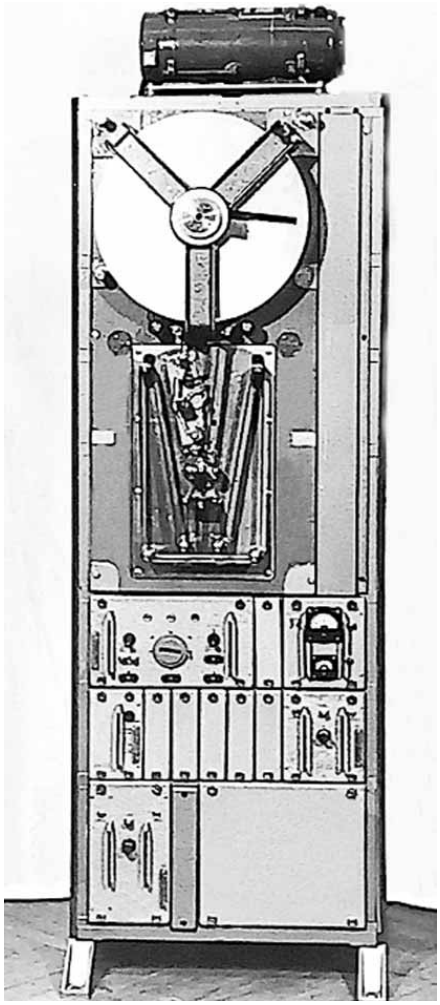
Провідні науковці та інженери НДІ ЕМП не залишались осторонь від виникаючих нових вимог до АТМЗ, намагались йти в ногу з часом, а інколи і випереджали його. В цьому процесі їм завжди сприяли представники Замовника, зокрема Військове представництво 4054 під проводом його керівника Ситника Б.В., а згодом під керівництвом полковника-інженера Лисенка Ю.В., який в молодості брав участь у випробуваннях радянської атомної зброї на острові Нова Земля. А після того все життя присвятив забезпеченню технічного оснащення підрозділів радіорозвідки Радянського Союзу і України.

Розглянемо деякі характерні вироби із низки створених зразків спеціальної апаратури магнітного запису та відтворення аналогових і цифрових сигналів, яка окрім зазначених вище функцій АТМЗ включала і функції обробки радіосигналів.

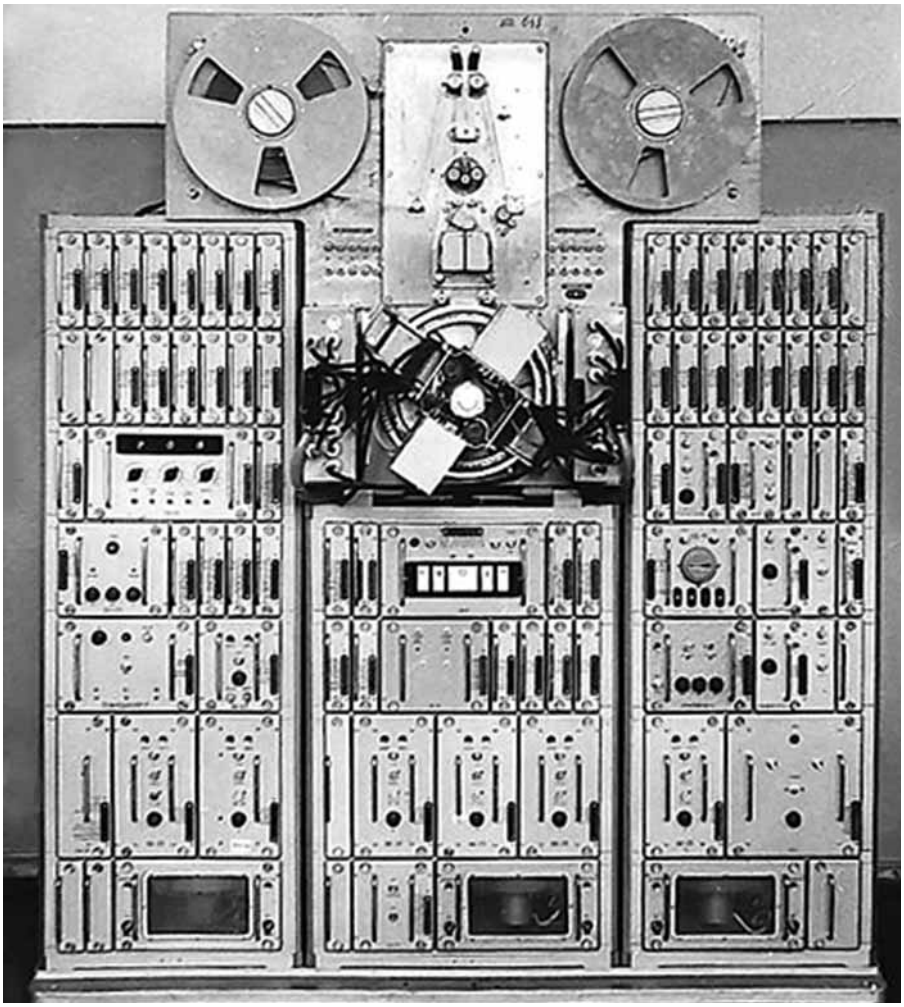
Вироби «Поле-П», «Поле-2» (Головний конструктор Мачинський В.К., Зволинський В.М.)

Вироби **«Поле-П»**, **«Поле-2»** – багатоканальні пристрої перетворення швидкості надходження інформації (транспонування частотного спектру) для застосування в складі комплексу «Поле». Перші вироби АТМЗ у НДІ ЕМП, в яких застосована обробка записаного сигналу [1].

Вироби мають відповідні габарити, масу та енергоспоживання. Конструк-

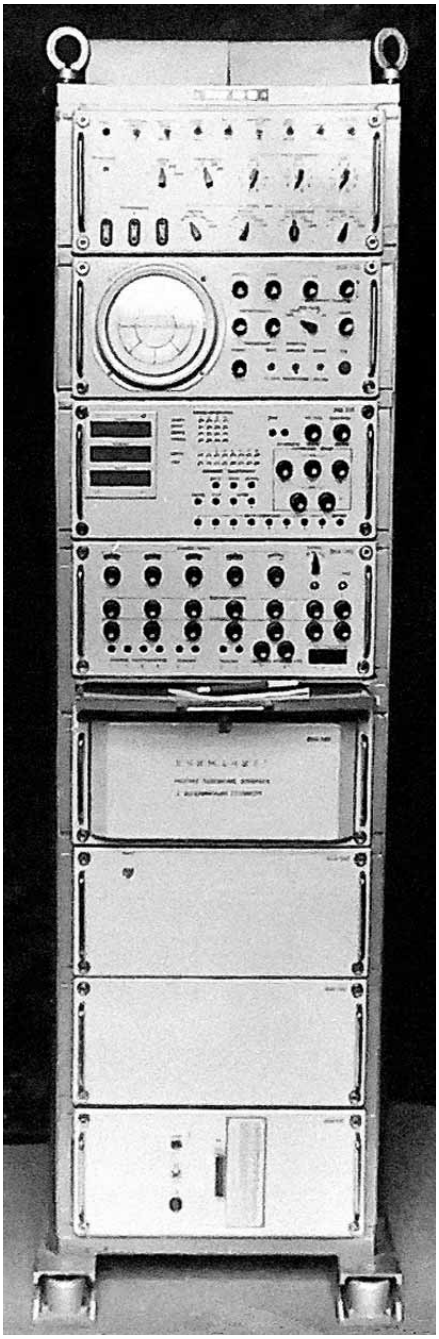


Виріб «Поле-П»



Виріб «Поле-2»

Барановський Б.В.



Виріб «Стеньга-К»

тивно реалізовані у вигляді стійок з вертикальним розташуванням стрічкопротягувального механізму (СПМ) та електронних блоків з застосуванням базових несучих конструкцій. В якості елементу пам'яті використовувалась імпортна магнітна стрічка завширшки 2,54 см.

В роботі брали участь заступники Головного конструктора: з радіоелектронної частини - Любченко О.М.; з конструкторської частини - Данилевський В.Ф., з технологічної частини – Барановський Б.В.; інженерно-технічні робітники: Савчук В.П., Голдаєвич Л.М., Рожнятовський А.Ф., Лінкина Л.Д., Векліч В.П., Копилова А.Ф., Шпаченко В.П., Школяренко В.М., Поліщук С.Н., Іщенко Є.Г., Кривенко С.І., Верлинський П.Х., Миронова Л.М., Межерицький В.А., Теремецький В.М., Писаренко В.І., Алексеєва М.Є., Рахманова С.Т., Мозолюк В.М., Колач Л.А. та інші.

Розробка 1966-1969рр. Виготовлено і надано Замовнику (в/ч 43753) 2 експериментальних зразка виробу для роботи в складі комплекса «Поле» на полігоні під Москвою [1].

Виріб «Стеньга-К» («МУЗ-7») (Головний конструктор Слуцький А.М.)

Апаратуру «**Стеньга-К**» призначено для реєстрації, довготривалого зберігання та обробки радіосигналів складної структури (спецрадіопередач) при не сприятливих умовах радіоприймання на тлі підвищеного рівня завад (при малих відношеннях сигнал/шум).

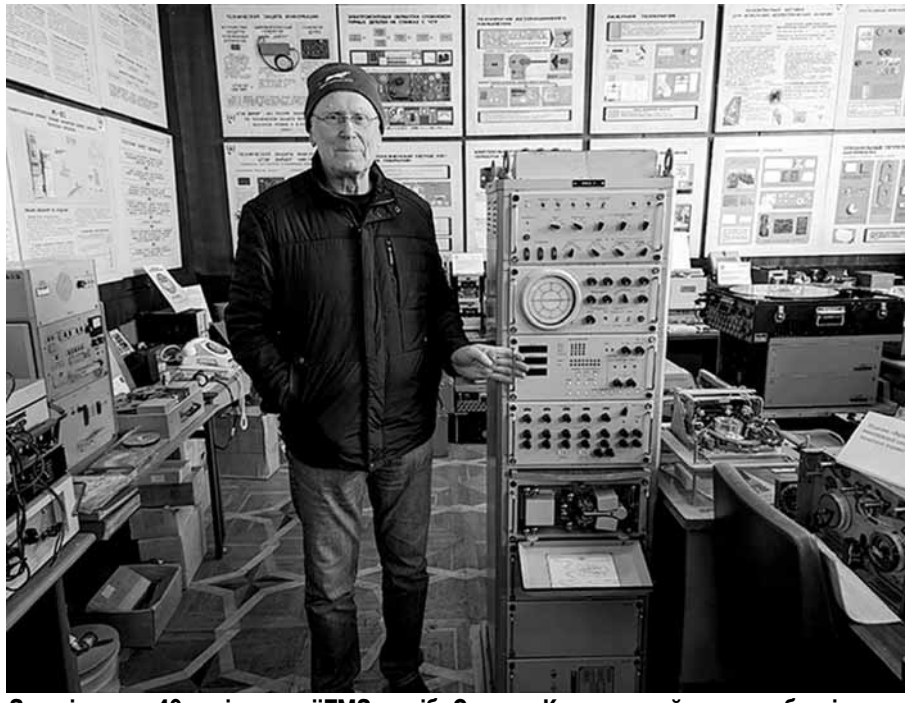
У виробі «Стеньга-К» для зберігання перехоплених радіосигналів використовувався чотириканальний пристрій магнітного запису-відтворення на кільцевій магнітній стрічці довжиною близько 2 м завширшки 2,54 см. Використання кільцевої стрічки дозволяло одноразовий запис перетворювати на періодичне відтворення цього запису для подальшого його аналізу.

Конструктивне виконання виробу у вигляді стійки з набором необхідних функціональних блоків з використанням базових несучих конструкцій. При цьому у верхній частині стійки (4 блока) розташовані блоки приймання спецрадіопередач, їх аналізу та обробки з використанням кореляційних методів; в нижній частині стійки знаходиться блок СПМ, електроніка СПМ з лічильником хронометражу роботи виробу та блоки живлення. Між верхньою та нижньою частинами стійки знаходиться висувний столик для здійснення робочих записів оператором виробу у штатному зошиті при бойовій роботі.

Основні технічні характеристики виробу «МУЗ-7» [6, 10]: кількість каналів – 4; смуга вхідного сигналу з внутрішніми фільтрами 0,03 – 10 кГц; відношення сигнал/завада в смузі частот вхідного сигналу 34 дБ; обсяг інформації, що записується – 500 кбіт; керування апаратом місцеве та дистанційне; електроживлення – 220 В 50 Гц; споживана потужність 800 Вт; вага – 210 кГ; габарити – 442 х 500 х 1668 мм. Кількість обслуговуючого персоналу – 1 люд.

Експлуатується виріб у приміщеннях, коливання температури в яких допускається від мінус 10 до плюс 50 °С при відносній вологості не більше 98% при температурі 40 °С.

Рік створення – 1977-1979 рр. Дослідні зразки виробу виготовило дослідне виробництво НДІ ЕМП і відправило Замовнику в/ч 30882. Конструкторська документація на виріб була передана для серійного виробництва підприємству п/с Г-4828 (м. Київ, завод



Зустріч через 40 років в музеї ТМЗ: виріб «Стеньга-К» та один з його розробників Ягічев О.М.; блок з відкритою кришкою - СПМ виробу

НВО «Маяк»), яке його випускало протягом низки років.

В розробці брали участь заступники Головного конструктора: з радіоелектроніки Крамаренко А.М., з технологічної частини Курсенко А.З., з конструкторської частини Проскурко В.М.; інженерно-технічні робітники: Ягичев О.М. (розробка обчислювального частотоміра), Біренберг Л.Я., Василевський В.О. та Ковінченко М.М. (розробка магнітофона виробу), Абрамов В.С., Смірнов Ю.М., Фомкин Л.В.; Гордєєв Д.О., Лисенко Ю.В. (представники Замовника) та інші.

Виріб «Соловка» («Р-384-4С») (Головний конструктор Ратушняк Е.М.)

Апаратура **«Соловка»** призначена для роботи у стаціонарних умовах та у пересувних комплексах радіорозвідки і забезпечує реєстрацію, відображення, аналіз та відтворення телекодової (цифрової) двійкової інформації в послідовних та паралельних каналах передавання даних та телеграфії. Замовником був один із підрозділів ГРУ ГШ МО СРСР.

Виріб «Р-384-4С» (шифр ДКР – «Соловка») розроблявся на початку 80-х у відділі мікроелектроніки НДІ ЕМП. Відділом на той час керував Євген Михайлович Ратушняк, який і був головним конструктором ДКР «Соловка».

Цікавою є передісторія рішення про постановку цієї роботи. У 70-ті роки для візуалізації та аналізу двійкової інформації використовувалися, переважно, паперові самописці рулонного типу. Їх головними недоліками були обмежені можливості аналізу інформації та величезна непродуктивна витрата паперу. Тому інтенсивно велися пошуки інших способів вирішення необхідних завдань, що дозволяють багаторазово використовувати носій інформації.

НДІ ЕМП теж був залучений до цієї роботи. Серед інших велися експерименти з матеріалами, що мають термопластичний ефект. До групи інженерів, що працювали над цією темою, входили:

Марчевський В.А.

Герасимук Л.М.

Трачевський В.В., Пасічник А.А., Гукалов С.П., Варламов В.А., Марченко А.А., Герасимук Л.М., Трунов Б.М. та ін. Незважаючи на їхні зусилля, практичний результат був далеко не очевидний. Головна причина полягала у труднощі серійного освоєння термопластичного носія з необхідними характеристиками. А це завдання було покладено на контрагента у м. Шостка. Коротше – час минав, і наближався «розбір польотів», здатний позначитися на репутації деяких керівників і не тільки у НДІ ЕМП.

Хто був автором рятівної пропозиції використовувати для вирішення поставлених завдань напівпровідникову пам'ять у поєднанні з електронно-променевою трубкою достеменно не відомо. У жовтні 1980 р., тривав етап ескізно-технічного проекту. У його рамках було розроблено та виготовлено два макети. Перший з урахуванням зсувних регістрів. Його автор – Наконечний Ю.І. Другий на базі статичних ОЗП із довільною вибіркою. Його автор – молодий талановитий інженер Клюковський В.А. Випробування показали значну перевагу варіанта з урахуванням ОЗП. Члени комісії від Замовника були приємно вражені можливостями та зручністю візуалізації та аналізу. Надалі з їхньої подачі в апаратуру, на етапі робочого проекту, були додані додаткові функції аналізу, не передбачені початковим ТТЗ (див. нижче). З цього моменту розробники відчували велику зацікавленість та підтримку з боку представництва Замовника (ПЗ) на чолі з полковником-інженером Лисенком Ю.В. [14].

Робочий проект проводився дуже напруженому ритмі. Практично весь обсяг робіт було виконано двома інженерами: Клюковським В.А. та Бебешко С.А. Обсяг пам'яті пристрою становив 64 кбіт. До того моменту МЕП-ом були освоєні в серійному виробництві статичні ЗП з довільною вибіркою ємністю 1 кбіт типу 132РУ5. Таким чином, 64 мікросхеми розміщені на 4-х платах і склали «серце» приладу. Як елемент відображення був обраний єдиний з військовим прийманням кінескоп типу 16ЛК2Б з електромагнітним відхиленням. Відхиляючу котушку йому довелося погоджувати із замовником окремим протоколом, оскільки вона не випускалася з військовим прийманням. Непростим завданням наших конструкторів і технологів виявилося забезпечення працездатності високовольтного блоку живлення анода кінескопа за умов підвищеної вологості, заданих у ТТЗ. Проектування та виготовлення спеціального оснащення знадобилося для штампування контактів комутаційного поля вхідних сигналів. Це поле являло собою матрицю 16 х 16 пар контактів, що замикаються спеціальним штирем.

До складу апаратури входять виріб «Соловка», одиночний комплект ЗІП та комплект експлуатаційної документації. Конструктивно виріб виконано у вигляді приладного моноблоку Апаратура «Соловка» забезпечує наступні режими роботи та параметри: реєстрацію, відображення та аналіз одноканального потоку дискретної інформації, що надходить зі швидкістю 200000 дв.од/с;

Виріб «Соловка» («Р-384-4С»)

Бебешко С.А.

реєстрацію, відображення та аналіз до 16 незалежних потоків дискретної інформації, що надходить зі швидкістю 200000 дв.од/с в кожному каналі; об'єднання двійкових сигналів 2-16 паралельних каналів зі швидкістю від 16 до 2976 дв.од./с в кожному каналі у послідовний двійковий сигнал зі швидкістю до 47616 дв.од./с; реєстрацію та відображення двійкового сигналу одноканального потоку у вигляді растру на екрані ЕЛТ, що містить 32 рядки при кількості двійкових елементів в рядку до 512 та 16 рядків при кількості елементів в рядку від 513 до 1024 з можливістю прискореної або уповільненої зміни ємності рядку. Поточне значення кількості елементів в рядку відображається на цифровому табло вимірювання за допомогою перебудовуємих електронних візирів часових параметрів зареєстрованого сигналу з відображенням результатів вимірювання на цифровому табло. Забезпечується прискорена та уповільнена перебудова положення візирів на екрані, а також їх маркування частотою модуляції по яскравості; перегляд на екрані ЕЛТ всього обсягу пам'яті шляхом поелементного або порядкового пришвидшеного або уповільненого зміщення інформації, що відображається у будь-якому напрямку по обсягу пам'яті; збільшення масштабу інформації, що відображається до 64 разів; вивід зареєстрованої інформації у зовнішні кола з внутрішньою тактовою частотою, що змінюється в межах 50-500000 дв.од./с та зовнішньою тактовою частотою до 500000 дв.од/с; оперативний контроль працездатності виробу за допомогою схеми вбудованого контроля.

Основні технічні характеристики виробу «Соловка» («Р-384-4С») [5, 9]: кількість каналів реєстрації та відображення дискретної інформації – 16; максимальний обсяг пам'яті – 65536 дв.од. (одноразрядних слів); максимальний обсяг одночасно відтворюємої інформації 16384 дв.од.; рівні вхідних сигналів: логічного нуля – від мінус 100 до плюс 0,6В; логічної одиниці – від 2,2 до 100 В; рівні вихідних сигналів: логічного нуля – від 0 до 0,4В; логічної одиниці – від 2,4 до 4,5 В; максимальна швидкість запису інформації в кожному каналі – 200 х 103 дв.од./с; керування апаратом місцеве та дистанційне режимами («ПУСК», «СТОП», «ВІВОД») запису, відтворення та виводу інформації; електроживлення – 220 ± 10% В; 127 ±10% В 50 Гц; споживана потужність не більше 220ВА; маса – 43,9кг; габарити – 475 х 482 х 278мм. Кількість обслуговуючого персоналу – 1 люд.

Умови експлуатації відповідають умовам експлуатації виробу «МУЗ-8».

Рік створення – 1980 - 1983. В ході робіт проведено виготовлення 6-ти дослідних зразків, їх налаштування, попередні випробування, коригування КД за результатами цих випробувань. Після цього успішно проведено Державні випробування, що проходили на стрімкому березі Чорного моря між Миколаєвом та Одесою. Дослідні зразки виробу НДІ ЕМП відправило Замовнику - ГРУ ГШ МО СРСР.

Для серійного виготовлення виробу, вже під назвою «Р-384-4С», було обрано завод «Юпітер» у місті Славутич. Він входив до складу КНВО «Маяк». Передача КД та технологічного оснащення відбувалася у 1984 - 1985 рр. Випуск першої установчої серії виробів був запланований на кінець 1986 р. Але аварія на Чорнобильській АЕС, розташованій буквально за кілька кілометрів від території заводу «Юпітер», поламала всі плани.

У Москві було ухвалено рішення про підготовку серійного виготовлення на телевізійному заводі у м. Кишинів. Частині технічного персоналу заводу «Юпітер», причетного до виробу, було запропоновано переселитися до Кишинева та продовжити роботу там. Як згадує учасник подій, заступник Головного конструктора Бебешко С.А., у жовтні 1986р. ці хлопці, разом із співробітниками нашого відділу впровадження займалися евакуацією документації, оснащення та доробку на нове місце. На заводі в Кишиневі випуск виробу відбувався практично до 1991р.

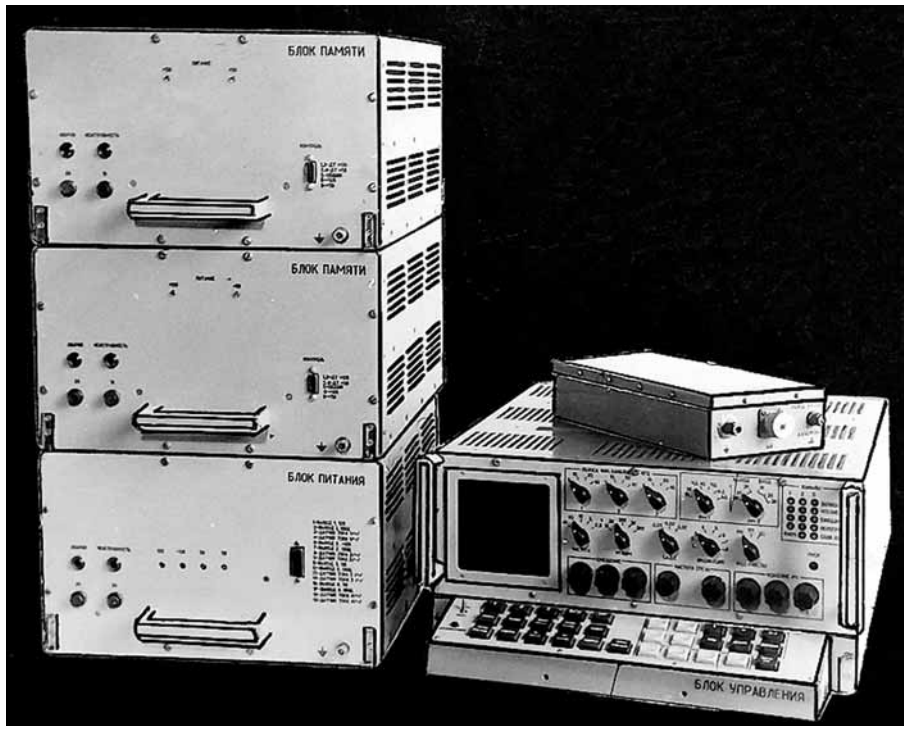
В розробці брали участь заступники Головного конструктора: електронної частини Сусленко В.Л., Бебешко С.А., з технологічної частини Учень К.А., з конструкторської частини Марчевський В.А., з додаткових вимог Желєзняк В.К.; інженерно-технічні робітники: к.т.н. Герасимук Л.Н., Мачульський А.В. (метрологія), Наконечний Ю.І. (розробка пульта керування та відображення), Платонов А.Н. (розробка радіоелектронних пристроїв наскрізного каналу), Клюковський В.А. (розробка систем автоматики та обробки інформації) та інші.

Виріб «МУЗ-8» (Головний конструктор Слуцький А.М.)

Виріб «**МУЗ-8**» призначений для багатоканального запису та багатократного читання сигналів з виходів СХ, КХ, УКХ та гідроакустичних приймальних пристроїв у напівавтоматичній системі виявлення, обробки аналізу, розпізнавання та класифікації спецрадіопередач.

Виріб може встановлюватись на постах, на надводних і підводних кораблях ВМФ, а також в загонах радіорозвідки берегових служб та автомобілях.

До складу виробу входять в форматі базових несучих конструкцій (БНК) наступні блоки: блок управління, блок пам'яти (2шт), блок живлення, фільтр



Виріб «МУЗ-8»

мережевий та комплект з'єднувальних кабелів, а також комплект ЗІП та експлуатаційна документація.

В якості БНК застосовано корпуси блоків за ГОСТ 23701-79. Кожний блок за винятком фільтра мережевого встановлюється на амортизаційній рамі, яка відповідає типорозміру рам за ГОСТ 23701-79. Корпус кожного блоку складається з передньої та задньої рамки, які стягнуті верхньою та нижньою стінками.

На рамках кріпляться передня та задні панелі, на яких розташовано органи керування, світлової індикації, вхідними та контрольними роз'єднувачами, блок має нижню кришку та П-образний кожух.

Несучі рамки блоків виготовлено з литого алюмінію; стінка, кришка та кожух – штамповані. Електронні блоки виконано на друкованих платах зі фольгованого двохстороннього склотекстоліту.

Вперше в СРСР розроблено безкінематичну апаратуру запису та зчитування сигналів для обробки спецрадіопередач (авторське свідоцтво. на винахід №199378 з пріоритетом від 02.06.1982 р.), яка дозволяє забезпечити аналіз тонкої структури сигналу. Виріб належить до 5 покоління. В розробці застосовано автоматизацію управління виробом з використанням засобів ЕОТ, яка побудована на мікропроцесорному комплекті серії 580, самодіагностика та можливість адаптації до внутрішніх обурюючих факторів; використано мікросхеми та мікросборки пятого ступеню інтеграції.

Виріб уявляє собою 3-х канальний апарат запису та читання інформації, яка надходить з виходів проміжної частоти (ПЧ) та низької частоти (НЧ) радіоприймальних та гідроакустичних пристроїв. Аналогові сигнали, які надходять на його вхід, перетворюються аналого-цифровим перетворювачем (АЦП) у цифровий код та запамятовується в комірках пристрою оперативної памяті (ПОП), яка виконана на мікросхемах серії 565.

Зберігання записаної інформації в ПОП можливе тільки при наявності напруг живлення. При знятті напруг живлення записана інформація знищується.

Під час запису по двом каналам або одному каналу використовується весь обсяг наявних комірок і таким чином збільшується час запису інформації у 1,5 та в 3 рази відповідно. Апаратура має функціональний контроль систем та індикацію їх справності. Застосовано мікро-ЕОМ в системах керування режимами роботи виробу.

В апаратурі наявні функціональні пристрої для проведення експрес-аналізу інформації, що надходить (амплітудний, частотний та фазовий дискримінатори).

Основні технічні характеристики виробу «МУЗ-8» [10-13]: кількість каналів – 3; тривалість запису в смузі частот: (0 – 40) кГц – 2,5 с; (0 – 20) кГц – 5 с; (0 – 10) кГц – 10 с; (0 - 5) кГц – 20 с; відношення сигнал/завада в смузі частот від 0 до 40 кГц не менше 35 дБ; нерівномірність АЧХ в смузі частот від 0 до 40 кГц не більше 1 дБ; смуга частот, що записуються зі входів ПЧ, кГц: (215 ±20), (215 ±10), (215 ±5), (215 ±2,5), (128 ±20), (128 ±10), (128 ±5), (128 ±2,5); смуга частот, що записуються зі входів НЧ, кГц (0 - 40), (0 - 20), (0 - 10), (0 - 5); час готовності виробу після подачі на нього електроживлення - 5 хвил.; час безперервного запису – 24 години; керування апаратом місцеве та від ЕОМ «Электроника-60»; електроживлення – 220 В 50 Гц; споживана потужність 600 ВА; габарити: блок керування– 585 х 402 х 235 мм, маса - 30 кг; блок живлення - 530 х 335 х 235 мм, маса – 20 кг; блок пам'яті – 585 х 402 х 235 мм, маса – 20 кг; фільтр мережевий – 310 х 60 х 144 мм, маса – 5 кг; надійність – наробіток виробу на відмову не менше 1000 год, призначений ресурс не менше 25000 год. Кількість обслуговуючого персоналу – 1 оператор з середньотехнічною освітою.

Річний випуск: по першому року 10 шт, другому - 20 шт, по третьому - 30 шт. Гуртова ціна при серійному виробництві по першому року випуску - 52000 руб, по другому – 49900 руб., по третьому – 48750 руб.

Умови експлуатації: група 1.8 УХЛ (не працююча в русі) для опалюваємих приміщень та група 2.1.1 за ГОСТ В.20.39.304-76 з наступними обмеженнями: робоча температура до мінус 10 °С; лімітна температура мінус 50 °С; відносна волога 98% при температурі 35 °С.Термін експлуатації 5 років включно з 2 роками зберігання на складі. Апаратура стійка до транспортування автотранспортом, морським, повітряним та залізничним транспортом.

Рік створення – 1983 - 1984. Дослідні зразки виробу виготовило дослідне виробництво НДІ ЕМП і відправило Замовнику – в/ч 30882. Серійне виробництво з 1986р., виробник - підприємство п/с Г-4828.

В розробці брали участь заступники Головного конструктора: з радіоелектроніки Крамаренко А.М., з технологічної частини Курсенко А.З., з конструкторської частини Проскурко В.М., по спецдослідженням Желєзняк В.К.; інженерно-технічні робітники: Іванова Т.П., Орлович Ю.П., Михайлова Т.Н., Смірнов Ю.М., Ситник О.Т., Єфіменко В., Хахамов В.Є., Сніжко Г.К. та інші.

Вироби «Наставка» (Головний конструктор Слуцький А.М.)

Виріб **«Наставка»** – безкінематичний апарат реєстрації аналогової інформації у цифровій формі на твердотільній пам'яті великого обсягу.

Обладнання виробу дозволяло проводити реєстрацію та первинний аналіз інформації, для детального аналізу забезпечувалося поєднання з відповідними вимірювальними приладами та мікроЕОМ «Електроніка-60».

Виріб «Наставка» розроблявся для потреб морської радіотехнічної розвідки та був розвитком виробу «Стеньга-К», розглянутого вище.

Метою розробки виробу «Наставка» було усунути недоліки виробу «Стеньга-К» (значна незручність для аналізу представляла фіксована довжина кільця магнітної стрічки і неможливість виділити довільний фрагмент записаного сигналу) і забезпечити можливість виділення будь-якого фрагмента записаного сигналу та його безперервне відтворення для тонкого аналізу та передачи його в мікроЕОМ для аналізу, систематизації та довгострокового зберігання [14].

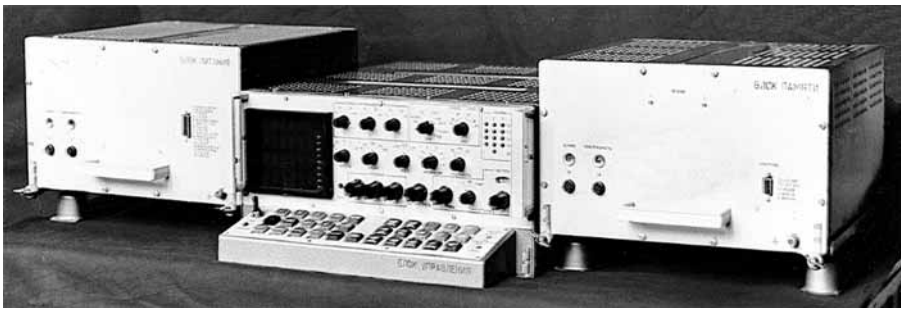
Спочатку вибір упав на пристрої, що з'явилися, на циліндричних магнітних доменах (ЦМД). Вони не мають механічних рухомих елементів, мають більш високу щільність запису ніж магнітна стрічка і невеликі габарити. Але ЦМД є пристроєм з довільним доступом і для їх застосування була потрібна додатково специфічна елементна база. Оцінки, зроблені на попередньому етапі, показали складність виконання вимог ТЗ при зберіганні інформації в пристроях, що запам'ятовують, на ЦМД.

Керівники військового предствництва пішли на зустріч і надали дозвіл проводити розробку виробу на елементній базі, що знаходиться на стадії державипробувань на підприємствах Міністерства електронної промисловості СРСР. Це дозволяло застосувати елементну базу, яка ще не мала військового прийманя у дослідних зразках виробу.

Структурно виріб «Наставка» представляв:

- три вхідні восьмирозрядні АЦП, реалізовані на резистивних матрицях R-2R;

- електронну восьмирозрядну пам'ять із довільним доступом;



Виріб «Наставка»

Слуцький О.М.

- три рахункові мультиплексовані формувачі адреси пам'яті з регістрами початкової адреси та таймерами для обмеження максимальної адреси каналу/фрагменту;

- три вихідні цифроаналогові перетворювачі;

- керуючу мікроЕОМ на БІС 580ВМ80, що забезпечує режими роботи виробу відповідно до установок органів управління та клавіатури, індикацію режимів роботи та результатів вимірювань, керування виділенням фрагмента запису, формуванням горизонтальної розгортки для його відображення, обчислення частоти та різниці частот за виміряним періодом вбудованого генератора та друк.

- підсистему попереднього аналізу з генераторами синусоїдальних сигналів та обчислювальним частотоміром;

- інтерфейси з вимірювальними приладами, цифровим пристроєм і мікроЕОМ.

Блоки пам'яті реалізовані мікросхемах динамічної пам'яті 565РУ3 (16Кх1). Ємність одного блоку пам'яті становила 512 кілобайт, штатний виріб комплектувався двома блоками пам'яті (1 МВ), і було передбачено підключення до 4 блоків (2МВ). Загальний обсяг підключеної пам'яті визначався автоматично, при включенні виробу, і розбивався на 1, 2 або 3 рівні частини, які могли використовуватись як незалежно, так і паралельно (многоканальний режим).

Вихідний вхідний сигнал оцифровувався АЦП і безперервно записувався по кільцю пам'ять, виділену для каналу. З появою сигналу, що вимагає аналізу, запис припинявся і в пам'яті залишався фрагмент радіосигналу для подальшого аналізу.

Завдяки використанню пам'яті з довільним доступом за допомогою маркерів початку та кінця фрагмента можна було виділити будь-який фрагмент записаного сигналу та закільцювати його для подальшого аналізу. При цьому за допомогою множинних ЦАП формувався сигнал горизонтальної розгортки постійної амплітуди, синхронізований з початком кільця і протяжністю відтворюваного фрагмента. Це забезпечувало відображення всього фрагмента, що відтворюється, на весь екран осцилографа незалежно від його довжини і частоти дискретизації, що значно полегшувало роботу оператора.

Аналіз проводився за допомогою вбудованих генераторів синусоїдального сигналу, швидкодіючого прецизійного обчислювального частотоміра з автоматичним перемиканням діапазонів вимірювання, а також зовнішніх пристроїв, що не входять до комплекту виробу. Результати вимірювань документувалися на цифровому пристрої друку МПУ16-3.

При необхідності оцифровані фрагменти записаних сигналів могли передаватися в мікроЕОМ «Електроніка-60» для подальшої програмної обробки, систематизації та довготривалого зберігання. Це дозволяло створювати бібліотеки сигналограм, обмінюватися ними між підрозділами та навчати операторів.

Конструктивно виріб «Наставка» складався з блоків: керування, живлення, пам'яті.

На фото зліва блок живлення живить блок управління (в середині). Справа блок пам'яті, об'єм – 512 кілобайт. Штатно в комплекті 2 блоки пам'яті, максимально 4. На об'єм пам'яті блок керування налаштовується автоматично, при включенні живлення. Підключена пам'ять розподіляється між каналами програмно, завдяки цьому забезпечується повне використання підключеної до блоку управління оперативної пам'яті.

Основні технічні характеристики виробу «Наставка» [8, 14]: кількість каналів 3; смуга частот вхідного аналогового сигналу 0 - 40 кГц; відношення сигнал/перешкода у смузі частот вхідного сигналу 35 дБ; розрядність АЦП 8 біт; обсяг інформації, що записується – від 512 до 2048 кбайт; керування апаратом місцеве; електроживлення – 220 В 50 Гц; споживана потужність 400 ВА; маса – 92 кг (з кабелями); габарити: блок керування– 585 х 402 х 235 мм, маса – 30 кг; блок живлення – 530 х 335 х 235 мм, маса – 20 кг; блок пам'яті – 585 х 402 х 235 мм, маса – 20 кг;. Гуртова ціна на початок 1992р. при серійному виробництві – 577 тис. руб.

Умови експлуатації: група 1.8 УХЛ (не працююча в русі) для опалюваємих приміщень та група 2.1.1 за ГОСТ В.20.39.304-76, інші вимоги аналогічні вимогам до виробу «МУЗ-8».

Рік створення – 1981-1984. Дослідні зразки виробу виготовило дослідне виробництво НДІ ЕМП і відправило Замовнику в/ч 30882. Згодом, конструкторська документація на виріб була передана для серійного виробництва на завод «Топаз» у м. Донецьк, яке його випускало протягом низки років.

Виріб «Наставка-В» (Головний конструктор Крамаренко А.М.)

Виріб **«Наставка-В»** – безкінематичний апарат реєстрації аналогової інформації у цифровій формі для системи «Выручка-Э».

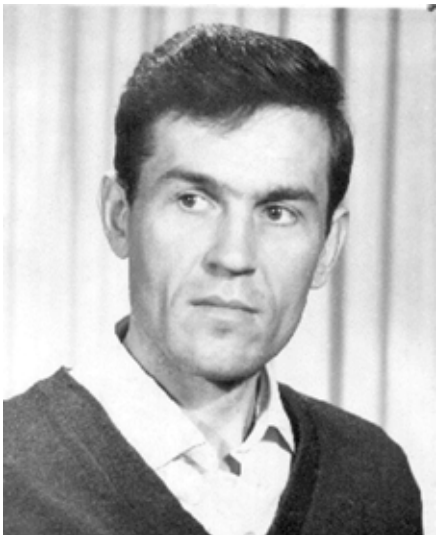
Крамаренко А.М.

З урахувнням досвіду експлуатації виробу «Наставка» у Замовника та його додаткових вимог, було проведено його модернізацію. Модернізований виріб отримав назву «Наставка-В» (конструктивно і візуально та по основним параметрам вироби майже не відрізнялись), завдяки якій можна було реєструвати як низькочастотні детектовані сигнали, так і сигнали безпосередньо з виходу проміжної частоти 215 кГц радіоприймачів. Наводимо далі деякі додаткові можливості цього виробу, а саме: наявні три незалежні канали з можливістю паралельного запису інформації. Забезпечуються багатократне відтворення обраної ділянки запису. Вихід інформації, що відтворюється – в цифровій та в аналоговій формах. Сигнал, що відтворюється може вводитись в ЕОМ для подальшої обробки. Зберігання записаної інформації можливе тільки за наявності напруги живлення. При знятті напруги живлення записана інформація знищується.

Основні технічні характеристики виробу «Наставка-В» [8, 14]: кількість каналів 3; запис сигналів з проміжною частотою 215 кГц та смугою пропускання ±20 кГц в смузі частот вхідного аналогового сигналу 0-40 кГц; відношення сигнал/перешкода у смузі частот вхідного сигналу 35 дБ; розрядність АЦП 8 біт; обсяг інформації, що записується – від 512 до 2048 кбайт; керування апаратом місцеве; електроживлення – 220 В 50 Гц; споживана потужність 500 ВА; маса близько 93 кг (з кабелями); габарити: блок керування – 585 х 402 х 235 мм, маса – 30 кг; блок живлення - 530 х 335 х 235 мм, маса – 20 кг; блок пам'яті – 585 х 402 х 235 мм, маса – 20 кг; Гуртова ціна на початок 1992 р. при серійному виробництві - 600 тис. руб.

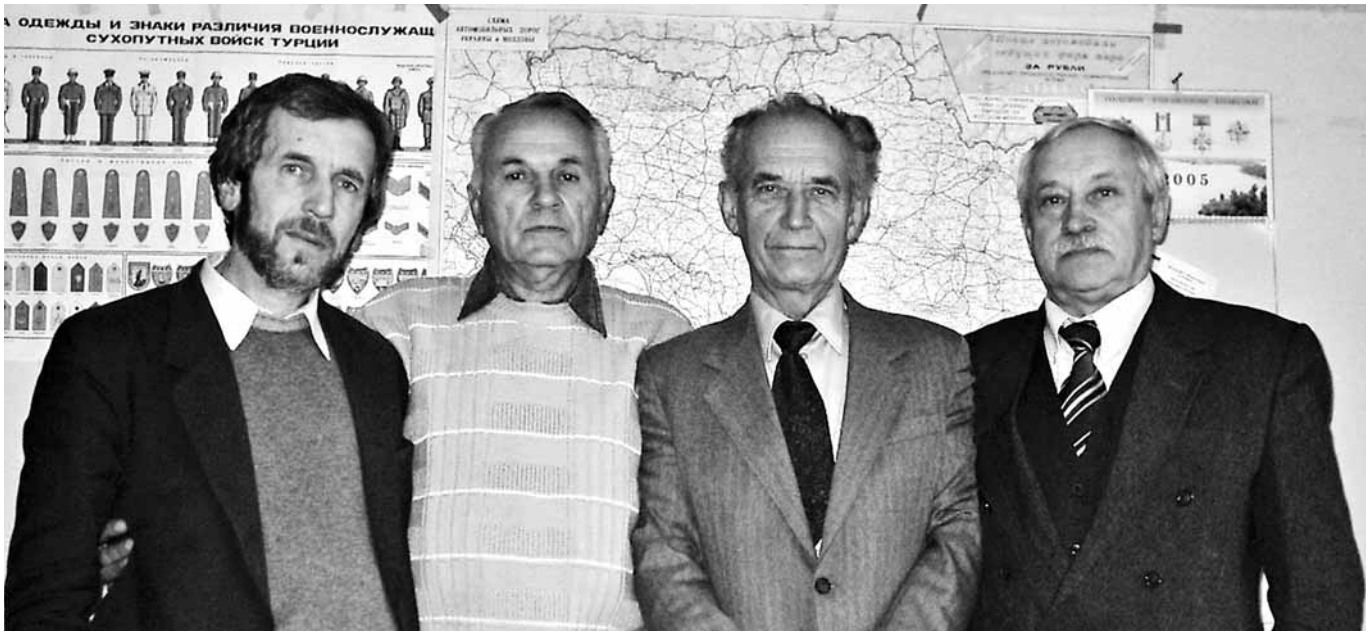
Рік створення – 1986-1987. У 1990-1991р. доопрацьовано КД за результатами дослідної експлуатаці у Замов-

Учень К.А.



Желєзняк В.К.

Ковтун С.Л.



Зустріч в НДІ ЕМП: Провозін О.П. – начальник Центру ТЗІ НДІ ЕМП, автор статті, Чеховський А.Г. – начальник РЕР ЧФ, Лисенко Ю.В. – начальник ВП 4054, Солдатенко Г.Т. – Головний конструктор фірми «ЕПОС»

ника. Виготовлено: 4 дослідних зразка і успішно проведено випробування в повному обсязі вимог ТТЗ Замовника; три нових комплекти виробу, відправлено Замовнику – в/ч 30882. Умови експлуатації як для виробу «Наставка», див. вище.

В розробці обох виробів брали участь заступники Головного конструктора: з радіоелектроніки Крамаренко А.М., з технологічної частини Курсенко А.З., Учень К.А., з конструкторської частини Проскурко В.М., по спецдослідженням Желєзняк В.К.; інженерно-технічні робітники: Баранець П. (розробник АЦП/ЦАП); Ягічев А.М. (розробник системи зберігання, запису-вибірки, мікроЕОМ та програмного забезпечення); Носановський В.Я. (розробник не стандартного допоміжного цифрового обладнання); Ковтун С.Л., Шапірштейн С.Я., Нечунаєв Ю.А. (розробники оригінальної імпульсної системи живлення), в частині оформлення документації вищезазначених (окрім «Соловки») виробів Сперанська Р.В. - керівник групи фахівців («Бізнес та безпека», №1, 2025р.) та інші.

До виробів «Стеньга-К», «Соловка», «МУЗ-8», «Наставка» та «Наставка-В» висувались вимоги з протидії іноземним технічним розвідкам, зокрема в частині захисту від витоку інформації, що оброблювалась каналами ПЕМВН. За результатами робіт всі вироби відповідали вимогам Норм Держтехкомісії СРСР для відповідної категорії об'єктів. Спецдослідження виробів, розробку вимог та рекомендацій по блокуванню та усуненню виявлених каналів витоку інформації, перевірку ефективності реалізації зазначених вимог виконували спеціалісти Головної науково-дослідної лабораторії НДІ ЕМП (начальник к.т.н. Желєзняк В.К), пізніше Головного науково-дослідного відділу КНВО «Маяк» (начальник Провозін О.П.) такі як Белов С.В., Терпіль О.С., Худяков В.О., Волощенко М.М., Діброва Т.І., Гавро О.В., Михайлов І.П. та інші.

Насамкінець наведу характеристику виробам і спільній роботі з НДІ ЕМП начальника радіоелектронної розвідки (РЕР) Чорноморського флоту СРСР Чеховського А.Г., яку він дав в своїх спогадах [14].

«Перебираючи документи і схеми раціоналізаторської роботи, що залишилися з минулих років, я виявив загублену фотографію дорогого мені виробу «Соловка». Цей виріб розроблено та виготовлено у НДІ ЕМП м. Київ. Його випробування проходили на Чорноморському флоті у м. Севастополі Державною комісією, головою якої я був. Цей виріб мені дорогий тим, що він був першою і досить успішною спробою цифрової обробки аналогових сигналів для радіоелектронної розвідки (РЕР).

На сьогодні це прообраз флешки та комп'ютера. На фотографії видно три куби перших мікросхем пам'яті та процесорний блок управління. Який дар передбачення мали конструктори даного підприємства, і яких зусиль

Лисенко Ю.В. та Хурс І.К. в кулуарах Науково-технічної ради МПЗЗ СРСР.

зробив колектив військових представників, очолюваних полковником-інженером Лисенком Ю.В., щоб на початку 80-х років довести, що майбутнє буде за цифровою та комп'ютерною обробкою сигналів. А в той час були і противники цього напрямку і досить впливові, які не хотіли обтяжувати себе новими турботами і ставили конструкторам приблизно таке питання: «Якщо є відпрацьовані методи запису на магнітній стрічці, навіщо теж записувати у важкі куби електронної пам'яті, тим більше, що обсяг інформації електронної пам'яті набагато менше, ніж можна записати на магнітну стрічку?!». А зараз практично немає магнітної стрічки і користувачі інформації повсюдно зберігають її в електронному вигляді. Хто мав рацію?

Відмінною рисою колективів конструкторів і військових представників УНДІ ЕМП був їхній тісний зв'язок з видобувними підрозділами РЕР Чорноморського флоту (ЧФ) та інших флотів. Тому безпосередньо від нас вони знали, що технічна оснащеність частин РЕР відстає від розвитку засобів зв'язку та радіоелектронного озброєння нашого супротивника, що багато завдань вирішуються за рахунок творчості раціоналізаторів з особового складу кораблів та частин РЕР. Колектив НДІ ЕМП був перейнятий патріотичною відповідальністю за обороноздатність нашої колишньої Батьківщини і тому всіляко надавав технічну допомогу нашим раціоналізаторам, виступав ініціатором необхідності розробки нових та вкрай необхідних технічних засобів.

Важливою сполучною ланкою між діючими частинами РЕР та виробництвом були, звичайно, військові представники. Потрібно велике спасибі сказати полковнику-інженеру Лисенку Ю.В. Він не лише на кораблях та частинах РЕР вивчав процес видобутку та обробки інформації, але безпосередньо на території НДІ ЕМП в одному з приміщень військового представництва обладнав міні приймальний центр. Призначив туди відповідального мічмана Гордєєва Д.А., і «в умовах максимально наближених до бойових» досліджував і перевіряв нові технічні рішення, які потім застосовувалися конструкторами в нових виробах. Тим більше, треба враховувати, що з нього ніхто не знімав виконання своїх виробничих обов'язків.

Завдяки цьому НДІ ЕМП розробляв та випускав технічні засоби необхідні для вирішення вкрай нагальних та злободенних завдань. Технічні засоби РЕР, що випускались НДІ ЕМП, відрізнялися від виробів інших родинних підприємств своєю оптимальною приналежністю до вирішення конкретних завдань, зручністю користування, порівняно невеликими обсягами та ергономічними показниками. Їх можна було встановлювати на будь-який навіть найменший розвідувальний корабель і передавати з корабля на корабель у морських походах.

Для прикладу можна показати, наскільки відрізнялася київська апаратура від інших споріднених виробників, наприклад, від підприємства НВО «ВЕКТОР» м. Ленінград. Приблизно одні завдання виконували вироби «МУЗ-7» (НДІ ЕМП) та «ОХОТА» (НВО «ВЕКТОР»), це аналіз та ідентифікація випромінювань засобів зв'язку.

«МУЗ-7» являв собою одну стійку завишки не більше 1,6 метра, а «ОХОТА» мала 12 стійок висотою близько 1,8 метра, з яких знаходили застосування тільки дві стійки, при цьому технічні характеристики «ОХОТА» поступалися «МУЗ-7», в якому вже були закладені принципи процесорної обробки. Хочеться тому пригадати ще один «ШЕДЕВР» Ленінградського «ВЕКТОРА» - це знову розроблений ними короткохвильовий пеленгатор. За визнанням самих конструкторів «ВЕКТОРА» через великі габарити їх пеленгатора його можна було розмістити тільки на крейсері!

Я вдячний долі в тому, що на посаді головного інженера та начальника РЕР ЧФ понад десять років (з 1977 по 1989 рр.) мені надалася можливість здійснювати взаємодію з НДІ ЕМП. Я був головою державних комісій з прийому на озброєння «МУЗ-6», «МУЗ-7», «МУЗ-10» та «Соловка». Пам'ять зберегла велику повагу до таких Головних конструкторів як Слуцький А.М., Зволинський В.М., Біренберг Л.Я., Ратушняк О.М., яких, на жаль, вже немає серед нас та інших товаришів. Це були конструктори, як кажуть від Бога. Для них робота на моє переконання була швидше захопленням, ніж примусовим обов'язком. У спілкуванні з ними не відчувалося, що вони на голову компетентніші в радіоелектроніці, не виявляли принизливого ставлення до свого опонента, якщо він не розумів або не сприймав їхні пропозиції, і просто були тактовними людьми».

А ось характеристика нашої роботи командира в/ч 30882 Хурса І.К. - нашого Замовника на Науково-технічній раді (НТР) нашого Міністерства.

Виступаючи на засіданні НТР Хурс І.К. сказав, що «користуючись нагодою, хочу подякувати НВО «Маяк» за творчу працю по створенню потрібних нам засобів. Самих добрих слів вони заслуговують за розробку й створення дуже ефективної для нас апаратури «Стеньга-К», «Наставка», «Соловка» і взагалі за розуміння цієї проблеми в ході наших спільних робіт!» [15].

(Далі буде.)

Олександр Провозін
Заст. Голови правління АТ «НДІ ЕМП»

Література.

1. Річні звіти діяльності та накази по підприємству за 1966 – 1991рр.

2. Дэвис Г.Л. Применение точной магнитной записи. М., «Энергия», 1967г.

3. Справочник по технике магнитной записи. Под ред. О.В. Порицкого, Е.Н. Травникова. Киев, «Техніка», 1981г.

4. ГОСТ 20940-82. Аппаратура точной магнитной записи многодорожечная. Основные параметры и общие технические требования. М, Госстандарт СССР.

5. Альбом иллюстраций аппаратуры регистрации и отображения дискретной информации «Соловка», инв. №2985, 1982г.

6. ЛЩ.750.041 ТО. «МУЗ–7». Техническое описание. 1980г.

7. ЛЩ.750.041 ИЭ. «МУЗ–7». Инструкция по эксплуатации. 1980г.

8. Каталог научно-технической продукции. Киевский НИИЭМП , выпуск №1, г. Киев, 1992г.

9. Минмашпром Украины. НИИ ЭМП. Каталог «Продукция изготавливается и поставляется по договору». Киев, 1993г.

10. МПСС СССР. Полуавтоматическая аппаратура записи радиосигналов с выходов СВ, КВ, УКВ и гидроакустических приемных устройств «МУЗ-8», буклет, 1987г.

11. Изделие «МУЗ-8». Карта технического уровня и качества продукции. ЛЩ3.060.125 КУ. 1984г.

12. ЛЩ1.750.055 ТУ. Технические условия «МУЗ-8». 1984г.

13. «МУЗ-8». Технико-экономическая характеристика. ЛЩ1.750.055 Д9. 1984г.

14. Спогади: провідних фахівців НДІ ЕМП Ягічева О.М., Бебешка С.А.; Замовників Лисенка Ю.В. та Чеховського А.Г.

15. Состояние, проблемы и основные направления работ по повышению технического уровня специзделий и БРЭА магнитной записи и меры по техническому перевооружению предприятий в XI пятилетке. (САМЗ). МПСС, Научно-технический Совет, 2 сентября 1982г. инв. №5190.

XXIII МІЖНАРОДНИЙ ПРОМИСЛОВИЙ ФОРУМ-2025

МІЖНАРОДНІ СПЕЦІАЛІЗОВАНІ ВИСТАВКИ

- МЕТАЛООБРОБКА
- УКРЗВАРЮВАННЯ
- УКРВТОРТЕХ
- ГІДРАВЛІКА ПНЕВМАТИКА
- ПІДШИПНИКИ
- УКРЛИТВО
- АВТОМАТИЗАЦІЯ І РОБОТОТЕХНІКА
- БЕЗПЕКА ВИРОБНИЦТВА
- ЗРАЗКИ, СТАНДАРТИ ЕТАЛОНИ, ПРИЛАДИ
- ПІДЙОМНО-ТРАНСПОРТНЕ СКЛАДСЬКЕ ОБЛАДНАННЯ
- ІНДУСТРІАЛЬНІ ПАРКИ

27–29 травня

Генеральний інформаційний партнер:

Обладнання та інструмент для професіоналів

KYIV GLOBAL EXPO

Місце проведення:
МВЦ, м. Київ,
Броварський пр-т, 15,
станція метро «Лівобережна»

+38 (095) 268-05-85,
+38 (096) 505-52-66
plast@iec-expo.com.ua
www.iec-expo.com.ua

XIV Міжнародна спеціалізована виставка

ЄвроБудЕкспо'2025

ЗА ПІДТРИМКИ:

Міністерства розвитку громад, територій та інфраструктури України

Асоціації міст України

Асоціації малих міст України

Всеукраїнської Асоціації об'єднаних територіальних громад

Національного Експертно-Будівельного Альянсу України

Федерації роботодавців України

14–16 жовтня

Генеральний медіа-партнер:

3 1999 ГРУПА ВИДАНЬ

Capital Build Капітал Будівництво | Concrete & Asphalt Бетон&Асфальт | Special Equipment Спецтехніка

Генеральний інформаційний партнер:

Prof Build

Генеральний інтернет-партнер:

BUILD PORTAL

МІСЦЕ ПРОВЕДЕННЯ:

м. Київ, Броварський пр-т, 15

станція метро «Лівобережна»

+38 (050) 449-10-77

a.nenko@iec-expo.com.ua

www.iec-expo.com.ua

Протипожежний захист підземних, вбудованих та прибудованих об'єктів електроенергетики в умовах ущільненої забудови міст

Наземні електричні підстанції під час війни занадто вразливі від налетів ворожих дронів та ракет, що призводить до повного знеструмлення міст і окремих населених пунктів та призводить до запинки роботи підприємств оборонного комплексу та інших об'єктів народного господарства. В зв'язку з цим редакція пропонує умови будівництва і захисту підземних, вбудованих та прибудованих об'єктів електроенергетики в умовах ущільненої забудови міст.

Державний науково-дослідний, проектно-вишукувальний технологічний інститут з перспектив розвитку енергетики "Енергоперспектива" виконав науково-дослідну роботу щодо аналізу існуючого стану забезпечення підприємств енергетичної галузі з обґрунтування вимог пожежної і вибухової безпеки щодо будівництва і експлуатації підземних, вбудованих та прибудованих об'єктів електроенергетики в умовах ущільненої забудови міст. Метою виконання цієї роботи є розроблення норм і типових проектних рішень, унеможливлення пожеж і вибухів на споруджуваних об'єктах, забезпечення їх безпечну експлуатацію та запобігання негативному впливу на здоров'я осіб, професійно не пов'язаних з експлуатацією та обслуговуванням.

Розроблені документи можуть використовуватися в процесі проектування підземних та вбудованих і прибудованих об'єктів електроенергетики в умовах ущільненої міської забудови.

Об'єктом дослідження науково-дослідної роботи є існуючий стан забезпечення підприємств енергетичної галузі нормативно-технічними документами з пожежної і вибухової безпеки щодо будівництва і експлуатації підземних, вбудованих та прибудованих об'єктів електроенергетики в умовах ущільненої забудови міст.

Для виконання науково-дослідної роботи використані документи міжнародної, національної і галузевої стандартизації, які унормовують питання пожежної і вибухової безпеки об'єктів, результати власних досліджень та розробок.

За відсутності національних нормативів, виходячи з усталеної практики і економічної доцільності, надані обґрунтовані рекомендації щодо рішень із забезпечення пожежної і вибухової безпеки будівництва і експлуатації підземних, вбудованих та прибудованих об'єктів електроенергетики в умовах ущільненої забудови.

Завдяки виконанню роботи удосконалена нормативно-технічна база та інформаційне забезпечення підприємств, установ та організацій електроенергетичної галузі України і, як наслідок, зменшена можливість виникнення позаштатних ситуацій на об'єктах галузі із суб'єктивних причин.

Для більш чіткого розуміння викладеного тексту науково-дослідної роботи подаються терміни, вжиті в документах, та визначення позначених ними понять, які викладені в окремому розділі, а саме:

Терміни і визначення понять

Розподільний пристрій (РП)

Електросистема, що служить для прийому і розподілу електроенергії і містить комутаційні апарати, збірні і з'єднувальні шини, допоміжні пристрої (компресорні, акумуляторні тощо), а також пристрої захисту, автоматики та вимірювальні прилади.

Закритий розподільний пристрій(ЗРП)

РП, обладнання якого розташоване в будівлі.

Комплектний розподільний пристрій (КРП)

РП, що складається з повністю або частково закритих шаф чи блоків з вбудованими в них апаратами, пристроями захисту та автоматики, що постачається в зібраному або повністю підготовленому для збирання вигляді.

Підстанція

Електросистема, що служить для перетворення і розподілу електроенергії та складається з трансформаторів чи інших перетворювачів енергії, розподільних пристроїв, пристроїв управління та допоміжних споруд.

Залежно від переважання тієї чи іншої функції підстанцій вони називаються трансформаторними або перетворювальними.

Прибудована трансформаторна підстанція (ПТП)

Підстанція, яка безпосередньо примикає до основної будівлі.

Вбудована трансформаторна підстанція (ВТП)

Закрита трансформаторна підстанція, яка вписана в контур основної будівлі (споруди).

Внутрішньоцехова підстанція

Підстанція, розташована всередині виробничої будівлі (відкрито або в окремому закритому приміщенні).

Підземна трансформаторна підстанція

Закрита трансформаторна підстанція, яка розташована нижче рівня землі.

Трансформаторна комплектна (перетворювальна) підстанція

Підстанція, яка складається з трансформаторів (перетворювачів) і блоків (КРУ чи КРУН і інших елементів), що поставляються в зібраному або повністю підготовленому для збирання вигляді. Комплектні трансформаторні (перетворювальні) підстанції (КТП. КПП) або частини їх. що встановлюються в закритому приміщенні, відносяться до внутрішніх установок, що встановлюються на відкритому повітрі. - до зовнішніх установок.

Камера

Приміщення, призначене для встановлення апаратів і шин.

Закрита камера

Камера, закрита з усіх боків і має суцільні (не сітчасті) двері.

Обгороджена камера

Камера, яка має отвори, захищені повністю або частково несуцільними (сітчастими або змішаними) огорожами.

Вибухова камера

Закрита камера, призначена для локалізації можливих аварійних наслідків при пошкодженні встановлених в ній апаратів і що має вихід назовні або у вибуховий коридор.

Коридор обслуговування

Коридор уздовж камер або шаф КРУ, призначений для обслуговування апаратів і шин.

Вибуховий коридор

Коридор, в який виходять двері вибухових камер.

Ввідно-розподільний пристрій (ВРП)

Сукупність конструкцій, апаратів і приладів, які установлюються на вводі лінії живлення в будівлю або в її відокремлену частину, а також на лініях, що відходять від ВРП.

Далі викладені основні вимоги щодо розміщення та забезпечення вимог пожежної безпеки підземних, вбудованих та прибудованих об'єктів електроенергетики в умовах ущільненої забудови міст.

Загальні вимоги

1. «Електроустановки (проектування, монтаж, наладка та експлуатація) повинні відповідати вимогам чинних Правил улаштування електроустановок, Правил технічної експлуатації електроустановок споживачів, Правил техніки безпеки під час експлуатації електроус-

тановок споживачів, НПАОП 40.1-32-01 Правила будови електроустановок. Електрообладнання спеціальних установок, НАПБ А.01.001-2004 Правила пожежної безпеки в Україні та інших нормативних документів.

Будівельну частину електроустановок слід виконувати відповідно до протипожежних вимог будівельних норм, ПУЕ та НПАОП 40.1-32-01».

2. На закритих розподільних пристроях і підстанціях напругою 35 кВ і вище повинні передбачатися протипожежні заходи в залежності від належності підстанцій до певної групи, визначеної в таблиці :

Група	Номінальна напруга підстанцій	Потужність встановлених силових трансформаторів
I	500 кВ і вище	Незалежно від потужності
	220 і 330 кВ	200 МВ.А і вище
	Закриті підстанції 110 кВ і вище	63 МВ.А і вище
II	220 і 330 кВ	від 40 до 200 МВ.А
	110 і 154 кВ	63 МВ.А і вище
III	220 кВ	менше 40 МВ.А
	110 і 154 кВ	менше 63 МВ.А
	35 кВ	менше 80 МВ.А

3. Службові і допоміжні приміщення в будівлях і спорудах повинні відділятися від приміщень з технологічним обладнанням (розподільних пристроїв, силових маслонаповнених трансформаторів і т.п.) стінами з негорючих матеріалів з межею вогнестійкості не менше 2 год.

4. З'єднання, відгалуження та окінцювання жил проводів і кабелів повинно здійснюватись за допомогою опресування, зварювання, паяння або затискачів (болтових, гвинтових).

Місця з'єднання жил проводів і кабелів повинні мати мінімальний перехідний опір, щоб уникнути їх перегрівання і пошкодження ізоляції стиків. Струм втрат ізоляції стиків повинен бути не більше струму втрат ізоляції цілих жил проводів і кабелів.

5. Все електрообладнання (трансформаторів, апаратів, світильників, розподільних щитів, щитів управління) підлягає зануленню або заземленню відповідно до вимог ПУЕ.

Забороняється в приміщеннях і корпусах ЗРП упорядковувати комори і інші підсобні та допоміжні приміщення, що не відносяться до розподільного пристрою, а також зберігати електротехнічне обладнання, матеріали, запасні частини, ємності з горючими рідинами, а також балони з різноманітними газами.

6. Для очищення електротехнічного обладнання від бруду і відкладань повинні використовуватись, як правило, пожежобезпечні миючі сполуки і препарати. У виняткових випадках при неможливості по технічним причинам використовувати спеціальні миючі засоби допускається застосовувати горючі рідини (розчинники, бензин і т.п.) в кількостях, що не перевищують разове використання до 1 літра.

При застосуванні горючих рідин повинна використовуватись тільки тара, що закривається, із матеріалу, що не б'ється.

7. Кабельні канали ЗРП повинні бути постійно закриті негорючими плитами. Місця підводу кабелів до комірок ЗРП і до інших споруд повинні мати негорюче ущільнення вогнестійкістю не менше 0,75 години.

Кабельні канали ЗРП повинні мати вогнестійке ущільнення в місцях проходу кабелів з кабельних споруд в ці канали, а також в місцях розгалуження каналу.

Негорючі ущільнення повинні виконуватись в кабельних каналах в місцях їх проходу з одного приміщення в друге, а також в місцях розгалуження каналу і через кожні 50 м по довжині.

Підземна трансформаторна підстанція

1. У громадських будівлях і спорудах іншого призначення дозволяється розміщення підземних трансформаторних підстанцій, КТП, ЗРП напругою до 10 кВ.

Улаштування та розміщення підземних трансформаторних підстанцій, КТП, ЗРП необхідно виконувати відповідно до вимог ПУЕ та цього розділу НД.

2. Приміщення підземної трансформаторної підстанції камери трансформаторів повинні бути I ступеню вогнестійкості.

Дверні прорізи закритих камер для встановлення масляних трансформаторів повинні бути захищені протипожежними дверима 1-го типу з межею вогнестійкості не менше ЕІ 60 з ущільненнями в притворах та мати пристрої для самозачинення. У дверному прорізі слід передбачати поріжок або пандус висотою не менше 0,15 мм.

3. При розміщенні підземної трансформаторної підстанції і необхідно виконати такі умови:

- виключити можливість проникнення вологи через стіни, перекриття та підлогу, її підтоплення ґрунтовими і паводковими водами та наслідків пошкодження водопровідних або каналізаційних мереж;

- відстань між зовнішніми стінами будівель та стінами підземної ТП повинна бути не менше ніж 800 мм.

4. Кожна підземна трансформаторна підстанція повинна мати окремий вихід назовні.

5. Вентиляція приміщень трансформаторної підстанції повинна бути незалежною від інших приміщень і забезпечувати відвід тепла при роботі трансформаторів та видалення диму після пожежі.

6. Місця проходу повітропроводів крізь стіни та перекриття приміщень не повинні зменшувати нормативну межу вогнестійкості протипожежної перешкоди.

7. У місцях проходу крізь стіни та перекриття слід встановлювати вогнезатримуючи клапани з нормативною межею вогнестійкості не менше 60 хв.

8. У спорудах підземних трансформаторних підстанцій, ввідно-розподільних пристроях, КТП, ЗРП слід застосовувати кабелі, які не поширюють горіння з індексом НГ.

9. В кабельних каналах підстанцій кабелі прокладаються без установлення на них з'єднувальних муфт.

10. Прокладання кабелів через стіни і перекриття підстанції повинно виконуватись відповідно до НАПБ В.05.023-2005/111 у трубах з ущільненням негорючим матеріалом. Для підвищення пожежної безпеки кабелів слід виконувати вогнезахисне покриття кабелів з врахуванням вимог НАПБ В.05.023-2005/111.

11. Перекриття кабельних каналів і подвійної підлоги повинні бути виконані знімними плитами з негорючих матеріалів в рівень з чистою підлогою приміщення. Маса окремої плити перекриття повинна бути не більше 50 кг.

12. Під трансформаторами, масляними вимикачами і іншими маслонаповненими апаратами виконуються маслоприймачі, розраховані на утримання повного об'єму масла, незалежно від маси ізоляційного масла. Маслоприймач перекривають гратами з шаром гравію завтовшки 25 мм.

13. Відповідно до НАПБ В.05.037-2007 усі приміщення підстанції повинні обладнуватися автоматичними системами пожежної сигналізації.

14. Масляні трансформатори незалежно від напруги та потужності повинні обладнуватися автоматичними системами водяного пожежогасіння.

Прибудована і вбудована трансформаторна підстанція

1. Будівлі і приміщення прибудованих і вбудованих трансформаторних підстанцій і камери трансформаторів повинні бути I або II ступеню вогнестійкості.

2. Улаштування та розміщення вбудованих і прибудованих ТП, КТП, ЗРП необхідно виконувати відповідно до вимог розділу глави 4.2 ПУЕ.

3. Трансформаторні приміщення і ЗРП не допускається розміщувати:

- безпосередньо над і під приміщеннями з вибухонебезпечними зонами будь-якого класу;

- безпосередньо під і над приміщеннями, в яких може знаходитися більше 50 чол. в період більше 1 год.;

- під приміщеннями виробництв з мокрим технологічним процесом, під душовими, убиральнями, ванними і т.п.

4. Масляні трансформатори, розміщені всередині приміщень, належить встановлювати кожний в окремій камері, розташованій в першому поверсі і ізольованій від інших приміщень будівлі.

5. Кожна камера масляних трансформаторів повинна мати окремий вихід назовні або в суміжне приміщення з негорючими підлогою, стінами і перекриттями, які не містять вогненебезпечних і вибухонебезпечних предметів, апаратів і виробництв.

6. В одному загальному приміщенні з розподільним пристроєм (РП) напругою до 1 кВ і вище допускається встановлення одного масляного трансформатора потужністю до 0,63 МВ.А, або двох масляних трансформаторів потужністю кожний до 0,4 МВ.А, відділених від решти частини приміщення перегородкою з межею вогнестійкості ЕІ 60.

7. В камерах РП, які мають виходи у вибуховий коридор, допускається встановлення трансформаторів з масою масла до 600 кг.

8. Бакові масляні вимикачі з масою масла більше 60 кг повинні встановлюватись у відокремлених вибухових камерах з виходом назовні або в вибуховий коридор. В кожній камері повинен передбачатися поріг, розрахований на утримування повного об'єму масла.

9. В закритих окремо розташованих, прибудованих і вбудованих в виробничі приміщення підстанціях, в камерах трансформаторів, масляних вимикачів та інших маслонаповнених апаратів з масою масла в одиниці обладнання більше 600 кг повинен бути улаштований пандус або поріг із негорючого матеріалу в дверному прорізі камер або в прорізі вентиляційного каналу, розрахований на утримання 20% масла трансформатора або апарата. Повинні бути також передбачені заходи проти розтікання масла через кабельні споруди.

10. При розміщенні камер над підвалом, на другому поверсі і вище, а також при улаштуванні виходу з камер в вибуховий коридор під трансформаторами, масляними вимикачами і іншими маслонаповненими апаратами виконуються маслоприймачі:

- При масі масла до 60 кг - поріг або пандус для утримання повного об'єму масла;
- при масі масла від 60 до 600 кг - приямок, розрахований на повний об'єм масла або поріг (пандус) при виході з камери;
- при масі масла більше 600 кг - маслоприймач, розрахований на утримання 20% масла з відводом його в дренувальну систему або маслоприймач на повний об'єм масла без відводу в дренувальну систему. В останньому випадку маслоприймач перекривають гратами з шаром гравію завтовшки 25 мм.

11. Двері (ворота) камер, які містять маслонаповнене електрообладнання, повинні бути протипожежними з межею вогнестійкості не менше 0,75 год., якщо вони виходять в приміщення, яке не відноситься до цієї підстанції, а також якщо вони знаходяться між відсіками вибухових коридорів і РП.

12. Підстанції з сухими трансформаторами дозволяється розташовувати всередині будинку або споруди в окремому приміщенні, в тому числі у підвалах.

При цьому повинна бути забезпечена можливість транспортування обладнання ТП для заміни і ремонту.

При розміщенні ТП у підвалах необхідно виконати такі умови:

- виключити можливість їх підтоплення ґрунтовими і паводковими водами та внаслідок пошкодження водопровідних або каналізаційних мереж;
- відстань між зовнішніми стінами будівлі та стінами ТП повинна бути не менше ніж 800 мм. Допускається зменшення цієї відстані до 200 мм, якщо забезпечується вентиляція простору між стінами.

13. Прорізи в міжповерхових перекриттях, стінах, перегородках і т.п. повинні бути закриті негорючим матеріалом, який забезпечує межу вогнестійкості не менше 0,75 год. Отвори в місцях проходження кабелів повинні мати ущільнення з межею вогнестійкості 0,75 год.

14. Перекриття кабельних каналів і подвійної підлоги повинні бути виконані знімними плитами з негорючих матеріалів в рівень з чистою підлогою приміщення. Маса окремої плити перекриття повинна бути не більше 50 кг.

15. Виходи з РП повинні передбачатися:

- при довжині до 7 м - один;
- при довжині від 7 до 60 м - два по кінцям або на відстані 7 м від кінців;
- при довжині більше 60 м, крім виходів по кінцях, передбачаються додаткові з таким розрахунком, щоб відстань від будь-якої точки коридору обслуговування, керування або вибухового коридору до виходу була не більше 30 м.

16. Вибухові коридори великої довжини належить розділяти на відсіки довжиною не більше 60 м негорючими перегородками з межею вогнестійкості не менше ЕІ 60, з улаштуванням виходів назовні або в сходову клітку.

Внутрішньоцехові трансформаторні підстанції

1. Внутрішньоцехові підстанції можуть розміщуватись на першому і другому поверхах в основних і допоміжних приміщеннях виробництв, що відповідно до протипожежних вимог віднесені до категорії Г чи Д, І чи ІІ ступеню вогнестійкості, як відкрито, так і в окремих приміщеннях.

2. Розміщення внутрішньоцехових підстанцій у приміщеннях з виробництвами категорії В за протипожежними вимогами може бути допущено за узгодженням у кожному окремому випадку з органами держпожнагляду. Розміщення підстанцій без маслонаповненного устаткування такому узгодженню не підлягає.

3. ТП і ПП, РП до 1 кВ і вище з електроустаткуванням загального призначення (без засобів вибухозахисту) забороняється споруджувати безпосередньо у вибухонебезпечних зонах будь-якого класу.

Вони повинні розташовуватися в окремих приміщеннях, що задовольняють вимогам п.п.5.7.2-5.7.8 НАПБ В.01.056-2005/111 або зовні, поза вибухонебезпечними зонами.

4. Огороджувальні конструкції приміщення внутрішньоцехової підстанції, в якому встановлюються комплектні трансформаторні підстанції(КТП) з масляними трансформаторами, а також закритих камер масляних трансформаторів і апаратів з кількістю масла 60 кг і більш, повинні бути виконані з негорючих матеріалів з межею вогнестійкості не менш ЕІ 60.

Система КТП із масляними трансформаторами і масляних трансформаторів вище другого поверху не допускається.

5. Під кожним масляним трансформатором і апаратом з масою масла 60 кг і більш повинен бути улаштований маслоприймальник як для трансформаторів і апаратів з масою масла більш 600 кг.

6. Двері камер маслонаповнених силових трансформаторів і бакових вимикачів повинні мати межу вогнестійкості не менш ЕІ 60.

7. РП, ТП(в тому числі КТП) і ПП допускається виконувати прилеглими двома чи трьома стінами до вибухонебезпечних зон з легкими горючими газами і ЛЗР класу 2 і до вибухонебезпечних зон класів 21 і 22.

Забороняється їх примикання до вибухонебезпечної зони класу 1, а також до вибухонебезпечних зон з важкими і зрідженими горючими газами класу 2.

8. РП, ТП і ПП забороняється розміщувати безпосередньо над і під приміщеннями з вибухонебезпечними зонами будь-якого класу.

9. Вікна РП, ТП і ПП, що примикають до вибухонебезпечної зони, рекомендується виконувати із склоблоків товщиною не менше 10 см.

10. РП, ТП (у тому числі КТП) і ПП, що живлять установки з важкими чи зрідженими горючими газами, як правило, повинні розміщуватись окремо, на відстані від стін приміщень, до яких примикають вибухонебезпечні зони класів 1 і 2, і від зовнішніх вибухонебезпечних установок згідно таблиці 11 НАПБ В.01.056-2005/111.

Завдяки виконанню цієї науково-дослідної роботи удосконалена нормативно-технічна база та інформаційне забезпечення підприємств, установ та організацій електроенергетичної галузі України і, як наслідок, зменшується можливість виникнення позаштатних ситуацій на об'єктах галузі із суб'єктивних причин.

Протипожежні вимоги до вогнестійкого ущільнення кабелів

На електростанціях і підстанціях найбільш небезпечні пожежі, що виникають в кабельних спорудах, які виводять з ладу енергопідприємства, завдаючи народному господарству значного матеріального збитку. Відсутність вогнезахисних ущільнень кабелів призводить до безперешкодного розповсюдження вогню через протипожежні перегородки між відсіками і протипожежні перекриття.

В місцях проходу кабелів через будівельні конструкції передбачаються вогнестійкі ущільнення отворів до забезпечення межі вогнестійкості не менше 45 хв.

Для проходу кабельних ліній через будівельні отвори, через стіни, перегородки і перекриття необхідно передбачати:

- заставні труби з негорючих матеріалів, для прокладки одиночних кабелів з обов'язковим ущільненням негорючим матеріалом;

- для пучків контрольних кабелів з максимальними розмірами по висоті і ширині не більше 100 мм і для одиночних кабелів азбоцементні труби або модульні кабельні проходки вогнестійкістю 45 хв. з габаритними розмірами по довжині не менше 200 мм і перетином:

100 х 100 мм . . . . . односекційні;
100 х 200 мм . . . . . двохсекційні;
100 х 300 мм . . . . . трьохсекційні;
100 х 400 мм . . . . . чотирьохсекційні.

Для основних потоків кабельних ліній об'єктів слід передбачати:

1) В кабельних спорудах (кабельних поверхах, тунелях, каналах, галереях) і електротехнічних приміщеннях - кабельні конструкції і полегшені перфоровані і гратчасті металеві лотки. Забороняється застосування металевих лотків з суцільним дном і коробів.

2) В технологічних приміщеннях і на естакадах - відкриту прокладку кабелів, а в місцях можливих механічних пошкоджень, як правило, в каналах, шахтах - в полегшених перфорованих і гратчастих лотках.

При установці металевих, коробів типу ККБ і КП виконуються в них перегородки і ущільнення з вогнестійкістю не менше 45 хв. в місцях: проходу кабелів через стіни і перекриття; на горизонтальних ділянках і естакадах через кожні 30 м довжини коробів; на вертикальних ділянках через кожні 20 м висоти і при проході через перекриття в місцях розгалуження в коробах основних потоків кабелів.

Прокладку силових кабелів по конструкціях в каналах, лотках і коробах слід передбачати однорядно, а контрольних кабелів пошарово або пучками відповідно до вимог ПУЕ, максимальним розміром в діаметрі не більше 100 мм або в окремих осередках спеціальних кабельних конструкцій розміром 100х100 мм (п. 9.3.3 НАПБ 05.028-2004).

Вказані кабельні конструкції, лотки і короби повинні застосовуватися тільки заводського виготовлення.

Для забезпечення пожежної безпеки необхідно передбачати в проектно-кошторисній документації багатократне ущільнення кабельних проходок, а саме: в період проведення програми укладання кабельних трас до їх здачі в експлуатацію - негорючими матеріалами (супертонке базальтове волокно, спеціальні матеріали, що спучуються, ущільнюючі вогнестійкі пакети і інші.).

Проходи кабельних ліній через стіни, перегородки і перекриття повинні бути ущільнений будь-якими негорючими матеріалами для забезпечення мінімальної межі вогнестійкості 45 хв. (п. 9.3.1 НАПБ 05.028-2004).

Перед здачею кабельного господарства в експлуатацію торці кабельних проходок з волоконними матеріалами і пакетами рекомендується покривати вогнезахисними матеріалами товщиною не менше 5 мм (п. 9.3.5 НАПБ 05.028-2004).

При застосуванні у виробничих приміщеннях металевих коробів типів ККБ, КП (в місцях можливих механічних пошкоджень) вихід окремих кабелів з них слід виконувати з використанням захисних виробів (патрубків, штуцерів, труб сальників і т.д.) (п. 9.3.6 НАПБ 05.028-2004).

Не допускається виконувати пучки кабелів більше 100 мм. При проходженні пучків кабелів через перегородки, стіни і перекриття, для забезпечення ущільнення кабелів їх слід розкладати, як правило, в один шар відділяючи кожний один від одного вогнестійким ущільнюючим матеріалом товщиною не менше 20 мм (п. 9.3.8 НАПБ 05.028-2004, та п.6.3.1.2 НАПБ В 05.023-2005/111).

Отвори (прорізи) в будівельних конструкціях навкруги кабельних проходок, коробів і труб повинні бути закладені цементними розчинами на всю товщину будівельних конструкцій до нормативної межі вогнестійкості (п. 9.3.9 НАПБ 05.028-2004).

Місця проходу в приміщення закритих розподільних пристроїв і в приміщення щитів управління і захисту відкритих розподільних пристроїв повинні мати негорючі перегородки і ущільнення, з межею вогнестійкості не менше 45 хв. (п.2.3.82 ПУЕ, п.9.3.1 НАПБ 05.028-2004, п.6.3.2 НАПБ В 05.023-2005/111).

Компанія ООО «Рокстек УА» є офіційним дістриб'ютором **«Roxtec International AB»**, Швеція, на території України і реалізує рішення з герметизації кабельних и трубних вводів, які проходять через будь-які технічні отвори та перекриття. Основне завдання цих технологій - це захист безпечних зон від проникнення в них різних руйнівних і шкідливих факторів.

Компанія пропонує модульну систему герметизації, яка забезпечує герметичність (по воді до 4 атмосфер, по газу до 2,5 атмосфери), пожежостійкість зі збереженням герметичності EI 120, підтвердженими Українським та международними сертифікатами).

Якість продукції компанії підтверджено багатьма міжнародними сертифікатами , а також українськими сертифікатами пожежної безпеки і вибухозахисту.

Модульні системи успішно застосовуються і зарекомендували себе в усіх галузях промисловості, в тому числі в енергетиці. Вони гарантовано захищають кабельні і трубні вводи на АЕС, ГАЕС, ГЕС, ТЕС, ПС(10кВ, 35кВ, 110кВ, 220кВ).

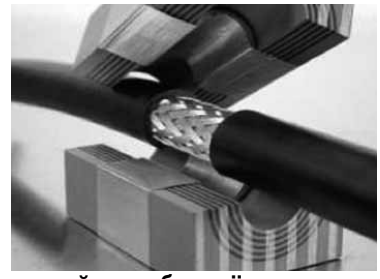
Компанія надає підтримку на всіх етапах: від проектування нестандартних рішень до монтажу і наступного обслуговування.

Компанія ООО «Рокстек УА» розташована в м. Києві по вул. Победи, 9.

Нижче надаються загальні відомості про конструктивні особливості проходок, які можуть застосовуватись на енергетичних підприємствах України.

Наземні кабельні лотки ВРП повинні мати вогнестійке ущільнення в місцях проходу кабелів з кабельних споруд в ці

Розміщення кабелю в модульній кабельній проходці



Загальний вид кабельної проходки

лотки, а також в місцях розгалуження на території ВРП.

Негорючі ущільнення, повинні виконуватися в кабельних каналах в місцях їх проходу з одного приміщення в інше, а також в місцях розгалуження каналів і через кожні 50 м по довжині.

Місця ущільнення кабельних лотків і каналів повинні бути позначені нанесенням на плити червоних смуг. При необхідності робляться написи пояснень.

В кабельних лотках і каналах допускається застосовувати пояси з піску або іншого негорючого матеріалу завдовжки не менше 0,3 м.

Кабельні канали і наземні кабельні лотки ВРП повинні бути постійно закриті негорючими плитами.

Косюк В.В,
фахівець з пожежної безпеки
в електроенергетиці

Наставник – Людина справи

Цього жвавого стрункого чоловіка доволі добре знали в кабінетах УкрНДІПБ, Департаменту державного нагляду (контролю) у сфері пожежної, техногенної безпеки та цивільного захисту ДСНС України, Мінпаливенерго України. І лише вкрита інеєм голова видаєв ньому немолоду людину. Це – Володимир Косюк. Його життєве багатство – 90 років, які він святкує 5 квітня 2025 року.

Заступник начальника УПО УВД Вінницької області підполковник в.с. Косюк В.В.

Скільки себе пам'ятає, завжди трудився на ниві пожежної безпеки. У 78 вийшов на заслужений відпочинок. Проте не порвав із улюбленою правою всього життя. Володимир Вікторович – активний автор фахових публікацій у багатьох часописах.

– Відверто кажучи, відчуваю себезначно молодшим, – хвалиться підполковник у відставці Володимир Косюк. – Либонь, насамперед треба дякувати хорошій генетиці: моя мама, Парасковія Федорівна, раділа цьому світові майже століття. Окрім того, не маю шкідливих звичок. Дружу з фізкультурою й працею.

Старший пожежний інспектор Талалаєвського РОВД лейтенант Косюк В.В. (праворуч) серед працівників РОВД.

Трудитися почав змалку. З молодшою сестричкою Надією рубали в лісі дрова й на санчатах за три кілометри їх везли дохати. Так щомісяця. До слова, полюбляю багато ходити... Любов до ходьби прокинулася в юні літа. Що вдієш, мусиш, коли школа в сусідній Грабівці – за п'ять кілометрів від рідної Вікторівки. От щодня хлопець і долав по 10000 метрів. Ну а

Старший пожежний інспектор Білопольського РОВД ст. лейтенант Косюк В.В. разом з дружиною Галиною Іванівною.

Біля святкової трибуни першого травня 1960 р.

Відповідальний черговий офіцер Білопільського РОВД ст. лт. Косюк з помічником чергового. 5 квітня 1962 року.

На охороні урожаю від пожеж старший пожежний інспектор Білопольського РОВД ст. лейтенант Косюк В.В. з дільничним уповноваженим РОВД Лейтенантом міліції Ткачем Миколою Павловичем.

Лагерний збір на інженерному факультеті Вищої інженерної школи МВС. 1963 р.

Зустріч з гродадськістю міста Вінниці.

повну середню освіту здобував у Олишівці, що за 10 кілометрів від домівки. З юних літ Володя бачив себе агрономом – мріяв трудитися на рідній землі Чернігівщини. Але стати студентом столичної сільськогосподарської академії не судилося.

– У Вікторівці мешкав начальник пожежно-сторожової охорони Литвиненко Ф.Д. Він і порадив вступати до Київського пожежно-технічного училища. Іспити до закладу тоді проводили у вересні. Я їх успішно склав, і 1952 року був зарахований до училища, – пригадує Володимир Вікторович.

По закінченні на хорошо та відмінно училища молодий лейтенант потрапив на Сумщину в якості старшого пожежного інспектора Талалаївського району (тепер це Чернігівщина – Авт.). Тамтешні шляхи – не пройти й не проїхати. Хіба що на підводі. От молодому фахівцеві й видали коня. Норовливого, необ'їжджeного. Та в колгоспах треба бувати. Отож лейтенант запрягав буланого і – в дорогу. Проте не завжди діставалися місця разом. Молода тварина доволі часто демонструвала свій норов. Вирвалася й тікала до райвідділу. Ну а Косюк на своїх двох поспішав виконувати службові обов'язки. Коня інспектор приборкав за півроку. А ще через шість місяців його перевели до Краснопільського району. Там лейтенант продемонстрував неабияке вміння працювати, став досвідченішим інспектором пожежного нагляду. В цей час до Краснопільського району приєднали частину розформованого Миропільського району, куди на самостійний участок за 40 км від райцентру був напрвлений молодий фахівець. По функційним обов'язкам відповідав за постійне інформування радянські і партійні органи про стан пожежної безпеки на об'єктах району в цілому, а це помітно познакчилоля на покращенні протипожежго стану об'єктів, закріплених за ним миропільської зони. Після року служби та позитивних результатах роботи Володимир опинився в більш розвинутому промислово Білопільському районі на самостійній та більш відповідальній роботі. У своє розпорядження Косюк отримав новенький мотоцикл К-750-Н.1– тогочасну мрію будь-якого інспектора.

«Із залізним конем порозумілися значно швидше», – усміхається ветеран. У постійній битві за збереження врожаю від нашестя «червонного півня» п'ять років офіцер мотався курними дорогами Білопільщини. 1959-го його за вдумливу, грамотну роботу відзначили перехідним Червоним вимпелом. Ну а ще через чотири роки старший лейтенант вступив на інженерний факультет Вищої інженерної школи МВС. Дипломований капітан Косюк – інженер протипожежної техніки та безпеки, так в дипломі значиться його фах, переїхав на Вінничину. У цьому благодатному краї майже два десятиліття опікувався протипожежним захистом енергетичних об'єктів. Зокрема, патронував будівництво Ладижинської ДРЕС. На живописному березі водосховища Ладижинської ГЕС на річці Південний Буг – розказує Володимир Вікторович - встановлений гранітний камінь, на якому викарбувано «Здесь в марте 1968 года высажен десант строителей Ладыжинской ГРЭС». Десант будівельників ДРЕС виглядав, як невелике місто в голому полі біля водосховища, де булло встановлено більше 100 дерев'яних будівельних вагончиків

Міжрайонні пожежно-тактичні навчання на Ладижинській ДРЕС.

Розгляд проектної документації Ладижинській ДРЕС.

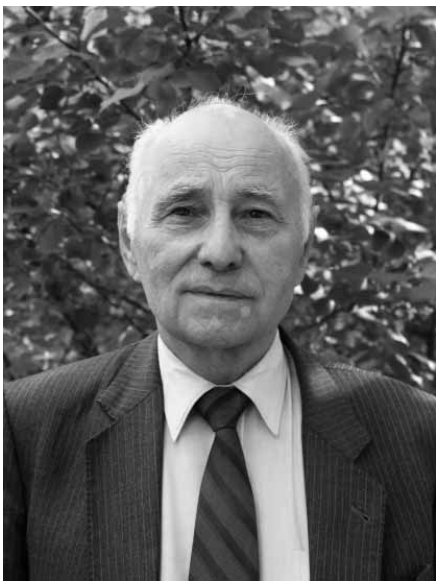
для розміщення в них керівництва будівництвом та будівельників. Усі ці тимчасові будівлі з'єднувалися між собою доріжками з бетонних плит розміром 50х50 см.

Перше обстеження будівництва ДРЕС припало на травень цього року. Будівельний майданчик, розміщений на узліссі живописного Південного Бугу, де після дощу по бездоріжжю не було можливості ні пройти ні проїхати. Молодого інженера пожежного нагляду перевзули в гумові чоботи і головний інженер будівництва ДРЕС повів до котловану головного корпусу. Вразив масштаб будівництва, котлован завглибшки 15-20 метрів, в якому працюють якісь іграшкові бульдозери, екскаватори, скрепери, автосамосвали та інша техніка. Це були перші кроки в великій енергетиці інженера держпожнагляду. Тоді не було ще розроблено постійних нормативних документів з визначення вимог пожежної безпеки для будівництва енергетичних об'єктів, тому приходилося використовувати тимчасові інструкції, викладені в наказах Міненерго СРСР (розмазані ротопрінтні примірники). Це спонукало потім розробляти нормативні документи, працюючи в енергетичних інститутах. На території ДРЕС було побудовано пожежне депо, де розмістилися потім організовані дві пожежні частини з охорони ДРЕС та міста Ладижина. Крім того, Володимир Вікторович контролював роботу підстанції «Вінницька-750», виробничо-енергетичного об'єднання «Вінницяенерго». Був активним пропагандистом, організатором, учасником навчань із протипожежного захисту. Провів силу-силенну спеціальних семінарів. На закріплених за ним об'єктах регулярно проводив пожежно-тактичні навчання, на які залучалися гарнізони пожежної охорони з суміжних районів Винницької області.

Зустріч у військовій частині м. Кут-Кашен Азербайджанської РСР з сином Леонідом і його товаришем Олександром.

На деяких з цих навчань були присутні керівники Управління пожежної безпеки Міненерго УССР, що потім після переїзду до Києва помогло в улаштуванні на роботу в Управління ВОХР і ПБ Міненерго УССР. До 1985 року Володимир Вікторович обіймав посаду заступника начальника Вінницького обласного відділу пожежної охорони УВС. З неї й подав у відставку. Із класним фахівцем вище керівництво не збиралося розлучатися. Проте за рік підполковник Косюк усе-таки вийшов на заслужений відпочинок. Хоча насолоджуватися вільним життям не збирався. Отож прийшов в Управління ВОХР і ПБ Міненерго УССР, де впізнали підполковника, роботу якого спостерігали відповідальні працівники Управління ВОХР при проведенні пожежно-тактичних навчань на Ладижинській, ДРЕС та підстанції «Вінницька-750». Крім того, рекомендацію на роботу в Міністерстві енергетики та електрифікації дав заступник начальника УПО МВС УРСР полковник Грипас. Це були перші кроки уже опитного працівника пожежної охорони в великій енергетиці. Потім, коли виповнилоля 60 років, заступник Міністра Магда І.І. рекомендував перейти на роботу в енергетичні інститути, зокрема в НДІ «ВНІ І ПІЕнергопром». Від 1995-го Володимир Вікторович – головний фахівець із пожежної безпеки ДНДПВТІ «Енергоперспектива». На цій посаді працював 15 літ. Потім ще три роки відповідав за пожежну безпеку в стінах Мінпаливенерго України. За цей час ним була створена повна нормативно-технічна база для енергетичних підприємств, яка складає більше 30 нормативних документів українською та російською мовами. Упродовж багатьох років Володимир Косюк – активний дописувач журналів «Бізнес і безпека», «Охорона праці і пожежна безпека», «FS технології безпеки», «Промислова безпека», «Охорона праці», «Пожежна та техногенна безпека» та інші, адже фахівцеві є чим поділитися із зацікавленим читачем. До слова, Володимир Вікторович підготував довідник «Пожежна безпека енергетичних підприємств». Одне слово, активне життя ветерана-вогнеборця триває... ★

Біля Чорного моря. Обстеження Одеської ТЕЦ. Перший заступник начальника Управління ВОХР, начальник відділу пожежної безпеки міністерства Енергетики Косюк В.В. та директор з охорони праці Одесаобленерго Савицький А.Г.



Перший заступник начальника Управління ВОХР, начальник відділу пожежної безпеки міністерства Енергетики Косюк В.В.

В колі рідних та друзів. Наставнику, Косюку Володимиру Вікторовичу виповнилося 80 років. Середа Олексій Якович урочисто поздоровляє ювіляра.

Друзі біля президентського палацу. 2005 рік.

Шановний, Володимире Вікторовичу!

Вітаємо Вас з великим ювілеєм – 90-річчям! Ця дата – не просто цифра, а символ мудрості, мужності та безмежної відданості своїй справі. Ваше життя – це справжній приклад того, як можна прожити його гідно, з честю та користю для людей.

Ви присвятили себе важливій і відповідальній справі – пожежній безпеці, ставши справжнім наставником для багатьох поколінь. Ваш досвід, знання та наполегливість допомогли зберегти тисячі життів і багато майна. Ви завжди були і залишаєтеся взірцем працьовитості, відповідальності та любові до своєї справи.

Ваша біографія – це історія людини, яка пройшла довгий і складний шлях, але ніколи не здавалася. Ви завжди знаходили сили рухатися вперед, вдосконалювати себе та допомагати іншим. Ваші публікації, напрацювання та участь у розробці нормативних документів з пожежної безпеки стали вагомим внеском у розвиток цієї галузі в Україні.

Ви – справжній герой, який навчив нас цінувати працю, відповідальність і вірність своїм ідеалам. Ваша енергія, оптимізм і любов до життя надихають усіх навколо. Ми пишаємося Вами і дякуємо за все, що Ви зробили та робите для своєї родини, колег і всієї країни.

Бажаємо Вам міцного здоров'я, радості, тепла від близьких і ще багато щасливих моментів у житті! Нехай Ваше серце завжди наповнюється гордістю за свої досягнення, а оточуючі діляться з Вами своєю любов'ю та повагою. **З ювілеєм, Вас!**

Дякуємо за Ваш приклад і за те, що Ви є з нами!

З пошаною та вдячністю,
редакція журналу «Бізнес і безпека»

Аналіз методів випробувань вогнегасних порошків з визначення їх вогнегасної здатності

Проаналізовані нормативні документи, в яких зазначені методи випробування з визначення вогнегасної здатності вогнегасних порошків. Наведено відмінності у методах вогневих випробувань за класом пожежі А та В. Обґрунтовано необхідність вдосконалення методів вогневих випробувань вогнегасних порошків з визначення їх вогнегасної здатності, а також розроблення національного стандарту на методи випробувань вогнегасних порошків, призначених для гасіння пожеж класу Д.

Вогнегасні порошки (далі - ВП) широко застосовуються в сьогоденні. Вони використовуються як у первинних засобах пожежогасіння так і у автоматичних системах пожежогасіння та пересувній протипожежній техніці. Їхнє використання зумовлене тим, що вони мають високу спроможність швидко припиняти горіння, а універсальний механізм вогнегасної дії порошків дозволяє їх використовувати як один із найбільш прийнятих і екологічно безпечних вогнегасних засобів [1].

Незважаючи на відносно високу вартість, складність в експлуатації і зберіганні, ці сполуки, завдяки своїм властивостям знайшли широке застосування. Порошкові сполуки є, зокрема, єдиним засобом гасіння пожеж лужних металів, алюмінійорганічних та інших металоорганічних з'єднань. ВП у комбінації з іншими засобами гасіння (наприклад, з повітряно-механічною піною) застосовують і для ліквідації великих пожеж нафтопродуктів.

Одним з найважливіших параметрів ВП є їх вогнегасна здатність під час гасіння пожеж класів А та В. Окрім відомих експериментальних методів [2] визначення вогнегасної ефективності ВП, що застосовуються в лабораторних умовах на невеликих за розмірами модельних вогнищах, розповсюдження набули стандартизовані методи визначення вогнегасної здатності ВП, що передбачають гасіння модельних вогнищ відносно великого розміру із використанням переносних порошкових вогнегасників.

Саме такі методи закладені в ДСТУ 3105-95 [3], ГОСТ Р 53280.4-2009 [4], ISO7202:2012 [5] та EN 615 [6].

В той же час, за ствердженнями окремих авторів [7], існує необхідність у диференційованому підході до оцінювання вогнегасної здатності ВП в залежності від умов їх подальшого застосування, враховуючи в такому оцінюванні і економічну складову.

Метою даної роботи є проведення аналізу сучасних нормативних документів, що встановлюють вимоги до випробувань з визначення вогнегасної ефективності ВП. Проведення такого аналізу дасть можливість обґрунтувати доцільність впровадження диференційованої оцінки вогнегасної здатності ВП в залежності від специфіки їх подальшого застосування.

З метою визначення особливостей проведення випробування з визначення вогнегасної здатності в разі гасіння пожеж класів А та В авторами було проаналізовано наступні нормативні документи [3-6]. Слід зазначити що посилання на методи випробувань зазначені у [5], [6] відповідають методам у ISO 7165-2009 [8], EN 3-7 [9] відповідно.

За результатами аналізу зазначених вище нормативних документів було визначено, що випробування з визначення вогнегасної здатності ВП при гасінні пожеж класу А та В згідно їх вимог за процедурою проведення схожі і проводяться в наступній послідовності:

- підготовка до випробувань (дотримання умов проведення випробувань зазначеного у відповідному нормативному документі; підготування місця проведення випробувань; встановлення модельного осередку пожежі, піддону для палива; приготування потрібної кількість води і палива; заряджання вогнегасника);
- проведення випробувань (підпалення модельного вогнища з допомогою факела; витримування часу вільного горіння; проведення оператором гасіння з певної відстані і сторін);
- реєстрування отриманих первинних результатів.

Основні параметри проведення випробувань з визначення вогнегасної здатності ВП під час гасіння пожеж класу А наведено в таблиці 1.

Слід зазначити, що у вище перелічених нормативних документах [3-6] під час проведення випробувань з

Таблиця 1 - Основні параметри проведення випробувань вогнегасних порошків з визначення вогнегасної здатності за класом пожежі А

Параметри випробувань	Нормативні документи			
	ДСТУ 3105-95	ГОСТ Р 53280.4-2009	ISO7202:2012	EN 615:2009
Умови проведення випробувань	Відкритий майданчик, швидкість вітру не більше 3 м/с	Відкритий майданчик, швидкість вітру не більше 3 м/с, або приміщення з об'ємом більше 1000 $м^3$	Приміщення	Приміщення
Модельне вогнище	Штабель (дерево хвойних порід кількістю 72 бруски квадратного перетину з розміром сторони (40^{0}_{-2}) мм, довжиною (500±10) мм), піддон 400×400×100 мм	Штабель (дерево хвойних порід кількістю 72 бруски квадратного перетину з розміром сторони (39±1) мм, довжиною (500±10) мм),, піддон 400×400×100 мм	Штабель (дерево, 12 рядів по 6 брусків довжиною 500 мм, (40-2)×(40-2) мм, 72 шт.)	Штабель (дерево довжиною 500 мм, з розміром сторони (39±2) мм)

Продовження таблиці 1.

Паливо для розпалу модельного вогнища	Бензин, (1,1±0,05) дм^3, вода (5,0±0,1) дм^3	Бензин (1,1) дм^3, вода (30±2) мм	1,1 дм^3 гептану	Гептан у об'ємі, щоб забезпечити горіння 2 хв 30 с, вода 30 мм
Час вільного горіння	8 хв	(7±1)хв	До зниження маси штабеля на (55±2)%	8 хв
Відстань до осередку пожежі	1,8 м	1,5 – 0,5 м	1,8 м	На розсуд оператора гасіння
Час контролю повторного займання	10 хв	10 хв	Не вказано	3 хв
Випробувальний прилад	Випробувальний прилад на основі	Випробувальний прилад на основі	Вогнегасник	Вогнегасник закачаного
	закачного вогнегасника ОП-3(3) з місткістю корпусу (3,5±0,2) дм^3	закачного вогнегасника ОП-3(3) з місткістю корпусу (3,5±0,2) дм^3		типу, місткістю корпусу 6 кг або 9 кг

Основні параметри вогневих випробуваннь з визначення вогнегасної здатності ВП під час гасіння пожеж класу В наведено в таблиці 2.

Таблиця 2 – Основні параметри проведення випробувань вогнегасних порошків з визначення вогнегасної здатності за класом пожежі А

Параметри випробувань	Нормативні документи			
	ДСТУ 3105-95	ГОСТ Р 53280.4-2009	ISO7202:2012	EN 615
Умови проведення випробувань	Відкритий майданчик, швидкість вітру не більше 3 м/с	Відкритий майданчик, швидкість вітру не більше 3 м/с, або приміщення з об'ємом більше 1000 м^3	Відкритий майданчик, швидкість вітру не більше 3 м/с	Відкритий майданчик, швидкість вітру не більше 3 м/с
Паливо	розміри вогнища Бензин, (37±1) дм^3, вода (18±1) дм^3	розміри вогнища Бензин, (55±1) дм^3, вода (110±2) дм^3	розміри вогнища 1/3 води і 2/3 гептану	розміри вогнища 1/3 води і 2/3 гептану
Час вільного горіння	60 с	(60±5) с	60 с	60 с
Відстань до осередку пожежі	1,5 м	(2,0± 0,5) м	На розсуд оператора гасіння	На розсуд оператора гасіння

визначення вогнегасної здатності ВП за класом пожежі А та В використовують різне паливо, а саме:

- в ДСТУ 3105 [3] в якості палива використовують бензин автомобільний марки А-76 або А-80 згідно з ДСТУ 4063 [10];
- в ГОСТ Р 53280.4-2009 [4]в якості палива використовують бензин автомобільний марки «Нормаль-80» згідно з ГОСТ 51105 [11];
- в [5, 6] якості палива використовують промисловий гептан (суміш аліфатичних вуглеводнів, що має температуру початку кипіння не нижче ніж 84 ?С і температуру закінчення кипіння не вище ніж 105 ?С та характеризується різницею між температурами початку і закінчення перегонки не більше ніж 10 ?С, вмістом ароматичних сполук не більше ніж 1 % (об) та густиною за температури 15 ?С від 0,680 до 0,720 г/см3).

Проте параметри горіння промислового гептану і бензину відрізняються. В [12] було проведено дослідження режимів вільного горіння бензину автомобільного марки А-76 і н-гептану і встановлено, що швидкість вигорання бензину вища за швидкість вигорання н- гептану, під час його го-

ріння розвивається більш висока температура. Під час горіння н-гептану щільність диму менша, ніж у процесі горіння бензину. Це пояснюється утворенням значної кількості сажі під час горіння ароматичних вуглеводнів, які у великій кількості містяться у бензині. Так для прикладу, тривалість гасіння макетних вогнищ пожежі піною низької кратності у разі використання як пального бензину марки А-76 у всіх випадках була значно більшою, а проміжок часу до повторного займання – меншим, ніж у разі використання н-гептану. Відповідно можна зробити припущення, що параметри подавання ВП на гасіння бензину будуть значною мірою відрізнятись від гасіння н-гептану.

У всіх вище названих нормативних документах [3-6] вказано що випробування повинні проводитись за допомогою певного типу вогнегасника, проте в [5,6] не вказано який тиск має бути і вогнегасниках, що в свою чергу відіграє важливу роль у процесі гасіння, оскільки із збільшенням тиску у вогнегаснику збільшується витрата ВП.

Наведені вище методи випробувань ВП з визначення їх вогнегасної ефективності значної мірою залежать від досвіду та вмінь оператора (своєчасність приведення у дію вогнегасника, вибору правильної позиції для проведення пожежогасіння модельного вогнища, врахування параметрів горіння осередку).

Крім того, всі методи передбачають подавання ВП збоку модельного вогнища із заданої відстані, що відповідає умовам експлуатації вогнегасників. В той же час, робота систем порошкового пожежогасіння, за окремими винятками, передбачає подавання ВП зверху у зону горіння, а робота пожежних автомобілів порошкового гасіння вимагає подавання ВП на значну відстань.

Відомі дослідження [13, 14] дозволяють стверджувати, що важливою складовою, що впливає на ефективність застосування ВП для гасіння є особливості взаємодії його часток з конвективними тепловими потоками вогнища пожежі, а газопорошкові струмені переносних вогнегасників радикально відрізняються від струменів, що утворюються модулями систем порошкового пожежогасіння, зокрема імпульсної та короткочасної дії за ДСТУ 3972-2000 [15].

Слід відмітити, що в Україні відсутня нормативна база, яка регламентує технічні вимоги та методи випробувань вогнегасних порошків, призначених для гасіння пожеж класу Д, що унеможливлює проведення їхньої сертифікації.

Як відомо, «Федеральною державною установою «Всероссийский орден «Знак Почёта» научно-исследовательский институт противопожарной обороны» розроблено норми пожежної безпеки НПБ 714-98 [15], які розповсюджуються на вогнегасні порошки спеціального призначення, які призначено у якості вогнегасних речовин в автоматичних та інших засобах для гасіння тільки (виключно) металів та їхніх сполук, а також горючих та легкозаймистих рідин, газів, електроустановок під напругою електричного струму, а також встановлюють класифікацію, основні параметри, вимоги щодо безпеки застосування, загальні технічні вимоги і методи випробувань.

Основні показники технічного рівня та якості вогнегасних порошків спеціального призначення за вимогами [15] наведено у таблиці 3.

Цими ж нормами регламентовано модельні вогнища, які представляють собою квадратні про твіні з листової сталі зі стороною (500±10) мм, висотою (150±10) мм і товщиною стінок 2,5-3,0 мм. Модельні вогнища маючи однакові геометричні розміри відрізняються між собою масою горючого навантаження.

Сутність методики визначення показника вогнегасної здатності полягає у визначенні маси вогнегасного порошку, необхідної для гасіння вогнегасником, обладнаним насадком-розпилювачем, одиниці площини відкритої поверхні горіння модельного вогнища.

Для гасіння модельних вогнищ класів Д1 (магній), Д2(натрій), Д3(тризобутілалюмінія) застосовують відповідно порошок магнію: 12,5 кг металевого натрію та 12 л. ТІБА. Як і в попередніх методиках визначення показників вогнегасної здатності проводяться за результатаи гасіння оператором.

Таблиця 3 – Показники технічного рівня та якості вогнегасних порошків спеціального призначення [15]

Найменування показника	Норма					
	Порошки для гасіння пожеж за ГОСТ 27331					
	класуД1 (магній)		класу Д2 (натрій)		класу Д3 (ТІБА)	
	універсальний	цільовий	універсальний	цільовий	універсальний	цільовий
Густина неущільненого порошку кг/м^3, не менше	700	700	700	500	700	450
Густина ущільненого порошку, кг/м^3, не менше	1000	900	1000	600	1000	550
Вологість, % (мас.)	0,35	0,3	0,35	0,4	0,35	0,5
Схильність до вологопоглинання,%, не більше	2,5	2,0	2,5	3,0	2,5	4,0
Текучість, кг/с, не менше	0,28	0,28	0,28	0,20	0,28	0,15
Текучість при масовій долі залишку у вогнегаснику, % (мас.), не більше	15	15	15	18	15	21
Показник вогнегасної здатності, кг/м^2, не більше	20	12	50	10	50	20
Середній термін зберігання, років, не менше	5	5	5			

Відповідно виникає необхідність у проведенні досліджень спрямованих на обґрунтування удосконалених методів випробувань ВП з визначення їх вогнегасної здатності виходячи з наступних умов: виключити вплив оператора на результат гасіння, випробування проводити із врахуванням умов подальшого застосування ВП.

Одним із таких шляхів вирішення цієї проблеми може бути застосування малогабаритних модулів порошкового пожежогасіння із дистанційним запуском, що здатні забезпечити однаковість умов проведення випробувань. Застосування таких модулів дозволить легко змінювати інтенсивність та напрям подавання ВП. Проведення досліджень спрямованих на розроблення та валідацію таких методів випробувань ВП є предметом наступних досліджень авторів.

За результатами проведення аналітичних досліджень можна зробити наступні висновки:

1. Встановлено, що сучасні нормативні документи [3-6], які встановлюють вимоги до випробування вогнегасних порошків, мають незначні відмінності у методах з визначення вогнегасної здатності за класами пожеж А та В, зокрема у відстані з якої ведеться гасіння, кількості та виду пального тощо. При проведенні випробувань за такими методами результат значної мірою залежить від досвіду та вмінь оператора (своєчасності приведення у дію вогнегасника, вибору правильної позиції для проведення пожежогасіння модельного вогнища, врахування параметрів горіння осередку).

2. Існує необхідність у проведенні досліджень спрямованих на обґрунтування удосконалених методів випробувань вогнегасних порошків, що будуть враховувати умови їх подальшого застосування та максимально виключати вплив оператора, що проводить випробування, на результат гасіння.

Огурцов С. Ю., канд. техн. наук ст. наук. співр., Стилик І. Г., Антов А. В., канд. техн. наук, ст. наук. співр.

СПИСОК ЛІТЕРАТУРИ

1. А.Н. Баратов, Л.П. Вогман. Огнетушащие порошковые составы. Стройиздат. Москва, 1982.

2. ДСТУ 3105-95 Пороши вогнегасні. Загальні технічні вимоги і методи випробувань. – К.: Держстандарт України, 1998.

3. ГОСТ Р 53280.4-2009 Установки пожаротушения автоматические. Огнетушащие вещества. Часть 4. Порошки огнетушащие общего назначения. Общие технические требования и методы испытаний» встановлено такі вимоги до випробувань. – М.: Стандартинформ, 2009. – 7-8 с.

4. ISO 7202:2012 Fire protection -- Fire extinguishing media – Powder, 2012.

5. . EN 615 - Fire protection - Fire extinguishing media - Specifications for powders (other than class D powders), 2009.

6. Сабинин О.Ю., Агаларова С.М. Огнетушащие порошки. Проблемы. Состояние вопроса. //Пожаровзрывобезопасность: Сб.науч. тр.- М.: 2007, т.16, № 6, с.63-68.

7. ISO 7165-2009 Fire fighting — Portable fire extinguishers — Performance and construction, 2009.

8. EN 3-7 : Portable fire extinguishers. Characteristics, performance requirements and test methods, 2012.

9. ДСТУ 4063-2001 Бензини автомобільні. Технічні умови, 2001.

10. ГОСТ 51105-97 Топлива для двигателей внутреннего сгорания. Неэтилированный бензин, 1997.

11. Провести дослідження з порівняння ефективності пін під час гасіння різних неполярних горючих рідин з метою обґрунтування можливості заміни пального, яке використовується для випробування піноутворювачів: Звіт про НДР. – К.: УкрНДІПБ, 2007.

12. О.Ю. Сабинин. Эксперементальное изучение влияния технологических свойств порошковых составов на их огнетушащую способность при импульсном способе пожаротушения// Пожаровзрывобезопасность. – М.: 2008. - № 6. – С. 64-74.

13. В.И.Горшков. Тушение пламени горючих гидкостей. Пожнаука. Москва, 2007.

14. ДСТУ 3972-2000 Техніка пожежна. Установки порошкового пожежогасіння. Загальні технічні вимоги. Методи випробувань, 2000.

15. НПБ 174-98 Порошки огнетушащие специального назначения. Общие технические требования. Методы испытаний. Классификация. М. ФГУ ВНИИПО МВД России.*

Вплив цільових добавок до води на ефективність гасіння пожеж твердих речовин

Наведено результати експериментальних досліджень з визначення впливу цільових добавок на основі силікату натрію та карбонату калію до води на ефективність гасіння пожежі твердих речовин системою спринклерного пожежогасіння у спеціальному боксі для проведення вогневих випробувань ВБК 280. Під час досліджень встановлено відносну вогнегасну ефективність водного вогнегасного розчину із вмістом цільових добавок на основі рідкого натрієвого скла та карбонату калію у воді, порівняно із водою без добавок під час натурних вогневих випробувань з гасіння дерев'яних стандартних модельних вогнищ пожежі класу А.

За результатами попередніх досліджень [1], у лабораторних умовах, визначено відносну вогнегасну ефективність водної вогнегасної речовини (далі – ВВР) з цільовими добавками, а саме з 1 %-м вмістом Na_2SiO_3 та K_2CO_3 у рівних пропорціях під час гасіння модельного вогнища пожежі з деревини, порівняно із водою без добавок.

У житлових та громадських будинках, зокрема висотних, як технічні засоби пожежогасіння використовують пожежні кран-комплекти та спринклерні системи пожежогасіння [2-5]. Підвищення ефективності систем пожежогасіння для протипожежного захисту будинків різного призначення є актуальною науково-технічною задачею. Значний обсяг наукових робіт стосовно дослідження щодо підвищення відносної вогнегасної ефективності ВВР та її використання в системах пожежогасіння висвітлено в роботах [6-9]. Проте ці роботи не враховують особливості застосування ВВР для відокремлених систем пожежогасіння від господарсько-питного водопроводу. Отже, основне завдання досліджень полягає у наближенні до натурних умов дослідження з гасіння вогнищ пожежі твердих речовин, а саме деревини, що за пожежною класифікацією належить до пожеж класу А.

Експериментальні дослідження проведено шляхом моделювання умов гасіння пожежі системою спринклерного пожежогасіння у будівлі для визначення відносної вогнегасної ефективності досліджуваної ВВР, порівняно з водою без добавок. Критеріями відносної вогнегасної ефективності ВВР під час експери ментальних досліджень прийнято: час гасіння (*t, с*) модельного вогнища пожежі твердих речовин досліджуваною ВВР, та водою без добавок за однакових умов її подачі; загальна кількість ВВР (*R,* л) або води без добавок, що було витрачено під час гасіння модельного вогнища.

Мета дослідження полягає в експериментальному визначенні впливу цільових добавок до води на ефективність гасіння пожеж твердих речовин, порівняно з водою без добавок системою спринклерного пожежогасіння під час натурних вогневих випробувань.

Матеріали та методи дослідження. Застосовано методику полігонних натурних вогневих випробувань для досліджень відносної вогнегасної ефективності водних вогнегасних речовин. Результати досліджень оброблено методами обчислювальної математики із використанням програмного комплексу «Microsoft Office».

Результати дослідження. Експериментальні дослідження здійснювали у спеціальному боксі для проведення вогневих випробувань ВБК 280 на випробувальному стенді (що моделює сприн-

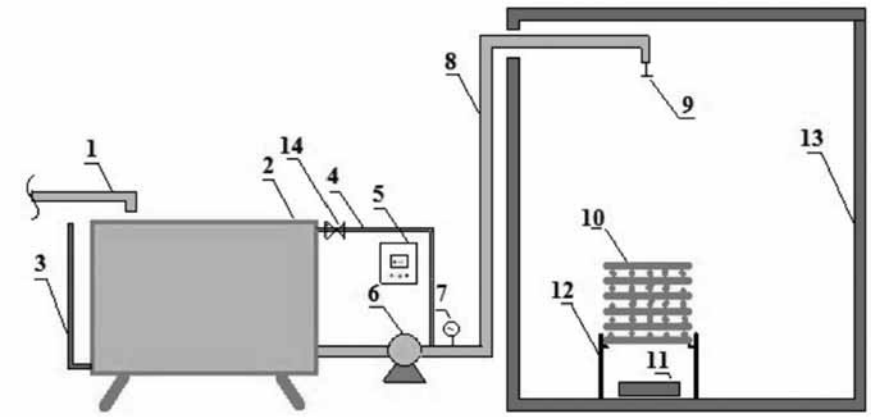


Рис. 1. Схема випробувального стенда для проведення натурних вогневих випробувань: *1) наливний трубопровід; 2) резервуар; 3) індикатор об'єму води в резервуарі; 4) байпасна лінія регулювання тиску; 5) блок управління насосною станцією; 6) насос; 7) манометр; 8) подавальний трубопровід; 9) спринклерний зрошувач; 10) модельне вогнище пожежі класу 13А; 11) деко для палива; 12) підставка; 13) випробувальний бокс ВБК 280; 14) кран*

клерну систему пожежогасіння), до складу якого входять: горизонтальний насос відцентрового типу Д160-112 з витратою води Q – 160 м³/год та максимальним напором води Н – 112 м, резервуар об'ємом 1,4 м³, обладнаний байпасною лінією для можливості регулювання тиску за допомогою крана 14. На рис. 1 зображено схему випробувального стенда для проведення натурних вогневих випробувань.

Під час експериментальних досліджень використано стандартні модельні вогнища пожежі класу А, що за класифікацією [10] відповідають моделі 13А.

Як горючий матеріал для цього модельного вогнища використано соснові бруски з поперечним перерізом $40^{\pm 2}$ мм на $40^{\pm 2}$ мм та довжиною $500^{\pm 5}$ мм. Штабель складається із 12 шарів, у кожному шарі по шість брусків. Площа горіння стандартного модельного вогнища класу 13 А згідно з [5] становить 4,7 м² та відповідає пожежному навантаженню 386,4 МДж/м². Вологість деревини була в межах від 10 до 14 %, що контролювалося за допомогою вологоміра типу ВПК-12[11]. Випробування проведено за таких кліматичних умов:

- температура повітря: 12 °С (± 0,5°С);
- відносна вологість повітря: 72 % (± 1 %);
- атмосферний тиск: 94,9 кПа (692 мм рт. ст.).

У випробувальному боксі 13 встановлюють металеву підставку 12 висотою $350^{\pm 10}$ мм для встановлення модельного вогнища класу 13А 10 та металеве деко 11 з геометричними розмірами 400*400 мм (± 10 мм) та висотою борта 100 мм (± 5 мм). Спринклерний зрошувач 9 улаштований над модельним вогнищем пожежі 10 на висоті 2,7 м від рівня підлоги, що відповідає висоті житлового приміщення. На рис. 2 зображено модельне вогнище пожежі класу 13А (див. рис. 2, а) та спринклерний зрошувач 9 випробувального стенду (див. рис. 2, б).

Експериментальні дослідження проводили у такому порядку. На першому етапі після повного заповнення резервуара 2 водою без добавок у металеве деко 11, що знаходиться під модельним вогнищем пожежі 10 класу А, наливають 4 л води (± 50 мл) та 2,0 л (± 20 мл) бензину марки А-92. За командою керівника проведення випробувань паливо в деку 11 підпалюють факелом та одночасно вмикають секундомір. Наявність цього об'єму бензину забезпечує час його горіння не менше 150 с. Вільне горіння модельного вогнища пожежі

Рис. 2. Загальний вид модельного вогнища пожежі класу А (а) та спринклерного зрошувача (б) випробувального стенду для проведення натурних вогневих випробувань

Рис. 3. Фрагмент натурних вогневих випробувань

класу А триває (300 ± 5) с, яке контролюється секундоміром.

На рис. 3 зображено фрагмент натурних вогневих випробувань.

Після закінчення часу вільного горіння модельного вогнища пожежі класу А, за командою керівника проведення випробувань, вмикають другий секундомір і одночасно за допомогою блока управління насосною станцією 5 вмикають насос 6 та розпочинається подавання води зі спринклерного зрошувача 9 на гасіння модельного вогнища пожежі 10, при цьому тиск у системі становить 0,15 МПа (± 0,01 МПа), що контролюється за допомогою манометра 7.

Модельні вогнища пожежі класу 13А вважають погашеними, якщо полум'я ліквідовано і через 10 хв після завершення гасіння видиме полум'я у вогнищі пожежі відсутнє. Появу короткочасних спалахів протягом зазначеного часу після закінчення гасіння не беруть до уваги. Якщо під час досліджень штабель модельного вогнища пожежі 10 розвалюється, дослід вважають недійсним і проводять новий. Після завершення гасіння водою без добавок стандартного модельного вогнища пожежі класу 13А вимикають насос 6 та одночасно вимикають секундомір, а час гасіння фіксують та вносять дані до протоколу. Також до протоколу вносять дані щодо об'єму витраченої води на гасіння модельного вогнища пожежі, які визначають за допомогою індикатора об'єму води 3 в резервуарі 2. Для води без добавок експериментальні дослідження повторюють тричі.

Другий етап проведення експериментальних досліджень починають з наповнення резервуара водою та додавання до води Na_2SiO_3 та K_2CO_3 з їх рівним пропорційним вмістом для утворення 1 %-го водного розчину. Після приготування розчину досліджуваної 1 % ВВР дослід повторюють тричі за наведеною вище методикою. Результати експериментальних досліджень з визначення впливу цільових добавок до води на ефективність гасіння пожеж твердих речовин, а саме пожежі класу А сприн-

Табл. Результати гасіння стандартних модельних вогнищ пожежі класу 13А водою без добавок та ВВР з 1 %-м вмістом цільових добавок Na_2SiO_3 та K_2CO_3 у рівних пропорціях

Досліджувана ВВР у системі пожежогасіння	Тиск P, МПа	Загальний об'єм ВВР на гасіння, R, л	Середній об'єм ВВР на гасіння, $R_{сер}$, л	Час гасіння t, с	Середній час гасіння $t_{сер}$, с
Вода без добавок	0,15	1333	1318	713	705
		1397		747	
		1225		655	
ВВР з 1 % вмістом Na_2SiO_3 та K_2CO_3 у рівних пропорціях	0,15	1176	1114	562	541
		1065		517	
		1121		544	

клерною системою пожежогасіння, наведено в таблиці.

Висновки:

1. Об'єм ВВР, що була використана на гасіння модельних вогнищ пожежі класу А, за однакових умов подачі ВВР з цільовими добавками становить у середньому 1 114 л, що на 18 % менше, ніж для води без цільових добавок.

2. Час гасіння модельних вогнищ пожежі класу А за однакових умов подачі ВВР, з 1 %-м вмістом Na_2SiO_3 та K_2CO_3 в рівних пропорціях, порівняно із водою без цільових добавок, становить у середньому 541 с, що на 28-31 % менший, ніж для води без цільових добавок.

3. За результатом експериментальних досліджень з визначення впливу цільових добавок до води під час натурних вогневих випробувань з гасіння модельних вогнищ пожежі класу 13А доведено відносну вогнегасну ефективність ВВР з 1 %-м вмістом Na_2SiO_3 та K_2CO_3 у рівних пропорціях, порівняно із водою без цільових добавок.

Ст. наук. співроб., пров. наук. співроб. О.О. Сізіков, канд. техн. наук – УкрНДІ цивільного захисту;
Наук. співроб. Я.В. Балло – УкрНДІ цивільного захисту;
Наук. співроб. В.С. Бенедюк – УкрНДІ цивільного захисту

Література

1.Жартовський С.В. Виявлення впливу хімічного складу водних вогнегасних речовин на основі Na_2SiO_3 та K_2CO_3на їх вогнегасну ефективність під час гасіння вогнищ класу А / С.В.

Жартовський, В.В. Ніжник, Р.В. Уханський, Я.В. Балло // Теорія і практика гасіння пожеж та ліквідації надзвичайних ситуацій : матер. Міжнар. наук.-практ. конф. – Черкаси, 2016. – С. 46-49.

2. ДБН В.2.2-24:2009 Будинки і споруди. Проектування висотних житлових і громадських будинків, Мінрегіонбуд України, наказ від 12.02.2009 р., № 67. – 114 с.

3. ДБН В.2.5-64-2012 Внутрішній водопровід та каналізація. – Ч. І. Проектування. – Ч. ІІ. Будівництво. Наказ Мінрегіону від 31.10.2012 р., № 553. – 168 с.

4. ДБН В 1.1-7-2002 Пожежна безпека об'єктів будівництва. Наказ Мінрегіону України від 23.01.2007 р., № 18. – 42 с.

5. ДБН В.2.5-56-2014 Системи протипожежного захисту. Наказ Мінрегіону від 13 листопада 2014 р., № 312. – 182 с.

6. Антонов А.В. Провести дослідження з розкриття особливостей процесів припинення горіння горючих речовин під час застосування сучасних вогнегасних речовин та технологій їх подавання / А.В. Антонов, В.О. Дунюшкин, В.М. Жартовський, С.В. Жартовський, В.О. Боровиков, О.М. Тимошенко, М.І. Копильний. – К. : Вид-во УкрНДІЦЗ, 2015. – 147 с.

7. Антонов А.В. Вогнегасні речовини : навч. посіб. / А.В. Антонов, В.О. Боровиков, В.П.

Орел, В.М. Жартовський, В.В. Ковалишин. – К. : Вид-во "Пожінформ-техніка", 2004. – С. 12-24.

8. Звіт про науково-дослідну роботу "Провести теоретичні і експериментальні дослідження процесів придушення полум'я вогнегасними речовинами і виявити шляхи підвищення їх ефективності" / кер. А.В. Антонов, канд. техн. наук, ст. наук. співроб. – К. : Вид-во УкрНДІПБ МВС України, 1995. – 318 с.

9. Козяр Н.М. Підвищення ефективності застосування водних та водопінних вогнегасних речовин : автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 21.06.02 – "Пожежна безпека" / УкрНДІПБМНС України. – К. : Вид-во "Лібра", 2009. – 4-8 с.

10. ДСТУ EN 3-7:2014 Вогнегасники переносні. – Ч. 7. Характеристики, вимоги до робочих параметрів і методи випробувань (EN 3-7:2004+A1:2007, IDT) наказ Мінекономрозвитку від 30.12.2014 р., № 1494. – 157 с.

11. Пилопродукция и деревянные детали. Методы определения влажности // ГОСТ 16588-91. – [Чинний від 1993.01.01.]. – 5 с.

Порівняння вогнегасних речовин для гасіння пожеж легкозаймистих та горючих рідин

Ефективне та швидке гасіння горючих рідин є однією з найбільш, не вирішених проблем пожежогасіння. Дуже складними та небезпечними є пожежі, які виникають у резервуарних парках з наявністю великої кількості резервуарів великого об'єму, заповнених бензином, сирою нафтою, мазутом, спиртом тощо. Гасіння таких пожеж супроводжується підвищеним ризиком для особового складу та складністю управління силами і засобами. Способи гасіння цих пожеж, потребують їх удосконалення та створення нових більш ефективних способів.

Ефективне та швидке гасіння горючих рідин є однією з найбільших не вирішених проблем пожежо-гасіння. Дуже складними та небезпечними є пожежі які виникають у результаті горіння горючих та легкозаймистих рідин бензинів, сирої нафти, мазутів, спиртів тощо. [1] Як свідчить практика, такі пожежі часто можуть бути розвинутими та затяжними, а їх гасіння потребує залучення великої кількості сил і засобів пожежогасіння та характеризується великими матеріальними збитками і високим рівнем ризику для життя та здоров'я людей. Усе це потребує удосконалення уже відомих способів гасіння та створення нових, більш ефективних.

Пожежі в резервуарах зазвичай починаються з вибуху пароповітряної суміші в газовому просторі резервуара зі зривом даху або зі спалаху "багатої" суміші без зриву даху, але з порушенням цілісності його окремих місць. Сила вибуху, як правило, значна в тих резервуарах, де наявний великий газовий простір, заповнений сумішшю парів нафтопродукту з повітрям (низький рівень рідини). Залежно від сили вибуху у вертикальному металевому резервуарі може спостерігатися така ситуація: дах зривається цілком, його відкидає убік на відстань 20 - 30 м, рідина горить на всій площі резервуара; дах трохи піднімається, відривається повністю або частково, потім затримується в напівзануреному стані в палаючій рідині; дах деформується й утворює невеликі щілини в місцях кріплення до стінки резервуара. У зруйнованих зварних швах самого даху в цьому випадку горять пари ЛЗР над утвореними щілинами [2]. При пожежі в залізобетонних (підземних) резервуарах від вибуху відбувається руйнування покрівлі, у якій утворюється отвір великих розмірів, потім у процесі пожежі може

облалитися покриття по всій площі резервуара через високу температуру і неможливість охолодження їх несучих конструкцій. У циліндричних горизонтальних, сферичних резервуарах від вибуху найчастіше руйнується днище, у результаті чого рідина розливається на значну площу, створюється загроза займання сусідніх резервуарів і споруд.

Зрозуміло, що такі умови можуть постійно змінювати характер горіння, створювати небезпеку скипання горючої рідини та різкого збільшення площі горіння, хаотичного перекидання вогню в різних напрямках, розливу горючої рідини по прилеглій території. Ці фактори додатково посилюють складність гасіння у важкодоступних місцях, «кишенях», під землею, в обвалуванні, в об`ємі резервуара або (у групі резервуарів) та потребують перегрупування сил і засобів, зміни плану гасіння та використання різних способів, засобів гасіння та основне - ефективних вогнегасних речовин.

Виходячи з вище сказаного та враховуючи усі специфічні особливості горіння і гасіння горючих рідин, необхідно порівняти та проаналізувати характеристики відомих засобів гасіння та визначити найбільш ефективні з них, з метою їх подальшого вдосконалення та використання їх на практиці.

Аналіз останніх досліджень та публікацій

Проблемою гасіння горючих рідин займалася велика кількість авторів [1-4], які пропонували різні варіанти її вирішення. Найбільш поширеним способом гасіння таких пожеж, стало гасіння повітряно-механічною піною [3] Цей спосіб забезпечує досить тривалу ізоляцію поверхні горючої рідини від газової фази, в якій відбувається процес горіння. Також піни володіють досить значною охолоджуючою дією. Завдяки здатності пін розтікатися вони можуть проникати у важкодоступні місця, що полегшує гасіння так званих «кишень». Однак вогнегасні піни мають ряд недоліків: мала стійкість пін за умови дії інтенсивних теплових потоків від полум'я палаючої рідини і від контакту піни з полярними горючими рідинами; складнощі з подаванням пін на великі відстані; знесення пін конвективними потоками, їх руйнування в ході підльоту до резервуара та зіткнення з поверхнею рідини; висока вартість ряду піноутворювачів і технічних засобів подачі пін, особливо в разі використання підшарового способу подачі; більшість пін забруднюють горючі рідини, що призводить до неможливості їх подальшого використання за прямим призначенням або ускладнює їх подальшу переробку; до складу пін входять потенційно екологічно небезпечні речовини – піноутворювачі, а також цей спосіб потребує досить багато часу на підготовку до гасіння.

Таблиця 1. Порівняльні характеристики вогнезахисних речовин для гасіння пожеж класу «В»

Параметри	Аерозольне гасіння	Газове гасіння	Порошкове гасіння
Тривалість часу необхідного для гасіння	5	4	2
Зручність подачі вогнегасної речовини	5	1 (ПГ) 3 (ССП)	3
Тривалість часу збереження вогнегасної здатності, після подавання ВР	5	5	2
Вартість захисту умовного об'єму	5	2	4
Інгібуюча здатність	5	3	4
Флегматизуюча здатність	5	4	4
Охолоджуюча здатність	2	3	3
Екранувальна здатність	4	1	3
Ізолювальна здатність	1	1	3
Вогнегасна ефективність	5	3	4
Всього:	42	30	32

Постійно тривають експериментальні наукові дослідження із вдосконалення цього способу гасіння. [3]. Зокрема дослідники працюють над збільшенням дальності подавання піни, [4] розробкою екологічних піноутворювачів [5], використанням плівкоутворюючих ПУ [6], які утворюють більш стійку по відношенню до полярних ГР піну, розробкою вогнегасних пін, що тверднуть. Впровадження цих заходів вдосконалення, скоріш за все допоможе вирішити багато проблемних питань, притаманних цьому способу гасіння, проте не вирішить питання великих затрат часу, зусиль та ресурсів, необхідних для подачі піни в осередок пожежі, та високої вартості обладнання для подавання піни – насосів, трубопроводів, корозійностійких ємностей для зберігання піноутворювача.

Альтернативними варіантами є використання для гасіння горючих рідин вогнегасних порошків, газів, дисперсної води, вогнегасних емульсій та поєднання цих способів, але жоден з цих варіантів не володіє одночасно значною кількістю характеристик, які б дозволяли ефективно, дешево, надійно та швидко гасити горіння рідин.

Деякі автори [1,7] пропонують використовувати для гасіння рідин тверду гранульовану вуглекислоту, гранули піноскла, тверді пористі матеріали та гелеутворюючі системи, проте ці способи на даний момент перебувають на стадії наукових розробок тому інформації про їхнє використання практично у літературі немає.

Кожен з основних способів гасіння рідин має свої переваги та недоліки. Так наприклад вогнегасні порошки дають суттєвий вогнегасний ефект мають інгібуючу, флегматизуючу, розбавляючу, охолоджуючу дію [8, 9] проте, вони мають високу вартість, дуже малий час зависання в захищуваному об'ємі, мають схильність до злежування, а процес подачі їх на гасіння пожежі є недостатньо зручний та займає багато часу. Також вони мають недостатній охолоджуючий та ізолюючий ефект та не можуть в повному обсязі запобігти повторному загорянню рідини, після їх подавання [10].

Гасіння дисперсною водою відбувається шляхом [1] охолодження верхніх шарів киплячої рідини до температури нижчої за температуру спалаху, тобто основним механізмом припинення горіння є охолодження. Також присутній ефект розбавлення горючого середовища парою, що утворюється під час випаровування краплин [9] проте майже відсутня інгібуюча та ізолювальна дія. Також для успішного гасіння [1] дисперсною водою великих за площею поверхонь ГР необхідно створити умови згасання полум'я над всією поверхнею рідини. Ці умови повинні бути створені на час, протягом якого нагріті стінки резервуара будуть охолоджені до температури, нижчою за температуру самоспалахування ГР або поверхневий шар рідини має бути охолоджений до температури, нижчої за її температуру спалаху.

Стаціонарно встановлені у верхній частині резервуара розпилювачі в більшості випадків не в змозі вирішити таке завдання, оскільки вони часто виходять з ладу за відсутності постійного обслуговування або під час вибуху пароповітряної суміші, з якої, як правило, починається пожежа. Пересувні установки пожежогасіння дисперсною водою в наш час, не пристосовані для таких цілей.

Газове гасіння реалізовує механізм розбавлення горючого середовища та флегматизування частинок що беруть участь у горінні, що призводить до охолодження та переривання ланцюгових реакцій горіння. [11,12,13] Також окремі газоподібні вогнегасні речовини (двоокис вуглецю) мають додаткову охолоджувальну дію, однак газові речовини як і вода не мають ізолюючої та екранувальної дії, що є необхідною умовою гасіння пожеж класу «В» [1]. Також не завжди вдається забезпечити в зоні горіння необхідної концентрації ГВР протягом тривалого часу для запобігання повторного займання [13]. Крім цього використання газових речовин є дорого вартісним, потребує спеціальних трубопроводів, ємностей для зберігання газу, іншого обладнання яке важко забезпечити в умовах реальної пожежі, що робить

його застосування на практиці малоефективним.

З позиції екологічних аспектів існують значні обмеження на використання газових вогнегасних речовин [14,15], і зважаючи на постійне погіршення екологічної ситуації, обмеження на їх використання будуть лише посилюватися.

Механічні способи (відкачування горючої рідини, накриття дзеркала горючої рідини негорючим матеріалом, перемішування, покриття вогнегасною піною, плівкоутворювачем) можуть дати ефект гасіння пожежі, але їх можна застосувати лише за певних умов які дозволять реалізувати ці способи (цілісність обладнання, можливість наближення до зони горіння, тощо). Мета: аналіз і порівняння вогнегасних речовин для гасіння пожеж легкозаймистих та горючих рідин та визначення оптимальної танедо- рогої вогнегасної речовини на основі вогнегасної ефективності та експлуатаційних характеристик.

Виклад основного матеріалу: Для порівняння характеристик вогнегасних речовин було обрано вогнегасні речовини які мають схожі механізми припинення горіння. За результатами дослідження складено таблицю 1, в котрій наведено орієнтовні дані щодо характеристик вогнегасних речовин для гасіння горючих та легкозаймистих рідин.

Градація показників таблиці базується на шкалі, де мінімальна перевага дорівнює «1» максимальна перевага дорівнює «5» що є узагальненим показником таких понять: Тривалість часу, необхідного для гасіння час, необхідний для повного припинення горіння при стандартному вогневому випробуванні. Зручність подачі вогнегасних речовин – сумарна кількість операційних дій, які необхідно здійснити в процесі підготовки до початку та в процесі подачі вогнегасної речовини. Тривалість збереження вогнегасної здатності, після подавання ВР – загальний час збереження вогнегасної дії в умовному об'ємі після подавання ВР. Вартість – загальна вартість вогнегасних речовин та витрати на підготовку та подачу вогнегасних речовин в осередок пожежі в умовному об'ємі. Вогнегасна ефективність – наявність в способі гасіння вогнегасних властивостей та характеристик, необхідних для гасіння пожеж класу «В». «ПГ» показник за умов використання пересувною пожежною технікою. «ССП» показник за умов використання в складі стаціонарної системи пожежогасіння в умовно герметичному об`ємі.

Як бачимо з таблиці, незначну загальну перевагу має аерозольне гасіння. В порівнянні з іншими вогнегасними засобами, які можна використовувати для гасіння ЛЗР та ГР, вогнегасні аерозолі мають певні переваги за окремими критеріями, а саме:

Вогнегасний аерозоль у разі гасіння ним пожеж класу В діє комплексно, чим забезпечується його висока вогнегасна ефективність [16, 17]. Внаслідок утворення дрібнодисперсної конденсованої фази, нейтральних газів та продуктів згоряння АУС аерозоль при потраплянні в зону горіння суттєво сповільнює усі ланцюгові фізико-хімічні процеси, необхідні для горіння рідини, має хорошу охолоджуючу, флегматизуючу, інгібуючу та екрануючу дію. Це зумовлюється процесами розбавлення горючого середовища газоподібними негорючими продуктами реакції горіння АУС, продуктами розкладу твердих частинок аерозолю і вигорянням кисню в атмосфері захищуваного середовища [18,19]; інгібуванням хімічних реакцій в полум'ї свіжоутвореними дрібнодисперсними твердими частинками аерозолю (K_2CO_3, $KHCO_3$, KON, KCl, та ін.) і продуктами їх розпаду (K_2O, KO та ін.) [16]; захист дзеркала горючої рідини від теплової радіації полум'я, завдяки поглинанню і розсіюванню аерозольними частинками променів, що йдуть від зони горіння; зниження температури зони горіння завдяки поглинанню тепла при нагріванні, плавленні, випаровуванні і розкладанні твердих частинок аерозолю; припинення горіння шляхом перемішування горючої рідини (при підшаровому гасінні) [18], тривалим часом захисної дії завислих частинок вогнегасного аерозолю в умовно герметичному об'ємі близько 25хв, що цілком достатньо для унеможливлення подальшого продовження горіння через охолодження нагрітих огороджувальних конструкцій.

Вогнегасний аерозоль має низькі значення кількості вогнегасної речовини необхідної для створення в об`ємі вогнегасної та флегматизуючої концентрації. Ми порівняли показники для різних газових речовин, які використовуються в Україні, (табл. 2) і, як бачимо значення показника аерозолю є значно меншим за інші речовини газового гасіння, з чого можна зробити висновок, що ефективність гасіння аерозолем є більшою, а розхід речовини при цьому – менший. Також аерозолі є екологічними і не підпадають під заборону Монреальського та Кіотського протоколів на відміну від газових ВР [14, 15] характеристики котрих наведено в таблиці 2 .

Як бачимо з таблиці 2 вогнегасні концентрації газових ВР є на декілька порядків вищі за вогнегасну концентрацію аерозолю. Мінімальна вогнегасна концентрація (МВК) такої речовини як IG-541 є в десять разів вища за вогнегасну концентрацію аерозолю, а для речовини додекафтор-2 це значення майже в 30 разів є вищим за МВК аерозолю. Системам пожежогасіння, які працюють на основі аерозоле-утворювальної суміші (АУС) не потрібні спеціальні ємності для газів чи піноутворювача, агрегати для подачі газів під надлишковим тиском, насосне обладнання, запірні арматури, генератори піни або розпилювачі, труби, розгалужувачі, складні електронні системи управління тощо, що значно спрощує процес подавання вогнегасного аерозолю з відповідним фазовим складом, в осередок пожежі.

Гасіння аерозолями має суттєві економічні переваги: з 10 кг АУС – утворюється до 50000 л вогнегасного аерозолю (для порівняння – утворення аналогічного об'єму вогнегасної піни середньої кратності необхідно використати близько 30 літрів піноутворювача). Але трактувати та порівнювати вогнегасну піну з аерозолем не є коректно, оскільки вогнегасна піна забезпечує максимальний вогнегасний ефект за рахунок ізолювання горючої поверхні від повітря. Влаштування аерозольної системи пожежо-гасіння для захисту резервуара з горючою рідиною є значно дешевшим варіантом завдяки невеликій кількості обладнання, необхідного для її монтажу, та низькій вартості обслуговування установки в процесі експлуатації. Генератор вогнегасного аерозолю можна закріплювати як зверху так і внизу резервуара для подачі аерозолю на поверхню палаючої

Таблиця 2. Порівняльні характеристики вогнезахисної ефективності речовин газового гасіння які використовуються в Україні

Вогнегасна речовина	Хімічна назва	Вогнегасна концентрація г\м^3	Флегматизуюча концентрація г\м^3	Національний стандарт
FK-5-1-12	Додекафтор-2-метилпентан-3-	961	1346	ДСТУ 4466-5:2008[20]
HFC 227ea	Гептафторпропан	780	1092	ДСТУ 4466-9:2008[20]
IG-01	Аргон	833	1167	ДСТУ 4466-12:2008[20]
IG-100	Азот	661	926	ДСТУ 4466-13:2008[20]
IG-541	Азот (52%) Аргон (40%) Діоксид вуглецю (8%)	584	818	ДСТУ 4466-15:2008[20]
Діоксид вуглецю	Діоксид вуглецю	451	648	ДСТУ 5092:2008[21]
Вогнегасний аерозоль	Вогнегасний аерозоль	50	79	

рідини [23], при цьому установка при вибуху резервуара може залишитися неушкодженою завдяки надійному кріпленню до стінок резервуара та відсутності трубопроводів, які йдуть по зовнішній стінці резервуара і можуть деформуватися від вибуху, що, в свою чергу, призведе до виходу з ладу установки.

Спираючись на експериментальні дослід-ження вогнегасних аерозолів [1 – 4, 11, 22] в сфері об'ємного гасіння пожеж класу «В», відомо, що наразі він володіє найвищою вогнегасною ефективністю завдяки високій інгібуючій, флегматизуючій, охолоджувальній здатності та відповідно низькій вартості гасіння пожеж горючих рідин, як в умовно герметичному об`ємі так і на відкритому просторі.

Таким чином, спираючись на дані, отримані в результаті аналізу можемо зазначити, що аерозолі є майже універсальними вогнегасними речовинами у своєму застосуванні при гасінні дифузійного полум'я. Їх можна використовувати як в замкненому об'ємі так і на відкритому просторі. А змінюючи рецептуру АУС, створюючи нові способи подачі аерозолю в осередок пожежі, а також використовуючи різні види палива, можна впливати на вогнегасну ефективність одержуваних аерозолів, що, в свою чергу дасть змогу змінювати його вогнегасні характеристики та властивості, відповідно до певної потреби використання аерозолю, зокрема для гасіння великих пожеж в тому числі – на відкритому просторі.

Висновки: Враховуючи постійно зростаючі вимоги споживачів до вогнегасних засобів, а саме: поєднання в одній вогнегасній речовині високих показників вогнегасної ефективності та експлуатаційних переваг, – зручності подавання в осередок пожежі, тривалого часу захисту, можливості флегматизування горючої системи при незначних концентраціях, тривалого періоду зберігання та інш, та провівши аналіз і порівняння вогнегасних речовин для гасіння пожеж легкозаймистих та горючих рідин. Згідно зазначених критеріїв, можна зробити висновок, що вогнегасний аерозоль відповідає зазначеним критеріям оптимальної та недорогої вогнегасної речовини, що підтверджується найбільшою кількістю умовних балів, отриманих за зазначені критерії.

Ефективність вогнегасних аерозолів, а також простота технічних засобів та технологій їх використання є відправною точкою, яка може стати причиною обрання саме цих засобів для використання їх у стаціонарних системах та інших засобах пожежогасіння горючих та легкозаймистих рідин, поряд з уже впровадженими. Крім цього впровадження аерозольного пожежогасіння для ліквідації масштабних пожеж класу В є перспективним напрямом та потребує комплексного наукового дослідження, практичних випробувань, написання нормативних документів.

В. М. Баланюк,
В. С. Мирошкін,
Ю. О. Копистинський,
О. І. Гірський,
О. І. Гарасим'юк

Список літератури:

1. Дадашов І. Ф., Кірєєв О.О., Трегубов Д. Г., Тарахно. О. В. Гасіння горючих рідин твердими пористими матеріалами та гелеутворюючими сис-темами: монографія. Харків: НУЦЗУ. 2021. 240 с.

2. Баратов А.Н., Иванов Е.Н., Корольченко А.Я. Пожарная безопасность. Взрывобезопасность. Справочн. Изд.: М.: Химия, 1987. 269 с.

3. Ковалишин В.В., Васильєва О.Е., Козяр Н.М. Пінне гасіння: Львів. СПОЛОМ. 2007. С. 137.

4. Ковалишин В.В., Кирилів Я.Б, Грушовінчук О.В., Експериментальні дослідження процесу взаємодії струменів повітряно-механічної піни різної кратності під час їх польоту: Збірник наукових праць «Пожежна безпека». 2018. № 32. 31 с. 5. Боровиков В. О. Одержання та застосування екологічно безпечних піноутворювачів для гасіння пожеж: дис. канд. техн. наук 21.06.02 / Український НДІ пожежної безпеки. Київ. 2002. 237с.

6. Войтович Т. М. Вдосконалення технології «підшарового» пожежогасіння в резервуарах з нафтопродуктами: дис. д. ф. Львів. 2020. 216 с.

7. Корольов Р. А. Ковалишин, В. В. Штайн Б. В. «Аналіз способів гасіння пожеж в резервуарах з нафтопродуктами комбінованим способом» / Scientafic Journal (Sciense Rise) 2017. №6 (35). с 56.

8. Гарасим'юк О. І. Розвиток наукових аспектів комбінованого застосування вогнегасних аерозолів, газів та порошків: дис. кандидит. техн. наук. / Львів, 2016. 153 с.

9. Боровиков В. О. Вогнегасні речовини: минуле, сучасність і майбутнє частина II: плоди «століття технологій. URL security-info.com.ua/articles/?ELEMENT_ID=775 Fire and security/8 с.

10. НАПБ 05.035–2004 «Інструкція щодо гасіння пожеж у резервуарах із нафтою та нафтопродуктами» затверджено Наказом Мініс-терства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи 16.02.2004 р. No 75.

11. Бондаренко С.Н. Сучасні системи автоматичного пожежогасіння: Харків. НУЦЗУ 2001. С. 176.

12. Козяр Н.М. Підвищення ефективності об'ємного пожежогасіння: Збірник наукових праць. «Пожежна безпека». №25. 2014. 16 с.

13. Скоробагатько Т. М., Копильний М.І., В.О. Боровиков, Ефективність гасіння деякими газовими вогнегасними речовинам біодизельного палива та його сумішей з дизельним паливом: Науковий вісник Цивільний захист та пожежна безпека № 1 (3) 2017. Київ, 16с.

14. Монреальський протокол про речовини, що руйнують озоновий шар ООН; Протокол, Акт, Резолюція від 16.09.1987. URL http://parusconsultant.com/ ?doc=053O65D021.

15. Кіотський протокол до Рамкової конвенції Організації Об'єднаних Націй про зміну клімату (укр/рос) ООН; Протокол, Міжнародний документ від 11.12.1997. URL https://zakon.rada.gov.ua/laws/show/995_801.

18 Пожежна безпека, №41, 2022

16. Копистинський Ю.О. Баланюк В. М., Кошеленко В.В. Особливості механізму гасіння дифузійного полум'я аерозолями на основі хло-ридів та карбонатів калію: Матеріали IX Міжнар. наук.-практ. конф. м. Львів. Львів. 2009. 56с.

17. Баланюк В.М., Грималюк Б.Т., Кіт Ю.В., Левуш С.С. Вплив газової фази на ефективність вогнегасних аерозолів: Вісник НУ "Львівська політехніка". Технічні науки. №497. 2004. 17с.

18. Каримов Ф.Ф. О гомогенно-гетерогенном механизме протекания каталетических реакций в аерозолях Науч. произв. корпорация "Киев. ин-т автоматики. Киев. 1996. 44 с.

19. Баланюк В.М., Лавренюк О.І., Гарасим'юк О.І., Голонько О.Я. Особливості гасіння твердих та рідких горючих речовин вогнегасним аерозолем на основі солей калію: Збірник наукових праць Пожежна безпека. № 12. 2008. С. 60-64. 20. ДСТУ EN 15004-1:2014 Стаціонарні системи пожежогасіння. Системи газового пожежогасіння. Частина 1. Проектування, монту-вання та технічне обслуговування (EN 15004-1:2008, IDT) [Чинний від 2016-01- 01] Вид. офіц. Київ: Мінекономрозвитку України. 2014. 102 с. 21. ДСТУ 5092:2008 Пожежна безпека. Вогнегасні речовини. Діоксид вуглецю (EN 25923:1993 (ISO 5923:1989), MOD) [Чинний від 2010-10- 01] Вид. офіц. Київ: Український науково-дослідний інститут пожежної безпеки (УкрНДІПБ) МНС України, 2008. 10 с.

22. Бондаренко С. М. Розробка генераторів вогнегасячого аерозолю із покращеними характеристиками: дис кандидат. техн. наук. Харків, 2004. 184 с.

23. Кравченко А. В. Підшарове гасіння спиртів вогнегасним аерозолем: дис. доктор філософії. Львів. 2021. 189 с.

Умови та перспективи застосування вогнегасного аерозолю для гасіння пожеж на об'єктах підвищеної небезпеки

До об'єктів підвищеної небезпеки належать підприємства нафтогазовидобувної, переробної, хімічної та енергетичної галузей промисловості. Зазначені підприємства характеризуються великим пожежним навантаженням, одночасною наявністю твердих, рідких і газоподібних горючих речовин, їх перебуванням в різноманітних температурних і фізичних умовах та наявністю значної кількості потенційних джерел запалення.

З аналізу останніх пожеж в умовах війни можна зробити висновок, що пожежі на таких об'єктах поширюються як правило з максимальною швидкістю, існує можливість утворення вибухонебезпечних середовищ та інших пожежонебезпечних явищ та ситуацій. Для забезпечення швидкого, надійного та ефективного гасіння пожеж і попередження горіння та вибухів на таких об'єктах необхідний універсальний в своєму роді вогнегасний засіб, який би володів такими якостями як: висока вогнегасна ефективність як в обмежених об'ємах, так і на відкритому просторі, а також висока флегматизаційна ефективність. Найкраще цим вимогам відповідає вогнегасний аерозоль, у якого присутні всі вищеперелічені характеристики [1].

Відомо, що вогнегасний аерозоль [1,2] складається з дисперсних частинок неорганічних солей калію – K_2CO_3, KOH, KCL, які зависли у газовій суміші повітря з CO_2, N_2 та іншими газами. Полідисперсна фаза містить частинки з розмірами частинок від 0,01мкм до 0,1 мкм. Це забезпечує його високу вогнегасну ефективність у замкнених об'ємах, на відкритому просторі направленим струменем аерозолю, комбінованим застосуванням аерозолю разом з ударними хвилями на відкритому просторі та підшаровою подачею в резервуарах з горючою рідиною. Вогнегасний аерозоль можна використовувати для ефективного гасіння зазначеними способами майже всіх класів пожеж. Так, наприклад, об'ємна вогнегасна ефективність аерозолю на основі рецептури БАГР становить від 10 г/м³ до 33 г/м³ (Табл. 1).

Як бачимо з таблиці вогнегасні концентрації для більшості горючих речовин в лабораторних умовах не перевищують 26 г/м³, а в полігонних – 33 г/м³ на прикладі гептану. Для інших речовин мінімальна вогнегасна концентрація є ще меншою і становить в межах від 10 до 26 г/м³ для лабораторних умов. Так, для твердих горючих речовин вогнегасні концентрації є дещо меншими зважаючи на невелику швидкість їх згорання, оскільки горючі пари, які згоратимуть, над поверхнею ТГР утворюватимуться дещо повільніше.

Відповідно, для деревини вогнегасна концентрація становить 10-15 г/м³ для поліетилену – 12-16 г/м³, для поліетилметакрилату – 15-18 г/м³. Для горючих рідин вогнегасні концентрації є дещо вищими і, відповідно, становлять для

Таблиця 1. Вогнегасні концентрації аерозолю на основі неорганічних солей калію [1, 2, 3]

№ з/п	Клас пожежі	Вид горючої речовини	Вогнегасна концентрація аерозолю з АУС БАГР		
			Лабораторна установка, г/м³	Камера 65м³, г/м³	Направлений струмінь (вогнище), г/с
1	A Тверді горючі речовини	Деревина	10	15	-
		Поліетилен	12	16	-
		Поліметилметакрилат	15	18	-
2	B Горючі рідини	Гептан	26	33	(34в) 16,5
		Бензин А-95	21	32	(34в) 16,5
		Етанол	15	21	(5В) 15,5
3	C Горючі гази	Метан	12	16	-
		Бутан-пропан	14	19	-
4	D Горіння металів та металоорганічних сполук	Алюмінієва стружка	Флегматизування горючого середовища при концентрації від 65 г/м³		
5	F Горіння олив та жирів	Соняшникова олія	20	26	(5В) 12

н-гептану 26-33г/м³ та для етанолу – 15-21 г/м³ . Таким чином зазначені концентрації є досить невеликими порівняно з вогнегасними концентраціями порошків та газів як основних засобів об'ємного пожежогасіння.

Іншим перспективним способом застосування вогнегасного аерозолю для гасіння пожеж на об'єктах підвищеної небезпеки є його комбіноване використання разом з ударними хвилями, зокрема їх серіями в діапазоні частот від 8 до 20 Гц. Комбіноване застосування ударних хвиль із зазначеними характеристиками призводить до значного підвищення вогне-

Таблиця 2. Практичні параметри вогнегасної ефективності комбінованих ударних систем на основі ударних хвиль [4]

№ з/п	Вогнегасні компоненти	Аерозоль, г/м³	Газ, %		Рух, Па	Час підвищеної вогнегасної дії, с	Час загальної вогнегасної дії, хв	Відстань ефективної дії, L, м
			CO_2	N_2				
1	Аерозоль	25	–	–	–	–	25	–
2	Бінарна суміш аерозолю з CO_2	14	10	–	–	–	25	–
3	Бінарна суміш аерозолю з N_2	24	–	10	–	–	25	–
4	Комбінована система аерозолю з УХ	20	–	–	2500	0,5	25	4
5	Комбінована тернарна система аерозолю,CO_2 та УХ	10	7	–	2500	0,5	25	4
6	Комбінована тернарна система аерозолю, N_2 та УХ	15	–	11	2500	0,5	25	4

гасної ефективності вогнегасного аерозолю.

Авторами [4] експериментально визначено, що комбіноване застосування бінарних та тернарних систем вогнегасного аерозолю, вогнегасної газової речовини та ударних хвиль з тиском у 240 Па призводить до зменшення вогнегасних концентрацій для вогнегасного аерозолю, зокрема до 4,8 г/м^3 та до 5,8 для CO_2 , або для вогнегасного аерозолю – до 6,5 г/м^3 та до 8,2 для N_2, що є значно нижчим за їх індивідуальні значення, ймовірно, завдяки синергізму між її компонентами. Також автором встановлено, що дія серій УХ з тиском 240 Па на бінарну суміш вогнегасного аерозолю та газів призводить до ще більшого підвищення вогнегасної ефективності бінарної суміші аерозолю та газів. Вогнегасні концентрації становлять для аерозолю – 3,5 г/м^3 та для CO_2 – 2,8 %. Для бінарної суміші аерозолю та азоту ці співвідношення становлять для аерозолю до 4,1 г/м^3 та для N_2 до – 5,2 % при тиску ударної хвилі у всіх випадках в 240 Па. Значне підвищення вогнегасної ефективності можна пояснити синергізмом між компонентами комбінованих вогнегасних систем на основі ударних хвиль.

Тими ж авторами встановлено, що зазначений спосіб гасіння забезпечуватиме зменшення викиду CO_2 в 5 разів порівняно з індивідуальною вогнегасною концентрацією, та у комплексі з вогнегасними аерозолями – до 10 разів. Щодо часу гасіння пожежі, то він зменшується до декількох секунд з моменту подачі серій ударних хвиль та вогнегасних речовин, що забезпечить значне обмеження викидів в атмосферу продуктів горіння та побічних продуктів, які утворилися б при тривалішому процесі горіння та взаємодії з вогнегасними речовинами.

Також ефективним є спосіб застосування вогнегасного аерозолю для підшарового гасіння спиртів та інших рідин з низькою густиною. Так, в роботі [5] вказано, що при підшаровому гасінні вогнегасний аерозоль забезпечує високу ефективність та досить короткий час гасіння. Відповідно, в роботі [5] вказано, що вогнегасна ефективність для етанолу при підшаровому гасінні становить близько 2,3 г/с.

Таким чином при підшаровому гасінні реалізовується дія наступних чинників, які призводять до гасіння спирту після виходу аерозолю. При виході аерозолю забезпечується перемішування більш глибинних шарів рідини та зменшення температури поверхні рідини. Далі аерозоль виходить на поверхню та розбавляє зону парів та газів, де обмежує тепловий потік з зони горіння за рахунок його поглинання та розсіювання до дзеркала рідини, що відповідно, зменшує температуру її поверхні та інтенсивність її випаровування.

Крім цього в зону горіння потрапляє вже зафлегматизована аерозолем горюча суміш, яка в зоні горіння згорає з меншою швидкістю за рахунок інгібіювання ультрадисперсними частинками аерозолю ланцюгових реакцій окислення.

Таким чином сумарна дія вищеперелічених чинників забезпечує припинення горіння за досить короткий час.

Таблиця 3.Витрата вогнегасного аерозолю, що забезпечує гасіння спиртів підшаровим способом [5]

№ з/п	Вогнегасні компоненти	Аерозоль, г/м^3	Газ, %		Рух, Па	Час підвищеної вогнегасної дії, с	Час загальної вогнегасної дії, хв	Відстань ефективної дії, L, м
			CO_2	N_2				
1	Аерозоль	25	–	–	–	–	25	–
2	Бінарна суміш аерозолю з CO_2	14	10	–	–	–	25	–
3	Бінарна суміш аерозолю з N_2	24	–	10	–	–	25	–
4	Комбінована система аерозолю з УХ	20	–	–	2500	0,5	25	4
5	Комбінована тернарна система аерозолю,CO_2 та УХ	10	7	–	2500	0,5	25	4
6	Комбінована тернарна система аерозолю, N_2 та УХ	15	–	11	2500	0,5	25	4

Висновок

Таким чином необхідно зазначити, що вогнегасний аерозоль забезпечує реалізацію майже всіх хімічних та фізичних аспектів пожежогасіння, а саме: одночасне інгібіювання, флегматизування та охолодження зони горіння, що забезпечує його високу вогнегасну ефективність. Також підсумовуючи розглянуті способи використання аерозолю необхідно зазначити, що технології їх виготовлення є нескладними, експлуатаційні характеристики високими, розміри вогнегасних засобів на декілька порядків менші за порошкові аналоги, термін зберігання без обслуговування становить 10-15 років, а вогнегасна ефективність – в 2-4 рази вища за аналогічні порошкові або газові засоби пожежогасіння.

Таким чином зазначені характеристики вогнегасних засобів і систем на основі аерозольутворювальних сумішей забезпечуватимуть швидке, надійне та ефективне гасіння пожеж і попередження горіння та вибухів на об'єктах підвищеної небезпеки.

Баланюк В.М., Гарасим'юк О.І., Копистинський Ю.О., Пастухов П.В., Мірошкін В.С., Гірський О.І.
Львівський державний університет безпеки життєдіяльності

Література

1. Charles J. Kibert Solid particulate aerosol fire suppressants. Journal Fire Technology. Air Force and University of Florida. Technical science. U.S., 1994. Vol. 30, No 4. P. 387-399.

2. Баланюк В.М., Копистинський Ю.О., Лавренюк О.І., Журбинський Д.А. Перебіг окремих внутрішніх процесів у вогнегасних аерозолях під час гасіння дифузійного полум'я. Науковий вісник УкрНДІПБ. Технічні науки. Київ, 2008. №1 (17). С. 155-159.

3. Balanyuk V. M., Kozyar N. M., Garasymuyk O. I. Study of fire–extinguishing efficiency of environmentally friendly binary aerosol-nitrogen mixtures. Eastern-european journal of enterprise technologies. Technical science. Kharkiv, 2016. No3/10 (71). С. 4-12.

4. Баланюк В.М., Наукові основи зменшення впливу на довкілля пожеж на їх початковій стадії дією ударних хвиль: автореферат дис. докт. тех. наук: 21.06.02. Львів, 2019. с 45.

5. Кравченко А.В., Підшарове гасіння спиртів вогнегасним аерозолем: дис., докт., філософії: 21.06.02. Львів, 2019. с 172.

Аналіз ефективності застосування загороджувальних смуг для локалізації та гасіння пожеж у природних екосистемах

Пожежі у природних екосистемах вносять певну частку у загальну статистику пожеж, що трапляються у країні та демонструють тенденцію до щорічного зростання. До пожеж у природних екосистемах відносяться лісові, торф'яні, на відкритих територіях (ландшафтні, степові), а також пожежі на сільськогосподарських угіддях. Відповідно до статистичних даних Центру Пожежної Статистики Міжнародної Асоціації Пожежно-рятувальних служб (CTIF) [1], який аналізує стан пожеж у 23 країнах світу, щороку приблизно 17% усіх пожеж у цих країнах виникає у природних екосистемах.

Стосовно України, то слід зазначити, що у 2015 році кількість пожеж у природних екосистемах у порівнянні з 2014 роком збільшилася у 2 рази (з 12,8 тис. у 2014 році до 25,1 тис. у 2015), а їх площа на 13,8% (з 26,7 тис. га у 2014 році до 31 тис. га. у 2015) [2]. Внаслідок таких пожеж вогнем знищується унікальна флора і фауна біосферних заповідників та національних парків, господарські споруди та дачні будинки, тим самим заподіюється шкода екосистемі та завдаються матеріальні збитки державі й населенню. Світовий досвід боротьби з пожежами у природних екосистемах вказує на застосування вогнеборцями загороджувальних смуг, що створюються розпиленням водних розчинів хімічних речовин з вогнезахисними властивостями. За межі таких смуг вогонь не поширюється. В Україні наразі такий спосіб локалізації пожеж не застосовується. Натомість Правилами пожежної безпеки у лісах України [3] передбачено прокладання мінералізованих смуг із застосуванням спецтехніки для видалення наземних горючих матеріалів. Такий спосіб призначений для локалізації пожеж на об'єктах інфраструктури. Створення загороджувальних смуг з розчинів хімічних речовин може застосовуватися у місцях, де прокладання мінералізованих смуг неможливе через важкодоступність пожежі.

Тобто спосіб створення загороджувальних смуг з розчинів хімічних речовин є мобільнішим у застосуванні [3, 4].

Більшість лісових пожеж є низовими. Їхня кількість у середньому становить 97 – 98 %, а площа – близько 87 – 89 % від усіх зареєстрованих При цьому розподіл пожеж за видами суттєво залежить від регіону.

У помірному кліматичному поясі низові пожежі становлять 90 – 98 %, верхові – 1 – 10 %, ґрунтові – до 1 % [5, 6].

У сучасних системах локалізації горіння лісових масивів активно використовується група методів, серед яких можна виділити як найбільш широко застосовувану облямівку пожежі захисними мінералізованими смугами у поєднанні з охороною та гасінням, охороною кромки у поєднанні з гасінням периферії пожежі або всієї її площі та охороною кромки пожежі до періоду дощів [7-9]. У будь-якому випадку застосовують так звані бар'єрні смуги, утворені із зволоженого лісового горючого матеріалу (ЛГМ) і розташовані попереду фронтів його піролізного та полум'яного горіння, рови, смуги зі згорілого або вирубаного лісу, паркани та огороджувальні структури, що перешкоджають передачі піролізованих частинок з однієї секції до іншої, а також зменшення променистого теплового потоку, що призводить до прогріву нових шарів лісового горючого матеріалу та його інтенсивного піролізу, а також бар'єрних завіс [10]. Найбільш простим та ефективним способом локалізації лісової пожежі є створення загороджувальних смуг із зволоженого лісового горючого матеріалу перед фронтами його полум'яного горіння та піролізу. Товщина таких смуг та об'єм рідини, необхідний для зволоження матеріалу, повинні бути достатніми для зниження температури перед фронтом горіння матеріалу, запобігання доступу окислювача до зони горіння та витіснення продуктів горіння матеріалу та окислювача із зони горіння парами рідини [10].

Автори роботи [10] у дослідах показали, що для локалізації горіння листя в більшості випадків (навіть в умовах поривчастого вітру) можна обмежитися застосуванням загороджувальної смуги у вигляді шару, змоченого водою. Ширину такої смуги та об'єм води, необхідний для зволоження, можна визначити за теплотою, акумульованою в смузі, у порівнянні з теплотою, що виділяється на фронтах горіння та піролізу лісового паливного матеріалу.

Що стосується голок хвої, то потрібні спеціалізовані комбінації бар'єрних смуг, змочених рідинами різного компонентного складу. Встановлено, що найбільш ефективною (з точки зору гарантованої локалізації пожежі та мінімальної витрати рідини) є наступна комбінація смужок: розчин ОС-5 (5%), розчин бішофіту (5%). Шари хвої становлять найбільшу пожежну небезпеку, оскільки по них дуже швидко поширюються фронти піролізу та полум'яного горіння. Крім того, хвоя може переноситися повітряними потоками з однієї ділянки лісу до іншої. В результаті переважно оптимальні для хвойних лісів бар'єрні смуги та їх комбінації можуть застосовуватися і в змішаних лісах.

Найчастіше для гасіння лісових пожеж застосовуються такі методи гасіння:

- нахльостування або закидання ґрунтом крайки лісової пожежі;
- гасіння водою або розчинами хімікатів; прокладання мінералізованих смуг;
- відпал лісових горючих матеріалів або метод пуску зустрічного вогню;
- гасіння із залученням авіації; штучне викликання опадів; використання газофазних, порошкових вогнегасних речовин і пін; гасіння з використанням вибухових речовин.

Найбільш поширеним способом гасіння лісової пожежі високої інтенсивності є створення загороджувальних або мінералізованих смуг, відпалу, запущеного від опорної смуги, яка може бути створена за допомогою засипання ґрунтом або розчинами хімікатів. Опорна смуга прокладається на відстані не менше ніж 80 м від фронту пожежі. У тилу лісової пожежі і на флангах, як правило, створюється загороджувальна мінералізована смуга без етапу відпалу [11].

Підвищення ефективності боротьби з лісовими пожежами пов'язують із використанням водопінних засобів пожежогасіння, використанням компресійних і твердих пін [12], застосуванням гелеутворюючих і піноутворюючих складів, які продемонстрували високі вогнезахисні характеристики відносно лісової підстилки у попередніх роботах [12].

Відомим способом є пожежогасіння швидкотвердіючою негорючою мінеральною піною. Тверді піни виявляють гарний ізолювальний і теплозахисний ефект (низька теплопровідність). Їх застосовують для вогнезахисту під час гасіння пожежі (оперативний вогнезахист), а також наносять заздалегідь. Під дією теплового випромінювання тверді піни руйнуються тільки після повного випаровування з них вологи й подальшого займання. Установлено, що час вогнезахисної дії таких пін в основному зумовлений часом випаровування з них вологи. Поширення такі вогнегасні піни не набули через складність технології їх отримання. Є суттєві труднощі в подачі піни. Крім того, такі піноутворюючі суміші містять токсичні компоненти. Значної частини недоліків, що мають раніше розроблені швидкотвердіючі піни, позбавлені швидкотвердіючі піни на основі наночастинок кремнезему [12]. Вони містять невеликі кількості малотоксичних речовин, однак технологія їх отримання доволі складна й вимагає розробки спеціальної техніки для їх генерації.

Зараз цей засіб гасіння лісових пожеж знаходиться на стадії впровадження.

З вище перелічених способів гасіння пожеж в природних екосистемах ми бачимо, що всі ці способи за певних умов володіють, як певними перевагами так і мають свої недоліки. Тому актуальним залишається вдосконалення існуючих способів гасіння пожеж та розробка нових, в тому числі поєднання одного або декількох відомих способів для створення ефективних загороджувальних смуг. Створення загороджувальних смуг із стійкої піни [13] та вдосконалення і розробка обладнання для її подачі з метою захисту різноманітних природних екосистем від пожеж, причиною яких є займання лісу, торфу, степу, а також сільськогосподарських угідь. Створення таких загороджувальних смуг, на наш погляд, є одним із перспективних способів локалізації та гасіння пожеж в природних екосистемах.

Кирилів Я.Б.,
кандидат технічних наук,
Ковалишин В.В.,
доктор технічних наук, професор.
Львівський державний університет безпеки життєдіяльності

Література

1. World Fire Statistics. CTIF Report (Світова пожежна статистика. Звіт Міжнародної Асоціації Пожежно-рятувальних служб), 2015. – 63 р.

2. Наказ ДСНС України від 7 квітня 2016 року №168 «Про організацію заходів з протидії пожежам у природних екосистемах у 2016 році – 6 с.

3. НАПБ А.01.002-2004 Правила пожежної безпеки у лісах України – Введ. 2005-07-24. – К: Офіційний вісник України від 06.08.2007, 2005.

4. Ліхньовський Р.В., Білошицький М.В., Боровиков В.О., Жартовський С.В., Копильний М.І., Корнієнко О.В. Загороджувальні смуги як спосіб локалізації пожеж у природних екосистемах. Науковий вісник: Цивільний захист та пожежна безпека 2016. № 2(2). С. 55-59.

5. Воробьёв Ю.Л., Акимов В.А., Соколов Ю.И. Лесные пожары на территории России: состояние и проблемы. М. : ДЭКС-ПРЕСС, 2004. 312 с.

6. Effectives Loschen. Bevelkenugshytz Magazin fur Zivil und Katastrophenchuts. 2001. № 1. S. 22.

7. A. Fuentes and J. L. Consalvi, Experimental study of the burning rate of small-scale forest fuel layers, Int. J. Therm. Sci., 74, 119–125 (2013).

8. A.M. Eritsov and V.G. Gusev, Improving the technologies of creating barrier and support strips in case of quenching forest fires in areas of forest aviation operations, Vestn. Povolzhsk. Gos. Tekhnol. Univ., 1, 42–56 (2016).

9. V. Fateev, M. Agafontsev, A. Filkov, and S. Volkov, Determination of smoldering time and thermal characteristics of firebrands under laboratory conditions, Fire Safety J., 91, 791–799 (2017).

10. A. O. Zhdanova, A. V. Zakharevich, G. V. Kuznetsov, and K. O. Ponomarev, Analysis of the efficiency of combined barrier strips for localizing the burning of needles and leafage, Journal of Engineering Physics and Thermophysics, Vol. 95, No. 4, 939–944 (2022).

11. Абдурагимов И. М. Прорывные технологии пожаротушения. Лесной комплекс Сибири. 2015. № 5. С. 80 – 85.

12. Підвищення ефективності гасіння низових лісових пожеж шляхом використання бінарних вогнегасних систем з роздільним подаванням : дис. ... канд. техн. наук : 21.06.02 / Савельєв Дмитро Ігорович; Нац. ун-т цивіл. захисту України. – Х., 2020. – 170 с.

13. Сукач Р.Ю., Ковалишин В.В., Кирилів Я.Б., Войтович Д.П. Створення загороджувальних смуг вогнегасними пінами підвищеної стійкості для запобігання поширенню трав'яних пожеж. Пожежна безпека: збірник наукових праць 2022. №40. С. 84-91.

Аналіз та проблеми гасіння комбінованих пожеж за наявності легких металів чи фосфорних сполук

Горіння металів, спричинене займанням горючого пилу, надзвичайно небезпечне через можливість вибуху. При горінні металів, температура може сягати понад 2000 °С, відповідно, вода у такому випадку розкладається на водень та кисень і може утворюватися сильно вибухонебезпечний газ оксиген (вибухонебезпечні властивості оксигену), тому вода, не повинна використовуватися для гасіння. Окрім того, вода, яка контактує з горючим металом, призведе до збільшення інтенсивності горіння. До відомих горючих металів та їх сплавів відносять: цезій, літій, калій, рубідій, натрій, натрій-калій, магній, алюміній, ніобій, титан, фосфід алюмінію, гідрид алюмінію і літію, літій амід та інші [1].

Реаліями сьогодення є застосування фосфорних бомб російськими військами на території України, які є забороненими протоколами Женевської конвенції 1977 року. Фосфорні боєприпаси – зброя, яка містить білий фосфор поширює запальну дію, температура горіння якої сягає 1000°С на значній території, площа якої може досягати кількох сотень квадратних метрів.

Надзвичайно актуальною проблемою сьогодення є боротьба з пожежами, пов'язаними з горінням сполук фосфору. Небезпечні чинники фосфорних боєприпасів при детонації розповсюджуються в радіусі до кількох сотень метрів. При цьому дія сполук фосфору є подібною до напалму. Через високу температуру горіння фосфор спричиняє тяжкі та болісні каліцтва, а при вдиханні парів може випалювати легені. Також сполуки фосфорних боєприпасів здатні продовжувати горіння після вибуху [2].

Пожежі та вибухи, які виникають з причин загоряння металів та сполук фосфору, що наявні у боєприпасах, є актуальною проблемою, яку потрібно вирішувати, шляхом розроблення ефективних способів та засобів гасіння пожеж таких класів з врахуванням їх особливостей.

Звичайні протипожежні засоби, такі як водні розчини, на жаль, не можна використовувати для гасіння палаючого фосфору, оскільки ця речовина має тенденцію до швидкого повторного спалахування кожного разу, коли вона отримує доступ до повітря, наприклад, після випаровування води, яка була використана для гасіння.

Є дослідження щодо гасіння з використанням розчинів солі міді, оскільки цей реагент утворює незаймисту плівку фосфіду міді та міді поверх фосфору.

Також є ряд експериментів з гасіння фосфорних сполук з використанням мідного купоросу, розчинів солей, марганцевокислого калію, азотнокислого срібла, сірчанокислої міді.

Для попередження займання фосфору на невеликих площах землі чи предметів використовують пісок або ґрунт.

У літературних джерелах наводяться рекомендації, що для екстреного гасіння фосфорної пожежі можна застосувати розчин мила у воді, проте коли розчин висихає, фосфор стає горючим.

Для гасіння легких металів використовуються такі вогнегасні речовини:

- вогнегасний порошок для гасіння легких металів, до складу якого входить NaCI, мелений шлак з відходів металургійного виробництва, аеросил [3];
- засипання палаючого магнію великою кількістю сухого графіту;
- універсальним засобом для гасіння палаючого магнію і його сплавів є сухий мелений флюс, що вживається при плавленні магнієвих сплавів. Запас цих флюсів повинен постійно бути на робочих місцях і зберігатися в герметичній тарі. Для гасіння пожеж магнієвих сплавів при обробці різанням застосовують патрони, заряджені флюсом;
- застосування трихлориду бору для гасіння магнієвого полум'я.

Трихлорид бор взаємодіє з палаючим магнієм, утворюючи

хлорид магнію, який припиняє доступ повітря до палаючої поверхні;

• засипання палаючого магнію сухим пилоподібним карналітом або піском.

Для подавання вогнегасного порошку при гасінні легких металів застосовуються насадки-заспокоювачі. Основними вимогами до насадок-заспокоювачів для подачі вогнегасного порошку є плавне висипання вогнегасного порошку з мінімальною швидкість та проста конструкція насадки-заспокоювача, яка забезпечить надійну експлуатацію.

У методиках подавання порошку здійснюється за допомогою Г-подібної насадки, відбивання порошку відбувається від дна напівциліндра. При гасінні легких металів необхідно подавати на горючу поверхню порошок з мінімальною швидкістю, щоб він накривав поверхню, але не розкидав палаючі ошурки.

У патенті [4] запропонована насадка-заспокоювач (рисунок 1), конструкція якого складається із еліптичного днища з циліндричним корпусом та параболічним дзеркалом. Така конструкція є більш ефективною, оскільки тут значно сповільнюється рух газопорошкової суміші і, як наслідок, більша її кількість потрапляє на об'єкт гасіння.

Дослідний екземпляр цієї насадки виготовлений і проходить дослідно-експериментальні випробування. Розпочались випробування нової насадки комбінованої дії, яка може подавати вогнегасний порошок та піну.

Рисунок 1 – Дослідна насадка-заспокоювач

За результатами проведеного аналізу сучасного стану питання щодо розроблення і застосування вогнегасних порошків для гасіння пожеж класу D та сполук фосфору виявлено, що шляхами підвищення ефективності порошкового пожежогасіння в Україні є створення нових рецептур таких порошків із застосуванням вітчизняної сировинної бази, а також удосконалення технічних засобів їх подавання.

Обґрунтовано параметри, розроблено схемні рішення, розроблено та виготовлено насадку-заспокоювач порошкового вогнегасника спеціального призначення і за результатами експериментальних досліджень готуються рекомендації з гасіння комбінованих пожеж за наявності легких металів.

Ковалишин В.В.,
доктор технічних наук, професор,
Петровський В.Л.,
Веселівський Р.Б.,
кандидат технічних наук, доцент,
Марич В.М.,
кандидат технічних наук,
Ковалишин Вол.В.,
кандидат технічних наук,
Великий Н.Р.
Львівський державний університет безпеки життєдіяльності

Література

1. Ковалишин. В. В., Марич В. М., Ковалишин Вол., В. Лозинський Р. Я. Проблеми гасіння магнію та його сплавів.Пожежна безпека.2016.№28.С. 58–63;

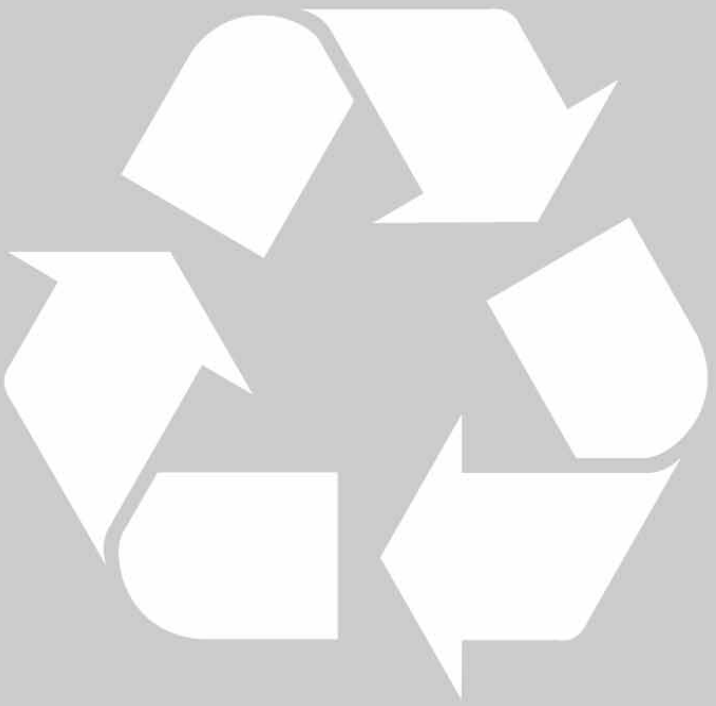
2. Фосфорні боєприпаси - перша допомога. Медична справа. URL: https://www.medsprava.com.ua/article/2480-fosforn-bopripasi-persha-dopomoga.;

3. Ковалишин В. В., Марич В. М., Ковалишин Вол. В., Гусар Б. М., Кирилів Я. В. Патент на винахід № 124876 Вогнегасний порошок для гасіння легких металів, електроустановок під напругою за наявності магнію, алюмінію та їх сплавів. Заявка а 2018 01936 26.02.2018, Опубл.: 09.12.2021 р.;

4. Ковалишин В. В., Марич В. М., Ковалишин Вол. В., Мірус О. Л., Гусар Б. М. Патент на винахід № 123702. Заспокоювач для подавання вогнегасного порошку при гасінні пожеж класу D1. Заявка а 2018 03705 06.04.2018, Опубл.: 20.05.2021 р.

plast EXPO UA

XVI Міжнародна спеціалізована виставка технологій та обладнання для переробки полімерів



27–29 травня 2025

Генеральний інформаційний партнер:

Упаковка

KYIV GLOBAL EXPO

Місце проведення:
МВЦ, м. Київ,
Броварський пр-т, 15,
станція метро «Лівобережна»

+38 (066) 921-47-51
plast@iec-expo.com.ua,
1212@iec-expo.com.ua
www.iec-expo.com.ua

НАБЛИЖАЄМО ЕНЕРГЕТИКУ МАЙБУТНЬОГО СЬОГОДНІ

XVII МІЖНАРОДНА СПЕЦІАЛІЗОВАНА ВИСТАВКА

ВІДНОВЛЮВАНОЇ ЕНЕРГЕТИКИ, ЕКОЛОГІЇ, ЕНЕРГОЕФЕКТИВНОСТІ

14–16 жовтня

EcoEnergy Expo'2025

МІЖНАРОДНИЙ ВИСТАВКОВИЙ ЦЕНТР
м. Київ, Броварський пр-т, 15
станція метро «Лівобережна»

+38 (095) 268-05-84
lyudmila@iec-expo.com.ua
www.iec-expo.com.ua

IX МІЖНАРОДНА
СПЕЦІАЛІЗОВАНА ВИСТАВКА

MINING &
MINERALS EXPO

14–16 ЖОВТНЯ 2025

ТЕХНОЛОГІЇ, ОБЛАДНАННЯ, МАТЕРІАЛИ ДЛЯ ГІРНИЧОДОБУВНОЇ ТА ВУГІЛЬНОЇ ПРОМИСЛОВОСТІ

МІЖНАРОДНИЙ ВИСТАВКОВИЙ ЦЕНТР
м. Київ, Броварський пр-т, 15
станція метро «Лівобережна»

+ 38 (066) 921-47-51
sher@iec-expo.com.ua
www.iec-expo.com.ua

VIII Міжнародна спеціалізована виставка технологій, обладнання та матеріалів для адитивного виробництва та 3D друку

Addit EXPO 3D

Актуально для 3D стоматології

27–29 травня 2025

KYIV GLOBAL EXPO

МІСЦЕ ПРОВЕДЕННЯ:
МВЦ, м. Київ,
Броварський пр-т, 15,
станція метро «Лівобережна»

☎ +38 (095) 268-05-87
✉ helen@iec-expo.com.ua
🌐 www.iec-expo.com.ua

Утилізація по-японськи

Площа Японії — лише 278 тис кв.км, тому країною освоєна й облагороджена кожна п'ядь. Зрозуміло, що нема де захоронювати сміття, тому японці розробили й успішно впровадили в життя власну філософію безвідходного існування.

Філософія раціональності

Японці здебільшого проповідують синтоїзм, суть якого — гармонійне співіснування з природою та людьми, дбайливе ставлення до речей. Синтоїсти вважають, що у багатьох предметів є своя духовна сутність — «ками». Душею наділені не тільки, наприклад, камінь, дерево, музичний інструмент, але навіть плаття, журнальний столик або глиняна тарілка. Звідси — концепція життя «моттаїнай»: «Перш ніж щось викинути, подумай, як це можна використати повторно».

Стосунки зі сміттям у японців історично розвивалися так само, як і в інших країнах. Ганчір'я, папір, дерево, метал знаходили в селянських і міських господарствах повторне застосування. Коли ж з'явилися в побуті вироби з пластика й плівки, перед Японією гостро постала проблема їх утилізації.

Особливо слід враховувати той факт, що японці — великі естети і дуже люблять упаковувати подарунки в окремі коробочки, купувати в одноразовій тарі продукти й напої. Довелося змінювати звички.

Коли сміття, що не розкладається, почало накопичуватися в геометричній прогресії, Японія на урядовому рівні ввела програму сортування твердих побутових відходів та їх максимального скорочення за допомогою зниження кількості одноразових товарів зокрема. Сьогодні всі сипучі продукти можна зважити в магазинах у полотняний мішечок і потім використовувати цю упаковку повторно. Напої часто продаються в біорозкладних пакетиках або наливаються з автомату в ємність покупця. У супермаркети японці ходять зі своїми сумками, в крайньому випадку беруть на касі паперові пакети.

Але головне завдання програми «нульових відходів» — привчити населення «на автоматі» упорядкувати побутове сміття.

Клади подібне з подібним

Сьогодні японці звично сортують сміття у своїх будинках на кілька категорій, ретельно розкладаючи його в різні пакетики й контейнери для збору вторсировини. Ось, наприклад, пляшка з-під соєвого молока. Її не можна викинути цілком. Корпус з ПЕТ (поліетилентерефталату з додаванням гліколю) складується в одне місце, пластмасовий ковпачок — в інше, плівкова етикетка відклеюється і кладеться в особливий мішечок. «Важко тільки перший місяць, — кажуть емігранти, які живуть в Японії. — Потім напрацьовується навичка, і вже починаєш отримувати задоволення від своєї свідомості, екологічної місії».

Сміття виноситься мешканцями будинків у певний час (зазвичай зранку) у прозорих пакетиках, щоб працівники сміттєвоза бачили, що лежить всередині. Зазвичай ці пакети мають різні розміри й кольорові відтінки (жовтий, рожевий, блакитний). У певний день приймається конкретний вид сміття. У різних муніципалітетах країни — різна кількість категорій для сортування. Часи збору різного виду сміття встановлюються місцевою владою. Окремо збираються метал, пластик, пляшки, ганчір'я, папір, батарейки (сольові, лужні, ртутні, срібні, літієві), старі меблі, побутова техніка, коляски, велосипеди.

Утилізація великогабаритного сміття — окрема історія. На нього наклеюється спеціальна марка, яку покупець отримує ще в магазині, в момент покупки цієї речі. Отже, в ціну вже закладено вартість її подальшої утилізації.

Екологія важливіше за прибуток

Люди старшого покоління пам'ятають «невбивані» холодильники, радіоприймачі, автомобілі, створені в 50-х роках минулого століття в різних країнах світу. Сьогодні ж техніка недовговічна: попрацює 3-5 років — і на звалище. Тому що ремонтувати її ніде не беруть, та й запчастини і вдень зі свічкою не знайдеш. Виявляється, виробники електронних пристроїв, автомобілів та іншої техніки з якогось часу навмисно скорочують термін служби виробів, щоб змусити споживача регулярно здійснювати дорогі покупки. Цей бізнес-хід називається «заплановане старіння». На збільшення прибутку працюють і підрозділи маркетингу великих корпорацій: людям пропонують придбати нову версію старого товару з додатковим функціоналом або з новим дизайном. Отже, японці в останні роки загальмували маховик наживи: зобов'язали своїх виробників почати випускати продукцію з максимально пролонгованим терміном експлуатації.

Сьогодні 75% населення країни Висхідного Сонця вважають за краще купувати товари багаторазового використання, що дозволило значно скоротити кількість відходів і активізувати рециклінг.

Зламану, або таку, яка не піддається ремонту, побутову техніку, електронну апаратуру (телевізори, плеєри, комп'ютери, планшети) у Японії забирають у населення спеціальні утилізатори (не звичайне «звалище») на завод, який здійснює рециклінг таких предметів. Там їх розберуть на дрібні складові (більше 100 найменувань) і вирішать, як далі бути з пластиковим корпусом, дротами, гумовими компонентами, склом і мікросхемами.

Якщо ж під час покупки побутової техніки людина заздалегідь оплатила в магазині вартість її утилізації, вона наклеює на побутовий непотріб спеціальний ярлик і залишає його біля сміттєвих баків: у цьому випадку працівники сміттєвоза самі здадуть викинуту техніку на переробку.

Спроба «по-партизанськи» викинути великогабаритний мотлох на вулицю загрожує штрафом у кілька тисяч ієн.

Для гостей країни — свої правила

На вулицях Японії теж впроваджено сортування сміття. У всіх містах стоять різнокольорові контейнери, які збирають відходи чотирьох категорій:

- які неможливо спалити;
- які можуть бути спалені;
- ті, що переробляються;
- великогабаритні.

На контейнерах намальовано піктограми, дохідливо зображено види вторсировини, для збирання яких вони призначені. Причому контейнери влаштовані так, що залізні банки з-під пива та напоїв можна викинути тільки в контейнер з відповідним круглим сміттєприймачем; для пакетів «тетрапак» і пластика — свій контейнер, для скляної тари — свій. Упаковку від йогурту доведеться розділити на дві частини: пластикову соломинку і кришку викинути в один контейнер, а паперовий стаканчик — в інший.

Сучасний спосіб спалювання відходів

У розряд спалюваних відходів потрапляють не тільки картон, папір, ганчірки, але ще багато іншого брухту, якому не знайшлося іншого застосування. У більшості країн спалювання ТПВ вважається неекологічним, оскільки сміттєспалювальні заводи виділяють в атмосферу багато канцерогенних продуктів згоряння. Але дві країни є винятком з цього правила: Японія і США, оскільки в цих державах застосовується найсучасніша технологія утилізації — плазмова газифікація. У цей спосіб відходи в лічені секунди спалюються потужним потоком плазми з температурою вище 1200 С^(о). У результаті смоли й випаровування в плазмовій камері не утворюються, в атмосферу нічого не викидається, а від 15 тонн сміття залишається всього 3 тонни шлаку, який теж не викидається, а очищається й потім використовується в будівництві. Попіл спресовують у великі щільні брикети, які йдуть в основу фундаментів висотних будівель. А ще з цих брикетів роблять насипні острови, де будують виробництва, аеропорти й елітні житлові квартали. Найвідоміший з таких проектів — острів Одайба в Токійській затоці, на якому розташований парк розваг «Леголенд».

Плазмові сміттєспалювальні заводи виділяють багато енергії, яка йде в міські електромережі. Виробництво вважається повністю безпечним, тому знаходиться, як правило, в межах міста. На завод приводять екскурсантів: школярів та туристів. А сміттєспалювальний завод «Maishima Incineration Plan» («Майсіма») в місті Осака оточений розкішним парком і виглядає ну зовсім як арт-об'єкт, шедевр промислової архітектури. Він був побудований в 1997-2001 роках за проектом великого віденського художника Фріденсрайха Гундертвассера. Будівля виглядає дуже незвично всередині і зовні, нагадує казковий замок. При ньому функціонує музей, центр реабілітації інвалідів, готель і ресторан.

Наталія Смирнова
для **vtorma.ua**

Компанія «ВТОРМА» працює на ринку України з 2003 року. Ми закуповуємо, сортуємо і продаємо виробникам вторсировину, а також самостійно переробляємо різні відходи виробництва без шкоди для екології.

Місія компанії — збереження навколишнього середовища й природних ресурсів країни за рахунок правильної переробки відходів.

Щорічно у «ВТОРМА» зростає географія впливу: вже діють філії в декількох містах України: Бровари, Біла Церква, Чернігів, Ніжин, Прилуки, Львів, Миколаїв.

19-21 БЕРЕЗНЯ 2025

INTER BUILD EXPO

ІНТЕРБІЛДЕКСПО

МІЖНАРОДНА БУДІВЕЛЬНА ВИСТАВКА

Місце проведення:

МІЖНАРОДНИЙ ВИСТАВКОВИЙ ЦЕНТР

Київ, Броварський пр-т, 15
(метро Лівобережна)

ВІДБУДУЄМО РАЗОМ!

АВІТОН

Проектування, монтаж, технічне обслуговування засобів протипожежного захисту та систем опалення, оцінка протипожежного стану о'бєктів, а саме:

- Проектування установок пожежогасіння (водяне, пінне, газове, порошкове, аерозольне), пожежної сигналізації, систем протидимного захисту, оповіщення та управління евакуацією людей при пожежі, пожежного спостереження, пристроїв для захисту будинків і споруд від розрядів блискавки та вогнезахисту конструкцій.
- Монтаж, технічне обслуговування установок пожежогасіння (водяне, пінне, газове, порошкове, аерозольне).
- Монтаж, технічне обслуговування установок пожежної сигналізації.
- Монтаж, технічне обслуговування систем оповіщення та управління евакуацією людей при пожежі.
- Монтаж, технічне обслуговування систем пожежного спостереження.
- Спостереження за установками пожежної автоматики о'бєктів.
- Монтаж, технічне обслуговування пристроїв для захисту будинків і споруд від розрядів блискавки.
- Вогнезахисна обробка деревини (поверхнева) та тканин.
- Захист вогнезахисними матеріалами металевих, залізобетонних та інших конструкцій.
- Оцінка протипожежного стану о'бєктів.
- Технічні засоби безпеки всіх видів (охорона, відеонагляд, системи контролю доступом).
- Автоматика будинків та споруд в комплексі.
- Супровід підприємств для отримання дозвільних документів, при перевірках та будівництві, розробка інструкцій, ІТЗ ЦЗ, ПЛАС.
- Електротехнічна лабораторія до 1000 В.

ТОВ «АВІТОН»
08304, Київська обл., м. Бориспіль,
вул. Привокзальна, 50,
т/факс (04595)7-23-48, т. (04595)7-24-69,
моб. (066)136-36-41, (068)128-35-67,
e-mail: aviton.ua@ukr.net, www.aviton.com.ua

Ліц. Серія АЕ №184191 від 21 грудня 2012 р. ДІПБ МНС України