Бізнес і безпека

Бізнес і безпека

№ 1/2025 (160)

ISSN 1819-9429

40226 - передплатний індекс в Укрпошті

www.bsm.com.ua

- ДРОНІЗАЦІЯ В УКРАЇНІ - БЛОКЧЕЙН У ПИТАННЯХ ТА ВІДПОВІДЯХ - ЧИ БЕЗПЕЧНИЙ ЕЛЕКТРОТРАНСПОРТ ДЛЯ ЛЮДИНИ? - СТАНДАРТИ З КІБЕРБЕЗПЕКИ ДЛЯ РОЗУМНИХ МЕРЕЖ - ПРОТИРАДІАЦІЙНІ УКРИТТЯ - - ЧИМ НЕБЕЗПЕЧНИЙ МАЗУТ ДЛЯ ЛЮДИНИ? - МАГНІТНІ ГРАБЛІ МГ-2 - НАЙПОПУЛЯРНІШІ КАМЕРИ ВІДЕОСПОСТЕРЕЖЕННЯ 2024 РОКУ - АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ - - ЯК ВИЯВИТИ ШПИГУНСЬКЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НА СМАРТФОНІ - ЗАХИСНІ СПОРУДИ - - ВИХОВАННЯ ДОБРОЧЕСНОСТІ ТА БОРОТЬБА З КОРУПЦІЄЮ В ОБОРОННОМУ СЕКТОРІ -

BUNKER-OK

УКРИТТЯ Й КОМЕРЦІЙНІ ПРОДУКТИ БЕЗПЕКИ

bunker-ok.com.ua

Компанія «БУНКЕР-ОК» є виробником надійних захисних укриттів. Тепер у Вас з'явився унікальний шанс придбати укриття без зайвих націнок та тривалих пошуків. Ми виготовляємо укриття за всіма вимогами та стандартами: ДСТУ Б (В.2.6-2:2009), ДСТУ-Н Б (А.3.1-34:2016), ДСТУ Б (В.2.6-168:2011), та іншими. Надійність укриттів доведена полігонними випробуваннями.

Переваги наших укриттів:

- Мобільність
- Висока стійкість та надійність
- Автономне життєзабезпечення
- Модульність
- Швидкий монтаж і демонтаж
- Компактність та естетика

Ідея розробки та **створення мобільних укриттів** зародилася на фронті **серед військових ЗСУ**. Більша частина поранень в бою, в міських умовах, це кулеві та осколкові ураження від **боєприпасів та уламків зруйнованих будівель**.

Методом випробувань та багатьох консультацій з фахівцями, було знайдено та вирахувано: оптимальні форми, склад матеріалів та наповнення укриттів, які **дозволять зберегти життя нашим побратимам та цивільному населенню**.

До розробки проєкту долучився доктор технічних наук «Заслужений діяч науки і техніки України», завідувач кафедри залізобетонних конструкцій та транспортних споруд Одеської Державної Академії Будівництва та Архітектури - **Євген Клименко зі своєю командою**.

Контакти для консультації та замовлення: тел. +380 (93) 856 34 63, Email: info@bunker-ok.com.ua

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

ТОВ «Пайрокул» – прогресивна, іноваційна компанія, представлена на ринку протипожежного захисту України вже більше 10 років.

Ствол пожежний ручний комбінований RamboJet

Повна назва: Ручний комбінований пожежний ствол POK RamboJet

Ствол пожежний ручний комбінований RamboJet з регулюванням витрати призначено для формування і подавання компактного або розпиленого (із змінним кутом факела) струменя води, а також, у разі встановлення твердого картриджа PYROCOOL TS в трубку ствола, розчину поверхнево-активної речовини (ПАР).

Ствол пожежний ручний комбінований RamboJet застосовується для гасіння лісових пожеж та полів, сипких матеріалів (вугілля, вугільний пил, зерно, борошно тощо), соломи, текстильних матеріалів або паперу, під час гасіння яких необхідна саме змочувальна дія. Його призначено також для гасіння пожеж у квартирах або автомобілях, де велика кількість води через завдання значних збитків є небажаним.

Найсуттєвішою перевагою під час використання пожежного ствола Rambojet 01 з твердим картриджем PYROCOOL TS є зменшення витрати води як мінімум на 50 %.

Вода, що проходить через трубку ствола, омиває поверхню картриджа та вимиває з нього змочувальник. Отримана суміш води і змочувальника має істотно нижчий поверхневий натяг у порівнянні з чистою водою. Завдяки цьому досягається значне підвищення здатності проникнення вогнегасної суміші в палаючий твердий матеріал.

Характеристики:

- **Габаритні розміри (ДхВхШ), мм: . . . . . .572 х 242 х 110**
- **Вага, кг: 2,85**
- **Пропускна здатність (витрата) за тиску 6 бар, л/хв: 250**
- **Кут розпилювання струменя (за 0,5 МПа):**
  Суцільний струмень, розпилений у діапазоні . . . . . .від 30˚ до 130 ˚
- **Приблизна кратність піни: . . . . . .Змочувальний розчин**
- **Виробник: . . . . . .POK (Франція)**
- **Гарантія: . . . . . .12 місяців**

вул. Князя Романа Мстиславича, 18-163, Київ, 02192
+380 (44) 543-89-70, +380 (95) 571-13-98, pyrocool101@gmail.com, pyrocool.uk@gmail.com

МОВЛЕННЯ ТЕРИТОРІАЛЬНИХ ГРОМАД

Місцеве радіомовлення, перш за все – мовлення територіальних громад заловольняє потреби населення в доступі до локального інформаційного контенту та забезпечує оперативне інформування про надзвичайні ситуації

+38 056 790 05 79
+38 056 790 05 80
office@ozons.com.ua
director@ozons.com.ua
www.ozons.com.ua

OZON S ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ОРГАНІЗАЦІЇ МОВЛЕННЯ ТЕРИТОРІАЛЬНИХ ГРОМАД

БЛОК ОПОВІЩЕННЯ B0-FM-06 З ВБУДОВАНИМ МАЛОПОТУЖНИМ РАДІОПЕРЕДАВАЧЕМ

Забезпечує трансляцію контенту місцевої студії, а також контенту НСТУ та інших радіомовників. За командою з автоматизованого робочого місця (АРМ) місцевої (МАСЦО) або територіальної автоматизованої системи центрального оповіщення (ТАСЦО) переключається на трансляцію екстрених повідомлень.

СИГНАЛЬНО-ГУЧНОМОВНІ ПРИСТРОЇ З АВТОНОМНИМ ЕЛЕКТРОЖИВЛЕННЯМ

Забезпечує радіофікацію місць з масовим перебуванням людей При отриманні команди на оповіщення про надзвичайну ситуацію у будь-який час включається на повну потужність.

СПЕЦІАЛІЗОВАНІ ПРИЙМАЧІ ЕФІРНОГО РАДІОМОВЛЕННЯ

Забезпечує оповіщення всередині приміщень з трансляцією інформаційних мовних повідомлень через динамік. При отриманні команди включається незалежно від налаштування користувача на повну гучність. Має індикацію пропущених повідомлень.

ПРИЗНАЧЕННЯ СИСТЕМИ

- ТРАНСЛЮВАННЯ МІСЦЕВОГО КОНТЕНТУ
- ВИКОРИСТАННЯ КОНТЕНТУ НСТУ, ІНШИХ РАДІОМОВНИКІВ
- ІНТЕГРАЦІЯ В ТЕРИТОРІАЛЬНУ СИСТЕМУ СПОВІЩЕННЯ

АЛГОРИТМ РОБОТИ СИСТЕМИ

МОЖЛИВОСТІ СИСТЕМИ

Мовлення громад стимулює розвиток громадянського суспільства: ініціює публічні дискусії щодо місцевих проблем, підвищує компетенцію громадськості щодо питань місцевого самоврядування, сприяє процесу децентралізації, ефективному захисту прав і свобод громадян, сприяє інформаційній безпеці держави.

Окрім керування сигнально-гучномовними пристроями система мовлення може використовуватися для надання різноманітної інформаційно-розважальної інформації для населення, зокрема: новин, звітів про діяльність місцевих органів влади, комерційної реклами, привітань, оповіщення про важливі події місцевого рівня, а також популяризації національних ідей.

НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ МОВЛЕННЯ ТЕРИТОРІАЛЬНИХ ГРОМАД

Мовлення територіальних громад здійснюється аудіовізуальними засобами масової інформації територіальних громад, які функціонують у порядку та на умовах, встановлених ЗАКОНАМИ УКРАЇНИ:

«Про засади діяльності мовлення територіальних громад в Україні»
«Про телебачення і радіомовлення»
«Про інформацію»

ІНСТРУКЦІЄЮ НАЦІОНАЛЬНОЇ РАДИ УКРАЇНИ З ПИТАНЬ ТЕЛЕБАЧЕННІ І РАДІОМОВЛЕННЯ

«Організація місцевого радіомовлення, мовлення територіальних громад»
та ін. нормативно-правовими актами.

НВП «OZON S»

ПРОПОНУЄ НАСТУПНІ РІШЕННЯ ДЛЯ ТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ ТА ВПРОВАДЖЕННЯ СИСТЕМИ МОВЛЕННЯ ТЕРИТОРІАЛЬНИХ ГРОМАД

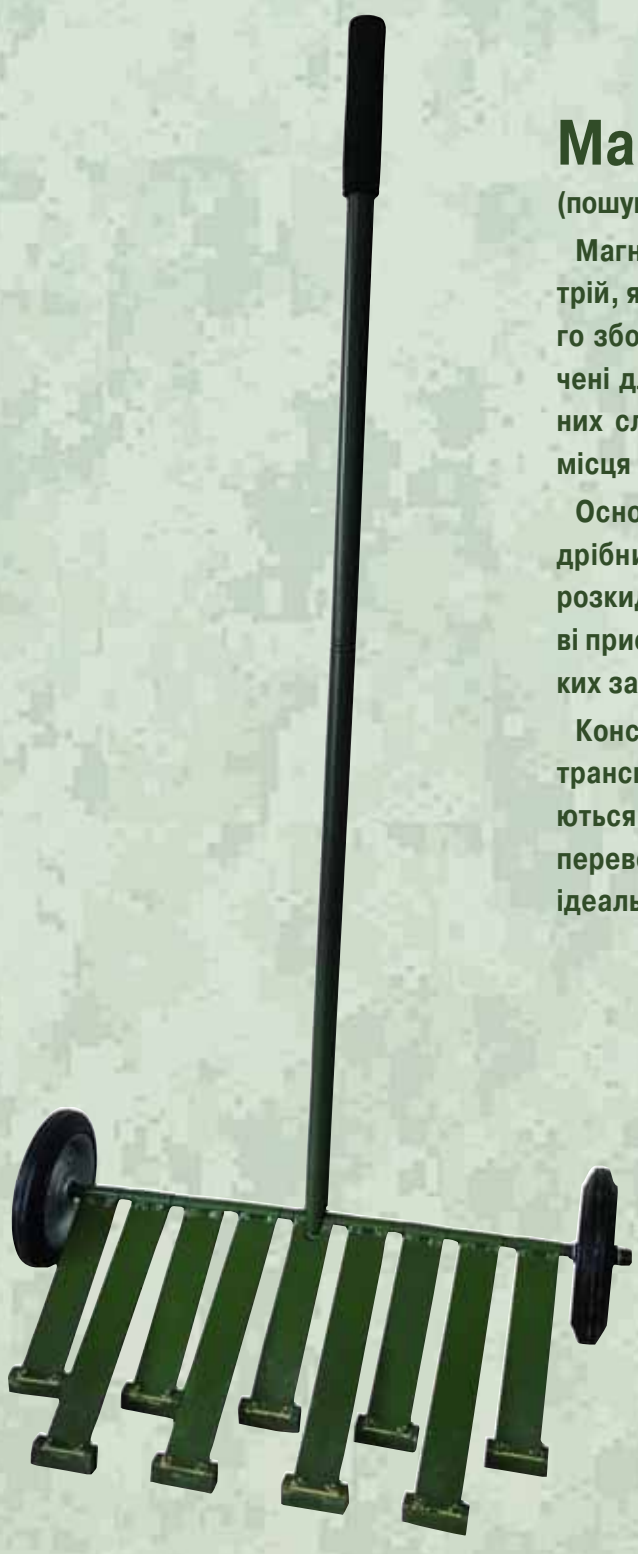
1. ПАКЕТ «ІНДИВІДУАЛЬНИЙ»

2. ПАКЕТ «СУСПІЛЬНИЙ»

3. ПАКЕТ «ПОВНЕ ПОКРИТТЯ»

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

Бізнес і безпека

№ 1/2025 (160)

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

Видається з 10 квітня 1996 року.

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 № 21 від 07.12.2025 р.

Друк офсетний.
Папір крейдований.
Формат 60 х 84 1/8.
Обсяг 10 ум. др. стор.
Підписано до друку 07.02.2025 р.
Наклад 12 000 екз.
Передплатний індекс – 40226.
Періодичність: 6 на рік.
Ціна договірна.
м. Київ – 2025

☆ ☆ ☆

ISSN 1819-9429

АКТУАЛЬНО

НОВИНИ 2-14
Тенденції дронізації в Україні на сучасному етапі 17
Блокчейн у питаннях та відповідях 21
Ідея створення легкого штурмового літака 27
Чи безпечний електротранспорт для людини? 29
Стандарти з кібербезпеки для розумних мереж – системний аналіз 35

ФІЗИЧНИЙ ЗАХИСТ. ОХОРОНА. ЦИВІЛЬНИЙ ЗАХИСТ. ТЕХНІЧНІ ЗАСОБИ БЕЗПЕКИ

Група компаній ALD ENGINEERING COMPANY надійний партнер у будівельній галузі 47
BunkerOK: Захищений простір для бізнесу та суспільства 48
ПРУ (протирадіаційне укриття) – обов'язкове для встановлення на підприємствах критичної інфраструктури 50
Чим небезпечний мазут для людини, водойм та ґрунту? Чи завжди є небезпечним вантажем? 52
Забутий елемент: екран протипилового фільтра в сховищах і ПРУ з електроручними вентиляторами 53
Найпопулярніші камери відеоспостереження 2024 року 54
Апаратне забезпечення інформаційної безпеки держави 60
Впровадження автоматизованих систем централізованого оповіщення територіальних громад 70

ПОРАДИ

Виховання доброчесності та боротьба з корупцією в оборонному секторі 75

Axis представляє новий чип наступного покоління ARTPEC-9

Axis Communications щойно представила ARTPEC-9 — чип наступного покоління, який революціонізує захоплення зображень, підсилює штучний інтелект (ШІ) та посилює кібербезпеку. ARTPEC-9 є першим системним чипом (SoC) від Axis, який підтримує AV1, що покращує ефективність передавання даних та знижує витрати на зберігання без втрати якості.

Цей новий чип покращує та оптимізує характеристики, які були ключовими в попередніх версіях, такі як надзвичайно низька бітрейт, розширена аналітика на основі ШІ, висока якість зображень та посилена кібербезпека.

Однією з найважливіших інновацій ARTPEC-9 є підтримка стандарту відеокодування AV1, розробленого Alliance for Open Media (AOM). Це перший випадок, коли цей стандарт інтегровано в системи мережевого відеозапису. Разом із технологією стиснення Axis Zipstream, використання AV1 дозволяє знизити витрати на зберігання, не порушуючи якість деталей запису.

«Завдяки піонерській підтримці стандарту AV1, ARTPEC-9 забезпечує відмінну бітрейт та кращу сумісність із клієнтами, що є великим кроком вперед для галузі», — заявив Йохан Паулссон, технічний директор Axis Communications.

«Ключові слова тут — «легкий доступ» і «відкритість», концепції, які ідеально відповідають нашому підходу до виконання обіцянки інновацій для створення розумнішого та безпечнішого світу. Крім того, як і всі наші SoC, ARTPEC-9 спеціально розроблений для забезпечення високоякісного мережевого відеозахоплення. Як завжди, ми зберігаємо повний контроль над усім процесом виробництва SoC».

ARTPEC-9 використовує ключові технології, які дозволяють Axis забезпечувати обробку зображень у складних умовах освітлення. Ці технології включають Axis Lightfinder та Axis Forensic Wide Dynamic Range (WDR), які є основоположними для технології Axis Scene Intelligence, що використовує алгоритми, навчені в реальних умовах, для надання метаданих.

Ця комбінація покращує продуктивність аналітичних додатків, забезпечуючи більш точні та надійні результати. Таким чином, рішення Axis пропонують високорівневу аналітику, швидкий та точний криміналістичний пошук і значно зменшують кількість помилкових тривог, навіть у складних сценаріях спостереження.

З ARTPEC-9 та десятилітнім досвідом Axis у обробці зображень, команди з безпеки можуть бути впевнені, що отримають надійні та високоякісні результати в будь-яких умовах.

Кібербезпека є основним елементом дизайну ARTPEC-9. Завдяки функціям, таким як безпечне завантаження та цифрово сертифікована операційна система, чип гарантує, що кожен пристрій захищений від кіберзагроз, запобігаючи використанню неавторизованого або підробленого програмного забезпечення.

Крім того, оскільки його дизайн розроблений внутрішньо, Axis зберігає повний контроль над процесом виробництва. Це мінімізує ризики, пов'язані з третіми сторонами, та підвищує загальну безпеку пристрою від виробництва до впровадження.

За словами компанії, ARTPEC-9 підвищує рівень аналітики на основі ШІ, пропонуючи більш просунуту продуктивність та точніші можливості виявлення. Це означає, що аналітика може ідентифікувати менші об'єкти та втручатися раніше, щоб забезпечити дієву інформацію для цілей безпеки, захисту та операційних потреб. Ці можливості не лише підвищують операційну ефективність, але й зменшують кількість помилкових тривог та оптимізують прийняття рішень на основі даних, навіть у складних умовах спостереження.

Axis інтегрує AV1 — відкритий стандарт наступного покоління для відеокодування, розроблений для революціонування мультимедійної передачі в галузі спостереження. Завдяки цій сумісності з AV1 та просунутої обробки зображень, чип ARTPEC-9 забезпечує високоякісне відео з винятковою деталізацією та чіткістю, встановлюючи новий стандарт ефективності бітрейт.

У поєднанні з технологією стиснення Axis Zipstream, AV1 забезпечує плавні та ефективні відеопотоки, як на місці, так і в хмарі. AV1 наразі сумісний із AXIS Camera Station та провідними постачальниками рішень для управління відео (VMS), такими як Genetec та Milestone, які працюють над підтримкою цієї технології, з подальшими інтеграціями, запланованими на майбутнє.

Axis також представила свої нові камери AXIS Q1728 та AXIS Q1728-LE, розроблені для максимального використання можливостей процесора ARTPEC-9. Вони будуть доступні через канали розповсюдження Axis у першому кварталі 2025 року. Обидві камери пропонують роздільну здатність 4K при 60 кадрах за секунду та високочутливі світлові сенсори 1/1.2", що ідеально підходить для різноманітних умов спостереження.

AXIS Q1728 має модульний дизайн, сумісний із різними захисними корпусами, тоді як AXIS Q1728-LE спеціально розроблена для зовнішнього використання, з інтегрованою системою очищення та підігріваним переднім склом з використанням нанотрубок вуглецю. Обидві моделі доступні з ширококутними (6-13 мм) або телеоб'єктивними (15-48 мм) лінзами, що дозволяє обрати ідеальну конфігурацію відповідно до потреб моніторингу.

★

Еволюція гуманоїдних роботів в автоматизації: приклад Optimus від Tesla

Гуманоїдні роботи вже багато років захоплюють нашу уяву, еволюціонуючи від фантазій наукової фантастики до реальних інновацій. Яскравим прикладом того, як технології змінюють автоматизацію, є робот Optimus від Tesla. Коли мова йде про автоматизацію завдань, що є занадто небезпечними або монотонними для людей, робот Optimus може стати вирішенням проблеми дефіциту робочої сили для багатьох компаній. Ця стаття фокусується на тому, як Optimus має змінити індустрії, зокрема у виробництві та логістиці, через виконання монотонних завдань. Також буде розглянуто потенційне застосування робота в інших секторах.

Візія Tesla щодо Optimus

Презентуючи гуманоїдного робота Optimus на своєму заході AI Day у 2021 році, компанія Tesla (в основному відома своїми електричними автомобілями) увійшла на ринок робототехніки. Генеральний директор компанії Ілон Маск стверджує, що Optimus прагне виконувати «завдання, які є нудними, небезпечними та повторюваними». Хоча ці завдання є важливими для промислових процесів, вони часто призводять до травм та фізичного напруження на працівників на робочому місці.

Optimus має зріст 5 футів 8 дюймів (близько 173 см), вагає 125 фунтів (приблизно 57 кг) і може піднімати 45 фунтів (близько 20 кг). Технологія Full-Self Driving (FSD) від Tesla дозволяє роботу автономно орієнтуватися в навколишньому середовищі, приймати рішення в реальному часі та навчатися новим навичкам, спостерігаючи за оточенням. Завдяки цим здібностям, Optimus може стати універсальним помічником у будь-якому середовищі, вклю-

чаючи підприємства, домівки, склади та інші місця, де збираються люди.

Обробка монотонних та повторюваних завдань

Здатність Optimus виконувати монотонні завдання з точністю та ефективністю є однією з його сильних сторін, і це може радикально змінити галузі, що залежать від людської праці. Наприклад, Optimus може використовуватися в виробництві для управління повторюваними операціями на конвеєрних лініях, такими як транспортування матеріалів, підйом компонентів і закручування гвинтів. Хоча ці завдання не потребують складних рішень, виробництво залежить від них, і вони вимагають постійності та витривалості — якраз тих якостей, в яких робот Optimus має перевагу. Автоматизуючи ці завдання, компанії можуть знизити ризик людських помилок, підвищити продуктивність і поліпшити якість продукції.

Optimus також може автоматично керувати контролем запасів, сортуванням пакунків і переміщенням товарів на складах, тим самим підвищуючи ефективність логістики. У ситуаціях, де точність і швидкість мають вирішальне значення, роботи, які можуть регулярно виконувати свої завдання без втоми, очевидно мають перевагу. Це надзвичайно важливо в таких галузях, як електронна комерція, де клієнти вимагають швидкої доставки, або під час пікових навантажень. Якщо компанії наймуть Optimus для виконання фізично важких завдань, людські працівники зможуть зосередитися на більш складних і важливих завданнях.

Підвищення безпеки та зменшення дефіциту робочої сили

Використання Optimus та подібних роботів має переваги в поліпшенні безпеки в промислових умовах. Серед повсякденних небезпек, з якими стикаються промислові працівники, — це високі температури, важке обладнання або контакти з небезпечними матеріалами. Ці завдання є надзвичайно небезпечними для людей, але роботи можуть виконувати їх без будь-якого ризику. Завдяки своїй людській маневреності та автономним здібностям, Optimus може брати на себе ці обов'язки, знижуючи потребу в присутності людини в небезпечних умовах і зменшуючи ризик нещасних випадків на виробництві.

Особливо в таких галузях, як виробництво і логістика, де робочі місця, що потребують значних фізичних зусиль, інколи важко заповнити, роботи, такі як Optimus, також допомагають у вирішенні проблеми нестачі кадрів. Компанії шукають роботів як потенційне вирішення проблеми з пошуком та утриманням кваліфікованих працівників у конкурентному ринку праці. Optimus може бути використаний для небезпечних або повторюваних завдань, звільняючи людей для професій, які потребують винахідливості, творчості та здатності вирішувати проблеми. Завдяки цьому зросте рівень задоволення від роботи, а ефективність операцій поліпшиться, оскільки співробітники зможуть зосередитися на більш цікавих проектах, а не на рутинних завданнях.

Потенційні майбутні застосування в різних галузях

Хоча спочатку Optimus був розроблений для промислового використання, у нього є багато інших потенційних застосувань поза виробництвом та логістикою. Деякі майбутні споживачі робота, в залежності від того, як буде розвиватися технологія, можуть належати до сфер послуг та охорони здоров'я. Наприклад, гуманоїдні роботи можуть допомагати в догляді за пацієнтами в медичній сфері, забезпечуючи доставку ліків, моніторинг життєвих показників і транспортування обладнання. Ці інструменти не лише спрощують медичні процедури, але й звільняють час лікарів та медсестер, щоб вони могли зосередитися на кожному пацієнті окремо.

Серед робіт у сфері послуг, які Optimus та подібні роботи можуть виконувати, є обслуговування клієнтів, управління готелями та навіть приготування їжі. Роботи, які можуть спілкуватися з людьми і виконувати різноманітні завдання, можуть бути надзвичайно корисними для осіб у багатьох різних галузях, оскільки компанії прагнуть автоматизувати все більше процесів для покращення обслуговування клієнтів.

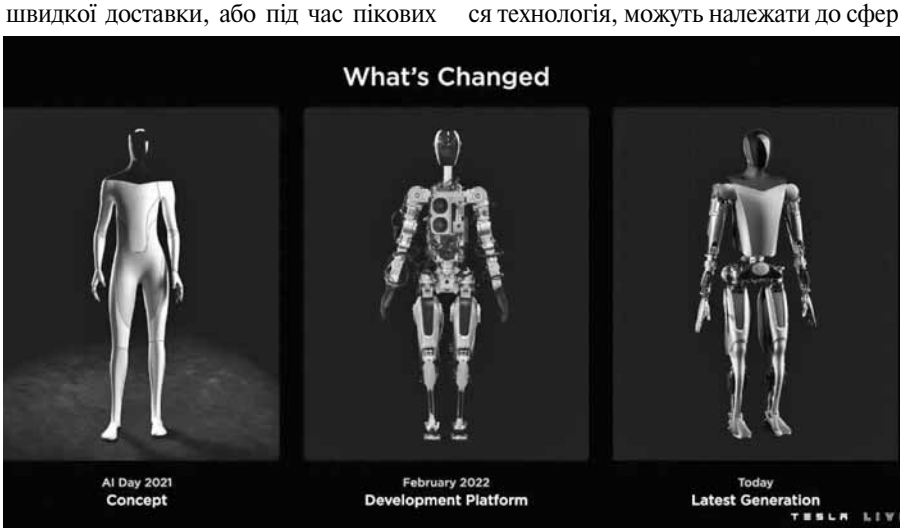
Проблеми та етичні дилеми

Хоча гуманоїдні роботи, такі як Optimus, мають багато переваг, існують також етичні питання та проблеми, які потребують вирішення. Можливість втрати робочих місць через виконання роботами роботи, яка раніше була доступна тільки людям, викликає серйозні питання. Автоматизація несе ризик втрати робочих місць у секторах, що здебільшого залежать від людської праці, хоча вона має здатність знижувати витрати та підвищувати продуктивність. Якщо люди, яких звільняють через автоматизацію, повинні знайти нову роботу, уряди, бізнеси та суспільство загалом мають оплатити переучування та перенавчання робочої сили.

Крім того, наявність роботів у багатьох промислових середовищах, особливо тих, що вимагають співпраці людей і роботів, викликає питання безпеки. Хоча Optimus має сенсори та систему прийняття рішень на основі штучного інтелекту, дизайн Tesla підкреслює, що безпечна взаємодія між людиною та роботом залежить від ретельного тестування та постійного вдосконалення, навіть якщо Optimus оснащений кількома засобами безпеки. Оскільки гуманоїдні роботи стають все більш поширеними, важливо приділяти велику увагу етичним питанням автономії роботів, конфіденційності даних і можливому зловживанню.

Майбутнє гуманоїдних роботів в автоматизації

Експоненціальний розвиток технологій, здається, сприяє зростанню застосування гуманоїдних роботів в автоматизованих процесах. Для Ілона Маска бачення Optimus виходить за межі складів чи виробничих приміщень, оскільки він уявляє майбутнє, де «фізична праця стане вибором». Optimus та інші подібні роботи можуть врешті-решт виконувати більшість ручних робіт, дозволяючи людям зосередитися на інтелектуальних, творчих та міжособистісних заняттях.



Хоча до досягнення цього бачення ще далеко, Optimus є великим кроком до майбутнього, коли люди та роботи співпрацюватимуть для підвищення ефективності та продуктивності.

Серед багатьох інших можливих переваг для компаній, гуманоїдні роботи можуть значно підвищити операційну ефективність, допомогти подолати дефіцит робочої сили та покращити безпеку на робочих місцях. Більш розвинуті роботи змінять не лише наші способи роботи, а й цілі галузі. Як і з будь-якими новаторськими інноваціями, ми повинні ретельно зважити етичні, соціальні та економічні наслідки цієї технології, щоб забезпечити вигоду для всіх від автоматизації і підтримку людей, коли ми рухатимемося до більш автоматизованого майбутнього.

Висновок

Tesla's Optimus представляє новий рубіж у розвитку гуманоїдних роботів в автоматизації. Його здатність виконувати повторювані та монотонні завдання може революціонізувати галузі, підвищуючи їх продуктивність, безпеку та здатність вирішувати проблему нестачі робочої сили. Хоча майбутнє гуманоїдних роботів ще невизначене, введення Optimus знаменує нову еру в автоматизації, коли люди та роботи можуть співпрацювати для досягнення більш високих рівнів продуктивності та інновацій. Роботи, як Optimus, матимуть все більший вплив на природу праці, оскільки більше секторів розглядають перспективи автоматизації. ★

Eurocontrol впроваджує цифрову платформу для управління повітряним рухом у публічному хмарному середовищі

EUROCONTROL, міжнародна цивільно-військова організація, яка підтримує європейську авіацію та відповідає за управління мережею повітряного руху в Європі, успішно впровадила першу цифрову платформу для управління повітряним рухом у публічному хмарному середовищі, розроблену компанією Indra за підтримки ATOS і Microsoft. Цей крок є частиною програми інтегрованого управління мережею (iNM) та сприяє цифровізації систем, що керують мережею європейської авіації.

Це рішення є важливим етапом у галузі управління повітряним рухом, оскільки його можна інтегрувати в публічну хмару або, за необхідності, в приватну інфраструктуру, що дозволяє всім учасникам процесу більш гнучко управляти трафіком, отримувати критичні дані в реальному часі та забезпечувати вищу операційну стійкість.

Indra інтегрувала передові рівні кібербезпеки у всю технічну реалізацію і застосувала найвищі стандарти безпеки в публічній хмарі Microsoft Azure для захисту всіх даних, що обробляються системою, а також для посилення безпеки операцій у такій критичній сфері, як повітряний рух. З іншого боку, розробка цифрової платформи Indra в публічній хмарній інфраструктурі створює основи для майбутніх розробок в управлінні повітряним рухом, які будуть незалежні від різних апаратних інфраструктур, що їх підтримують, знижуючи витрати на фізичні середовища.

Цифрова платформа, розроблена компанією Indra, також прийматиме першу версію найбільшої в світі авіаційної інформаційної системи – eEAD (електронна європейська база даних AIS), яка централізує глобальні дані високої якості в єдиній базі даних з покращеними можливостями порівняно з поточною.

Завдяки розвитку компанії EUROCONTROL вдалося запустити першу версію системи eEAD у «тіні» в безпечному середовищі, де реальні користувачі зможуть виконувати і перевіряти функціональні можливості. Таким чином, забезпечується співіснування з поточною версією EAD (Європейська база даних AIS), яка продовжить свою роботу, аби гарантувати надійність обробки, розподілу і попередньої інформації для польотів на глобальному рівні, — зазначає компанія.

«Ця цифрова платформа є важливим етапом у цифровізації управління повітряним рухом і відкриває шлях до незалежності інфраструктур і повного використання хмари в європейській авіації. Цей піонерський крок EUROCONTROL дозволяє оптимізувати операції та дасть змогу ефективно реагувати на майбутні виклики, адаптуючи їх до хмари. Ми в Indra пишаємося тим, що є частиною цього інноваційного розвитку, який підтверджує нашу прихильність до сталого розвитку авіації в Європі та світі», — зазначає Віктор Мартінес Гарсія, директор з управління повітряним рухом (ATM) Indra для Північної Європи та Канади.

Відомий як iNM, програму інтегрованого управління мережею буде завершено до кінця десятиліття і вона має на меті революціонізувати операційні системи EUROCONTROL через впровадження потужної, масштабованої та інтегрованої цифрової архітектури, яка сприятиме підвищенню ефективності, безпеки та сталості всієї європейської авіаційної мережі. ★

Home Office

SECURITY & POLICING

HOME OFFICE EVENT

Безпека та поліція: Глобальна подія безпеки уряду Великої Британії

З 11 по 13 березня 2025 року знову відбудеться захід «Безпека та поліція» в Міжнародному виставковому та конференц-центрі Фарнборо. Це офіційна глобальна подія уряду Великої Британії з безпеки, яку організовує Спільний центр безпеки та стійкості Міністерства внутрішніх справ Великої Британії (JSaRC). Подія надає світову можливість для зустрічей та обговорення останніх досягнень у сфері національної безпеки та стійкості з провідними британськими постачальниками, представниками урядів Великої Британії та інших країн, а також високопосадовцями в галузі правоохоронних органів та безпеки.

У 2024 році захід зібрав понад 8 700 учасників, серед яких були високопосадовці та міжнародні делегації з 75 країн. Понад 385 експонентів представили різні сектори ланцюга постачання безпеки, продемонструвавши найкращі рішення та можливості в цій галузі. Учасники також мали доступ до представників 38 урядових відомств Великої Британії, що підкреслює широку урядову участь у заході.

Для заходу «Безпека та поліція» не передбачено загальний вхід, тому всі відвідувачі та експоненти повинні отримати схвалення Міністерства внутрішніх справ, що гарантує спілкування з релевантною аудиторією, яка має повноваження ухвалювати операційні рішення.

Незалежно від розміру вашої компанії, «Безпека та поліція» пропонує унікальну можливість продемонструвати свої продукти та можливості цільовій аудиторії старших прийнятельників рішень, покупців, міжнародних делегацій, поліційних служб та урядових відомств Великої Британії та інших країн.

Можливості для демонстрації та взаємодії

«Безпека та поліція» надає експонентам можливість демонструвати свої продукти та можливості безпосередньо тим, хто приймає операційні та закупівельні рішення. Цільова аудиторія включає постачальників безпеки національної інфраструктури, головних поліцейських, представників поліції, служби екстреної допомоги та урядових агентів, що забезпечує ефективне налагодження контактів з потенційними клієнтами та партнерами.

Цього року знову буде представлена програма основних виступів та сесій, які будуть вести високопосадовці уряду

Великої Британії, представники поліції та промисловості в рамках основного театру брифінгів, сцени Spotlight та зони інновацій.

Також цього року буде запущена Зона вогневої безпеки та стійкості, що об'єднає провідних професіоналів, які планують та готуються до великих надзвичайних ситуацій відповідно до Закону про цивільні надзвичайні ситуації Великої Британії, тим самим забезпечуючи локальну та національну стійкість. Зона покаже останні досягнення у галузі вогневої безпеки та стійкості у Великій Британії. Учасники зможуть взаємодіяти з високопосадовцями галузі, отримати цінну інформацію від експертів і розширити свої мережі контактів.

Одним із яскравих моментів заходу буде Імерсивний досвід, організований JSaRC, який надасть відвідувачам наративний, змістовний та інноваційний досвід, що дасть змогу ознайомитися з технологіями та рішеннями для вирішення актуальних та майбутніх загроз і викликів безпеки.

Святкування інновацій: Нагорода за інновації у безпеці від ADS

Відомий Приз за інновації у безпеці від ADS святкує своє 20-річчя на заході 2025 року, вшановуючи передові розробки британських компаній у сфері безпеки. Ця нагорода користується великою повагою, а фіналісти отримують значну видимість. Конкурс служить платформою для експонентів, щоб продемонструвати проривні продукти та послуги, підкреслюючи акцент події на інноваціях.

Критерії для відвідувачів та профіль учасників

Строгі критерії відбору відвідувачів забезпечують участь лише перевірених професіоналів, що максимізує потенціал для змістовних дискусій та партнерств. У 2024 році захід привернув увагу високопосадовців урядів, поліцейських з Великої Британії та інших країн, служб екстреної допомоги та перших реагувальників, покупців можливостей і представників таких агентств, як Міністерство внутрішніх справ, Міністерство оборони, митниця, імміграція та національна інфраструктура.

Відгуки учасників попередніх заходів підкреслюють цінність події: 95% рекомендують її колегам. Дані опитувань 2024 року показали високий рівень задоволення: 85% оцінили свій досвід як хороший чи відмінний, 96% похвалили якість експонентів, а 93% відзначили важливість мережевих та лекційних сесій.

Ексклюзивні можливості для нетворкінгу та навчання

«Безпека та поліція» — це не просто виставка, а комплексна освітня та мережеві можливості. Учасники можуть брати участь у виступах та панелях, які проводять високопосадовці уряду Великої Британії, експерти з академічної та промислової сфер, отримуючи інсайти щодо останніх політик та ініціатив у сфері безпеки. Також є можливості для подальшого професійного розвитку (CPD) через партнерство з навчальними провайдерами, що допомагає учасникам залишатися в курсі стандартів та навичок галузі.

Експоненти отримують доступ до урядових зон, де вони можуть налагоджувати контакти з високопосадовцями та обговорювати останні ініціативи в сфері безпеки та правоохоронних органів.

Ідеальна платформа для професіоналів у сфері безпеки

«Безпека та поліція» є неперевершеною платформою для професіоналів у сфері безпеки для налагодження контактів з урядовими посадовцями та експертами галузі. Відвідувачі можуть ознайомитися з технологіями наступного покоління, відповідати на нові загрози безпеці та бути в курсі політичних змін. Захід також дозволяє учасникам побачити живі демонстрації нових технологій та зрозуміти їхнє застосування в імерсивних умовах.

«Безпека та поліція» залишається провідною подією Великої Британії в галузі безпеки, що створена для професіоналів, які прагнуть залишатися на передовій інновацій у сфері безпеки та стійкості. Завдяки широким можливостям для нетворкінгу, різноманітним експонентам та високому рівню знань, цей захід є вибором для тих, хто працює в галузі безпеки. Реєстрація на «Безпеку та поліцію» 2025 року вже відкрита, при цьому участь залежить від схвалення Міністерства внутрішніх справ, що гарантує безпечне та релевантне зібрання світових лідерів у сфері безпеки.

Для отримання додаткової інформації про участь та критерії для експонентів і відвідувачів, відвідайте офіційний вебсайт заходу www.securityandpolicing.co.uk. ★

Супутник NASA

Як військово-цивільне співробітництво трансформує кібербезпеку в космосі

За останнє десятиліття спостерігається стрімке зростання космічних технологій. Зниження вартості та підвищення доступності супутникових та інших космічних технологій призвели до того, що багато країн і компаній почали долучатися до цієї сфери. Космічні технології відіграють дедалі важливішу роль у повсякденній діяльності бізнесу, армій та житті звичайних громадян.

Разом із підвищенням доступності космічних технологій зростає співпраця між державними та приватними структурами, а також військовими та цивільними організаціями. Наприклад, компанія SpaceX, яка є приватним підприємством, регулярно доставляє людей та обладнання в космос для NASA. Пентагон також укладав контракти з SpaceX на використання її супутникової мережі Starshield для військових цілей. Загальне зростання масштабів, сфери застосування та взаємозалежності космічних технологій у державному та приватному секторах також сприяє потребі в розвитку кібербезпеки, яка відповідає швидко еволюціонуючій космічній інфраструктурі — та наземним технологіям, які її підтримують.

Це поєднання стрімкого зростання, поширення технологій та збільшення співпраці між державним і приватним секторами сприяє кільком основним тенденціям у сфері кібербезпеки в космосі. По-перше, зростає попит на розподілені кібербезпекові технології, які можуть працювати в різних організаціях та на розосереджених активах, таких як наземні станції та супутники. По-друге, це впровадження технологій «нульової довіри» для забезпечення безпечних з'єднань та обміну даними між різними організаціями, рівнями класифікації тощо. І, нарешті, зростання обізнаності громадськості щодо потенційних кібератак у космосі, що сприяє обговоренню питання про те, чи слід вважати космос сектором критичної інфраструктури.

Зростання міжсекторальної співпраці в космосі

Історично супутникові технології, як апаратне, так і програмне забезпечення, створювалися на замовлення і були доступні лише державним установам. Лише невелика кількість країн мала можливість запускати супутники в космос. Це забезпечувало певний рівень «безпеки через невідомість» від кібератак, яка тепер швидко зникає. За останні кілька десятиліть приватні компанії прискорили інновації в космічних технологіях і випередили державні космічні агенції за кількістю запусків. У першому кварталі 2023 року SpaceX запустила понад 700 космічних апаратів на орбіту, більшість з яких були супутниками зв'язку. Оскільки приватні компанії швидко розвивають та запускають супутники, уряди прагнуть співпрацювати з ними, щоб скористатися перевагами інновацій, які забезпечують приватні підприємства.

Це створює нагальні виклики для кібербезпеки. Уряди, які сподіваються використовувати комерційні супутникові мережі зв'язку для швидкої передачі даних по всьому світу, повинні бути впевнені, що конфіденційні дані, які вони передають, захищені. Якщо уряд купує супутники, вироблені приватною

компанією, він повинен знати, що технологія була розроблена з урахуванням найвищих стандартів кібербезпеки. Приватні компанії можуть використовувати комерційні готові рішення для створення своїх супутників, що підтвердилося під час доповіді на конференції BlackHat 2023, де дослідник виявив базові недоліки безпеки в кількох моделях комерційних та урядових супутників.

Уряди розуміють, що їм необхідно покладатися на інновації приватних компаній для створення нових технологій, щоб досягти цілей кібербезпеки в космосі, так само як вони покладаються на приватні компанії для виробництва та запуску супутників. Оскільки все більше критично важливих державних функцій та життя цивільних осіб залежать від взаємопов'язаної мережі державної та приватної космічної та наземної інфраструктури, кібербезпека цих активів стає важливішою, ніж будь-коли. Тривають дискусії щодо того, чи слід визначити космос сектором критичної інфраструктури урядом США. Це могло б призвести до збільшення регуляторних вказівок та фінансування для захисту кібербезпеки космічних ресурсів. Наразі космос є складовою кількох існуючих секторів критичної інфраструктури, але сам по собі не визнаний таким.

Створення Космічних сил США є значним кроком у сприянні співпраці та підкреслює зміну характеру ведення війни. Це також стало початком необхідної кампанії з підвищення обізнаності про безпеку в космосі. Тепер усі починають розуміти, що фінансування, дослідження нового покоління та захист усіх типів космічної інфраструктури є найважливішими. Це вимагає досягнення тонкого балансу між міжнародною співпрацею та захистом конфіденційної військової інформації, а також інтелектуальної власності державних підрядників та оборонно-промислової бази.

Зростання використання розподіленої кібербезпеки

Високо розподілена природа космічних активів створює серйозні виклики для кібербезпеки. Багато супутників уже знаходяться на орбіті, і оновлення їх вбудованих заходів кібербезпеки є складним або неможливим. Наземні станції, які передають і отримують сигнали від багатьох різних супутників, можуть стати ціллю для зловмисників, які прагнуть або викрасти цінні дані дистанційного зондування, перехопити засекречені військові дані, або навіть саботувати супутники на орбіті. Захист усіх цих активів, одночасно дозволяючи їм виконувати свою роботу зі збору та розповсюдження даних зі швидкістю, яка забезпечує світову діяльність приватного та державного бізнесу та військових операцій, є непростим завданням.

Однією з основних проблем є передача та отримання конфіденційних даних між цими активами, гарантуючи, що дані не будуть підроблені, пошкоджені або доступні несанкціонованим особам. Наприклад, дані дистанційного зондування, такі як зображення з високою роздільною здатністю з камер та інших датчиків, встановлених на супутниках, є цінними, але повинні передаватися швидко, щоб зберегти свою цінність для забезпечення місії. Як користувачі можуть отримати зображення з супутника, передати їх через мережу інших приватних та державних супутників і, зрештою, на наземну станцію, де хтось повинен ухвалити рішення, яке може бути питанням життя чи смерті, забезпечуючи цілісність даних на всьому шляху?

Безпечний обмін даними між різними космічними системами становить великий виклик для розподіленої кібербезпеки, особливо щодо надмірності та довіри. Наслідки підробки даних можуть бути значними. Навіть незначне відхилення від специфікацій під час космічного запуску, спричинене підробкою, може мати реальні наслідки, потенційно призводячи до втрати людських життів.

Необхідно підтримувати цілісний погляд на всіх учасників кіберпростору. Як приклад можна розглянути вторгнення Путіна в Україну, де супутниковий інтернет-провайдер, який широко використовується в Європі та українською армією, став ціллю безпрецедентної кібератаки. Це нагадує, що зі зростанням взаємозв'язку та складності космічних систем кібератаки стають все більш поширеними — і електронна війна вже стала реальністю.

Прискорення впровадження «нульової довіри»

Країни починають усвідомлювати, що принципи «нульової довіри», які виявилися необхідними для захисту систем на Землі, тепер повинні поширюватися і на системи, що працюють у космосі. Цей зсув підкреслюється «Дорожньою картою нульової довіри» Міністерства оборони, яка вказує, що як оборонно-промислова база, так і військові організації вже визначили «нульову довіру» одним із пріоритетів. Однак поточний виклик полягає в практичному впровадженні «нульової довіри» в унікальному контексті космосу.

Багато сфер потребують швидкого захисту за допомогою технологій «нульової довіри», таких як наземний зв'язок і супутники. Для операцій наземних станцій критично важливим є захист доступу до застарілих систем, а також інтеграція з сучасними активами. Захист стартових майданчиків також є важливим, оскільки це величезні об'єкти зі складними, потенційно вразливими системами промислового контролю. Космічні сили США ведуть у впровадженні інноваційних, розроблених приватним сектором рішень безпеки та, більш загально, у сприянні продуктивній співпраці між комерційними організаціями та оборонними відомствами для захисту космічного простору.

Зростання обізнаності громадськості про кіберзагрози в космосі

У проактивному ході для розширення обізнаності про вразливості в космосі уряд США запустив у серпні 2023 року супутник з явною метою стати ціллю для кібератак. Ця стратегічна ініціатива мала на меті оцінити стан кібербезпеки космічних технологій, одночасно підвищуючи обізнаність громадськості щодо потенційних загроз у космосі. Ця місія не лише висвітлила легкість проникнення в космічні активи, але й привернула увагу широкої громадськості, збільшивши глобальну підтримку для посилення кіберзахисту в космосі.

Незважаючи на очевидні ризики та зростаючу обізнаність про вразливості в космосі, питання про офіційне визнання космосу сектором критичної інфраструктури залишається предметом обговорення. Таке визнання підкреслило б внутрішню важливість захищених космічних технологій і встановило б рамки для впровадження регуляцій та нагляду. Це необхідний крок для захисту не лише наших країн, але й майбутнього космічних досліджень — і підтримка широкої громадськості може стати ключовим фактором.

Космос як новий рубеж кібербезпеки

У міру того, як космос вступає в нову еру та переоцінює свої пріоритети, технології — і ті, хто їх створює — продовжують залишатися на передньому краї всіх космічних ініціатив. Зі зростанням кількості атак немає сумнівів, що глибока співпраця та кібербезпека в космосі повинні стрімко розвиватися, щоб захистити зростаючий та змінюваний космічний простір. Інновації в області концепції «нульової довіри» та міцна співпраця між державними та комерційними структурами повинні стати нашим провідним принципом, щоб забезпечити безпечне майбутнє космосу.

★

Стан кібербезпеки: Складний ландшафт загроз підвищує рівень стресу

Звіт ISACA за 2024 рік про стан кібербезпеки пропонує огляд сучасних викликів і тенденцій у сфері кібербезпеки.

Стан кібербезпеки

Звіт ISACA за 2024 рік про стан кібербезпеки надає інсайти щодо сучасних викликів і тенденцій у цій сфері. У звіті підкреслено кілька ключових проблем, включаючи нестачу персоналу, дефіцит навичок, еволюцію загроз

Київ Україна
Травень 27-29
2025

Виставка систем охорони та безпеки

Expert Security

БЕЗПЕКА ЗОВСІМ ПОРЯД

МІСЦЕ ПРОВЕДЕННЯ:
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

та обмеження бюджету, а також визначено області прогресу, такі як зростання впевненості у можливостях реагування на загрози та підвищення обізнаності щодо оцінки кіберризиків.

Однією з найтривожніших тенденцій у звіті є зростання рівня стресу серед фахівців з кібербезпеки: 66% респондентів зазначили, що їхня робота стала значно або трохи напруженішою порівняно з тим, що було п'ять років тому. Цей підвищений стрес зумовлений насамперед ускладненням ландшафту загроз. Ситуацію погіршує те, що 57% організацій повідомляють про нестачу персоналу, що ще більше збільшує навантаження на наявних працівників.

Старіння робочої сили також стає все більшою проблемою: кількість респондентів у віці від 45 до 54 років тепер перевищує кількість тих, кому від 35 до 44 років. Ця тенденція, разом із мінімальним покращенням представленості осіб віком до 34 років і відсутністю зростання кількості керівників, які керують персоналом з менш ніж трьома роками досвіду, свідчить про те, що лідерам галузі необхідно розробляти плани щодо підготовки наступників, щоб вирішити потенційне збільшення плинності кадрів.

Залучення та утримання кваліфікованих фахівців залишається серйозним викликом. Хоча 44% співробітників перейшли до кібербезпеки з інших сфер, попит на досвідчених професіоналів продовжує перевищувати пропозицію. Кількість незаповнених вакансій у сфері кібербезпеки залишається високою: 64% організацій повідомляють про вакансії на різних рівнях. Заповнення цих посад також займає значний час: 37% організацій потребують 3-6 місяців для заповнення початкових позицій, і 38% займають стільки ж часу для заповнення позицій вищого рівня.

Стійкі прогалини в навичках

У звіті визначено стійкі прогалини в навичках у кількох критично важливих областях. Зокрема, «програмні навички» та «хмарні обчислення» названі 51% та 42% респондентів відповідно як найбільш значні прогалини. Це підкреслює потребу в професіоналах, які не лише розуміють технічні концепції, але й ефективно спілкуються, співпрацюють та адаптуються до змін.

Для вирішення цих прогалин організації все частіше вдаються до програм навчання та розвитку. Найпоширеніші підходи включають онлайн-навчальні сайти, корпоративні навчальні заходи та наставництво. Однак підвищення кваліфікації наявного персоналу та залучення нових талантів із необхідними навичками залишаються важливими викликами.

Використання штучного інтелекту (ШІ) у сфері безпеки залишається відносно низьким: 20% респондентів повідомляють про відсутність його використання. Однак його потенціал є незаперечним. Три основні сфери застосування ШІ включають автоматизацію виявлення та реагування на загрози, покращення захисту кінцевих точок і автоматизацію рутинних завдань із безпеки. Незважаючи на перспективність, відсутність участі фахівців із безпеки в розробці та впровадженні ШІ викликає занепокоєння щодо ефективної інтеграції та використання цієї технології.

Кібератаки продовжують зростати

Кібератаки продовжують зростати: 38% респондентів повідомляють про збільшення їх кількості порівняно з минулим роком. Кіберзлочинці та хакери залишаються основними загрозами, використовуючи такі методи, як соціальна інженерія, шкідливе програмне забезпечення та експлуатація невиправлених систем. Це підкреслює необхідність пильності та постійного вдосконалення практик безпеки для зменшення цих загроз.

Хоча 81% керівних команд бачать цінність у оцінці кіберризиків, лише 41% проводять їх щорічно. Це свідчить про зростання обізнаності, але також про потенційні прогалини в розумінні та впровадженні. Крім того, майже половина (45%) респондентів не знають про страхове покриття своєї організації у сфері кібербезпеки, що вказує на значну потребу в покращенні комунікації та освіти в цій галузі.

Звіт показує, що 49% команд з кібербезпеки підпорядковані Chief Information Security Officer (CISO), який найчастіше підзвітний Chief Information Officer (CIO) (26%) або Chief Executive Officer (CEO) (23%). Це свідчить про централізований підхід до керівництва в сфері кібербезпеки, де CISO відіграє ключову роль у узгодженні стратегій безпеки з цілями організації. Заохочує те, що 74% респондентів вважають, що їхня кіберстратегія узгоджена з цілями організації, а 56% вважають, що їхня рада директорів надає належний пріоритет кібербезпеці.

Звіт про стан кібербезпеки за 2024 рік підкреслює необхідність багатоаспектного підходу для вирішення еволюціонуючих викликів. Інвестування в таланти, усунення прогалин у навичках, використання технологій, покращення управління ризиками та посилення комунікації та співпраці дозволяють організаціям значно покращити свій рівень безпеки та зменшити потенційні ризики. Інсайти, надані цим звітом, є важливим посібником для організацій, які прагнуть ефективно орієнтуватися у складному та постійно змінюваному ландшафті кібербезпеки.

Конкретні дії для організацій:

Розробляйте та впроваджуйте проактивні стратегії найму: залучайте та утримуйте кваліфікованих фахівців з кібербезпеки, пропонуючи конкурентоспроможні зарплати, пільги та можливості професійного розвитку.

Інвестуйте в програми навчання та розвитку: підвищуйте кваліфікацію наявного персоналу та усувайте прогалини в навичках, надаючи доступ до онлайн-вебінарів, навчальних платформ, корпоративних тренінгів та програм наставництва.

Досліджуйте потенціал ШІ: впроваджуйте рішення на основі ШІ для автоматизації рутинних завдань, покращення можливостей виявлення та реагування на загрози та загального підвищення рівня безпеки.

Проводите регулярні оцінки кіберризиків: виявляйте вразливості та розробляйте стратегії з їх усунення для зменшення ймовірності та наслідків кібератак.

Забезпечуйте комплексне страхове покриття у сфері кібербезпеки: зрозумійте політику страхування своєї організації та переконайтеся, що вона забезпечує адекватне покриття потенційних ризиків.

Заохочуйте ефективну комунікацію та співпрацю: усувайте бар'єри між командами з безпеки, керівництвом та іншими відділами. Діліться інформацією, інсайтами та найкращими практиками для покращення загального рівня безпеки.

Персональні поради:

Будьте в курсі останніх загроз і тенденцій: постійно оновлюйте свої знання та навички через професійний розвиток, сертифікації та онлайн-ресурси.

Розвивайте сильні прогамні навички: комунікація, співпраця, критичне мислення та вирішення проблем є невід'ємними навичками для будь-якого фахівця з кібербезпеки.

Налаштовуйтесь на постійне навчання: ландшафт кібербезпеки постійно змінюється. Випереджайте зміни, дотримуючись підходу до навчання протягом усього життя.

★

По всьому світу лідери у сфері безпеки збираються разом, щоб спілкуватися та ділитися результатами досліджень своїх організацій. Ось кілька провідних конференцій з кібербезпеки у 2025 році.

Africa CISO Summit

Найробі, Кенія, 19–20 березня 2025 р.

Africa CISO Summit 2025 — це унікальний захід, який об'єднує понад 200 провідних лідерів у сфері кібербезпеки, осіб, що приймають рішення, та інноваторів з усього континенту. У березні Найробі стане місцем проведення ексклюзивного форуму, спрямованого на вирішення нагальних проблем регіону та висвітлення можливостей, які відкриваються завдяки новим технологіям та інвестиційним трендам.

Minorities in Cybersecurity Annual Conference

Даллас, Техас, 23–27 березня 2025 р.

Щорічна конференція Minorities in Cybersecurity (MiC) надає лідерам у сфері кібербезпеки можливість обговорити виклики галузі та кар'єрні прагнення. Учасники також обговорюють плани підтримки людей кольору та жінок у цій сфері, а також діляться порадами щодо просування корпоративною драбиною. Реєстрація обмежена 150 учасниками.

20th International Conference on Cyber Warfare and Security

Вільямсбург, Вірджинія, 28–29 березня 2025 р.

20-та Міжнародна конференція з кібервійни та безпеки (ICCWS) присвячена питанням кібервійни та кібербезпеки. Конференція дозволяє професіоналам у сфері кібербезпеки представити академічні дослідження своїм колегам у галузі.

WiCyS 2025

Даллас, Техас, 2–5 квітня 2025 р.

Конференція Women in Cybersecurity (WiCyS) 2025 надає лідерам у сфері безпеки можливість залучати та просувати жінок на посади, пов'язані з кібербезпекою. У програмі заходу — майстер-класи з написання резюме, сесії нетворкінгу та пробні співбесіди.

Cyber Security Asia 2025

Куала-Лумпур, Малайзія 21–22 квітня 2025 р.

Конференція Cyber Security Asia 2025 надає кібербезпековцям вищого рівня з Азіатсько-Тихоокеанського регіону та інших частин світу можливість для спілкування. У заході візьмуть участь понад 35 доповідачів, і понад 85% учасників будуть на рівні старших менеджерів, директорів або вище.

RSA Conference

Сан-Франциско, Каліфорнія 28 квітня – 1 травня 2025 р.

Учасники конференції RSA Conference зможуть спілкуватися з іншими лідерами у сфері кібербезпеки та постачальниками. Серед доповідачів — лідери галузі з великих корпорацій та державних організацій.

46th IEEE Symposium on Security and Privacy

Сан-Франциско, Каліфорнія 12–15 травня 2025 р.

46-й симпозіум з безпеки та конфіденційності від Інституту інженерів з електротехніки та електроніки (IEEE) дозволяє дослідникам та практикам обговорити спільні проблеми. Серед тем — захист даних, нові загрози та проблеми ланцюгів поставок.

Cybersecurity and Privacy Professionals Conference

Балтімор, Меріленд, 19–21 травня 2025 р.

Конференція Cybersecurity and Privacy Professionals Conference надає лідерам у сфері безпеки у вищій освіті можливість для спілкування та обговорення захисту даних та інших проблем галузі.

Black Hat USA

Лас-Вегас, Невада, 2–7 серпня 2025 р.

Black Hat об'єднує хакерів, кібербезпековців, розробників технологій та інших фахівців для обміну інформацією та спілкування.

Blue Team Con

Чикаго, Іллінойс, 6–7 вересня 2025 р.

Blue Team Con орієнтована на захисників кібербезпеки, надаючи їм простір для спілкування та обміну інформацією. Захід також включає можливості для розвитку кар'єри та освітні доповіді.

Global CISO Executive Summit

Новий Орлеан, Луїзіана 8–10 вересня 2025 р.

Global CISO Executive Summit, організований Evanta, заохочує керівників інформаційної безпеки (CISO) збиратися разом та ділитися стратегіями для залізниць, розвідкою про загрози та методами комунікації. Програма конференції створюється «CISO для CISO».

National Cyber Summit

Гантсвілл, Алабама 23–25 вересня 2025 р.

National Cyber Summit пропонує майбутнім лідерам у сфері безпеки можливість співпрацювати та дізнаватися про технології та розвиток у сфері кібербезпеки.

International Cyber Expo 2025

Лондон, Англія 30 вересня – 1 жовтня 2025 р.

International Cyber Expo — це глобальний захід для лідерів та керівників у сфері безпеки, де вони можуть спілкуватися, дізнаватися про нові технології та ділитися стратегіями захисту.

InfoSec World

Лейк-Буена-Віста, Флорида 17–29 жовтня 2025 р.

30-та конференція InfoSec World дозволяє учасникам отримувати кредити CPE, спілкуючись з тисячами колег. Серед минулих ключових доповідачів — лідери з OpenAI, Cybersecurity Collaborative та інших організацій.

SECURITY 500 Conference

Вашингтон, округ Колумбія 17 листопада 2025 р.

17-та щорічна конференція SECURITY 500 від журналу Security відбудеться у листопаді у Вашингтоні, округ Колумбія. Захід включає панельні дискусії та виступи впливових керівників у сфері фізичної та кібербезпеки, об'єднуючи лідерів із уряду та приватного сектору.

Global Cyber Conference

Цюрих, Швейцарія 22–23 жовтня 2025 р.

Global Cyber Conference (GCC) — це провідна міжнародна конференція з кібербезпеки та захисту даних для лідерів у сфері безпеки, зацікавлених сторін, державних службовців та науковців, які прагнуть підвищити кіберстійкість.

World Conference on Cyber Security and Ethical Hacking

Бангкок, Таїланд, 12–13 грудня 2025 р.

Всесвітня конференція з кібербезпеки та етичного хакінгу (WCCSEH) об'єднує науковців, військових та лідерів у сфері безпеки з усього світу для протидії загрозам, пов'язаним із хакерами.

★

Австралійці все частіше застосовують системи безпеки бо рівень злочинності зростає

Австралія стикається з тривожним зростанням рівня злочинності протягом останніх кількох років. З огляду на те, що пошкодження майна та крадіжки знаходяться на першому місці, тривога зростає як серед бізнесменів, так і простих громадян. Оскільки рівень злочинності з часом не йде на зниження, все більше австралійців звертаються до технологій, які можуть забезпечити спокій і безпеку.

Дані Бюро статистики Австралії за 2022-23 фінансовий рік показали, що приблизно 185 000 осіб стали жертвами проникнення до їхніх осель, а близько 55 000 осіб зазнали крадіжки автотранспорту – це на 25% більше, ніж раніше.

Лише в Брісбені рівень злочинності в передмістях зростає з 2021 року, що відображає тенденції, які спостерігалися до пандемії. Згідно з даними статистики злочинності Квінсленду, крадіжки залишаються найпоширенішим злочином, що підкреслює необхідність посилення засобів стримування та ефективніших стратегій на рівні громади для зменшення майнових злочинів.

Для Крістін Доусон, директора компанії Dawson Electric, та її працівників у Брісбені, зростання попиту на системи безпеки стало помітним. «Близько 18 місяців тому, коли злочинність серед молоді в Брісбені почала зростати, ми помітили значну рвст попиту на встановлення домашніх систем безпеки», – розповідає вона. «Ми бачимо більше випадків проникнення до будинків та крадіжок автомобілів, тому не дивно, що люди вживають більше заходів для захисту своєї власності».

Однією з головних тенденцій у сфері технологій безпеки є зростання популярності розумних домашніх систем. Доусон зазначає, що все більше власників житла обирають інтеграцію цих пе-

редових технологій у свої системи безпеки, щоб забезпечити більш комплексний та проактивний підхід до захисту майна. «Головна причина, чому люди обирають розумні технології, проста – це краща безпека дому. Більшість наших клієнтів встановлюють сенсорне освітлення та декілька камер спостереження», – додала вона.

Хоча в більшості випадків встановлення систем безпеки є лише запобіжним заходом, Доусон згадує історію успіху, яка демонструє їх ефективність. «У нас був клієнт у Купарі, який встановив камери спостереження та сигналізацію. Через кілька тижнів відбулася спроба проникнення, і камери виявили зловмисників, активувавши сигналізацію. Гучні звуки та спалахи світла виявилися достатніми, щоб відлякати злочинців, які негайно втекли з місця події», – розповіла вона.

Для споживачів вибір правильної камери або системи спочатку може здатися складним завданням, але при оцінці можливостей та функцій, які відповідають потребам безпеки їхнього майна, цей процес стає набагато простішим.

Нові гравці на австралійському ринку, такі як Lorex Technology (https://www.lorex.com/en-au), пропонують широкий вибір традиційних проводних камер, розумних дверних дзвінків, прожекторів та WiFi-камер для ринку домашньої безпеки Австралії. На фоні зростання кількості випадків крадіжок автотранспорту, проникнень до будинків та викрадень посилок, поява Lorex стала вчасною.

«Ми розуміємо, наскільки важливу роль відіграють засоби стримування у зменшенні таких інцидентів та забезпеченні безпеки наших громад», – сказав віце-президент Lorex Стів Хонг. «Ми інтегрували низку функцій у наші продукти, щоб створити проактивний та видимий підхід до боротьби з цими зростаючими загрозами. Насправді, найефективніша камера спостереження може і не записувати відео, оскільки сама її присутність та усвідомлення злочинцем наявності в ній передових функцій штучного інтелекту часто допомагають зазадалегідь відлякувати злочинців і запобігають виникнення інцидентів».

Камери Lorex, що працюють на основі штучного інтелекту, забезпечують точні сповіщення про рух у реальному часі зі спеціальними режимами виявлення людей, транспортних засобів, тварин та посилок, мінімізуючи помилкові спрацьовування. Користувачі можуть швидко реагувати за допомогою двостороннього аудіозв'язку, відправляючи попередньо записане повідомлення або спілкуючись безпосередньо з порушниками. Завдяки функції кольорового нічного бачення та роздільній здатності 4K, камери Lorex забезпечують чітке зображення навіть у умовах слабкого освітлення, фіксуючи критично важливі деталі для ідентифікації злочинців та збору доказів.

Тож по мірі розвитку технологій зростають і можливості для захисту домівок та громад.

★

Абстрактне зображення безпеки

Підвищення фізичної безпеки

Підвищити фізичну безпеку легко за наявності правильних інструментів

Кіберзлочинці постійно шукають можливості для використання вразливостей у всіх технологіях, включаючи системи фізичної безпеки. Як організації можуть захистити свої системи фізичної безпеки від кібератак?

Системи та пристрої фізичної безпеки, такі як камери відеоспостереження та системи контролю доступу, стали розумнішими, потужнішими та більш інтегрованими, ніж будь-коли раніше. Як частина публічних і приватних мереж, вони все більше об'єднуються для полегшення управління, прискорення комунікацій, збільшення обміну даними та, що найважливіше, надання можливостей фахівцям із безпеки захищати людей та організації.

Однак, хоча громадяни та бізнес отримують вигоду від цієї зростаючої взаємозв'язності систем безпеки, нові кіберзагрози, ризики та злочинна діяльність можуть призводити до нових вразливостей та ризиків у добре документованому поєднанні фізичної та кібербезпеки.

Злам системи безпеки

Як ми вже згадували в нашій статті «Кібербезпека в епоху державних кібератак», кіберзлочинцям достатньо лише однієї незахищеної камери або незахищених комунікацій між сервером і клієнтською програмою.

У міру зростання масштабів кібератак збільшується і кількість випадків, коли кіберзлочинці отримують доступ до приватних камер відеоспостереження для отримання відео та зображень. Злам системи безпеки може мати різні форми, включаючи brute force-атаки, аналіз мережевого трафіку (packet sniffing) та атаки типу «людина посередині». У останньому випадку кіберзлочинці можуть «підслуховувати» комунікації, які учасники вважали безпечними.

Незахищені пристрої – відкриті двері для загроз

Почати підвищення захисту вашої інфраструктури від таких вторгнень можна з простого кроку – змінити заводський пароль за замовчуванням. Згідно з нашими дослідженнями, 23% користувачів мають принаймні одну камеру, яка використовує стандартні облікові дані. Однак із зростанням взаємозв'язності систем через інтернет незахищений пристрій може стати шлюзом для доступу до великої кількості даних та інформації. Просто кажучи, робота з підвищення захисту фізичної системи безпеки також є роботою з захисту всіх інших систем і даних у цій мережі.

Стратегія підвищення безпеки

Враховуючи ці потенційні вразливості, має сенс мати стратегію безпеки, яка захищає як від фізичних, так і від кіберзагроз. Крім того, рішення повинно надавати користувачам інсайти щодо їхніх пристроїв і показувати, як покращити їхню безпеку. Така система включає в себе кілька різних ліній захисту, таких як шифрування, багаторівнева аутентифікація та авторизація. Цей комплексний підхід вимагає, щоб кожен пристрій захоплював дані та передавав їх до єдиної системи безпеки для управління, аналізу та зберігання зі стійким шифруванням, доступним лише автентифікованим і авторизованим користувачам.

Шифрування та аутентифікація

Все починається з шифрування – найпростішого кроку, який користувачі можуть зробити для захисту своїх даних. Коли дані зашифровані, навіть якщо неавторизована особа отримає до них доступ, вони будуть нечитабельними без відповідного ключа. Це досить простий процес, але він вимагає, щоб виробники вбудовували цю функцію у свої продукти безпеки. Якщо продукт не підтримує шифрування, це має бути сигналом для негайного реагування. Шифрування – це хороший спосіб приховати дані, але воно не може зупинити неавторизований доступ до вашої мережі. Для цього організації використовують різні форми аутентифікації. Аутентифікація – це процес визначення, чи є об'єкт тим, за кого себе видає, і перевірка, чи має цей об'єкт доступ до системи та на яких умовах.

Захист інфраструктури

Окрім шифрування, одним із ключових аспектів підтримки загальної стабільності системи є захист інфраструктури. Неправильно захищений пристрій або компонент може залишити вас вразливими. В ідеальному світі всі кінцеві точки будуть ретельно перевірені під час встановлення та підтримуватимуться в актуальному стані. Однак, коли на об'єкті є сотні пристроїв (наприклад, камери, точки контролю доступу та інші датчики), вручну керувати кожним із них може бути надзвичайно складно. Пошук необхідної інформації, визначення різних критеріїв та ручна перевірка кожного елемента роблять процес дуже трудомістким. Саме тому сучасні централізовані програми безпеки можуть моніторити стан системи та нада-

вати користувачам повний огляд, що допомагає їм передбачати проблеми та розробляти рішення проактивно.

Такий посібник не повинен бути переповнений технічним жаргоном та кодами, які більшість користувачів не зрозуміють. Він має бути написаний зрозумілою англійською мовою, містити прості правила та надавати об'єктивну оцінку того, наскільки безпечною є система.

Ефективне технічне обслуговування системи

Окрім дотримання найкращих практик, ключовим аспектом підтримки безпеки є забезпечення актуальності вашої системи. Згідно з нашими даними, лише 30% камер використовують останню версію прошивки. Це означає, що 70% нібито безпечних камер працюють на застарілій прошивці, яка потенційно може бути вектором атаки. Складне рішення не лише покаже користувачам стан цих кінцевих точок, але й матиме вбудовані функції конфігурації та оновлення. В результаті технічне обслуговування системи стає більш ефективним, а витрати знижуються.

Кожен несе відповідальність за кібербезпеку

Світ фізичної безпеки неймовірно швидко підключився до інтернету. Ми більше не живемо у «закритому» світі; навіть «герметичні» системи (ті, що працюють у внутрішній мережі без підключення до зовнішнього світу) можна зламати за допомогою USB-накопичувача. Кожен несе відповідальність за кібербезпеку – від виробника та інтегратора до консультантів і кінцевих користувачів. Оскільки кінцеві користувачі найбільше страждають від вразливих пристроїв, вони повинні переконатися, що постачальники та партнери, з якими вони працюють, також серйозно ставляться до кібербезпеки та надають їм інструменти для захисту від кіберзлочинності.

★

Законопроект сенатора Лі «No CBDC Act» має намір заборонити Федеральному резерву вводити цифрову валюту CBDC в США

ВАШИНГТОН — Сенатор Майк Лі (R-UT) знову представив законопроект No CBDC Act, щоб запобігти Федеральному резерву змінювати фінансовий сектор США та отримувати можливість контролювати транзакції споживачів через цифрову валюту центрального банку (CBDC). Президент Дональд Трамп нещодавно заборонив федеральним агентствам створювати CBDC через указ, і цей законопроект закріпить заборону в законі на постійній основі. Законопроект підтримують сенатори Тед Круз (R-TX) та Рік Скотт (R-FL). Представник Енді Оглс (R-TN) представляє супутній законопроект в Палаті представників.

«Сполученим Штатам не потрібно створювати цифрову валюту центрального банку, щоб зрозуміти, що це погана ідея», — заявив сенатор Лі. «Ми бачили це в Китаї з цифровим юанем. Під час перших випробувань Китай скасовував гроші своїх громадян через певний період часу, змушуючи китайців витрачати свої заощадження під тиском уряду. Мій законопроект захищає американців від подібного втручання, забороняючи Федеральному резерву або будь-якому федеральному агентству випускати чи вводити CBDC, як через прямий доступ до споживача, так і через посередницьку модель».

«CBDC — це не що інше, як інструмент для тиранів, щоб залякувати, контролювати та спостерігати за діяльністю американських громадян, і моїм обов'язком як патріота є зупинити їх», — заявив представник Оглс. «Я пишаюся тим, що є співкерівником цього зусилля разом із сенатором Лі».

Історія питання:

Під час адміністрації Байдена Федеральний резерв (Fed) розпочав розробку можливого проєкту — відомого як Project Cedar — для цифрової валюти центрального банку (CBDC), цифрового активу, який мав випускатися та контролюватися Федеральним резервом. CBDC мала змінити здатність фінансових установ працювати як кредитори, надаючи федеральному уряду можливість отримувати інформацію про кожну покупку, що здійснюється через CBDC.

Фінансові установи мали бути значно обмеженими у наданні кредитів, та мали виконувати роль лише гаманців. CBDC, в багатьох аспектах, мала дозволити Федеральному резерву замінити роль банків як фінансових посередників, надаючи уряду значно більше влади над економікою, інфляцією та інвестиційними рішеннями. Іншими словами, вільне підприємництво та фінансова конфіденційність отримали б серйозний удар зі створенням CBDC.

Насамкінець, Федеральний резерв мав би інформацію про кожну транзакцію з використанням CBDC; якщо ж він збереже технології створення та управління CBDC, **Великий Брат буде знати про кожну покупку американців.**

Підтримка:

«Американці вимагають фінансового захисту та конфіденційності після того, як вони зіткнулися з загрозою створення не обраними федеральними бюрократами інвазивної, всеосяжної цифрової валюти центрального банку, контрольованої урядом. З новим консервативним урядом настав час для Конгресу захистити індивідуальні свободи американців і заборонити уряду централізувати контроль над економікою. Heritage Action вітає сенатора Лі за представлення цього необхідного законопроекту для захисту прав американців і сприяння свободі від фінансових залякувань». — Раян Уокер, виконавчий віце-президент Heritage Action.

«Цифрова валюта центрального банку створює повністю відстежувану та контрольовану цифрову валюту, що має жахливі наслідки для громадянських свобод та економічної свободи. Замість того, щоб пропонувати розподіл грошей і держави, як у інновації Біткоїна від Сатоші, CBDC об'єднує владу держави та грошей у програмованій формі, що може бути легко зловживано і шкодить індивідуальній свободі та фінансовій незалежності.

Законопроект сенатора Лі No CBDC Act закріплює в законі заборону для Федерального резерву йти цим шляхом. Від імені споживачів, які цінують свої економічні свободи, свободу вибору та доступ до інноваційних технологій, ми вітаємо зусилля сенатора з цим законопроектом і сподіваємось, що ще більше законодавців приєднаються до цієї справи, щоб захистити наші права на фінансову конфіденційність». — Яель Оссовскі, заступник директора Consumer Choice Center.

«Сенатор Лі веде важливу боротьбу, щоб запобігти створенню урядом абсолютно нового інструменту фінансового контролю та спостереження. Федерально випущений CBDC буде або абсолютно непотрібним, або, що ймовірніше, глибоко небезпечним. Завдяки лідерству сенатора Лі Конгрес тепер чітко дає зрозуміти, що виконавча влада перевищила свої повноваження і повинна негайно припинити цей глибоко хибний крок». — Девід Вільямс, президент Taxpayers Protection Alliance.

★

На четвертий день після своєї інавгурації президент США Дональд Трамп почав виконувати свої обіцянки щодо криптовалютного ринку

Після того, як він прийшов до влади з демонстративним випуском «мемкоїн» разом зі своєю дружиною, сумнівів щодо його рішучої підтримки криптовалютного ринку не було. Він підтвердив це, підписавши указ під назвою «Посилення американського лідерства в цифрових фінансових технологіях».

Як це часто буває з указами виконавчої влади, документ не містить детальних політичних пропозицій. Однак він робить кілька важливих обіцянок.

По-перше, указ обіцяє сприяти доступу до публічних блокчейн-мереж. Наразі багато установ, зокрема банки, стикаються з труднощами у взаємодії з публічними блокчейнами, оскільки їх відкрита природа ускладнює визначення регуляторних меж. Коли будь-хто може взяти участь у мережі, перевірка клієнтів стає майже неможливою.

Це, разом з відкликанням Комісією з цінних паперів і бірж (SEC) свого суперечливого Staff Accounting Bulletin 121 (який зробив криптовалюти окремим класом активів, зобов'язуючи банки розглядати криптоактиви, що знаходяться на зберіганні, як зобов'язання і утримувати активи проти них), відкриває шлях для традиційних фінансових установ почати надавати криптовалютні послуги своїм клієнтам.

SEC також створила криптовалютну робочу групу на чолі з поважним комісаром Хестер Пірс. Комісія з торгівлі товарними ф'ючерсами (CFTC) ще не створила своєї власної регуляторної структури для криптоактивів, незважаючи на те, що ключове законодавство, яке зараз знаходиться в Конгресі, може підпорядкувати криптовалютні ринки наглядові CFTC.

Злиття криптоактивів та традиційних фінансів, хоча й суперечить антибанківському етосу крипто-пуристів, ймовірно, дасть поштовх крипторинкам, як і передбачали багато експертів після перемоги Трампа на виборах 2024 року.

По-друге, указ Трампа наголошує на «захисті та просуванні справедливого та відкритого доступу до банківських послуг», що є завуальованим натяком на припинення практики відмови в банківських послугах криптовалютним компаніям. Багато представників криптовалютної індустрії стикаються з труднощами у забезпеченні банківських відносин з авторитетними американськими установами, зазвичай через рамки управління ризиками в банках. Як саме адміністрація Трампа має намір змінити ці правила — ще невідомо, але можна припустити, що стосунки між криптовалютами та традиційними банками зблизяться.

По-третє, указ «забив останній цвях» у труну цифрової валюти центрального банку США, зазначаючи, що вона «загрожує стабільності фінансової системи». Цю заяву в основному відкидають центральні банки інших країн, незалежно від того, чи планують вони випускати цифрові валюти. Вона здебільшого висловлюється банками, які вважають себе під загрозою від можливих змін, викликаних цифровими валютами.

Можливе майбутнє для цифрових валют центральних банків та стейблкоїнів

Цікаво, що визначення цифрової валюти центрального банку (ЦВЦБ) в указі («форма цифрових грошей або грошової вартості, номінована в національній одиниці рахунку, що є прямим зобов'язанням центрального банку») є настільки широким, що включає не лише роздрібні та оптові ЦВЦБ, а й FedWire — власну послугу оптових платежів Федеральної резервної системи.

Хоча це, здається, виключає оптові ЦВЦБ, Федеральний резерв може знайти спосіб представити гроші центрального банку в цифровому вигляді для використання на фінансових ринках або для взаємодії з іншими центральними банками для покращення міжнародних платежів. Такі проекти можуть знайти вигоду в тому, щоб позбутися ярлика «ЦВЦБ», аби зробити їх привабливими для американських властей, але законодавчі ініціативи, які вже існують (Закон про антиспостереження за ЦВЦБ), орієнтовані переважно на роздрібні ЦВЦБ.

З іншого боку, згадка стейблкоїнів в указі як інструменту для просування та захисту суверенітету долара може свідчити про те, що нова адміністрація підтримуватиме зусилля приватного сектору щодо того, щоб токенізовані грошові розрахунки та міжнародні платежі здійснювалися через стейблкоїни.

Якщо так, це може призвести до суттєвого відхилення США від міжнародних зусиль щодо інтеграції грошей центральних банків на уніфіковані реєстри. Це ризикує серйозно знизити вартість цих проектів, оскільки долар відіграє таку важливу роль у фінансових ринках. Для Проекту Агори Банку міжнародних розрахунків та подібних ініціатив проведення їх без долара зменшить їхню цінність. Це також вимагатиме значного коригування їхніх принципів проектування, щоб замінити гроші центрального банку США на стейблкоїни.

Що Трамп 2.0 означає для криптоіндустрії

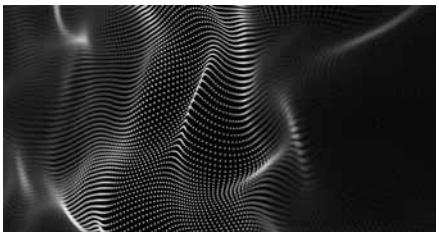
Позиція Трампа щодо криптовалют буде розділяти. Навіть серед прихильників цього класу активів випуск мемкоїну Трампа (при збереженні 80% його постачання) отримав критику як нахабне поглинання грошей, яке типово для найгірших форм спекулятивного користолюбства, що дало погану репутацію галузі.

Указ також відроджує передвиборчу обіцянку Трампа щодо «стратегічного резерву біткоїнів», основною метою якого, схоже, є збагачення власників біткоїнів.

Але скасування заважливої політики, характерної для адміністрації Джо Байдена (не кажучи вже про «регулювання через примус» колишнього голови SEC Гері Генслера щодо криптовалютних правил), створює середовище, в якому криптоактиви та бізнеси, що їх обслуговують, можуть процвітати в США. ЄС пережив короткий період відносної привабливості завдяки ясності свого Регламенту щодо ринків криптоактивів, але США, вже ставши домом для більшості талановитих фахівців галузі, готові активізуватися.

Льюїс МакЛеллан, редактор Digital Monetary Institute в OMFIF.

★



Чи можуть машини, які вже мислять, також і забувати?

Штучний інтелект уже неможливо зупинити, і тепер питання не тільки в його здатності до аналізу, а й у тому, що він може ігнорувати чи забувати.

Забуття економічної історії

Економічна історія навчала нас про фінансові цикли, кризи та макроекономічні зміни. Від Південно-морської бульбашки 1720 року до фінансової кризи 2008-го – історія попереджає про небезпеку спекуляцій, боргової залежності та надмірностей.

ШІ дедалі більше впливає на аналіз та економічну політику, але чи зможе він виявляти системні ризики, якщо віддаватиме перевагу лише новітнім даним? Якщо алгоритми ігноруватимуть історичні цикли, це може зробити економічну історію менш важливою та менш вивченою.

Небезпека фінансової амнезії

Фінансові ринки мають схильність забувати уроки минулого. Більшість алгоритмічних моделей тренуються на відносно коротких часових проміжках (10–20 років), що може посилювати короткострокове мислення.

Криза 2008 року стала прикладом такого «забуття»: ризикові моделі не передбачили краху ринку нерухомості, бо подібного не траплялося в недавній історії. Якщо ШІ зосередиться лише на посткризових даних, ринки можуть знову опинитися в ілюзії безпеки.

Загроза алгоритмічного відбору історії

ШІ не лише аналізує економіку, а й визначає, які історичні знання будуть доступними. Алгоритми формують інформаційний простір, надаючи перевагу певним джерелам, що може викривлювати сприйняття минулого.

Це особливо важливо у випадках складних і дискусійних економічних подій – наприклад, причин Великої депресії чи наслідків колоніалізму. Якщо ШІ буде підсилювати певні наративи, він може звузити економічну дискусію та створити ілюзію єдиної «правильної» інтерпретації.

Вплив на економічну політику

Центробанки та регулятори завжди враховували історичні кризи у своїх рішеннях. Проте з поширенням ШІ істо-

ричний аналіз може поступитися місцем алгоритмічному прогнозуванню. Якщо моделі навчатимуться лише на сучасних даних, чи зможуть вони виявити ризики, що колись уже спричиняли фінансові потрясіння?

Попри ці загрози, ШІ також може сприяти збереженню економічної історії – оцифровуючи архіви, виявляючи довгострокові закономірності та роблячи знання доступнішими.

Зрештою, вибір залишається за людиною: чи допоможе ШІ глибше зрозуміти економічне минуле, чи стане причиною його поступового забуття?

★

Як компанія-виробник військової техніки та озброєння має поводитись у медіапросторі, ось кілька порад від ШІ:

Створіть чітку комунікаційну стратегію

Розробіть список основних повідомлень, в якому чітко визначте, що ваша компанія робить і які її досягнення. Це допоможе вам правильно позиціювати свою діяльність в медіа, не порушуючи при цьому безпекових норм.

Визначте публічні межі — що можна і що не можна поширювати. Це важливо, щоб уникнути витоку інформації, яка може бути використана проти вас або вашого бізнесу.

Керування медіа-іміджем

Оборонні компанії мають тримати баланс між впізнаваністю та безпекою. З одного боку, вам потрібно створювати позитивний імідж, залучати інвесторів, партнерів і наймати співробітників, з іншого — обережно підходити до публічної демонстрації своїх технологій, методів роботи або внутрішніх процесів.

Ретельно обирайте канали комунікації — медіа чи закриті профільні заходи, соціальні мережі, або спеціалізовані групи. Можливо, інколи для вашої цільової аудиторії медіа не є найефективнішим каналом, і в таких випадках варто шукати альтернативи.

Перевірка та контроль за інтерв'ю

Перш ніж погоджуватись на інтерв'ю, ретельно перевірте журналіста та медіа, для яких він працює. Досліджуйте позицію медіа щодо війни, безпеки та інших ключових тем, щоб бути впевненим, що інтерв'ю не стане політичним інструментом чи способом маніпуляції.

Дізнайтесь про попередні запитання або хоча б тему матеріалу, щоб зрозуміти, чи готові ви відкривати певні аспекти вашої діяльності. Це дозволить підготуватися і уникнути неочікуваних ситуацій.

Визначте політику для інтерв'ю – якщо не хочете, щоб певна інформація потрапила у публікацію, варто заздалегідь обговорити ці моменти з журналістом і поставити обмеження.

Контроль над візуальним контентом

Будьте обережні щодо зображень і відео, що можуть потрапити в медіа. Враховуйте, що навіть деталі на фотографіях (наприклад, шеврони або специфічні інтер'єри) можуть дати корисну інформацію супротивнику. Тому потрібно контролювати, що зображується на публічних кадрах.

Дозволяйте лише зйомки, які не розкривають критичну інформацію, і визначайте чіткі правила для зйомок на території виробництва або під час тестувань.

Позиціонування через технологічні інновації

Ваша унікальність може бути вашим сильним аргументом, але не обов'язково розкривати секретні аспекти ваших розробок. Наприклад, ви можете наголосити на унікальних особливостях вашого продукту, не розкриваючи деталей технології. Наприклад, особливості конструкції, ефективність, гнучкість у застосуванні — це все можна презентувати, не порушуючи безпеку.

Вибудовуйте свою репутацію через експертні коментарі, аналіз ринку чи тенденцій у галузі. Це дозволить створити імідж компетентного і надійного партнера, не порушуючи політики безпеки.

Робота з кризами

Якщо медіа вже взяли вашу компанію в об'єктив, і ви отримали негативний відгук чи критику, будьте готові до кризової комунікації. Завжди зберігайте спокій і чітко пояснюйте свою позицію, не вдаючись до конфронтацій. Завжди пам'ятайте, що ваша мета — захистити репутацію, не дозволяючи ворогові отримувати інформацію, яку вони можуть використати.

Безпечний доступ до інформації

Під час інтерв'ю з іноземними журналістами – переконайтесь, що журналісти дійсно є представниками серйозних ЗМІ, і дізнайтесь про їхній досвід роботи, а також позицію їхніх видань.

Приділяйте увагу тому, щоб безпека персоналу і персональних даних була на першому місці. Можливо, вам слід застосовувати певні заходи збереження анонімності співробітників або партнерів.

Тренування команди

Проводьте регулярні тренінги для ваших спікерів і команди, що бере участь у медіа-активностях. Важливо, щоб кожен чітко розумів, що можна і що не можна говорити, які аспекти компанії повинні залишатися конфіденційними, а що — доступним для публікації.

Система внутрішніх комунікацій

Використовуйте заздалегідь сформовані внутрішні документи (типу медіакіт) для забезпечення консистентності в комунікаціях. Чітко зазначайте, хто і як з представників компанії уповноважений комунікувати з медіа, які теми обговорювати, а яких уникати.

В підсумку, важливо дотримуватись обережності в медіапросторі, зберігаючи баланс між необхідністю бути впізнаваним та забезпеченням безпеки технологій і персоналу. Чітка стратегія, контроль за комунікаціями і персональний підхід до кожного випадку можуть дозволити вам зберегти репутацію та конкурентоспроможність.

★

Протягом останнього року в галузі безпеки були значні досягнення у різних напрямках, зокрема в кібербезпеці, фізичній безпеці та в забезпеченні безпеки на транспорті. Ось кілька важливих напрямків:

Кібербезпека та захист від загроз штучного інтелекту

Штучний інтелект (ШІ) і машинне навчання відіграють важливу роль у захисті від кіберзагроз, а також використовуються для створення нових способів атак. Однак, є значні досягнення у застосуванні ШІ для покращення кібербезпеки:

Інтелектуальні системи виявлення загроз: За допомогою машинного навчання можна виявляти нові типи атак або аномалії в мережах. Ці системи можуть адаптуватися до нових загроз, виявляючи підозрілі активності навіть на ранніх стадіях.

Атаки на ШІ-системи: Водночас розвивається і протидія атакам на самі системи ШІ. Розроблені нові методи захисту, такі як техніки захисту від adversarial attacks (супротивних атак), коли моделі ШІ намагаються «обдурити» через маніпуляції з даними.

Приклад: Нова технологія розпізнавання загроз на основі ШІ, яка аналізує мережевий трафік і в реальному часі виявляє аномалії, що можуть вказувати на можливі зловмисні дії. Впровадження таких рішень в банківському секторі дозволяє швидко реагувати на кібератаки.

Захист фізичної інфраструктури та технічні інновації в безпеці

В останні роки велику увагу приділено автоматизації та роботизації в забезпеченні фізичної безпеки. Наприклад:

Роботи-охоронці: У великих компаніях та на виробничих об'єктах почали використовувати роботів для патрулювання та моніторингу територій. Вони обладнані камерами високої роздільної здатності, датчиками руху і навіть можуть взаємодіяти з людьми.

Безпека у транспорті: Впровадження інтелектуальних транспортних систем (ITS), які використовують сенсори і камери для моніторингу дорожнього руху, дозволяє виявляти порушення безпеки та реагувати на аварійні ситуації.

Приклад: Використання дронів для патрулювання великих складських або промислових комплексів. Такі дрони можуть автономно виконувати інспекції, передаючи відео в реальному часі для аналізу.

Захист даних і конфіденційність

Враховуючи високий рівень загроз конфіденційності особистих і корпоративних даних, з'явилися нові інструменти для забезпечення захисту інформації:

Блокчейн для безпеки даних: Технологія блокчейн не тільки в криптовалютному секторі, але й для забезпечення безпеки передачі даних. Зокрема, для перевірки автентичності документів або транзакцій, що дає змогу значно зменшити можливості для підробок.

Квантове шифрування: Розробка квантових алгоритмів для захисту даних від зламу. Квантова криптографія на основі принципів квантової механіки пропонує нові методи шифрування, які здатні витримувати атаки навіть з боку квантових комп'ютерів у майбутньому.

Приклад: Прототипи квантових ключових розподілів (QKD) починають застосовуватися в різних сферах, зокрема у банківському секторі для забезпечення високого рівня захисту транзакцій.

Розвиток біометричних технологій

Біометричні технології стали важливою частиною безпеки, особливо для верифікації особистості. Застосування нових методів, таких як розпізнавання обличчя, райдужної оболонки ока чи навіть аналізу поведінкових патернів (наприклад, аналізу підпису чи темпу набору тексту), дозволяють підвищити рівень безпеки без необхідності використовувати фізичні засоби (ключі, паролі).

Приклад: Застосування розпізнавання обличчя для безконтактної перевірки особистості на вхідних точках в аеропортах або в банківських відділеннях.

Програми з розпізнавання та прогнозування кримінальних загроз

Зростає роль великих даних і аналітики у прогнозуванні кримінальної діяльності. Використання алгоритмів аналізу великих даних дозволяє ефективно прогнозувати, де і коли можуть статися злочини, на основі історичних даних, патернів та інших параметрів.

Приклад: Впровадження таких систем у правоохоронних органах для профілактики злочинів або зменшення часу реагування на критичні ситуації.

Ці досягнення сприяють не тільки зниженню рівня загроз, але й забезпечують нові можливості для реалізації більш ефективних і масштабних стратегій безпеки в різних сферах. Враховуючи швидкість технологічного прогресу, можна очікувати нові інновації в галузі безпеки в найближчі роки.

★

Інновації в кібербезпеці у 2024 році: революція в цифровій безпеці

У 2024 році кібербезпека характеризується швидкими інноваціями, спричиненими зростанням складності кіберзагроз і збільшенням залежності від цифрової інфраструктури. Організації впроваджують новітні технології та стратегії для захисту даних і систем, акцентуючи увагу на проактивних заходах та зручних для користувачів рішеннях. Ось ключові інновації в кібербезпеці, які привертають увагу цього року.

Автентифікація без паролів

Перехід до систем автентифікації без паролів, які підтримують такі гіганти, як Microsoft, став значним кроком у цифровій безпеці. Ці системи використовують біометричні дані (наприклад, розпізнавання обличчя та відбитки пальців) та апаратні ключі замість традиційних паролів. Вони не лише зручніші, але й забезпечують надійний захист від фішингу та крадіжок облікових даних.

2. Виявлення загроз за допомогою ШІ

Штучний інтелект (ШІ) продовжує революціонізувати кібербезпеку, покращуючи можливості виявлення та реагування на загрози. Алгоритми машинного навчання здатні ідентифікувати аномалії в реальному часі, прогнозувати можливі атаки та автоматизувати відповіді для зменшення ризиків. Це особливо ефективно для боротьби з ransomware, фішингом та складними атаками.

Покращені заходи захисту даних

Нові нормативні вимоги та попит споживачів на конфіденційність стимулюють розвиток технологій захисту даних. Такі методи, як гомоморфне шифрування та безпечні багатосторонні обчислення, дозволяють обробляти дані без ризику несанкціонованого доступу. Ці технології набувають популярності в медицині та фінансах.

Захищені режими друку та обробки документів

Інновації, такі як Protected Print Mode від Microsoft, забезпечують додатковий рівень захисту, обмежуючи доступ до конфіденційних документів лише авторизованим особам. Це особливо важливо в умовах гібридної роботи.

Архітектура Zero Trust

Модель Zero Trust, яка передбачає постійну перевірку користувачів і пристроїв, набуває популярності. Вона значно зменшує поверхню для атак завдяки розширеним механізмам контролю доступу та мікросегментації.

Квантово-стійке шифрування

У зв'язку з розвитком квантових обчислень розробляються квантово-стійкі криптографічні алгоритми, які захищатимуть дані від майбутніх квантових комп'ютерів.

Децентралізовані системи ідентифікації

Системи децентралізованої ідентифікації на основі блокчейну дозволяють користувачам контролювати свої цифрові ідентифікатори, зменшуючи залежність від централізованих баз даних.

8. Покращення безпеки IoT

Виробники впроваджують апаратне шифрування, автоматичні оновлення прошивок та сегментацію мереж для захисту IoT-пристроїв, які часто стають ціллю для атак.

Виклики та перспективи

Незважаючи на прогрес, залишаються виклики, такі як нестача кваліфікованих фахівців і висока вартість впровадження нових рішень. Однак співпраця між урядами, приватним сектором та академічними установами обіцяє зробити цифрове майбутнє безпечнішим.

У 2024 році кібербезпека була спрямована на створення стійких систем, які могли б адаптуватися до еволюціонуючих загроз.

★★★

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

Тенденції дронізації в Україні на сучасному етапі

У статті розглянуто окремі питання, пов'язані зі справжнім революційним проривом у виробництві в Україні дронів різного військового призначення, які широко використовують у повітряному, наземному, надводному і підводному варіантах. Проаналізовано, як сучасні дронові інноваційні технології впливають на архітектуру військових операцій і приводять до змінення тактики ведення як загальновійськового бою, так і бойових дій на морі. Зазначено, що під час широкомасштабної війни дронізація актуалізувалася і набула в Україні системного характеру.

«Війну 4IR» можна описати як ситуацію, коли в ході бойових дій для знищення противника та його інфраструктури буде масово задіяна САЗ [смертоносна автономна зброя] без фізичного залучення людини на полі бою.

Оборонний вісник. 2022. № 3-4.

Четверта промислова революція поклала початок створенню сучасного науково-технічного та інтегрованого науково-виробничого ландшафту для старту нового етапу гонки озброєнь у світі, суть якого поляга є в створенні різних за призначенням роботизованих бойових платформ — дронів, які завдяки застосуванню штучного інтелекту (ШІ) здатні в найближчій перспективі повністю виключити участь людини на полі бою *(Горбулін В., Мосов С. Смертельна автономна зброя. Оборонний вісник. 2022. № 3-4. С. 18—24.)*.

Ера дронів розпочалася з використання безпілотних авіаційних комплексів (БпАК), і на сьогодні застосування дронів охопило не лише повітряний простір, а й земну поверхню, надводний і підводний простори. З початком широкомасштабної війни (24.02.2022) дронізація стала об'єктивною реальністю для України. На жаль, наша держава реально звернула увагу на питання безпілотної авіації лише після 2014 р., з початком збройного протистояння в південно-східному регіоні країни.

До того на озброєнні ЗСУ перебували лише застарілі розвідувальні БпАК радянського виробництва: т актичний БпАК ВР-3 «Рейс» і оперативно-тактичний БпАК ВР-2 «Стриж» *(Мосов С.П., Погорецький М.В., Салій С.М., Сєлюков О.В., Фещенко А.Л. Безпілотна авіація у військовій справі. За ред. С.П. Мосова. Київ: Інтерсервіс, 2019.)*.

Під час широкомасштабної війни дронізація набула системного характеру і здійснюється на інноваційній платформі. Її декомпозиція дозволяє виокремити такі складові:

1) застосування повітряних (UAV), наземних (UGV), надводних (USV) та підводних (ROV) дронів;

2) українське виробництво та імпорт дронів;

3) технічні інновації;

4) тактика застосування дронів.

Увесь світ уважно стежить за ходом боїв в Україні, спостерігаючи за стрімким розвитком технологій дронів, які домінують від самого початку воєнного конфлікту, а також за змінами, які відбувають у зв'язку з цим в оперативному мистецтві і тактиці.

Повітряні дрони. Початок широкомасштабної війни кардинально змінив ставлення до безпілотної авіації і не тільки. В Україні розпочалася системна дронізація, спрямована на посилення боєздатності військ, збільшення бойових втрат противника, особливо під час його наступу, а також на розширення можливостей асиметричних дій.

Війна в Україні спричинила справжній революційний прорив у використанні безпілотних літальних апаратів (БпЛА) не лише для потреб повітряної розвідки та коректування вогню, а й як зброї, чого раніше масово не спостерігалося, і тим самим фактично трансформувала сучасне поле бою.

Дронізація набула лавиноподібного характеру, що було зумовлено, з одного боку, допомогою США, європейських країн, Канади, Австралії та інших країн світу дронами різного призначення, насамперед БпАК, а з іншого боку, обмеженістю української авіації, нестачею озброєння і військової техніки та відсутністю необхідної кількості боєприпасів. Лише за півтора року війни, починаючи з лютого 2022 р., на забезпечення військових безпілотною авіацією українського та іноземного виробництва було виділено 40 млрд грн і взято на озброєння чи прийнято в експлуатацію 32 зразки БпАК різних типів від українських виробників, серед яких розвідувальні та ударні БпЛА, БпЛА--камікадзе та баражуючі боєприпаси. До наявних у ЗСУ безпілотників додалися нові комплекси: FPV-дрони Phoenix 03 Heavy UCAV; дрони-камікадзе E-300 Enterprise; багатоцільові D-80 Discovery; розвідувальні Windhover та ін. *(Виділили 40 мільярдів: Міноборони розкрило, які дрони закуповує для ЗСУ. Фокус. 14.08.2023. http://surl.li/mncttc)*.

Україні також вдалося збільшити власне виробництво деяких моделей БпАК у 100 разів порівняно з 2022 р. *(Виробництво дронів збільшили в 100 разів: Федоров розкрив, як посилять ЗСУ. Фокус. 17.07.2023. http:/ /surl.li/sqsyft)*.

На фронті вже в перший рік війни разом з українськими БпАК використовували комплекси іноземного виробництва. Крім добре відомих Bayraktar TB2 та FlyEye, застосовують БпАК виробництва китайських компаній SZ DJI Technology і Autel Robotics; ударний Revolver 860 Armed VTOL (Тайвань); баражуючі боєприпаси Switchblade 300 (США) і Phoenix Ghost Atlas (США); розвідувальні DeltaQuad Pro VTOL (Нідерланди), Vector (Німеччина) і EOS C VTOL (Естонія); багатоцільові PPDS (Австралія) і SkyRanger R70 (Канада) та багато інших *(Які безпілотники використовують ЗСУ та як вони працюють. Chas News. 17.08.2022. http://surl.li/nlycou)*.

Сьогодні понад 200 українських компаній виготовляють 90 % усіх типів БпАК, які ЗСУ використовують на полі бою. З'явилися нові розробки українських БпАК різного призначення: ударні RAM II UAV, SkyKnight 2, UJ-26 «Бобер», «Рубака», Vampire, «Хрущ»; розвідувальні SHARK, «Гор», «СКІФ»; багатоцільовий UJ-22 Airborne; дрон-камікадзе «Генерал Черешня» та ін.

Ринок безпілотників продовжує активно розвиватися, в тому числі з використанням краудсорсингових технологій і, що важливо, з урахуванням отриманого бойового досвіду.

Розробники постійно адаптують БпЛА до застосування в умовах інтенсивної дії засобів РЕБ, вдосконалюють зв'язок та системи корисного навантаження.

Однак наявність сьогодні у військах понад 200 різних типів БпАК *(Скільки дронів виготовила Україна в 2024 році: що кажуть у Міноборони. РБК-Україна. 23.10.2024. http://surl.li/ uvgpig)* не слід сприймати однозначно: з одного боку, це, безумовно, значне досягнення під час війни, а з іншого — проблема, пов'язана з розпорошенням ресурсів.

Потрібні оптимізація та уніфікація номенклатури, орієнтація на серійний випуск упродовж кількох років хоча б двох-трьох десятків типів БпАК, актуальних для ведення війни *(Володимир Горбулін: 170 типів безпілотників у ЗСУ — це і досягнення, і проблема одночасно. NV. 08.10.2024. http://surl.li/etrdrk)*. Крім того, це підтверджує тезу щодо відсутності у держави конкретної стратегії роботи з виробником.

Через масове використання FPV-дронів розвиток ударної безпілотної авіації набув тенденційного характеру, а поле битви в умовах високотехнологічного воєнного конфлікту фактично перетворилося на випробувальний полігон для пере вірки можливостей різних видів зброї, в тому числі безпілотників. FPV-дрони мають низку переваг — низька ціна, простота виробництва і висока точність застосування.

Наземні дрони

Спостерігається також тенденція до активного застосування наземних дронів різного призначення українського та іноземного виробництва, які стають впливовим фактором на полі бою. Зокрема, це роботизовані бойові платформи «Шабля» (Україна, 2023, оснащена кулеметною туреллю з відео- і тепловізійною камерами), Ironclad (Україна, 2024, оснащена тепловізійною камерою та бойовою туреллю), «Рись» (Україна, 2023), «Лють» (Україна, 2024, оснащена оглядовими камерами і кулеметом); роботизовані платформи «Каракурт»/«Мангал» (Україна, 2023, мінування, підрив, підвезення боєкомплекту), Ratel S (Україна, 2023, підрив); роботизовані логістичні платформи Sirko-S1 (Україна, 2024), THeMIS (Естонія, 2022), UGV Trail-Blazer (Чехія, 2024); робот-собака BAD.2

(Велика Британія, 2024) та ін.*(Список бойових наземних платформ України. Вікіпедія. http://surl.li/pybcpg)*. Ще на початку широкомасштабної війни було підтверджено ефективність застосування роботизованих платформ для виконання різних завдань, таких як вогнева підтримка загальновійськових частин, логістичні, розвідувальні операції, інженерні заходи, евакуація поранених тощо.

Наразі триває робота з інтеграції БпЛА і наземних дронів у єдиний центр керування всіма дронами на полі бою в режимі реального часу *(Об'єднає БПЛА і наземних роботів: в Україні створюють єдиний центр управління дронами (відео). Фокус. 15.08.2024. http://surl.li/ucwxjn)*.

Надводні дрони

Концепція морських дронів уже не перший рік розвивається в різних країнах світу, проте Україна стала першою державою, яка почала створювати власний флот морських дронів-камікадзе. В Україні налагоджено серійний випуск бойових надводних дронів, ефективність яких підтверджено конкретними результатами, досягнутими під час широкомасштабної війни, а саме: баланс у протистоянні на Чорному морі кардинально змінився. Ці дрони стали одним із вагомих факторів стримування російського флоту. Вони виконують різноманітні завдання, починаючи від розвідки і закінчуючи ударними діями.

До складу флоту надводних дронів України входять ударні дрони Sea Baby (Україна, 2022), «Микола-3» (Україна,

2022), «Мамай» (Україна, 2023); багатоцільовий Magura V5 (Україна, 2023) *(Українські безпілотні надводні апарати під час Російсько-української війни (з 2022). Вікіпедія.)*. Успішними розробками можна вважати також ударні дрони «Заєнота» і «Бахмут», логістичний дрон Stalker 5.0 тощо.

Щодо надводних дронів західних партнерів, то США і Німеччина свого часу передали Україні свої морські дрони без висвітлення подробиць у ЗМІ. Данія передала ВМС ЗСУ морські дрони SeaBat — автономні гідрографічні комплекси, призначені для фільмування донного рельєфу з метою підвищення ситуаційної обізнаності у підводному просторі.

Підводні дрони

Україна розробляє також свої підводні дрони, які, вочевидь, матимуть переваги в раптовості, непомітності та живучості. Як і створення надводних дронів, цей напрям є інноваційним. На сьогодні реалізується низка проєктів, і на стадії розроблення та випробувань перебувають ударні дрони «Марічка» (платформа AMMO.Ukraine) та Kronos (Highland Systems), а також безпілотні торпеди TLK 1000, TLK 400 і TLK 150 (кластер Brave1).

Україна вже оперує кількома типами підводних дронів зарубіжного виробництва, зокрема Remus-100 (Велика Британія, для виявлення, локалізації та ідентифікації мін на узбережжі); R7 (Бельгія, для огляду, спостереження, технічного обслуговування та відновлення підводних об'єктів).

Українське виробництво та імпорт дронів.

Отже, виробництво дронів в Україні на початку широкомасштабної війни перебувало у вкрай незадовільному стані. Причин цього було багато, але головною з них є недооцінка з боку військових фахівців значущості дронів у сучасних воєнних конфліктах, незважаючи на наявний з 1991 р. досвід збройних протистоянь у світі.

У 2022 р. Україна змушена була майже з нуля створювати вітчизняний ринок дронів, на якому сьогодні працюють сотні виробників: до 2022 р. було 20 компаній, станом на грудень 2023 р. — понад 200, які, зокрема, здійснюють сервіс та випуск супутніх продуктів *(Від нуля до армії стартапів. У 2023 році в Україні розвинулися сотні виробників дронів, роботів і РЕБ. Що заважає їм рости ще швидше? Forbes Ukraine. 23.12.2023. http://surl.li/mtzydr)*. Ця індустрія демонструє стрімке зростання через значну потребу у швидкій адаптації оборонних технологій для захисту держави під час широкомасштабної високотехнологічної війни, і виробництво дронів швидко перетворюється на окрему підгалузь машинобудування.

Україна, опинившись в епіцентрі жорстокої війни, стала одним із лідерів у розробленні та виробництві передусім БпАК. З лютого 2022 р., за даними МО України, допущено до постачання у війська понад 200 БпАК різних типів і призначень, понад 40 наземних роботизованих комплексів (НРК) вітчизняного виробництва. Більшість із них — саме у 2024 р.: лише за 9 місяців поточного року було допущено до експлуатації 140 БпАК і 33 НРК.

За період війни виробництво БпАК різко зросло: 2022 р. — 3—5 тис. од.; 2023 р. — 300 тис. од.; план на 2024 р. з виготовлення мільйону FPV-дронів і понад 10 тис. ударних безпілотників із середньою дальністю польоту перевиконано. За прогнозами, накопичений виробничий потенціал дозволяє випускати понад 3 млн. од. *(Україна збирає армію роботів. Коли вони вступлять у бій? Економічна правда. 17.04.2024. http://surl.li/hpepcr)*. Україні вдалося також масштабувати виробництво ударних безпілотників із дальністю польоту понад 1 тис. км.

Якщо БпАК уже впевнено посіли своє місце на полі бою, то питання застосування НРК вирішено лише частково, що зумовлено насамперед проблемами у забезпеченні їхнього руху бездоріжжям з різноманітними природними та штучними перешкодами. Певні зрушення в цьому напрямі дозволили з першої декади 2024 р. розпочати масове виробництво НРК різного призначення. На сьогодні завдяки державно-приватному партнерству сотні НРК вже використовують на полі бою.

На новий рівень Україна вивела й виробництво морських дронів, значно наростивши за останній рік обсяги продукції. Однак точну кількість виготовлених морських дронів складно визначити з відкритих джерел. Зважаючи на інформацію у ЗМІ щодо результатів збору коштів на їх виробництво, йдеться принаймні про десятки морських дронів різного призначення.

З метою стимулювання розвитку масового виробництва вітчизняних БпАК, а також максимального спрощення умов для їх випуску та постачання в липні 2022 р. Генштаб ЗСУ, Міністерство оборони, Міністерство цифрової трансформації і Держслужба спецзв'язку та захисту інформації започаткували спільний проєкт «Армія дронів», який реалізується в межах фандрейзингової платформи United24. Згодом цей проєкт фактично трансформувався в системну державну програму. Збори на БпАК підтримали

донори зі 100 країн і десятки світових компаній. Завдяки цьому за рік вдалося придбати тисячі БпАК і забезпечити ними бойові підрозділи. Під час виконання проєкту «Армія дронів» було реалізовано низку заходів, зокрема скасовано ПДВ на ввезення з-за кордону дронів та їх комплектування, створено полігон для тренувань та випробувань БпЛА, запроваджено спрощену процедуру отримання допуску до експлуатації БпАК (fast-track), дано старт масовому виробництву БпАК в Україні, забезпечено навчання тисяч зовнішніх пілотів на різні типи БпАК. Масове використання безпілотників і формування першого у світі флоту морських дронів привело до змінення доктрини ведення бою як на землі, так і на морі *(Армії дронів — рік. Масове виробництво дронів в Україні, ударні роти БПЛА, навчання операторів дронів — головні досягнення проєкту. Міністерство цифрової трансформації України. 26.07.2023. http://surl.li/idibne)*.

Міністерство цифрової трансформації України, МО України, Генштаб ЗСУ, Рада національної безпеки і оборони України, Міністерство економіки України та Міністерство з питань стратегічних галузей промисловості України 26 квітня 2023 р. презентували інноваційний кластер оборонних технологій (defense tech cluster) Brave1. Це єдина платформа для співпраці оборонних технологічних компаній, держави та військових, а також інвесторів, волонтерських фондів і медіа. Як показав досвід, скоординована робота та взаємодія учасників кластера дає змогу швидше знаходити й розвивати технологічні рішення у сфері безпеки та оборони. Вже профінансовано понад сотню проєктів на суму, яка значно перевищує $1 млн *(В Україні запустили defense tech cluster BRAVE1, який стимулюватиме розвиток військових інновацій)*. та оборонних технологій. Міністерство цифрової трансформації України. 26.04.2023. http://surl.li/tnlffb

Фінансування розробок з держбюджету потребує, крім іншого, прозорої відповіді на питання щодо виключних майнових прав на об'єкти права інтелектуальної власності, які створено під час розроблення нової зброї саме за державні кошти, враховуючи, що деякі винаходи (корисні моделі) підпадатимуть під дію п. 3 ст. 28 Закону України «Про охорону прав на винаходи і корисні моделі».

Україна також імпортує дрони і необхідне комплектування. Спочатку це були переважно квадрокоптери китайського виробництва невійськового призначення і турецькі розвідувально-ударні БпАК Bayraktar TB2. Після початку широкомасштабної війни почалося постачання БпАК різного призначення з інших країн: США (баражуючі боєприпаси Phoenix Ghost і Switchblade; тактичний безпілотний розвідник RQ-20 Puma); Данії (розвідувальний Heidrun); Німеччини (розвідувальний Vector); Австралії (багатоцільовий PPDS); Польщі (дрон-камікадзе Warmate); Тайваню (дрон-міномет Revolver 860) та ін.

За ініціативою Латвії в лютому 2024 р. для постачання БпАК в Україну створено так звану Коаліцію дронів, до складу якої увійшли Латвія, Велика Британія, Швеція, Данія, Німеччина, Литва, Естонія та Нідерланди. Очолили коаліцію Латвія і Велика Британія. Згодом до цієї коаліції приєдналися ще сім країн, зокрема Франція, Канада, Австралія. У липні 2024 р. члени Коаліції дронів підписали Меморандум про взаєморозуміння, згідно з яким має бути створено спецфонд на 45 млн. За даними Міноборони, Україна вже отримала тисячі БпАК від країн-партнерів. Крім того, завдяки спільним зусиллям було зібрано 50 млн для закупівлі ще 20—30 тис. безпілотників. Ще одним важливим рішенням Коаліції дронів стала можливість для українських виробників безпілотних технологій долучитися до тендерів, які організовує коаліція у межах Контактної групи з питань оборони України у форматі «Рамштайн».

Втім, залишається низка проблемних питань, пов'язаних з ризиками вітчизняного виробництва БпАК. Зокрема, це значна залежність від імпорту компонентів, переважно з Китаю; постачання мікрочипів, без яких неможливо виробляти безпілотники. Крім того, китайські напівпровідники в кілька разів дешеві, ніж тайванські, американські, канадські чи європейські, але вони недостатньо якісні і до того ж їх масово скуповує противник. Інша проблема — швидкоплинність вимог сучасної війни до застосування новітніх технологій, що потребує від виробників і зарубіжних партнерів майже миттєвої реакції — внесення відповідних змін у безпілотні технології, а також у технології РЕБ для протидії БпАК противника.

Технічні інновації

Сучасні дронові технології революційно впливають на архітектуру бойових дій. Розуміючи різницю в потенціалах з ворогом, Україна з допомогою західних партнерів зробила ставку на асиметрію — технічні інновації військового призначення, тобто активне створення та оперативне використання високотехнологічних видів озброєння, що має компенсувати переваги противника. Україна не мала сприятливого технологічного ландшафту для інновацій у сфері різних за призначенням дронів, але війна перетворила країну на своєрідну суперлабораторію передових технічних рішень, що дало можливість зробити гігантський технологічний стрибок і неймовірними темпами впроваджувати інновації.

Наочним прикладом є створення широкого спектра дронів — від БпАК різного призначення (розвідувальні; ударні тактичного, оперативно-тактичного й стратегічного характеру дії; багатоцільові; БпЛА-винищувачі) до наземних (ударні, транспортні, багатоцільові), надводних (ударні, транспортні, багатоцільові) і ударних підводних дронів.

Важливою інновацією став перехід до використання штучного інтелекту в технологічній гонці, яка розгорнулася під час широкомасштабної війни, з метою зменшення впливу людини на виконання завдань. Українські виробники не залишаються осторонь і розробляють окремі технології на базі ШІ. Машинне навчання і ШІ є одним з чотирьох пріоритетів defense-tech кластера Brave1. Так, у 2023 р. до експлуатації в ЗСУ було допущено БпАК Saker Scout, який має побудоване на алгоритмах ШІ програмне забезпечення. Комплекс складається з кількох БпЛА, один з яких виконує функцію розвідника і може самостійно розпізнавати ворожу техніку, навіть замасковану, визначати її координати та передавати цю інформацію на командний пункт, зокрема з використанням автоматизованої системи управління військами «Дельта». Його головним завданням є наведення на цілі FPV-дронів, які також входять до складу комплексу *(ЗСУ отримали дрон Saker Scout із повноцінним штучним інтелектом: чому це більше ніж важливо. Defense Express. 04.09.2023. http://surl.li/vcrmep)*.

Компанія Twist Robotics представила тестову версію свого програмного забезпечення на базі ШІ, яке здатне забезпечити оновлення українського арсеналу FPV-дронів. Інша компанія, DevDroid, у 2023 р. розробила бойовий модуль з використанням ШІ. Нейромережа дозволяє знаходити ціль — ворожих солдатів — на відстані 800 м, автоматично фіксувати її на полі бою, наводити кулемет і налаштовувати балістику. *(Горбулін В.П., Мосов С.П. Рої дронів — кульмінація дронізації воєн. Вісник НАН України. 2024. № 3. С. 3—11. https:// doi.org/10.15407/visn2024.03.003)*.

Вагомою інновацією стало інтегрування у БпЛА Nemesis терміналів супутникового зв'язку Starlink, що забезпечило безперебійність зв'язку і дозволило подолати обмеження звичайного зв'язку.

Сьогодні ШІ допомагає ударним дронам орієнтуватися в польоті та уникати перешкод, зокрема від РЕБ і РЕП, а українські розробники впритул підійшли до створення автономних ударних БпЛА з використанням алгоритмів ШІ.

Війни виграють не лише на полі бою, а й у лабораторіях та на виробництві. Щоб збільшити кількість і різноманітність інновацій, Україна кардинально мінімізувала бюрократію. Цей крок дозволив приватним компаніям отримувати оперативне схвалення, укладати контракти, внаслідок чого інновації швидко впроваджуються, а отже, виробляється і розгортається необхідна військовим зброя.

Тактика застосування дронів

Наявність сучасного озброєння та військової техніки вважають потенціалом, який перетворюється на конкретні бойові можливості завдяки розумінню того, як і за яких умов їх застосовувати на полі бою. Під час широкомасштабної війни сформувалася тактика застосування дронів, що кардинально вплинуло на ведення як загальновійськового бою, так і бойових дій на морі.

Слід зазначити, що спочатку дрони повітряного базування, а потім наземні, надводні та підводні дрони, системно вплинули на динаміку бойових дій, зробили війну більш динамічною, ніж очікувалося на її початку, і фактично змінили поле бою та надали доступні й недорогі можливості в масштабах, яких раніше не було. Саме ця війна спричинила революційний прорив у використанні БпЛА як зброї – ще ніколи і ніде не було на них такого попиту.

Одна з важливих змін на полі бою пов'язана з масовим застосуванням FPV-дронів із різними бойовими частинами для знищення військової т ехніки та живої сили противника. Значущою перевагою таких безпілотників є їхня низька ціна і висока точність застосування. Так, FPV-дрон, вартість якого не перевищує $1 тис., здатен нести заряд, який у разі успішного влучання може уразити і навіть повністю знищити БМП чи танк противника вартістю кілька мільйонів доларів. Для забезпечення більшої ефективності застосування FPV-дронів і обізнаності зовнішніх пілотів вони діють разом із розвідувальними БпЛА.

Масове використання FPV-дронів змушує противника шукати нові тактики застосування своїх підрозділів на полі бою, винаходити нові методи захисту військової техніки, стимулювати розвиток невеликих за розміром засобів РЕБ для захисту окремої одиниці техніки чи окопу від ураження FPV-дронами.

Модифіковані FPV-дрони успішно використовують також і як перехоплювачі проти розвідувальних та ударних БпЛА противника.

Застосування з боку України ударних дронів-камікадзе по об'єктах в оперативно-тактичній та оперативній глибині противника наочно продемонструвало реальність асиметричного підходу до ведення бойових дій — можливість завдавати ворогу точних і відчутних ударів за допомогою дешевих БпЛА.

Завдяки масовому використанню розвідувальних БпЛА зросла ситуаційна обізнаність військ під час вогневого ураження, що дозволило реалізувати окрему концепцію розвідувально-вогневих комплексів, які працюють у режимі реального часу, підвищити точність стрільби ствольної та реактивної артилерії, а також скоротити використання боєприпасів.

Розширення можливостей ведення розвідки об'єктів противника на тактичному й оперативному рівнях з отриманням інформації від розвідувальних БпЛА в режимі реального часу стало важливим фактором підвищення ефективності оперативного управління військами в умовах мобільної оборони або мобільного наступу, коли обстановка на полі бою може швидко змінюватися.

Застосування БпЛА для підвищення ситуаційної обізнаності військ стало обов'язковою процедурою перед початком маневрів чи атаки, обмежило тактичну раптовість дій з боку противника, змусило війська противника розосереджуватися і ховатися, що загалом ускладнює маневрування та проведення атак на українські позиції.

Дрони наземного базування стають важливим елементом ведення бойових дій під час широкомасштабної війни. Такі дрони виконують різні завдання: спостереження, транспортування боєприпасів, харчів, ліків, усього необхідного для облаштування позицій, евакуації поранених, мінування й розмінування, підриву та вогневого ураження противника (бойові модулі, оснащені протитанковими засобами, великокаліберними кулеметами та іншим озброєнням).

Однак використання наземних дронів має певні обмеження порівняно з дронами повітряного і надводного базування. Насамперед це пов'язано з труднощами орієнтування в щільній забудові, проблемами руху бездоріжжям, подолання різних перешкод на шляху (уламків снарядів, будівельного сміття, решток підбитої техніки), а також з небезпекою їх знищення, наприклад FPV-дронами противника.

Взаємодія з дронами повітряного базування збільшує ймовірність виконання завдань наземними дронами. Подальше масштабування дронів наземного базування може привести до кардинальних змін у тактиці ведення загальновійськового бою.

Українські дрони морського базування вже змінили тактику бойових дій на морі. Вони показали вражаючий результат в умовах реальних бойових дій у водах Чорного моря проти бойових кораблів противника. Фактично український прецедент застосування морських дронів поставив перед світом питання: яким має бути правильний баланс між традиційним військово-морським флотом і дронами морського базування?

Досвід воєнних конфліктів показує, що впровадження нової зброї веде не лише до розвитку воєнного мистецтва, а й до змінення структури і складу збройних сил протиборчих сторін. Саме такі зміни стали наслідком активної дронізації в Україні. Так, з метою нарощування спроможностей ЗСУ щодо ефективного використання дронів повітряного, морського та наземного базування було ухвалено рішення про створення окремого роду військ — Сил безпілотних систем (Указ Президента України № 51/2024 від 06.02.2024), а в структурі Генштабу ЗСУ з'явилося Головне управління безпілотних систем. Ще у лютому 2023 р. Генштаб ЗСУ започаткував створення окремих ударних рот БпАК. За рік планувалося організувати 60 таких підрозділів, але зрештою їх виявилося набагато більше. Також у серпні 2023 р. у складі Військово-морських сил ЗСУ було сформовано окрему бригаду для застосування морських безпілотників.

Отже, дронізація набула в Україні стратегічного характеру, що дає змогу посилювати війська й успішно забезпечувати асиметричність бойових дій у повітрі, на землі та морі.

У вирішенні питань підвищення обороноздатності держави, зокрема й дронізації, важливу роль відіграє НАН України. З початком широкомасштабної війни було актуалізовано і значно розширено тематику наукових досліджень, спрямованих на забезпечення оборони та безпеки держави. Перелік пріоритетних наукових досліджень та науково-технічних розробок за цим напрямом погоджується з Міністерством оборони України та Мі ністерством з питань стратегічних галузей промисловості України. Оборонна тематика в Академії реалізувалася спочатку в рамках цільової науково-технічної програми НАН України «Дослідження і розробки з проблем підвищення обороноздатності і безпеки держави», яку було започатковано ще в 2015 р. (постанова Президії НАН України № 5125 від 25.02.2015); потім у 2020—2024 рр. діяла цільова науково--технічна програма оборонних досліджень НАН України, яку було подовжено на 2025—2029 рр. Метою цих програм є створення установами НАН України розробок, спрямованих на підвищення обороноздатності і безпеки держави, та їх впровадження на підприємствах оборонно-промислового комплексу.

Враховуючи позитивні результати, досягнуті впродовж 10 років, досвід академічної підтримки науково-прикладних досліджень оборонного призначення, а також зважаючи на те, що розвиток оборонно-промислового комплексу і посилення його інноваційної складової завжди має бути одним із найголовніших пріоритетів державної політики, з боку держави доцільно актуалізувати питання підтримки та більшої інтеграції академічної науки у сек тор державно-приватного партнерства з метою зміцнення інноваційного фундаменту для створення перспективних зразків озброєння та військової техніки в Україні.

Володимир Павлович Горбулін
академік НАН України, перший віцепрезидент НАН України

Сергій Петрович Мосов
доктор військових наук, професор кафедри авіації та авіаційного пошуку і рятування Інституту державного управління та наукових досліджень з цивільного захисту

Блокчейн у питаннях та відповідях

Технологія блокчейн останнім часом стала потенційним розв'язанням проблем безпеки. Спочатку вона була розроблена як технологія, що лежить в основі таких криптовалют, як біткойн, нині блокчейн – це децентралізована і незмінна бухгалтерська книга, яка реєструє транзакції в мережі комп'ютерів. Його унікальні властивості, включаючи прозорість, незмінність та криптографічну безпеку, призвели до можливості його застосування далеко за межами фінансових операцій.

Технологія блокчейн – це вдосконалений механізм бази даних, який дозволяє організувати відкритий обмін інформацією у рамках бізнес-мережі. База даних блокчейна зберігає дані в блоках, пов'язаних між собою в ланцюжок. Дані хронологічно послідовні, оскільки не можна видаляти або змінювати ланцюжок без консенсусу з боку мережі. В результаті ви можете використовувати технологію блокчейн для створення незмінного або безстрокового реєстру для відстеження замовлень, платежів, рахунків та інших транзакцій. Система має вбудовані механізми, які запобігають несанкціонованому введенню транзакцій та створюють узгодженість у загальному поданні цих транзакцій.

У чому полягає важливість технології блокчейн?

Традиційні технології баз даних створюють низку проблем, пов'язаних з урахуванням фінансових операцій. Розглянемо приклад із продажем нерухомості. Після передачі грошей право власності переходить до покупця. Як покупець, так і продавець можуть самостійно реєструвати грошові операції, але жодної зі сторін не можна довіряти. Отримавши гроші, продавець може легко стверджувати, що він їх не отримав, а покупець може стверджувати, що гроші надіслано, навіть якщо це не так.

Щоб уникнути можливих юридичних проблем, довірена третя сторона повинна контролювати та підтверджувати транзакції. Присутність цього центрального органу не тільки ускладнює угоду, а й створює єдину вразливу точку. Від порушень у центральній базі даних постраждають обидві сторони.

Блокчейн передбачає такі проблеми шляхом створення децентралізованої, захищеної від несанкціонованого доступу системи для запису операцій. У разі угоди з нерухомістю блокчейн створює єдиний реєстр для покупця та продавця. Усі транзакції мають бути схвалені обома сторонами та автоматично оновлюватись у їх реєстрах у режимі реального часу. Будь-яка невідповідність історії транзакцій позначиться у всьому реєстрі. Ці властивості технології блокчейн зробили її популярною у різних секторах. Наприклад, вони використовувалися при створенні цифрової валюти Bitcoin.

Як різні галузі використовують блокчейн?

Експерти з безпеки вже звернули увагу на технологію блокчейн. Легко випустити з уваги потенційні переваги і недоліки будь-якої нової технології, коли галас навколо неї часом досягає лихоманки – як це відбувається з блокчейном.

Згідно з прогнозом Transparency Market Research до кінця 2024 року глобальний ринок застосування технології blockchain досягне 20 мільярдів доларів. Він має величезний потенціал для зниження витрат, особливо для фінансових установ, тому експерти вважають, що до 2025 року обсяг доданої вартості блокчейну зросте до 176 мільярдів доларів.

Блокчейн вторгається в багато галузей промисловості, і немає сумніву, що він пропонує важливі потенційні переваги для ділового світу. У сфері безпеки даних він може стати важливим інструментом перетворення. Якщо ви плануєте використовувати блокчейн, то виділіть деякий час, щоб зрозуміти його. Насамперед потрібно визначити, як він може допомогти вашому бізнесу. Вам потрібна чітка стратегія та вагомі причини для прийняття нової технології. Отже, де зараз використовується технологія блокчейн?

Енергетика

Енергетичні компанії використовують технологію блокчейн для створення однорангових платформ для торгівлі енергоносіями та спрощення доступу до відновлюваних джерел енергії. Як приклад розглянемо такі види використання:

– Енергетичні компанії, робота яких заснована на блокчейні, створили торгову платформу для продажу електроенергії між приватними особами. Власники будинків із сонячними батареями використовують цю платформу для продажу надлишків сонячної енергії сусідам. Процес практично повністю автоматизований: розумні лічильники створюють транзакції, а блокчейн їх записує.

– Завдяки ініціативам блокчейн-краудфандингу користувачі можуть спонсорувати та утримувати сонячні батареї в районах, де немає доступу до електроенергії. Також після встановлення сонячних батарей спонсори можуть отримувати орендну плату.

Фінанси

Традиційні фінансові системи (наприклад, банки та фондові біржі) використовують блокчейн-сервіси для управління онлайн-платежами, рахунками та ринковою торгівлею. Наприклад, інвестиційна холдингова компанія Singapore Exchange Limited, що надає послуги з торгових операцій по всій Азії, використовує технологію блокчейн для більш ефективного міжбанківського розрахунку. Впровадження технології блокчейн вирішило кілька проблем, серед яких пакетна обробка та ручна звірка кількох тисяч фінансових транзакцій.

Мультимедіа та розваги

Компанії зі сфери мультимедіа та розваг використовують блокчейн для керування даними про авторські права. Перевірка авторських прав грає ключову роль щодо справедливої винагороди творців. Для фіксації факту продажу чи передачі контенту, захищеного авторським правом, потрібно кілька транзакцій. Sony Music Entertainment Japan використовує блокчейн-сервіси підвищення ефективності технічних засобів захисту авторських прав. Успішне застосування стратегії блокчейна дозволило збільшити ефективність захисту авторських прав, знизивши витрати.

Роздрібна торгівля

Роздрібні компанії використовують блокчейн для відстеження переміщення товарів між постачальниками та покупцями. Наприклад, Amazon подала патент на систему розподіленого реєстру, яка використовуватиме технологію блокчейн для перевірки справжності всіх товарів, що продаються на платформі. На Amazon продавці можуть відображати свої глобальні ланцюжки поставок, дозволяючи учасникам (виробникам, кур'єрам, дистриб'юторам, кінцевим та вторинним користувачам) додавати події до реєстру після реєстрації в центрі сертифікації.

Електронна пошта

Декілька ініціатив та стартапів використовують блокчейн для забезпечення безпеки електронної пошти. Наприклад, такі компанії, як ProtonMail, використовують блокчейн для створення додаткових рівнів безпеки у своєму вже зашифрованому поштовому сервісі.

Іншим прикладом є Mailchain – протокол зв'язку web3, який використовує блокчейн для забезпечення децентралізованого зашифрованого зв'язку електронною поштою безпосередньо на платформах блокчейну. Такий підхід забезпечує безпеку, відстеження та незмінність електронної пошти.

Розробка децентралізованих програм (DApps) для електронної пошти, таких як EtherMail, дозволяє створювати за-

шифровані та анонімні поштові сервіси, які не залежать від традиційних поштових протоколів або серверів.

Якими можливостями володіє технологія блокчейн?

Нижче представлені основні можливості технології блокчейн.

Децентралізація

Децентралізація у блокчейні означає передачу контролю та прийняття рішень від централізованого суб'єкта (окремої особи, організації або їх групи) до розподіленої мережі. Прозорість децентралізованого блокчейну дозволяє нівелювати довіру учасників один до одного. Ці мережі стримують їхню владу або контроль одного над одним, що зберігає функціональні можливості мережі.

Незмінність

Незмінність означає, що дані неможливо змінити. Жоден учасник не може втрутитися у транзакцію після її внесення до реєстру. Якщо запис містить помилку, для її виправлення необхідно додати нову транзакцію. У мережі буде відображено обидві транзакції.

Консенсус

Система блокчейну встановлює набір правил, за допомогою яких учасники схвалюють транзакції. Нові транзакції можна реєструвати лише за згодою більшості учасників мережі.

Які ключові компоненти лежать в основі технології блокчейн?

Розподілений реєстр

Розподілений реєстр – це загальна база даних у блокчейн- мережі, в якій зберігаються копії транзакцій (наприклад, у вигляді загального файлу, що редагується всіма учасниками). У більшості спільних текстових редакторів будь-який користувач з правами редагування може видалити файл повністю. Однак, технології розподілених реєстрів мають суворі правила щодо того, хто і як може редагувати файл. Наприклад, не можна видаляти записи після реєстрації.

Смарт-контракти

Компанії використовують смарт-контракти для самостійного управління комерційними угодами без залучення третьої сторони. Смарт-контракти – це програми в блокчейн-системі, що автоматично запускаються при дотриманні заданих умов. Транзакції записуються до реєстру, якщо вони відповідають умовам перевірки « якщо,... то». Наприклад, у логістичної компанії може бути укладено смарт-контракт, за яким оплата здійснюється автоматично після прибуття товару до порту.

Криптографія з відкритим ключем

Криптографія з відкритим ключем – це система безпеки, що дозволяє однозначно ідентифікувати учасників блокчейн-мережі. Система генерує два різні ключі для кожного користувача мережі. Один ключ – публічний, загальний всім учасників мережі. Другий – унікальний приватний ключ. Поєднання приватного та публічного ключів розблокують дані у реєстрі.

Наприклад, Іван і Ірина – користувачі мережі. Іван записує транзакцію, зашифровану його приватним ключем. Ірина може розшифрувати її за допомогою свого публічного ключа. Таким чином, Ірина може переконатися, що Іван здійснив транзакцію. Якби Іван скористався недійсним приватним ключем, Ірина не змогла б скористатися своїм публічним ключем.

Як працює блокчейн?

Нижче наведено короткий огляд складного механізму блокчейн. Програмне забезпечення блокчейн автоматизує більшу частину процедури:

Крок 1. Запис транзакції

Блокчейн-транзакція відображає переміщення фізичних чи цифрових активів з одного боку до іншого блокчейн-мережі. Вона записується у вигляді блоку даних і може включати такі відомості:

– Хто брав участь у угоді?
– Що сталося під час угоди?
– Коли було проведено угоду?
– Де було проведено угоду?
– Які причини проведення правочину?
– Скільки активів було передано?
– Скільки попередніх умов було виконано під час угоди?

Крок 2. Досягнення консенсусу

Більшість учасників розподіленої блокчейн-мережі повинні підтвердити, що записана транзакція є дійсною. Залежно від типу мережі правила угоди можуть бути різними, але, як правило, вони встановлюються на початку процедури.

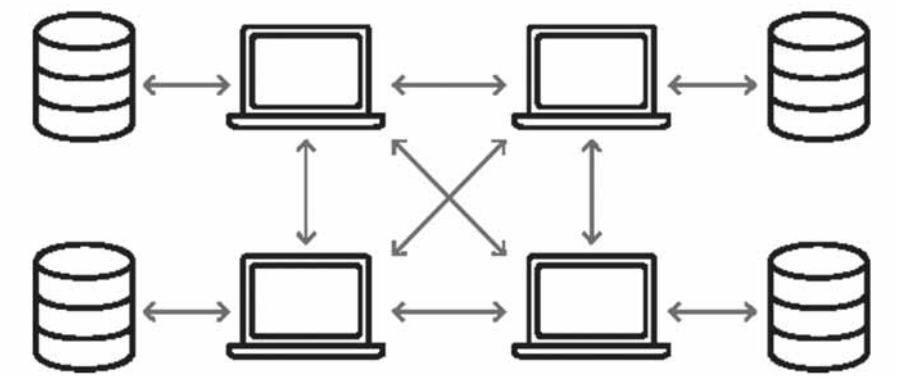
Крок 3. Зв'язування блоків

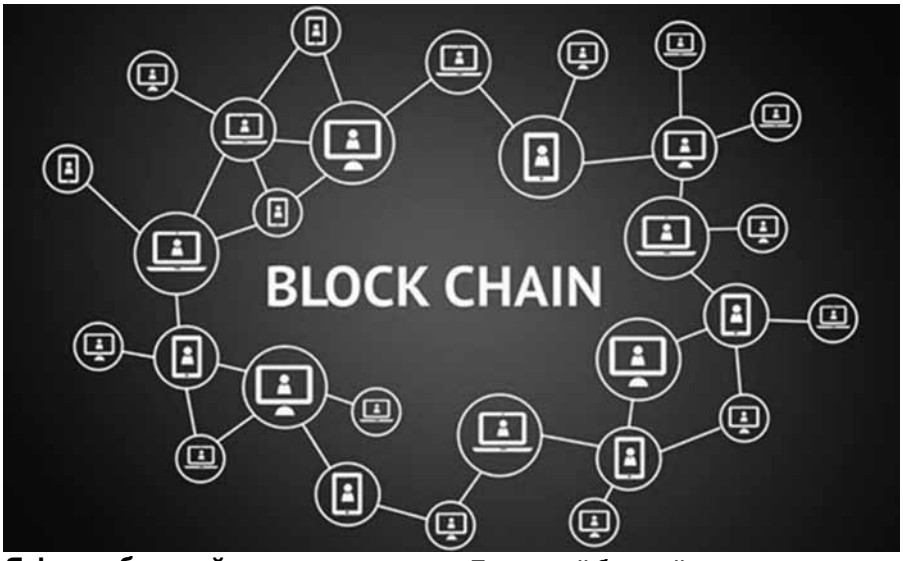
Коли учасники досягають консенсусу, транзакції до блокчейну записуються до блоків, еквівалентних сторінкам реєстру. Разом із транзакціями до нового блоку додається криптографічний хеш. Хеш діє як ланцюжок, що зв'язує блоки разом. Якщо вміст блоку навмисно або випадково змінюється, змінюється значення хешу, що допомагає виявити підробку даних.

Таким чином, блоки та ланцюжки надійно пов'язані, а їх редагування неможливе. Кожен додатковий блок посилює перевірку попереднього блоку і, отже, всього блокчейна. Такий принцип схожий на будівництво вежі з дерев'яних блоків. Блоки можна складати тільки зверху, а якщо прибрати один блок із середини, то впаде вся вежа.

Крок 4. Загальний доступ до реєстру

Система розповсюджує серед усіх учасників останню копію центрального реєстру.





Які типи блокчейн -мереж існують?

У блокчейні існує чотири основних типи децентралізованих або розподілених мереж:

Публічний блокчейн

Публічні блокчейни не вимагають дозволів і дозволяють будь-кому, хто бажає приєднатися до мережі. Усі учасники блокчейну мають рівні права на читання, редагування та перевірку інформації. Для обміну та майнінгу таких криптовалют, як Bitcoin, Ethereum та Litecoin, в основному використовуються публічні блокчейни.

Приватний блокчейн

Приватні блокчейни, які можна назвати керованими, контролюються однією організацією. Уповноважений орган визначає, хто може бути учасником і які права в мережі вони мають. Приватні блокчейни децентралізовані лише частково, оскільки включають обмеження доступу. Приклад приватного блокчейна є Ripple – платформа для обміну цифрової валюти.

Гібридний блокчейн

Гібридний блокчейн поєднує функції як приватних, і публічних мереж. Підприємства можуть створювати як приватні, і публічні системи дозволів. Таким чином, вони контролюють доступ до певних даних в блокчейні, але при цьому підтримують загальнодоступний доступ до інших даних. Вони використовують смарт-контракти, що дозволяють публічним учасникам упевнитися у проведенні приватних транзакцій. Наприклад, гібридні блокчейни можуть надавати публічний доступ до цифрової валюти, зберігаючи приватний доступ до банківської валюти.

Блокчейн-консорціуми

Блокчейн-консорціумами управляє група організацій. Вибрані заздалегідь організації поділяють відповідальність за функціонування блокчейну та визначення прав доступу до даних. Блокчейн-консорціуми часто віддають перевагу компаніям-однодумцям, які отримують вигоду із загальної відповідальності. Наприклад, Global Shipping Business Network – це некомерційний блокчейн-консорціум, що спеціалізується на цифровізації судноплавної галузі та розширенні співробітництва між операторами морських перевезень.

Що таке блокчейн – протоколи?

Термін « блокчейн -протокол» відноситься до різних типів блокчейн-платформ для розробки додатків. Кожен блокчейн-протокол адаптує базові принципи блокчейну до конкретних га-

лузей чи додатків. Нижче наведені деякі приклади блокчейн-протоколів.

Hyperledger Fabric

Hyperledger Fabric – це проект із відкритим вихідним кодом, орієнтований на розробку інструментів та бібліотек. Компанії можуть використовувати його для швидкого та ефективного створення приватних блокчейн-додатків. Hyperledge Fabric – модульна платформа загального призначення. Вона пропонує унікальні можливості для ідентифікації та контролю доступу. Завдяки цим можливостям вона підходить для відстеження ланцюжків поставок, торговельного фінансування, завдань лояльності та винагороди, а також для безготівкових розрахунків з фінансових активів.

Ethereum

Ethereum – це децентралізована блокчейн -платформа з відкритим вихідним кодом, яка використовується для створення публічних блокчейн-додатків. Ethereum Enterprise призначено для комерційного використання.

Corda

Corda це блокчейн-проект з відкритим вихідним кодом для бізнесу. Corda дозволяє створювати сумісні блокчейн-мережі, що гарантують сувору конфіденційність транзакцій. Компанії можуть використовувати технологію смарт-контрактів Corda для проведення швидких та безпечних угод. Більшість користувачів є фінансовими установами.

Quorum

Quorum – це похідний від Ethereum блокчейн-протокол із відкритим вихідним кодом. Він призначений для використання в приватному блокчейні, де тільки один учасник має всі вузли, а також у блокчейн -консорціумі, де кожен учасник володіє частиною мережі.

Як розвивалася технологія блокчейн?

Історія технології блокчейн почалася наприкінці 1970-х років, коли вчений-інформатик Ральф Меркл запатентував концепцію хеш дерева або дерева Меркла. Ці дерева є структурою даних, що зберігаються в пов'язаних за допомогою криптографії блоках. Наприкінці 1990-х років Стюарт Хабер та У.А. Скотт Сторнетта використовували дерева Меркла для створення системи, де неможливо підробити тимчасові мітки документів. Ця подія стала проривом в історії блокчейн.

Технологія продовжувала розвиватись протягом останніх трьох поколінь.

Перше покоління – Bitcoin та інші віртуальні валюти.

2008 року невідома людина чи група людей під псевдонімом Сатоші Накамото втілили технологію блокчейн у її сучасному вигляді. Для здійснення Bitcoin-транзакцій Сатоші обмежив розмір блоків інформації до 1 МБ.

Друге покоління – смарт-контракти.

За кілька років після появи валюти першого покоління розробники вирішили розглянути використання блокчейн не лише в рамках криптовалют. Наприклад, винахідники Ethereum вирішили використовувати технологію блокчейн в операціях з передачі активів. Значним внеском стала можливість використання смарт-контрактів.

Третє покоління – майбутнє.

У міру того, як компанії впроваджують нові додатки, технологія блокчейн продовжує вдосконалюватися. Компанії долають обмеження масштабу та обчислень, а потенціал розвитку блокчейну безмежний.

Якими перевагами володіє технологія блокчейн?

Технологія блокчейн має безліч переваг для управління транзакціями.

Розширені можливості забезпечення безпеки

Блокчейн забезпечує високий рівень безпеки та довіри, якої потребують сучасні цифрові транзакції. Завжди є ризик, що хтось маніпулюватиме базовим програмним забезпеченням, щоб заробити гроші нечесним шляхом. Але три принципи блокчейну – криптографія, децентралізація та консенсус – забезпечують максимально безпечну базову систему, до якої практично неможливо втрутитися. Система не має слабких місць, і жоден користувач не зможе внести зміни до запису транзакцій.

Підвищена ефективність

Операції між комерційними структурами можуть бути трудомісткими і займати багато часу, особливо щодо відповідності вимогам за участю третіх сторін. Такі особливості блокчейну, як прозорість та використання смарт-контрактів, прискорюють подібні ділові операції та роблять їх ефективнішими.

Швидший аудит

Компанії повинні мати можливість генерувати, обмінювати, архівувати і відновлювати електронні операції надійним способом, що піддається перевірці. Записи зберігаються у хронологічно незмінному порядку. Така прозорість даних значно прискорює аудит.

У чому різниця між Bitcoin та блокчейн?

Bitcoin та блокчейн відрізняються один від одного, хоч і є взаємозамінними. Оскільки в основі Bitcoin лежить технологія блокчейн, люди помилково почали використовувати термін Bitcoin для позначення блокчейну в цілому. Однак у технології блокчейн безліч застосувань і за межами Bitcoin.

Bitcoin – децентралізована цифрова валюта. Спочатку Bitcoin була створена для проведення онлайн транзакцій, але

тепер вона визнана цифровим активом, який конвертується у будь-яку світову валюту (наприклад, у долари чи євро). Публічний Bitcoin-блокчейн створює центральний реєстр, який перебуває під його керуванням.

Мережа Bitcoin

Усі транзакції Bitcoin реєструються у громадському реєстрі, а сервери по всьому світу зберігають його копії. Сервери подібні до банків. Однак банки володіють інформацією лише про гроші клієнтів, тоді як сервери Bitcoin отримують дані про кожну транзакцію Bitcoin, проведену в будь-якій точці світу.

Будь-хто, хто має другий комп'ютер, може налаштувати один із серверів як вузол. Це як відкрити свій власний Bitcoin банк замість банківського рахунку.

Майнінг Bitcoin

У громадській мережі Bitcoin учасники отримують криптовалюту через майнінг – процес розв'язання криптографічних рівнянь для створення нових блоків. Система відкрито розповсюджує вузлами кожну нову транзакцію в мережі. Приблизно кожні десять хвилин майнери збирають ці транзакції в новий блок, постійно додаючи їх у блокчейн, який виступає як кінцевий реєстр для Bitcoin.

Оскільки програмний процес досить складний і тривалий, майнінг потребує значних обчислювальних ресурсів. За свою роботу майнери одержують невелику кількість криптовалюти. Загалом майнери це сучасні клерки, які підтримують мережу Bitcoin та реєструють угоди за комісійні.

За допомогою криптографії всі учасники мережі приходять до консенсусу щодо володіння конкретними монетами.

У чому різниця між базою даних та блокчейном?

Блокчейн – це особлива система управління базами даних з ширшими можливостями. Нижче представлені деякі суттєві відмінності між традиційною базою даних та блокчейном.

– Блокчейн має на увазі децентралізований контроль без втрати довіри до існуючих даних. Цього неможливо досягти в інших системах баз даних.

– Компанії, що беруть участь у угоді, не можуть використовувати базу даних разом. Але в блокчейн-мережах кожна компанія має свою копію реєстру, а їх відповідність підтримується системою автоматично.

– Хоча в більшості баз дані можна редагувати або видаляти, в блокчейн їх можна тільки вносити.

Чим блокчейн відрізняється від хмари?

Термін «хмара» стосується обчислювальних сервісів, доступ до яких можна отримати онлайн. З хмари можна отримати доступ до програмного забезпечення як послуги (SaaS), продукту як послуги (PaaS), а також до інфраструктури як послуги (IaaS). Хмарні провайдери надають онлайн доступ до свого обладнання та інфраструктури. Вони надають набагато більше простого управління базами даних. Для отримання доступу до публічного блокчейну необхідно надати дані про апаратне забезпечення для створення копії реєстру. При цьому можна використовувати хмарний сервер. Також деякі провайдери пропонують готове рішення – блокчейн як послуга (BaaS).

Що таке блокчейн як послуга?

Блокчейн як послуга (BaaS) – це керований хмарний блокчейн-сервіс, що надається третьою стороною. Ви можете розвивати блокчейн-додатки та цифрові послуги, а провайдер надасть відповідну інфраструктуру та інструменти. Щоб швидко та ефективно впровадити блокчейн, потрібно просто налаштувати вже існуючу технологію.

Переваги технології блокчейн

– **Децентралізація**. Ланцюжок блоків працює на основі мережі учасників, що унеможливлює залучення централізованого управління. Це забезпечує більш рівний та прозорий доступ до інформації, а також управління системою.

– **Безпека**. Блокчейн використовує криптографію для забезпечення безпеки транзакцій та даних. Кожен блок пов'язаний із попереднім з використанням хеш-функцій, що максимально ускладнює можливість зміни інформації.

– **Прозорість**. Оскільки блокчейн є громадським реєстром, всі транзакції видно всім учасників мережі. Це підвищує довіру та відкритість у відносинах між учасниками. Однак це певною мірою є і недоліком блокчейну.

– **Ефективність**. Блокчейн може спростити та автоматизувати процеси, виключаючи необхідність залучення посередників та скорочуючи витрати на рутинні операції.

– **Надійність**. Ланцюжок блоків має високу стійкість до збоїв та атак, оскільки дані учасників зберігаються та перевіряються на всіх пристроях мережі. Це робить систему стійкою до відмови.

Недоліки технології блокчейн

– **Масштабованість**. Один з головних недоліків блокчейна – його обмежена масштабованість. При збільшенні кількості учасників мережі блокчейн швидкість проведення транзакцій знижується. Це відбувається через те, що кожен блок повинен бути перевірений кожним учасником у мережі, що потребує значного часу.

– **Споживання енергії**. Ланцюжок блоків особливо, який використовує алгоритм PoW, може споживати велику кількість енергії. Це пов'язано з процесом «майнінгу», який вимагає значних обчислювальних потужностей до виконання складних математичних завдань. Використання такої кількості енергії може бути не дуже бажаним з екологічної точки зору.

– **Атака 51%**. Блокчейн стикається з ризиком атаки 51%, коли один учасник мережі контролює більше половини обчислювальної потужності. У такому випадку цей користувач може контролювати та змінювати дані в блоках, порушуючи цілісність та безпеку мережі. Проте це (теоретично) можливе лише у маленьких блокчейн-мережах.

– **Неможливість зміни даних**. Дані, що були додані в блокчейн неможливо змінити. Це може бути недоліком блокчейну, у разі внесення до нього помилкових даних. Звичайно, деякі ланцюжки блоків передбачають таку можливість, але більшість немає.

– **Проблеми приватності**. Ланцюжок блоків є відкритим та прозорим реєстром, що викликає питання щодо приватності даних. Незважаючи на те, що адреси не пов'язані безпосередньо з іменами користувачів, активності в ланцюжку блоків можуть бути відстежені та проаналізовані, що створює можливі проблеми в галузі конфіденційності.

– **Відторгнення нових технологій**. Блокчейн – це відносно нова технологія, яку багато людей досі не готові прийняти. Або вони просто не розуміють її. Це створює перепони для масового прийняття та використання блокчейну у різних секторах суспільства.

На закінчення

Незважаючи на свої недоліки, блокчейн пропонує унікальні переваги та продовжує розвиватися. Йому ще далеко до масового впровадження, проте багато галузей вже вивчають його переваги та недоліки. Швидше за все, у найближчі кілька років компанії та уряди експериментуватимуть з новими способами застосування блокчейну та намагатимуться отримати з нього вигоду.

Є. Лукін

За матеріалами:

https://academy.binance.com/ru/articles/positives-and-negatives-of-blockchain

https://gerchik.co/ru/blog/kriptovalyuty/blokchejn-tehnologiya-budushhego

https://aws.amazon.com /ru/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc

https://powerdmarc.com/ru/blockchain-e-mail-security/

https://polygant.net/ru/blog/kak-blokchejn-mozhet-povysit-bezopasnost-dannyh/

https://miner-world.ru/blog/nachinayushim-majneram/kakie-u-blokchejna-est-nedostatki-i-preimushestva-podrobnyj-razbor

В Україні не вистачатиме понад 500 тисяч працівників

Конкуренція між державними установами та приватними компаніями стала одним із головних викликів на ринку праці. У 2025 році наша держава може зіткнутися з нестачею понад півмільйона кваліфікованих працівників.

Брак кваліфікованих кадрів уже зараз суттєво впливає на динаміку зарплат, що в контексті зростання ВВП викликає питання в економістів. Таку думку озвучив президент Конфедерації роботодавців Михайло Мірошниченко.

«ВВП зростає на 4%, а заробітні плати збільшуються на 14%. Так, зростання зарплат має бути більшим, ніж зростання цін і ВВП, але не в таких пропорціях», — сказав Мірошниченко.

За словами експерта, державний сектор приваблює стабільністю, тоді як приватний готовий пропонувати вищі зарплати, щоб залучити кваліфікованих спеціалістів. Це призводить до зростання плинності кадрів і загострення боротьби за кваліфікованих фахівців.

Основні чинники, що впливають на ситуацію:

- **Еміграція:** через війну та економічну нестабільність багато українців виїхали до Європи у пошуках вищого доходу.
- **Демографічний спад:** зменшення кількості працездатного населення створює додатковий дефіцит робочої сили.
- **Непопулярність технічних професій:** молодь дедалі менше обирає робітничі спеціальності, а це порушує баланс на ринку праці.

Раніше Європейська Бізнес Асоціація провела дослідження, яке показало, що 46% компаній планують розширення штату, 7% мають намір скоротити чисельність працівників, а 47% не планують змін у кадровій політиці.

Основними викликами для ринку праці залишаються: дефіцит робочої сили; невідповідність очікувань зарплати кандидатів можливостям бізнесу; мобілізація; відтік персоналу за кордон.

vinbazar.com/

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!

Ідея створення легкого штурмового літака

Значне збільшення використання Росією ударних безпілотників типу Shahed вимагає від України нових підходів для їх ефективного перехоплення та знищення.

Окрім використання зенітних гарматних та ракетних систем, були зафіксовані випадки перехоплення за допомогою гелікоптерів із застосуванням бортових кулеметів.

Крім того, існує значна ймовірність використання нових засобів для боротьби з ударними безпілотниками. Серед них розглядається легка бойова авіація, зокрема літаки типу Cessna AC-208.

Поява легких ударних літаків пов'язана насамперед з активним використанням піхоти у локальних війнах, де ворог мав обмежені види озброєння, відсутність серйозних засобів протиповітряної оборони, а переносні зенітні ракетні комплекси (ПЗРК) були недостатньо поширеними.

Одним із таких легких ударних літаків стала Cessna AC-208B, розроблена на базі літака Cessna 208B Grand Caravan, яких на сьогодні було вироблено понад 3 тисячі одиниць.

Розроблений у 1980-х роках, Cessna 208 Caravan є цивільним пасажирським літаком, що здобув широке визнання у світі завдяки своїй надійності та популярності.

Цивільний літак Cessna Caravan. Фото: Liberty Jet Management

Модернізацію літака у бойовий варіант здійснювала компанія Alliant Techsystems, яка у межах проєкту Combat Caravan розробила концепцію поліпшення можливостей літака шляхом інтеграції систем наведення, зв'язку та позиціювання. Проєкт був переданий компанії урядом США у 2008 році.

Модернізований літак отримав здатність виконувати завдання з розвідки, спостереження та здійснення ракетно-бомбових ударів.

Варто зазначити, що розробка модернізації мала на меті підтримку ослаблених Повітряних сил Іраку, які потребували літака для підтримки сухопутних з'єднань у війні проти терористичних воєнізованих формувань на своїй території.

Combat Caravan. Фото: АТК

Ще однією важливою особливістю є те, що розробка літака та його постачання були виконані всього за 11 місяців після завершення проєкту і проведення відповідної сертифікації — як військової, так і цивільної. Це дозволило використовувати літак не лише військовими, а й цивільними організаціями та компаніями.

Набір систем для розвідки та застосування озброєння

Головним напрямком модернізації стало встановлення систем для поліпшення обізнаності пілота. Літак обладнаний тактичними дисплеями, на які виводиться значна частина інформації про політ, система позиціювання, працездатність систем тощо.

Для захисту кабіни та пасажирів встановлені балістичні панелі, здатні витримувати влучання куль калібру 7,62 мм та захищати найважливіші частини літака.

Дисплеї також відображають інформацію із загальної системи позиціювання та передачі даних STAR, розробленої АТК. Ця система забезпечує можливості розвідки та управління вогнем удень і вночі.

Система включає компактний блок захисту двигуна (MPU), 18-дюймовий кольоровий дисплей Avedon та інтегровану систему управління вогнем.

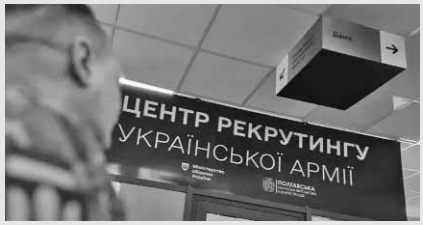
Кокпіт літака Combat Caravan. Фото: АТК

Інтегрована система управління вогнем поєднана з дисплеєм та підвісним контейнером MX-15D, який використовується для проведення розвідки, має тепловізійний канал та інтегрований блок лазерного цілевказання.

Типовий склад станції включає оптико-електронний блок, блок і пульт управління з маніпулятором типу джойстик. Залежно від моделі вона може додатково оснащуватися виносним рідкокристалічним монітором і пристроєм запису та зберігання відеоінформації. Для передачі на наземний пункт прийому й обробки інформації або переносний термінал прийому відеозображень використовується цифровий передавач і підвісний контейнер MX-POD із двома антенами УКХ-діапазону частот.

Спеціальності, які обирають в рекрутингових центрах ЗСУ

Топ 7 спеціальностей, які обирають в рекрутингових центрах української армії



Вакансії, пов'язані з БПЛА, водійськими та стрілецькими напрямками, користуються найбільшим попитом серед військовослужбовців, які долучаються до Сил оборони через центри рекрутингу української армії.

Вакансії, пов'язані з БПЛА, водійськими та стрілецькими напрямками, користуються найбільшим попитом серед громадян, які долучаються до Сил оборони через центри рекрутингу української армії.

Станом на середину січня 2025 року, топ 7 груп спеціальностей виглядає так:

- спеціальності, пов'язані з БПЛА – 16%;
- водії – 16%;
- стрілецькі спеціальності – 15%;
- штабні посади – 9%;
- артилерія – 6%;
- бойові медики, фельдшери, медсестри, лікарі – 5%;
- зв'язок та кібербезпека – 5%.

Протягом минулого тижня до центрів рекрутингу української армії звернулось 1 282 особи. Загалом з початку роботи центрів загальна кількість відвідувачів сягнула 35 337, з яких 7 800 з них вже стали кандидатами до лав Сил оборони України.

«Головна перевага долучитись до оборони України за допомогою рекрутингових центрів – це можливість обрати спеціальність за бажанням та здібностями кандидата. Також майбутній захисник отримає розширений пакет пільг та соціальних гарантій. Державна підтримка поширюється й на членів сімей військовослужбовців. В рекрутингових центрах підготовлені фахівці нададуть вам всю необхідну інформацію про військову службу, а також здійснять супровід кандидата на всіх етапах оформлення документів», - зазначив заступник міністра оборони України бригадний генерал юстиції Сергій Мельник.

Нагадаємо, в Україні працює 47 рекрутингових центрів української армії. Найбільшу активність демонструють мешканці Дніпропетровської, Харківської, Львівської, Запорізької областей та міста Києва.

Центри рекрутингу пропонують понад 10 000 вакансій у різних військових формуваннях, зокрема у Збройних силах України, Національній гвардії, Державній прикордонній службі та СБУ. Всі консультації щодо військової служби надаються з дотриманням умов конфіденційності.

Детальна інформація про роботу центрів рекрутингу та контакти доступні на сайті: https://recruiting.mod.gov.ua/.

/recruiting.mod.gov.ua/

Combat Caravan з підвісним контейнером MX-15D. Фото: Airforce Technology

Станція MX-15D (AN/AAQ-35) має оптико-електронний блок, змонтований на гіростабілізованій у чотирьох площинах платформі, залежно від вимог замовника, може оснащуватися шістьма різними приладами. Останнім часом можлива установка кольорової ТВ-камери високої роздільної здатності (HD) та вдосконаленого апаратно-програмного забезпечення.

Оптико-електронна система MX-15D. Фото L3 Harris WESCAM

Завдяки цьому літак здатен використовувати авіаційне озброєння з напівактивними головками самонаведення, зокрема високоточні бомби малого калібру та авіаційні ракети, як-от Hellfire.

Ці ракети є основою ракетного озброєння літака і дають змогу вражати надводні та наземні цілі на відстані до 10 км. При використанні ракет модифікації «К» літак здійснює лазерне цілевказання для точного ураження, а у разі використання варіанта ракети з активною головкою самонаведення лазерного цілевказання не потребується.

AC-208 оснащений турбогвинтовим двигуном Pratt & Whitney PT6, який забезпечує потужність 675 кінських сил.

Також літак обладнаний системою захисту AAR-47/ALE-47.

Елементи системи захисту літака AAR-47. Фото: Orbital ATK

Система ALE-47 може працювати в автоматичному, напівавтоматичному, ручному та обхідному режимах. Вона призначена для протидії ракетам, що наводяться за допомогою інфрачервоного випромінювання та радіочастот.

Замовлення на літак

ATK отримала низку замовлень на модифікацію C-208 від США. У 2009 році компанія завершила модифікацію 11 літаків, включаючи три розвідувальні версії RC-208B, п'ять навчальних варіантів C-208B та три AC-208B Combat Caravan. Третій AC-208B було поставлено в листопаді 2009 року.

Того ж року уряд США передав один AC-208 Combat Caravan Лівану. Повідомляється, що в січні 2011 року Військово-повітряні сили США розмістили замовлення на $14,7 млн з ATK на ще один літак AC-208 для Військово-повітряних сил Лівану (LAF), призначений для операцій проти повстанців. У жовтні 2016 року адміністрація США схвалила можливий продаж двох літаків Cessna AC-208 разом із пов'язаним обладнанням для Іраку.

У серпні 2016 року ATK виграла контракт на забезпечення логістичної підтримки для літаків Cessna 208B ISR Caravan та Cessna 208B Armed Caravan, що належать Військово-повітряним силам Іраку.

У березні 2018 року Orbital ATK, яку згодом придбала компанія Northrop Grumman, отримала контракт на $86 млн. Він покривав вимоги щодо озброєних літаків AC-208 ISR для Військово-повітряних сил Афганістану.

8 березня 645-а група авіаційних систем ВПС США уклала з компанією контракт на суму $86,4 млн за фіксованою ціною. На момент підписання угоди було виділено $42,3 млн із фондів афганських сил безпеки. Роботи над літаками у Форт-Ворті завершили до 9 червня наступного року.

У межах цього контракту сім літаків Cessna 208B Grand Caravan переобладнали в озброєну ISR-конфігурацію, як зазначено в оголошенні на сайті Федеральних можливостей бізнесу уряду США від 27 грудня.

1 вересня 2018 року Orbital ATK виконала ще один контракт на постачання AC-208 для AAF. Угода на суму $69,3 млн передбачала виділення $33,9 млн із фондів афганських сил безпеки. Цей контракт завершили до 30 листопада того ж року. Точна кількість літаків у межах угоди не була розкрита.

Уже після зміни влади в країні 12 літаків перелетіли до Таджикистану, де наразі перебувають, паралельно шукаючи нового власника, яким потенційно може стати й Україна.

Потенційні можливості у боротьбі з Shahed

Відповідно до технічного опису, літак має достатню кількість систем і необхідне озброєння для перехоплення ударних безпілотників типу Shahed. Насамперед, це ракети Hellfire, які, незважаючи на початкове призначення для боротьби з радянськими танками, мають модифікації з уламково-фугасною бойовою частиною. Наведення ракет здійснюється за допомогою напівактивної або активної ГСН у деяких модифікаціях.

Під час польоту ракета може розвивати швидкість до 450 м/с, а її дальність становить близько 10 км для наземних цілей. У разі

Ракета AGM-114 Hellfire K. Фото: US Army

стрільби в задню напівсферу по повітряних цілях ця дальність може становити від 5 до 8 км залежно від швидкості повітряної цілі.

Варто зазначити, що можливість використання ракет Hellfire проти повітряних цілей була підтверджена ще на початку 2000-х років, коли вони використовувалися у прототипі американської армійської системи протиповітряної оборони. Також цю можливість продемонстрували американські гелікоптери, які застосовували ракети Hellfire для перехоплення безпілотників під час навчань у Саудівській Аравії.

Cessna Combat Caravan під час пуску ракети AGM-114. Фото :US Air Force

Зважаючи на те, що використання цих ракет для повітряних цілей є доволі дорогим, цей варіант розглядається лише для літаків, які певним чином не були модернізовані. Технічно важливою є можливість установки інших ракет.

Так існує ймовірність інтеграції ракет Martlet виробництва британської компанії MBDA UK, а також американських ракет Stinger. Їх інтеграція можлива за умов короткотермінової та відносно недорогої модернізації.

У разі інтеграції ракет Martlet необхідно налаштувати підвісний контейнер для лазерного цілевказання, оскільки ракети мають напівактивну головку самонаведення. Це дозволяє якісніше супроводжувати ціль до її ураження. Вагомою перевагою ракети є її швидкість, яка становить 1,9 Маха, і дальність польоту до 10 км.

Сьогодні Україна вже використовує ракети цього типу, які входять до складу переносних зенітно-ракетних комплексів LMM, а також самохідних зенітно-ракетних комплексів Stormer HVM, що працюють паралельно з ракетами Martlet.

Також як опція можлива інтеграція кулеметного озброєння яке може складатись з 7.62 мм кулеметів, у тмоу числі авіаційний варіант FN MAG, який використовуєтсья для обстрілу наземних цілей.

Окрім своїх можливостей, важливу роль відіграє і вартість використання цих літаків, а також вартість години польоту. Так, для літаків Combat Caravan година польоту складає від 400 до 1 500 доларів, водночас залучення гелікоптерів Ми-8 разом з H145, який залучається для наведення, складає від 340 до 4 500 доларів США для Ми-8 та 1 870 євро і більше для H145.

Роман Приходько
mil.in.ua

Чи безпечний електротранспорт для людини?

Магнітне поле, джерелом якого є ядро Землі, оточує всю планету. На нього накладається поле Сонця, інших космічних тіл. Тому напруженість земного магнітного поля неоднорідна, залежить від географічного розташування об'єкта. Внесок у цю неоднорідність робить і людина. Наприклад, поблизу ліній електропередач, потужних електричних пристроїв показник завжди вищий, але загалом він залежить від дуже великої кількості факторів.

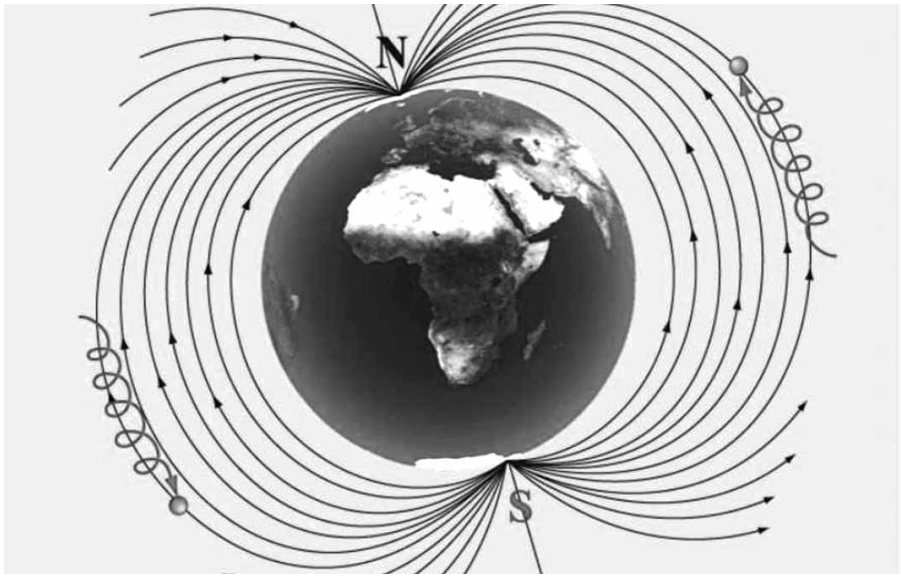
Вплив магнітного поля на людину

Вплив магнітного поля на людину величезний. Він позначається на швидкості перебігу біохімічних процесів, тривалості життя та багато іншого. Кожна молекула, з якої складається речовина, під дією магнітного поля поляризується аналогічно магнітним полюсам Землі. Це прискорює реакції в організмі, сприяє правильному обміну речовин.

Магнітне поле значно впливає на функціонування всіх систем і органів людини. При зменшенні напруженості зовнішнього поля, а також за надмірного збільшення організм виявляється у критичних умовах. Наочний приклад – магнітні бурі, що впливають як на фізичне, а й на психологічне здоров'я. У такі періоди спостерігається зростання кількості захворювань, збільшується кількість злочинів та просто нелогічних вчинків. Ускладнює ситуацію те, що людина не може встановити причини того, що відбувається, адже ступінь впливу на неї магнітного поля можна виміряти лише спеціальним приладом. Органи почуттів тут безсилі.

Власне, організм людини також генерує слабке електромагнітне поле. Нейрони в нервовій системі є носіями електричного заряду, а різних клітинах нашого організму й у крові є іони (заряджені частинки) металів. Важливим моментом є підтримання відносного балансу між зовнішніми та внутрішніми магнітними полями. Безперечним є факт, що зовнішні магнітні поля значною мірою визначають стан внутрішніх магнітних полів. Магнітні поля техногенного та природного походження впливають на циркадні ритми та фізіологічні функції людини, що в результаті позначається на загальному стані. У природних умовах на людину діють лише природні електромагнітні поля, до яких вона налаштувалася протягом усього процесу еволюції на планеті Земля. Коли ж у процес взаємодії втручаються штучні джерела магнітних, електричних і електромагнітних полів, відбувається, як мінімум порушення синхронізації роботи органів.

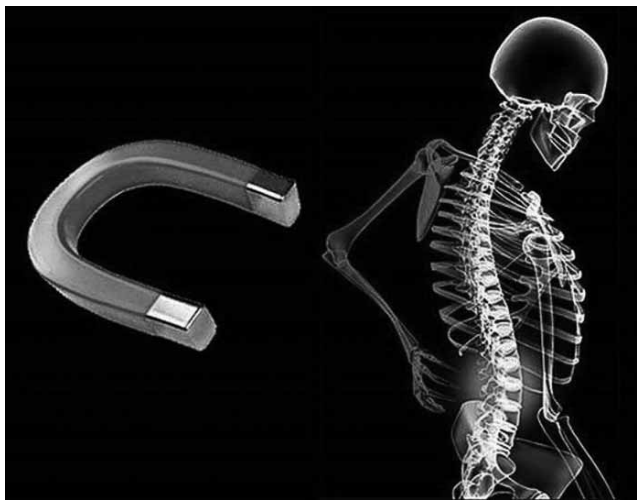
Лікарі та вчені експерти в галузі фізіологічних процесів, які відбуваються під впливом магнітного поля в людському організмі, звертають особливу увагу на вплив магнітного поля на кровонососудинну систему людини, ефективність перенесення кисню кров'ю, транспортування поживних речовин, але найбільш чутливою до магнітного поля є нервова система. На магнітні поля реагує і багато інших систем організму: ендокринна, серцево-судинна, дихальна,



кістково-м'язова та травна системи, органи почуттів і кров. У макромолекулах (нуклеїнові кислоти, протеїни тощо) під впливом магнітних полів виникають заряди та змінюється їх магнітна сприйнятливість. Магнітна енергія макромолекул у результаті такого впливу перевищує енергію теплового руху. Саме цей ефект дає можливість використовувати магнітне поле для запуску орієнтаційних та концентраційних змін усередині біологічно активних макромолекул. Цей ефект впливає на швидкість біохімічних та біофізичних процесів. Активність іонів є найважливішим регуляторним механізмом людського організму. Ця активність визначається, насамперед, зв'язком з макромолекулами та ступенем гідратації (тобто зв'язком із молекулами води). Завдяки зростанню іонної активності у тканинах організму під впливом магнітних полів відбувається стимуляція клітинного метаболізму, тобто збільшення обміну речовин.

Наприкінці 70-х років. минулого століття у різних країнах було проведено широкомасштабні дослідження щодо впливу магнітних полів промислової частоти на здоров'я людини. Ініціатором запровадження цієї норми була Швеція, в якій близько 20 років велися спостереження за здоров'ям півмільйона осіб, які мешкають в умовах підвищених рівнів магнітних полів промислової частоти.

Люди, які побували під дією електромагнітних полів, відзначають у собі зміну емоційного стану, часто скаржаться на дратівливість та гнівливість, запальність та плаксивість. Реакції людського організму на вплив різноманітних магнітних і електричних полів проявляються також як притуплення уваги, погіршення властивостей пам'яті, підвищення стомлюваності, сонливості і зменшення ефективності сну. При цьому хронічне опромінення протягом тривалого періоду посилює наведені вище реакції і збільшує ризики небажаних наслідків, які призводять до функціональних розладів різного характеру. Тут слід відзначити зміну біохімічних показників крові, появу головного болю різної локалізації, шуму у вухах та запаморочення, а також виникнення почуття сверблячки, болю в м'язах, кістках та суглобах. Останнім часом з'явилися дані щодо участі електромагнітних полів у формуванні злоякісних новоутворень.



У літературі обговорюється проблема схильності осіб, пов'язаних за родом професії з впливом ЕМП промислових частот, до розвитку хвороби Альцгеймера, а також бічного аміотрофічного склерозу. Передбачається, що в основі патогенезу даних захворювань лежить порушення гомеостазу іонів кальцію в нейронах, активація клітин мікроглії та їх подальша дегенерація, а також стимулюючий вплив ЕМП на продукцію бета-амілоїду. Описано симптоми, що свідчать про зміну вегетативної та соматичної іннервації верхніх кінцівок у контролерів ВТК підприємств із виробництва постійних магнітів.

Відзначено збільшення серцево-судинних захворювань та гіпертонічної хвороби у машиністів електролокомотивів та метрополітену.

У науковій літературі розглядаються питання впливу ЕМП на репродуктивну функцію організму. Так, результати дослідження репродуктивної функції чоловіків, які обслуговували трансформаторні установки із середньою величиною напруги 400 кВ, показали зниження питомої кількості новонароджених хлопчиків, а також збільшення більш ніж у 3 рази числа вроджених аномалій при порівнянні з контрольною групою, що працювали з обладнанням, в якому величина напруги струму не перевищували 70 кВ. Підтверджено збільшення розвитку онкологічної патології у дітей від 2,4 – 3,6 разів, чиї батьки працювали в електроіндустрії, у 3,5 – у дітей електриків, у 3,8 рази – у дітей зварювальників.

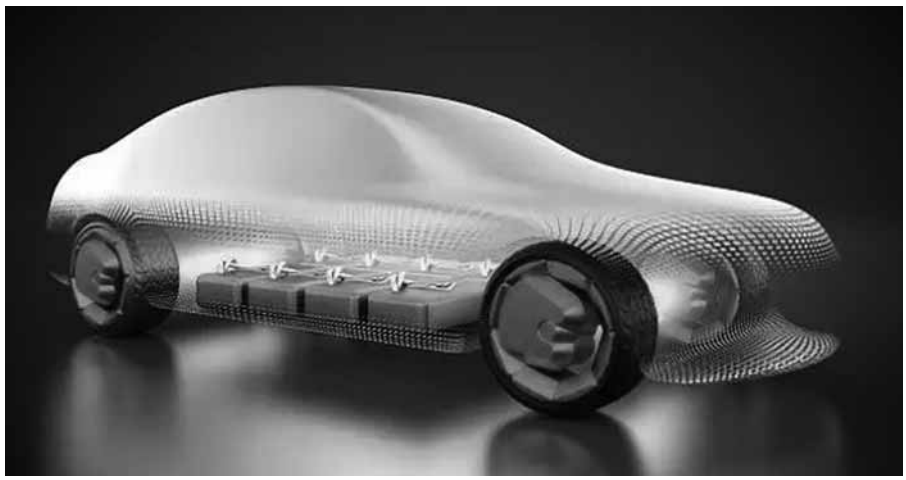
Міжнародна комісія із захисту від неіонізуючого випромінювання (ICNIRP) встановила рекомендації щодо допустимих рівнів електромагнітних полів, які беруться до уваги багатьма країнами. Ці рекомендації спрямовані на мінімізацію ризиків для здоров'я людини та ґрунтуються на великих наукових дослідженнях.

Тому безпечні рівні електромагнітної індукції для людини варіюються залежно від країни та міжнародних стандартів. В цілому, для частоти 50/60 Гц (промислова частота) гранично допустимі рівні магнітної індукції становлять близько 0,2 мТл (міліТесла) для тривалого впливу та 0,5 мТл для короткочасного впливу.

У людей, які регулярно піддаються впливу низькочастотних МП, індукція яких перевищує 0,1...0,2 мкТл, послаблюються імунна, репродуктивна та інші системи. Ймовірно виникнення лейкемії в малолітніх дітей.

Електромагнітні поля, що генеруються електротранспортом

Перехід на електротранспорт є однією з найактуальніших світових тенденцій. Багато розвинених високотехнологічних країн мають національні програми з розвитку екологічного електричного транспорту. Прикладом може бути програма Європейського Союзу «Green



Car Initiative», спрямована на фінансування розробок у галузі створення електричного автотранспорту (з електричними та з комбінованими, «гібридними» енергоустановками) та відповідної інфраструктури. Загальна сума коштів на цю програму сягає 1 млрд. євро.

Однак світові виробники електричного автомобілебудування зіштовхнулися із серйозними проблемами забезпечення електромагнітної сумісності всіх пристроїв на борту транспортної системи та електромагнітної безпеки користувачів електротранспорту. У зв'язку з цим тестування, моніторинг та аналіз магнітних полів (МП) в електротранспорті є актуальним завданням.

Автомобілі, що працюють на електричній тязі мають силові установки, датчики, пристрої систем управління, інформації та зв'язку. Електричні струми, що протікають через електродвигун, ланцюги живлення та батареї під час руху, генерують МП в низькочастотних діапазонах (ультранизькочастотні (УНЧ), 0,001-10 Гц; низькочастотні (НЧ), 10-300 Гц). Вищі гармоніки електромагнітного поля в електромобілі генеруються різноманітними електронними пристроями на борту, інформаційними системами та системами зв'язку. Наприклад, у гібридних автомобілях спостерігаються магнітні імпульси до 5 кГц, які генеруються під час перемикання двигуна внутрішнього згоряння та електричного режиму. Крім того, у всіх типах автомобілів генерується низькочастотне пульсуюче магнітне поле під час обертання сталевих колісних дисків. Частота f цього поля визначається швидкістю обертання коліс і зазвичай f < 20 Гц, але в спектрі присутні також гармоніки з вищою частотою.

Електромобіль є новою технологічною системою, яка тільки зараз виходить на широкий ринок. Виробництво та використання таких електромобілів поки не стало масовим, тому у світі відсутні досить великі та детальні вимірювання МП у таких транспортних засобах. Робіт про магнітні виміри в гібридних автомобілях дуже мало, а тестування полів у повністю електричних автомобілях практично не проводиться.

Оскільки в електромобілях, як і в інших видах електротранспорту, МП генеруються струмами, що течуть по струмових системах (проводах і кабелях) транспортного засобу, то можна вважати, що МП у всіх транспортних системах, що працюють на електричному струмі, матимуть схожі параметри. Однак це припущення вимагає перевірки. В матеріалах, викладених нижче є узагальнення мізерної інформації про МП в електромобілях та порівняння їх з результатами вимірювань, проведених в інших видах транспорту на електричній тязі.

Магнітні поля в електромобілі

Такі собі фахівці Vedholm і Hamerius [5] провели вимірювання магнітного поля (5–2000 Гц) у нерухомому гібридному електромобілі з увімкненим двигуном та кондиціонером. Вимірювання проводилися у 7 різних автомобілях у районі всіх чотирьох сидінь на рівні щиколоток, колін, стегон, грудей та голови. Оскільки автомобілі були нерухомі, поля, генеровані обертанням коліс, були відсутні. Магнітне поле, в якому знаходиться водій та пасажири, було отримано усередненням та представлено в таблиці.

У гібридах, у яких батарея була розміщена спереду (Авто 1–5), за відсутності руху спостерігалися поля невеликої інтенсивності. Більш сильні поля спостерігалися в автомобілях, де батарея була розміщена ззаду (Авто 6 і 7). У

Таблиця 1. Середнє магнітне поле (мкТл) у діапазоні частот (5–2000 Гц) у нерухомому гібридному електромобілі з увімкненим двигуном та кондиціонером

Точка виміру	Авто 1	Авто 2	Авто 3	Авто 4	Авто 5	Авто 6	Авто 7
Ліве переднє сидіння	0,12	0,11	0,15	0,22	0,14	2,6	3,2
Праве переднє сидіння	0,13	0,15	0,33	0,37	0,11	1,1	0,8
Ліве заднє сидіння	0,06	0,04	0,03	0,03	0,06	2,4	4,0
Праве заднє сидіння	0,11	0,10	0,04	0,04	0,03	1,3	1,5

цих автомобілях батарея розташована під багажником або під заднім сидінням, і струм тече через весь автомобіль із передньої частини, від генератора до батареї. Такий великий струмовий контур генерує значні МП. Максимальне поле 14 мкТл було відзначено біля заднього правого сидіння (як правило, дитячого) на рівні ніг.

Технічний університет м. Біля за дорученням Швейцарського федерального департаменту здоров'я провів вимірювання МП у двох гібридних автомобілях. Вимірювання було зроблено під час руху містом і в лабораторії, де імітувалися умови руху. Датчики МП були розміщені на передньому пасажирському сидінні, на підлозі біля сидіння водія, а також на місці дитячого крісла (заднє праве сидіння). Колеса були зроблені з немагнітних матеріалів, щоб унеможливити вплив МП, що виникає під час обертання феромагнітних мас коліс, на результати вимірювань. Під час цього дослідження встановлено, що інтенсивність МП постійно змінювалася під час руху автомобіля і сильно залежала від способу прискорення та гальмування. Найбільша інтенсивність спостерігається під час різкого прискорення та гальмування.

Під час руху МП в районі на дитячого сидіння було в межах 0,1–3 мкТл. МП в інших виміряних точках мало приблизно такий самий рівень. Було відзначено, що у гібридних автомобілях генерується суміш МП у частотному діапазоні 5–500 Гц. Варто взяти до уваги, що у цьому дослідженні вимірювальні прилади не фіксували МП нижче 5 Гц.

У роботі австралійських дослідників наведено результати вимірювань МП у різних точках гібридного автомобіля. Було знайдено, що інтенсивність поля в межах 0–35 мГс (0–3,5 мкТл). Максимальні поля вище за 10 мГс спостерігалися на частоті 12 Гц. На рис. 1 показано МП, виміряне в задній частині гібридного автомобіля під час руху в різному режимі (прискорення, гальмування).

Група дослідників із США досліджувала МП у різних електромобілях виробництва США, а також на заправній станції під час заряджання авто. Ці автомобілі використовували двигуни як постійного, так і змінного струму. Вимірювання показали, як і в попередніх випадках, що найбільші поля генерувалися під час максимального прискорення та рекуперативного гальмування. Найбільше поле було виявлено на місцях водіїв. Під час зарядки електромобіля найбільші поля, рівні 64,37 мГс, фіксувалися на відстані 50 см від панелі автоматичного переривача струму. За результатами вимірювань встановлено, що в електромобілях генеруються низькочастотні МП в діапазоні частот 60–420 Гц. Автори цього дослідження стверджують, що такі МП можуть загрожувати здоров'ю водіїв та пасажирів, і тому їх слід екранувати.

У спільному проекті армійської групи Army TACOM та Крайслер К. було проведено досить детальне дослідження МП у гібридному автомобілі Крайслер. При цьому було враховано, що в автівці було виконане екранування для зменшення цих полів. Поля вимірювалися індукційним магнітометром у широкому діапазоні частот (0-50 кГц). У досліджуваному автомобілі батарея була над задніми колесами. При силі струму в 200 А максимальне поле ~1200 мГс (120 мкТл) спостерігалося в районі заднього сидіння, а просторові градієнти доходили до 1000 мГс /м. Ці значення лежать у тих же межах, що і в електропоїздах.

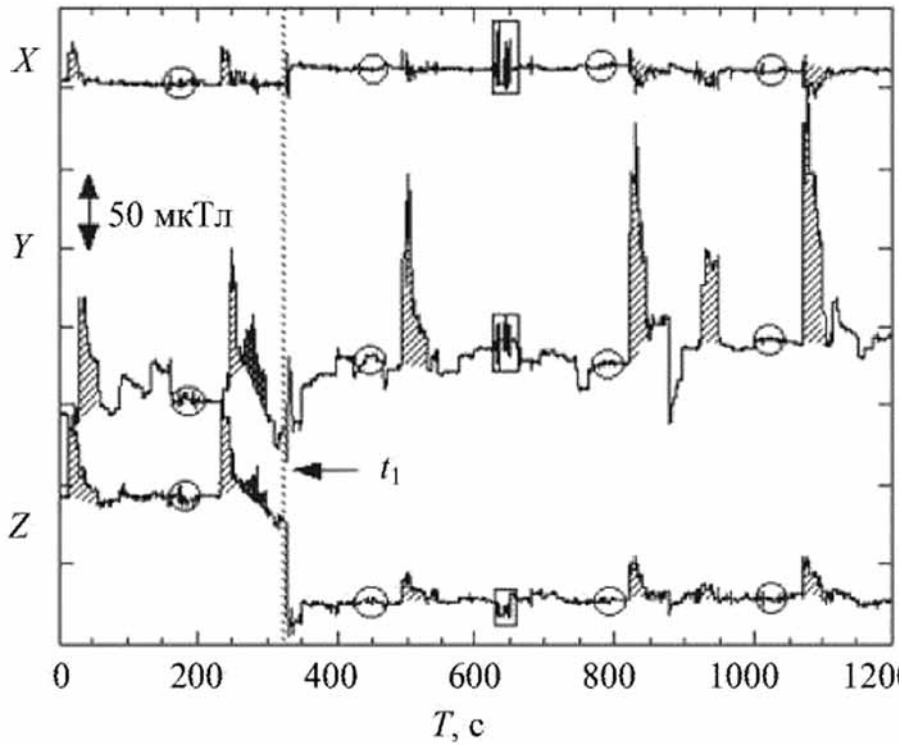


Рис.2. УНЧ магнітне поле (компоненти X , Y , Z) в електричці, що працює на постійному струмі, у вагоні з моторами. Заштрихована область – фаза прискорення, чорна область – підстанція, прямокутник – зустрічний поїзд, коло та еліпс – фаза гальмування. У момент t1 датчик був поміщений у точку безпосередньо над електродвигуном. Різка зміна поля в цей момент свідчить про великі просторові градієнти

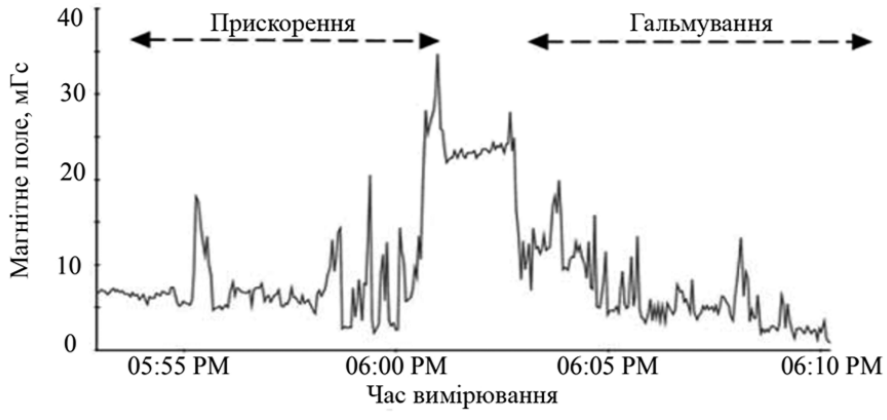


Рис.1. Магнітні поля на лівому задньому сидінні гібридного автомобіля

Магнітні поля в електропоїздах, метро, трамваї та тролейбусі

Автори даної роботи провели численні вимірювання МП у різних видах електричного транспорту, як то: електролокомотиви та електрички, що працюють як на постійному, так і на змінному струмі (16,34 Гц), метро, трамвай і тролейбус, що працюють на постійному струмі. Моніторинг полів, як правило, супроводжувався фіксацією інформації про умови руху (прискорення, уповільнення, гальмування, проходження підстанцій, зустрічних поїздів або інших феромагнітних мас тощо), що дозволило ідентифікувати джерела різних магнітних варіацій, що спостерігаються в електротранспорті. Приклади такої ідентифікації показані на рис. 2–4.

На рис. 2 представлена запис X-, Y- і Z- компонент МП, виміряного в пасажирському вагоні, тобто у вагоні із електродвигунами. Варіації МП у напрямку вздовж рейок (X -компонента) зневажливо малі порівняно з варіаціями Y- і Z- компонентів, перпендикулярних до рейок. Найбільші стрибки поля відбуваються під час прискорення поїзда, величина стрибків у Y -компоненті на цій ділянці колії досягає 150 мкТл. Дея-

ке збільшення поля відбувається також під час гальмування. Зустрічні або поїзди, що стоять уздовж шляху, викликають помітні варіації поля через вплив їх феромагнітних мас.

На рис. 3 наведено Y-компонента МП, виміряного в електровозі поблизу робочого місця машиніста. Видно, що максимальні значення варіацій досягають 100 мкТл. Варіації, що спостерігаються в X- і Z-компонентах, мають той же вигляд, що і в Y- компоненті, але з набагато меншою амплітудою. Тут при проведенні вимірювань нульові рівні датчиків відповідали полям, виміряним на платформі до відправлення поїзда (тобто звичайному тлі магнітного довкілля).

Дані наведені на рис. 3 дозволяють оцінити рівень постійного МП всередині поїзда. Видно, що величина поля всередині поїзда зазвичай набагато вище, ніж на платформі, тобто вища за рівень магнітного фону навколишнього середовища. Однак іноді, наприклад, при проходженні першої силової підстанції значення поля стає нижчим від рівня навколишнього середовища (на рис. 3 для часу T≈150-200 с значення поля негативно).

Типовий приклад запису МП у локомотивах, що працюють на змінному струмі (16,67 Гц) наведено на рис. 4. Вимірювання були виконані на лінії Цюріх-Берн. На рис. 4 а показані варіації трьох компонент, зареєстровані протягом 20 хв з частотою реєстрації 200 Гц. Більш детальний 20-секундний запис варіацій наведено на рис. 4, б. Цей рисунок показує «рушійну картину», що виходить в результаті безперервних вимірювань МП. Виявилося, що для швейцарських електровозів, як і для електропоїздів взагалі, можна пов'язати різні особливості МП з робочими режимами в різні моменти руху, як показано на рис. 4. Аналіз показав, що на робочому місці машиніста основним джерелом варіацій був струм у рейковому ланцюзі, який змінювався відповідно до обставин руху.

Рисунки 2–4 демонструють, що основними джерелами варіацій МП в електропоїздах є електричні струми в струмових ланцюгах. Ці струми і відповідно МП зменшуються/збільшуються при зміні режиму руху (прискорення, гальмування, проходження підстанції). Крім того, джерелом варіацій МП всередині є зовнішня феромагнітна обстановка, що змінюється (зустрічні поїзди, мости тощо).

Були проведені також вимірювання МП у трамваї ЛВС-86К. Досліджувалася залежність амплітудних значень МП від режиму експлуатації вагона (стоянка, розгін, рух, гальмування). Рівень УНЧ полів, що виникають у результаті змін струму в ланцюгу відповідно до потреб руху, змінювався в межах від нуля до кількох сотень мкТл. Встановлено, що в кабіні водія трамвая рівні індукції постійного МП скла-

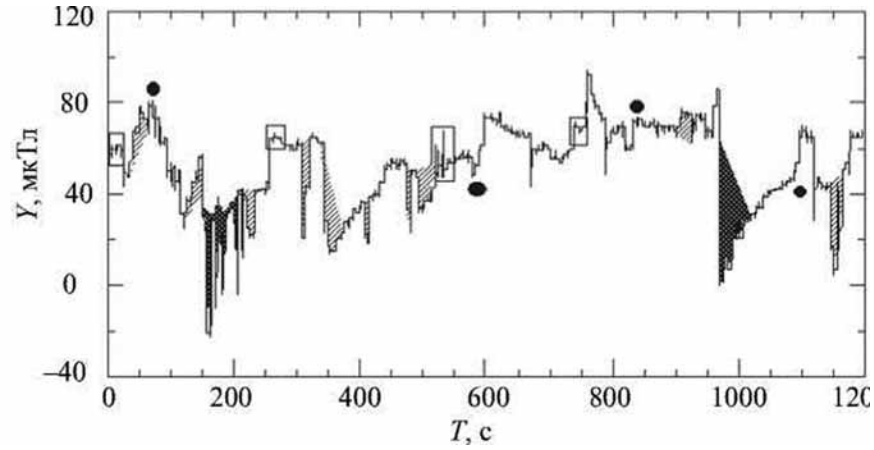


Рис. 3. Y -компонента УНЧ магнітного поля локомотива, що працює на постійному струмі, поблизу робочого місця машиніста (15 см від голови). • – моменти нульового струму. Інші позначення ті самі, що і на рис. 2

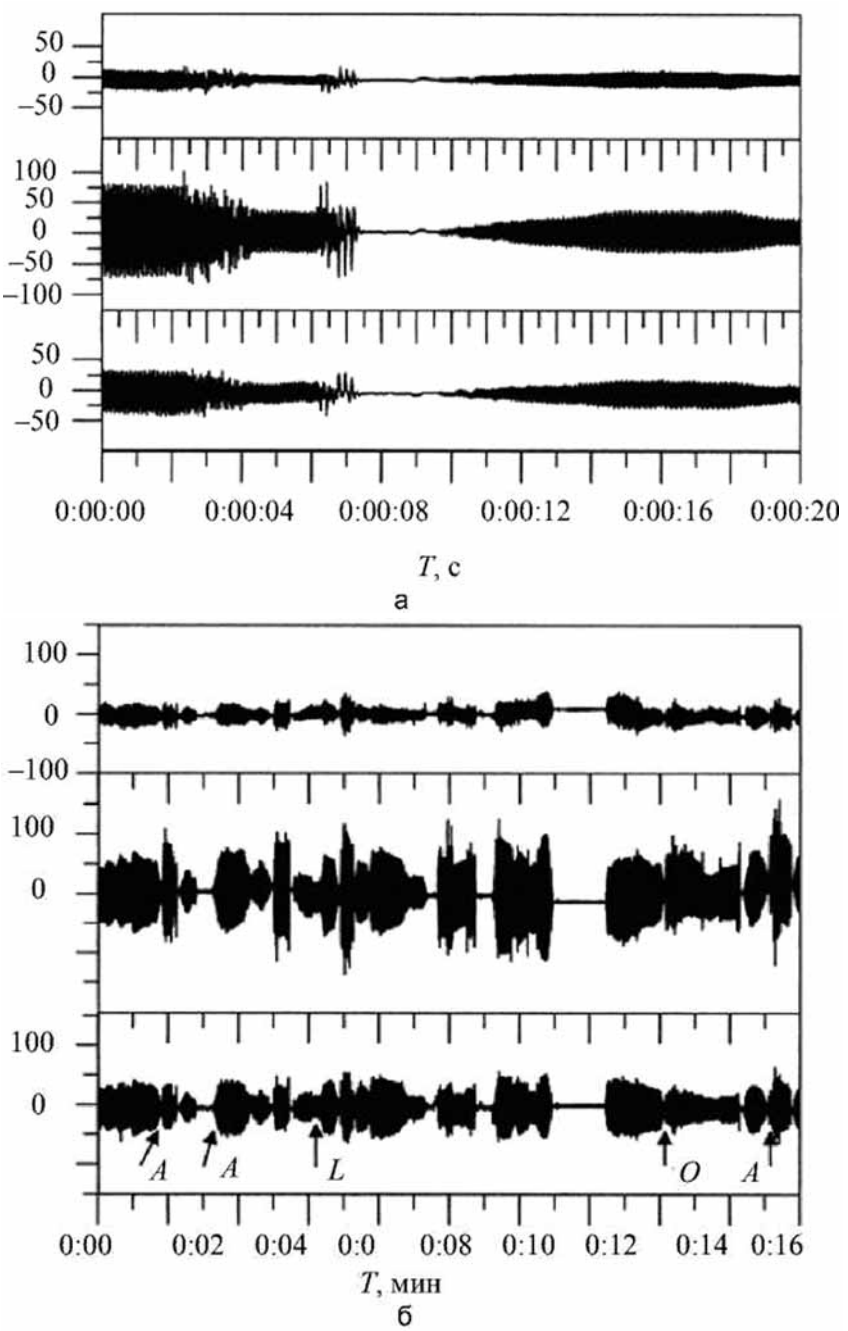


Рис. 4. Магнітне поле в швейцарскому електролокомотиві, що працює на змінному струмі (16,67 Гц): а – 20-хвилинна; б – 20-секундний запис. A – прискорення; L – низька швидкість; O – нульовий струм

ли 3,4-98 мкТл, у салоні для пасажирів – 14–500 мкТл. В окремих місцях, поблизу отворів у перегородці, що відокремлює кабіну водія трамвая від салону для пасажирів, значення індукції досягали 1000 мкТл (внаслідок виникаючих там явищ дифракції та інтерференції), що в 15 разів перевищує постійне поле Землі.

Джерелами постійних та змінних МП у трамваї є струмонесучі елементи, електро обладнання, печі електрообігріву. Високі рівні МП реєструвалися поблизу реостатного блоку. Найбільші значення індукції МП у салоні виявлено в зоні розташування сидінь пасажирів на початку вагона ліворуч по лінії розташування струмопровідних елементів, де знаходяться місця для пасажирів з дітьми та інвалідів. У вагоні трамвая реєструвалися значні градієнти МП, які є суттєвим біотропним параметром.

Також було проведено вимірювання у двох типах метропоїздів м. санкт-петербурга (вагон 81717 та автоматизований вагон ЕМА). Як з'ясувалося, джерелами МП в електропоїздах метрополітену є тягові двигуни, пускогальмові опори, групові перемикачі, кабелі струмоприймача, струмонесучий провід. Значні УНЧ варіації МП спостерігалися в кабінах машиністів петербурзького метро в горизонтальній Y-компоненті (перпендикулярно до рейок), де значення «від піку до піку» досягали 425 мкТл у кабіні машиніста вагона 81717 і 350 мкТл у ва-

гоні ЕМА. Таким чином, у цих місцях МП у 7-14 разів перевищує величину природного постійного поля Землі (близько 50 мкТл). У пасажирських салонах поле варіювало в межах 75-300 мкТл. Аналіз показав, що МП у поїздах метрополітену та на платформах неоднорідне в просторі.

Вимірювання МП у тролейбусі були проведені у москві та санкт-петербурзі. Досліджувалася залежність амплітудних значень МП від точки виміру та від режиму експлуатації тролейбуса (стоянка, розгін, рух, гальмування). Точки вимірювань були обрані поблизу джерел найбільших коливань індукції МП: у кабіні водія, в салоні на передньому пасажирському сидінні, над тяговим електродвигуном, над компресором та на задній площадці на трьох висотах від підлоги: 0,5 м; 1,0 м; 1,4 або 1,7 м. У кожній точці здійснювалося по 200 вимірів на секунду кожної з трьох компонентів індукції МП протягом 3 хв. Результати моніторингу записувалися разом із даними про режим руху тролейбуса за маршрутом.

У водійській кабіні тролейбуса зафіксовано найбільші значення Нср = 93±45 мкТл за головою водія в 20 см від проводів, якими течуть робочі струми до 200 А від струмоприймачів до контакторної панелі та тягового електродвигуна. У цій точці є найбільший розмах коливань: ΔН = Нмакс – Нхв = 20–36 = 168 мкТл. Найбільший розмах зареєстрований у горизонтальних компонентах: ΔX = 141 мкТл, ΔY = 172 мкТл, тоді як вертикальна компонента має менший, але теж значний розмах: ΔZ = 50 мкТл. Результати вимірювань свідчать, що МП у кабіні тролейбуса не тільки різко змінюється з часом, а й має просторовий градієнт близько 100 мкТл /м.

Аналогічне дослідження було проведено у тролейбусах марки ЗІУ-9 та ЗІУ-10 у санкт-петербурзі. Статистичний аналіз МП у кабіні та пасажирському салоні петербурзького тролейбуса показав, що в цілому характер поля та його відгук на умови руху за маршрутом мають такий же характер, що й у московському тролейбусі. Основна потужність спектра поля в петербурзькому тролейбусі також лежить в області УНЧ частот (менше 10-15 Гц). Розмах коливань МП в петербурзькому тролейбусі, як і в москві, залежить від режиму руху і значно збільшується при русі тролейбуса в пробках при частих розгонах і гальмуваннях.

Висновок

Порівняння вимірювань магнітного поля, проведеного у різних видах транспорту, показало, що ці поля кардинально відрізняються від синусоїдальних полів, що генерують лінії передач (50 Гц або 60 Гц). Магнітні поля в електричному транспорті, включаючи автомобіль, є мультичастотними полями, які швидко змінюються в часі та просторі автомобіля. Ці риси магнітного поля є наслідком підсумовування різномагнітних джерел магнітного поля на борту транспортного засобу і змінних режимів руху (прискорення, гальмування тощо). Однак більша частина магнітної енергії концентрується в найнижчих частотних діапазонах (квазістатичному та ультранизкому, 0,001-10 Гц).

Нижче наведені максимальні рівні полів, що зустрічаються в різних видах електротранспорту, включаючи електромобілі, у квазістатичному та ультранизькочастотному діапазоні:

Трамвай .....500 мкТл;
Метро .....450 мкТл;
Тролейбус .....350 мкТл;
Електромобілі / гібридні ..140 мкТл;
Електропоїзд .....120 мкТл;
Електрокар .....104 мкТл;
Легкий електробус .....80 мкТл.

Видно, що найбільші рівні полів зустрічаються у трамваї та метро. Виміряні до цього часу рівні полів в електричному автомобілі можна порівняти по порядку величин з магнітними полями, виміряними в електропоїздах – у вагонах електричок та на робочому місці машиніста електровоза. Ці магнітні поля значно перевершують поля від ліній передач, з якими людина зазвичай стикається вдома і на роботі.

З урахуванням того факту, що водії та пасажири електромобілів знаходяться в безпосередній близькості від джерел струму, очевидно, що для забезпечення їх електромагнітної безпеки необхідно вести пошуки розумних і недорогих способів зменшення магнітних полів. Зазвичай інженерно-технічний захист будується на заходах щодо обмеження емісійних властивостей джерел поля або на основі екранування поля. Це можуть бути багатошарові екрани, виготовлені із сучасних матеріалів на основі сплавів з аморфною та нанокристалічною структурою, які не ускладнюють конструкцію авто та можуть зменшувати низькочастотні магнітні поля, характерні для електротранспорту, у 5–10 разів.

Підготував Д.Мусієнко

Література

1. https://rucars.ru/ev-danger-myth
2. http://www.confcontact.com/2013-nauka-v-informatsionnom-prostranstve/tn15_mihajlov.htm
3. https://sites.znu.edu.ua/bio-eco-chem-sci/issues/files/2009/05/22/6557_1243256492_09kavpib.pdf
4. https://ntv.ifmo.ru/file/journal/124.pdf
5. Vedholm K., Hamnerius YK Personal Exposure Resulti ng from Low Level Low Frequency Electromagnetic Fields in Automobiles // Second World Congress for Electricity and Magnetism in Medicine and Biology, June 8-13, Bologna, Italy, 1997. – Abstract F -9. - 445 p.
6. https://mydozimetr.ru/blog/stati/vozdeystvie-elektromagnitnykh-izlucheniy-na-organizm-cheloveka/?srsltid=AfmBOophZE7MWyIGl-bgcifnSekWg_EwRM8GtKzO1I4IG4ZyX1EC7eDQe.
7. http://www.confcontact.com/2013-nauka-v-informatsionnom-prostranstve/tn15_mihajlov.htm

МІЖНАРОДНІ АГРОПРОМИСЛОВІ ВИСТАВКИ

www.animal-show.kiev.ua www.grainexpo.com.ua www.freshexpo.kiev.ua

+380 44 490 64 69 @ agro@kmkya.kiev.ua Agrovesna.vystavka

Стандарти з кібербезпеки для розумних мереж – системний аналіз

У останні роки було опубліковано численні стандарти, пов'язані з кібербезпекою інтелектуальних енергосистем (smart grids), що створило виклик для операторів у пошуку рекомендацій, які відповідають їхнім конкретним цілям та контекстам. Хоча кілька досліджень наблизилися до вирішення цієї проблеми, надаючи більш-менш комплексні огляди та аналізи стандартів кібербезпеки для інтелектуальних енергосистем, жодне з них не було присвячене актуальній та важливій темі заходів кібербезпеки. Ця стаття має на меті заповнити цю прогалину. Було проведено систематичний аналіз літератури, в результаті чого виявлено дев'ятнадцять широко визнаних стандартів, які визначають заходи кібербезпеки, застосовні до інфраструктури інтелектуальних енергосистем. Публікації описані щодо заходів, які вони визначають, та зіставлені з критеріями оцінки. У результаті ця стаття становить собою керівництво щодо стандартизованих заходів кібербезпеки для інтелектуальних енергосистем, де (на основі критеріїв) надаються рекомендації щодо вибору стандартів для конкретної галузі інтелектуальних енергосистем або специфічних цілей. Представлено методологію дослідження, а також критерії відбору та оцінки стандартів.

Забезпечення кібербезпеки розумних мереж вимагає нових, міждисциплінарних підходів, які поєднують традиційні та інноваційні технології та враховують нетехнічні аспекти, включаючи управлінські, політичні або правові [1,2.] Рекомендується насамперед застосовувати стандартизовані рішення та практики [3,4,] оскільки вони були розроблені в рамках системного, багатоетапного процесу розробки стандартів і обрані консенсусом численних експертів у галузі, які представляють різні середовища та часто різні частини світу. Порівняно з пропрієтарними рішеннями, заснованими на «експертних знаннях», стандарти пропонують перевагу високої гарантії повноти та зрілості, а також інших характеристик, пов'язаних із якістю.

За останнє десятиліття було опубліковано велику кількість стандартів для розумних мереж, що призводить до ситуації, коли оператори втрачають орієнтацію в цій надмірності літератури. Особливо якщо вони знаходяться на початку процесу вдосконалення на основі стандартів. Дослідження, описане в цій статті, сприяє вирішенню цієї проблеми шляхом ідентифікації стандартів, які визначають заходи захисту кіберфізичних та інформаційних систем у розумних мережах. Заходи кібербезпеки — це (технічні та нетехнічні) засоби захисту або контрзаходи (процеси, політики, пристрої, практики чи інші дії), які спрямовані на захист системи або активів від кібератак і зменшення ризиків кібербезпеки [5,6.] Ця стаття збирає всі стандарти, які описують заходи кібербезпеки, застосовні до розумних мереж, в одному місці та характеризує їх щодо цих заходів.

Це основано на структурованому аналізі, який продовжує підхід і результати попередніх досліджень автора, що стосувалися стандартів кібербезпеки для розумних мереж загалом [7], специфікацій вимог до кібербезпеки [8] та оцінок кібербезпеки для розумних мереж [9].

Також надаються (критеріально-орієнтовані) рекомендації, які мають на меті допомогти операторам вибрати стандарти, що є застосовними до їхньої сфери та відповідають їхнім індивідуальним цілям. Усе це разом має скласти комплексний посібник із стандартизованих заходів кібербезпеки для розумних мереж. В результаті системного триетапного аналізу літератури було визначено 19 відповідних стандартів або дефакто стандартів.

Таб. 1. Резюме ідентифікації літератури

Джерело	Усі метадані	Назва	Анотація	Ключові слова	Поглиблений огляд	Відповідні
ACM DL	26	0	16	1	8	6
Elsevier SD	7,114	0	37	4	10	10
IEEE Xplore	602	3	184	17	37	27
Springer	3,190	0	n.a.	n.a.	17	5
Wiley	3,683	3	34	3	8	4
EBSCOhost	265	5	123	6	22[1]	20[1]
Scopus	7,054	5	338	178	35	16
WoS	2,58[2]	3	n.a.	n.a.	39[1]	23[1]
Разом	22,192	19	732	209	176	112

1 Результати пошуку містять повторювані дані з інших баз даних.

2 Аналіз проводився лише за темою через відсутність опції повного доступу до метаданих.

У наступних розділах описано методологію дослідження разом із критеріями відбору та оцінки стандартів. Розділ 3 представляє стандарти, які оператори можуть використовувати як орієнтир при впровадженні заходів захисту в розумній мережі. Розділ 4 присвячено багатоаспектному аналізу, який охоплює взаємозв'язки між заходами контролю у визначених стандартах, охопленими сферами розумних мереж та доменами кібербезпеки. Нарешті, після обговорення пов'язаних досліджень наводяться висновки.

2 Метод дослідження

Аналіз проводився згідно з систематичним методом Вебстера та Вотсона?, який спрямований на повноту та повторюваність процесу огляду. У цьому підході пошук літератури починається з аналізу найбільш авторитетних джерел, баз статей та матеріалів конференцій. Після цього цитати в ідентифікованих документах перевіряються для виявлення попередніх публікацій, що мають відношення до теми. Цей крок називається зворотним аналізом. На наступному етапі, тобто прямому аналізі, шукаються документи, які посилаються на основні статті, визначені на попередніх кроках, з використанням наукової бази даних. Підхід є концепто-центричним – концепції визначають організацію аналізу літератури, а також його завершення (коли нові концепції більше не знаходяться). Дослідження включало три ключові етапи – ідентифікацію літератури, аналіз літератури та відбір стандартів.

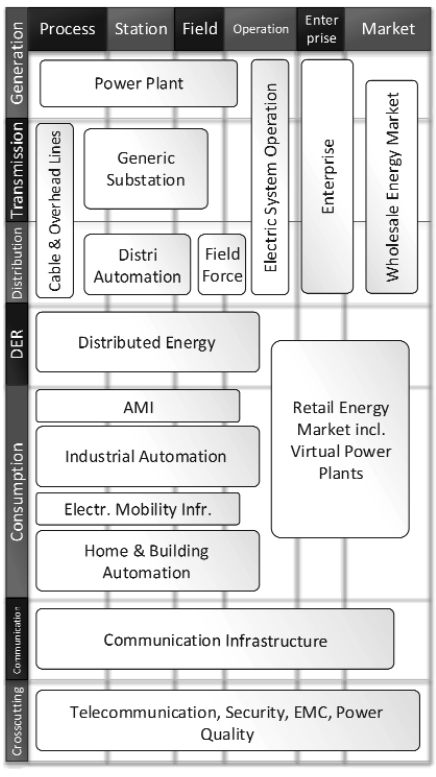
Пошук літератури. На цьому етапі проводився пошук за ключовими фразами: «розумна мережа» (smart grid), «безпека» (security) та «стандарт» (standard) у ресурсах найбільш визнаних видавництв у галузі комп'ютерних наук, кібербезпеки, електроенергетичних систем тощо, а також у кумулятивних базах даних, які зберігають інформацію від різних видавців. У першій спробі було знайдено 22 192 документи, у метаданих яких збігалися ключові фрази. Для обмеження кількості результатів у другій спробі пошук обмежувався лише заголовками, ключовими словами та анотаціями публікацій. В результаті було знайдено близько 700 документів. Читання описів цих публікацій дозволило виокремити 176 публікацій, які виявилися релевантними до дослідження. Подальший аналіз, який включав перегляд змісту документів, завершився визначенням 112 статей, що описують стандарти, пов'язані з кібербезпекою розумних мереж (див. Таблицю 1). Серед них 10 досліджень містили більш комплексні результати, тоді як більшість лише посилалися на деякі ініціативи стандартизації або стандарти.

Аналіз літератури. На цьому етапі було спрямовано зусилля на визначення стандартів розумних мереж (smart grid) та дій зі стандартизації. Він включав читання (повністю або частково) 112 статей, виз-

начених на попередньому етапі. Також було проаналізовано та відстежено посилання, що містяться в цих статтях. У результаті було виокремлено кілька дій зі стандартизації ([17,21,22,23,24]), а також деякі додаткові звіти (наприклад, [25,26,23,27]).

Дії зі стандартизації зосереджувалися переважно на розробці нових специфікацій, але часто вони також вказували на пов'язані ініціативи в цій галузі. Особливо корисною виявилася робота Міжнародної електротехнічної комісії (IEC), зокрема карта стандартів розумних мереж (Smart Grid Standards Map [28]), яка дозволяє проводити інтерактивний аналіз взаємозв'язків між стандартами та елементами електромережі, а також полегшує доступ до інформації про норми (див. Рисунок 1). У цьому дослідженні карта використовується для ілюстрації взаємозв'язків між визначеними стандартами та елементами інфраструктури розумних мереж (див. критерій застосовності, Таблиця 2). Взаємозв'язки стандартів NIST, NERC, DHS та інших американських стандартів, які відсутні на карті IEC, були доповнені автором. Під час пошуку стандартів розумних мереж, що стосуються питань кібербезпеки, насамперед були проаналізовані дії зі стандартизації та [10] більш комплексних наукових досліджень щодо стандартів ([11,12,13, 14,15,16,17,18,19,20]), виявлених на етапі ідентифікації літератури, щоб уникнути дублювання роботи.

Вибір стандартів. Для систематичного відбору стандартів, які описують засоби кібербезпеки, що застосовуються до розумної мережі, критерії відбору були



Мал 1. Компоненти розумної мережі на основі карти стандартів розумних мереж IEC28.

Таб. 2. Критерії оцінки стандартів

Критерій	Опис
Сфера	Тематична область, яку охоплює стандарт.
Тип	Рівень технічної деталізації або більш загальні рекомендації.
Застосовність	Елементи інфраструктури розумних мереж, до яких може бути застосований стандарт.
Охоплення	Географічне охоплення стандарту (національне або міжнародне).
Публікація	Дата публікації стандарту.
Актуальність	Рівень актуальності щодо кібербезпеки. Стандарти, які безпосередньо присвячені заходам або практикам кібербезпеки, фокусуються на них або містять детальні описи заходів контролю, вважаються високоактуальними. Низький рівень актуальності пов'язаний із стандартами, які лише згадують деякі заходи кібербезпеки.

Таб. 3. Стандарти розумних мереж або енергосистем, які описують засоби та практики безпеки.

№	Стандарт	Сфера застосування	Тип	Регіон	Рік публікації	Релевантність
1	NRC RG 5.71	Кібербезпека ядерної інфраструктури	Загальний	США	2010	Висока
2	IEEE 1686	Кібербезпека підстанцій	Технічний	Світовий	2007	Висока
3	Профіль безпеки для AMI	Кібербезпека AMI	Загальний	США	2010	Висока
4	NISTIR 7628	Кібербезпека розумних мереж	Загальний	США	2014	Середня
5	IEC 62351	Безпека комунікаційних протоколів	Технічний	Світовий	2007-2016	Середня
6	IEEE 2030	Інтероперабельність розумних мереж	Технічний	Світовий	2011-2016	Низька
7	IEC 62541	Модель безпеки OPC UA	Загальний	Світовий	2015-2016	Низька
8	IEC 61400-25	Комунікація вітрових електростанцій - IACS	Технічний	Світовий	2006-2016	Низька
9	IEEE 1402	Фізична та електронна безпека підстанцій	Загальний	Світовий	2008	Низька
10	IEC 62056-5-3	Безпека обміну даними AMI	Технічний	Світовий	2016	Низька
11	ISO/IEC 14543	Безпека домашніх електронних систем	Технічний	Світовий	2006-2016	Низька

сформовані на основі аналізу літератури, присвяченої оцінці стандартів [11,29,30,31,32,33,34,35,36,37,38,39,40, 41, 42, 43,44].

Зокрема, стандарти повинні відповідати таким вимогам:

(a) бути згаданими у дослідженнях або публікаціях, присвячених ідентифікації стандартів для розумних мереж;

(b) розроблені органом стандартизації або державною установою;

(c) містять визначення та описи заходів кібербезпеки, які можуть бути використані в розумних мережах;

(d) доступні англійською мовою.

Третій (c) критерій потребує особливої уваги, оскільки саме він чітко відрізняє норми, які входять до сфери цього дослідження.

А саме, стандарти мають визначати та описувати засоби кібербезпеки, які можуть бути безпосередньо застосовані або адаптовані до середовища розумних енергосистем. Застосування цього критерію призводить до того, що важливі документи, такі як IEEE C37.24045, Профіль захисту для шлюзу системи інтелектуального обліку електроенергії46 або Конфіденційність і безпека розширеної інфраструктури обліку [47], виключаються з фокусу цього аналізу. Перші дві публікації зосереджуються на вимогах до кібербезпеки, тоді як третя визначає профіль кібербезпеки на основі Common Criteria для шлюзів AMI.

Після застосування критеріїв до стандартів, визначених під час аналізу літератури, було відібрано 19 стандартів або серій стандартів. (Прикладом серії стандартів є IEC 62443 або AMI C12, тоді як окремі стандарти, що входять до серії, — це IEC 62443-3-3 або AMI C12.12.) Документи представлені в таблицях 3–5. Для полегшення порівняння стандартів було введено критерії оцінки, продемонстровані в таблиці 2, аналогічно до критеріїв відбору. Крім того, описи норм, які зосереджуються на змісті, пов'язаному із засобами захисту, наведено в розділі 3.

3 Результати

Стандарти, визначені під час аналізу, представлені в таблицях 3–5. Там ілюструються основні характеристики стандартів відповідно до критеріїв, описаних у розділі 2. Додаткові деталі щодо документів наведено в наступних підрозділах.

3.1.1 NRC RG 5.71

Комісія з ядерного регулювання США (NRC) у своєму регуляторному керівництві (Regulatory Guide, RG) 5.71 «Кібербезпека для ядерних об'єктів» проводить через життєвий цикл програми

Таб. 4. Стандарти, які описують засоби та практики безпеки, що застосовуються до IACS.

№	Стандарт	Сфера застосування	Тип	Регіон	Рік публікації	Релевантність
12	IEC 62443 (ISA 99)	Кібербезпека IACS	Технічний	Світовий	2008-2015	Висока
13	ISO/IEC 27019	Кібербезпека IACS	Загальний	Світовий	2013	Висока
14	NIST SP 800-82	Кібербезпека IACS	Технічний	США	2015	Висока
15	Каталог DHS	Кібербезпека IACS	Загальний	США	2009	Висока

Таб. 5. Загальні стандарти, які описують засоби та практики безпеки, які можуть бути застосовані до розумних мереж.

№	Стандарт	Сфера застосування	Тип	Регіон	Рік публікації	Релевантність
16	ISO/IEC 27001 та 27002	Управління інформаційною безпекою	Загальний	Світовий	2013	Висока
17	NIST SP 800-53	Управління інформаційною безпекою	Загальний	США	2013	Висока
18	NIST SP 800-64	Безпека систем у розробці	Технічний	США	2008	Висока
19	NIST SP 800-124	Безпека мобільних пристроїв	Загальний	США	2013	Висока

кібербезпеки для ядерної інфраструктури. Згідно з цим стандартом, створення програми вимагає:

1. Аналізу комп'ютерних систем і мереж;

2. Ідентифікації та документування критично важливих цифрових активів (CDAs);

3. Впровадження заходів безпеки.

4. Реалізація заходів, які забезпечують підтримку програми. Усі ці кроки детально пояснюються в основних розділах стандарту, а також зведені до шаблону програми безпеки, який наведено у Додатку А. Заходи безпеки, що стосуються третього кроку процесу, представлені у Додатках В і С. Вони базуються на базових контролях з високим рівнем впливу з NIST SP 800-53 та NIST SP 800-82, адаптованих до характеристик сектору ядерної енергетики. Додаток В включає технічні заходи безпеки, тоді як Додаток С – операційні та управлінські [48].

3.1.2 IEEE 1686

IEEE Std 1686-2013 IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities описує засоби захисту для інтелектуальних електронних пристроїв (IED). Ці заходи відповідають програмам захисту критичної інфраструктури (наприклад, NERC CIP). Вони в основному спрямовані на захист дій, пов'язаних із доступом, експлуатацією, конфігурацією, оновленням мікропрограмного забезпечення та отриманням даних із IED. У Додатку А наведено зразок таблиці відповідності [49].

3.1.3 Профіль безпеки для AMI

Профіль безпеки для розширеної інфраструктури обліку електроенергії (Advanced Metering Infrastructure, AMI) надає набір базових заходів контролю для захисту компонентів AMI. Ці заходи є результатом чотириетапного процесу, який включав:

1) аналіз випадків використання розумних мереж;

2) оцінку ризиків;

3) аналіз домену;

4) аналіз та адаптацію заходів контролю, визначених у каталозі DHS (див. розділ 3.2.4). Ці кроки детально описані у розділі 4. Набір заходів безпеки є відносно великим. Для кожного заходу, окрім опису, надається обґрунтування його застосування, а також, у разі необхідності, потенційні покращення або додаткові рекомендації.

Цей документ може використовуватися для підтримки процесу закупівель, слугуючи довідковим матеріалом для комунальних підприємств та постачальників [50].

3.1.4 NISTIR 7628

Внутрішній або міжвідомчий звіт NIST (IR) 7628 «Керівні принципи кібербезпеки для розумних мереж» пропонує підхід до побудови кібербезпеки, який включає визначення категорій логічних інтерфейсів, до яких належить аналізована система, і на основі цього визначення вимог безпеки, пов'язаних із цими інтерфейсами. Стандарт зосереджений на вимогах безпеки, однак у Додатку В також представлені заходи кібербезпеки, які відповідають цим вимогам. Вони охоплюють сім областей, включаючи конфігурації енергосистем та інженерні стратегії, локальний моніторинг, аналіз і контроль обладнання, а також централізований моніторинг і контроль (див. Табл. А2). Крім того, надано таблицю, яка містить приклади заходів контролю, що відповідають конкретним вимогам кібербезпеки, визначеним у стандарті.

Окремий документ «Посібник користувача NISTIR 7628», опублікований у лютому 2014 року, детально описує процес впровадження кібербезпеки в організації розумної мережі. У документі виділено 8 основних видів діяльності, які складають цей процес. Всі вони пов'язані з управлінням ризиками на основі Процесу управління ризиками кібербезпеки в електроенергетичному секторі DOE (RMP)51.

Посібник посилається на попередню версію NISTIR 7628 2010 року, тому він є доповненням до нього. NISTIR 7628 охоплює всю розумну мережу з усіма її компонентами, але також може бути адаптований для конкретних елементів розумної мережі [52].

3.1.5 IEC 62351

IEC 62351 «Управління енергетичними системами та пов'язаний обмін інформацією» — це група стандартів, присвячених інформаційній безпеці обладнання для управління енергетичними системами, включаючи системи управління енергією (EMS), промислові автоматизовані системи управління (IACS), автоматизацію розподілу та інші. Наразі група стандартів IEC 62351 налічує 12 публікацій. Стандарти є деталізованими та технічно орієнтованими. IEC 62351-3 до IEC 62351-6 зосереджуються на безпеці комунікаційних протоколів. IEC 62351-7 визначає абстрактний об'єкт даних для управління мережевими системами (NSM), який може бути адаптований до будь-якого комунікаційного протоколу. NSM є засобом забезпечення високого рівня безпеки в інформаційній інфраструктурі. IEC 62351-8 містить детальну специфікацію ролей доступу (RBAC) у контексті енергетичних систем, тоді як IEC 62351-9 присвячений управлінню ключами, а IEC 62351-14 — реєстрації подій безпеки. IEC 62351-10 описує архітектуру безпеки для енергетичних систем на основі фундаментальних заходів безпеки та надає відображення стандартів, пов'язаних із безпекою, на компоненти енергетичної системи.

3.1.6 Стандарти Smart Grid або енергосистем, які мають меншу відносність до заходів кібербезпеки

Серія стандартів IEEE Std 2030 присвячена питанням взаємодії Smart Grid. Техніки та принципи захисту конфіденційності та безпеки коротко описані в IEEE Std 2030 «IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads», IEEE Std 2030.2-2015 «Guide for the Interoperability of Energy Storage Systems Integrated with the Electric Power Infrastructure» та IEEE Std 2030.3-2016 «IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard».

Стандарт IEC 62541 «OPC Unified Architecture» є серією незалежних від платформи стандартів взаємодії для безпечного зв'язку в промислових автоматизованих системах керування (IACS). IEC TR 62541-2:2016 «OPC Unified Architecture – Part 2: Security Model» описує повну модель безпеки для архітектури, яка включає можливі загрози та функції безпеки, спрямовані на їх усунення. Ефективність цих функцій оцінюється.

IEEE 1402 «Guide for Electric Power Substation Physical and Electronic Security» є простим посібником, присвяченим фізичній та електронній безпеці електропідстанцій. Він містить короткі описи різних типів вторгнень, а також методи захисту для їх усунення. Цікавою та корисною частиною стандарту є Розділ 7, де наведено результати опиту-

вань щодо ефективності заходів безпеки. У Розділі 8 пояснюється підготовка плану безпеки та його основні елементи. Також наведено зразок форми оцінки безпеки.

Серія стандартів IEC 62056 визначає обмін даними для зчитування показів електричних лічильників, тарифів та управління навантаженням. IEC 62056-5-3 «Electricity metering data exchange – The DLMS/COSEM suite – Part 5-3: DLMS/COSEM application layer» описує техніки безпеки в специфікації мови пристроїв (DLMS) та COmpanion Specification for Energy Metering (COSEM).

ISO/IEC 14543 «Information technology – Home electronic system (HES) architecture» складається з 20 стандартів, присвячених різним компонентам систем управління домом, а також аспектам зв'язку та взаємодії. У ISO/IEC 14543-5-1:2010 та ISO/IEC 14543-5-7:2015 описані механізми безпеки для протоколів Intelligent Grouping and Resource Sharing (IGRS).

Серія стандартів IEC 61400-25 «Communications for monitoring and control of wind power plants» визначає уніфіковану інформаційну модель та протоколи для зв'язку між вітроелектростанціями та промисловими системами керування. IEC 61400-25-3 описує вибрані аспекти безпеки.

3.2 Стандарти, що описують заходи безпеки та практики, застосовні до IACS

Цей розділ представляє стандарти, які визначають заходи безпеки для промислових систем управління та автоматизації (IACS). IACS є важливою частиною розумної енергосистеми, яка відповідає за моніторинг та управління промисловими процесами у всій ланцюжку постачання енергії, від генерації до розподілу. Їх захист є необхідним для належного функціонування електромережі.

3.2.1 IEC 62443 (ISA99)

Стандарти ISA99, розроблені комітетом ISA99 (ISA – Міжнародне товариство автоматизації), стосуються електронної безпеки промислових систем автоматизації та управління (IACS). З 2009 року ці стандарти були прийняті в серії IEC 62443 Міжнародною електротехнічною комісією (IEC) Технічним комітетом 65 «Вимірювання, управління та автоматизація промислових процесів», Робочою групою 10, яка тісно співпрацює з комітетом ISA99. Недоліком цієї ситуації є певні проблеми сумісності, оскільки стандарти, опубліковані IEC, базуються на старіших версіях документів ISA99. Наприклад, різні публікації (наприклад, NIST SP 800-82) посилаються на ISA-62443-2-1 як на стандарт, який керує процесом розробки програми безпеки IACS, тоді як поточна версія публікації зосереджена на вимогах до системи управління інформаційною безпекою IACS (IACS-ISMS) і має іншу назву. Водночас версія IEC (IEC-62443-2-1) все ще зосереджена на програмі безпеки IACS. Стандарти та статус їх розробки представлені в таблиці 2. IEC-62443-2-1, ISA-62443-2-2, ISA-62443-2-3 та ISA-62443-3-1 містять описи заходів і практик для захисту IACS [61].

IEC 62443-2-1 Промислові комунікаційні мережі – Мережева та системна безпека – Частина 2-1: Створення програми безпеки для систем промислової автоматизації та управління описує базові елементи Системи управління кібербезпекою (CSMS) для промислових комунікаційних мереж (див. Рисунок 3) і надає рекомендації щодо процесу їх розробки. Ці елементи в основному пов'язані з політиками та процедурами і орієнтовані на персонал. Публікація вводить необхідний фон, обговорює різні типи IACS та відмінності між IACS і класичними ІКТ. Вона пояснює процес проведення оцінки ризиків для IACS, вказуючи на конкретні проблеми, такі як обов'язкове включення некібернетичних активів або питань безпеки. Розділ 4 описує розробку програми безпеки IACS. Публікація має загальний характер і є відносно об'ємною (164 сторінки). Значна кількість інформаційних рекомендацій міститься у додатках. Опублікований у 2010 році стандарт базується на рекомендаціях ISO/IEC 27001 та ISO/IEC 17799, що робить його дещо застарілим. Також назва може вводити в оману, оскільки насправді стандарт орієнтований на CSMS і спрямований на опис CSMS. Ці питання вирішуються супутнім документом ISA 62443-2-1 (найновіша версія датована листопадом 2015 року). Однак він досі знаходиться у версії чернетки, призначеній лише для внутрішнього використання ISA99 та пов'язаних сторін [61,63,64,65].

ISA 62443-2-2 Безпека для промислових автоматизованих систем керування – Керівництво з реалізації системи управління безпекою IACS має статус «заплановано» (див. Рисунок 2). Доступна чернетка стандарту (з квітня 2013 року), в якій деякі заходи контролю залишаються невизначеними. Цей стандарт, подібно до ISO 27019, дотримується принципів ISO 27002. Підхід до безпеки в цих стандартах полягає у визначенні активів, проведенні аналізу ризиків, врахуванні відповідних вимог (правових та інших) та виборі заходів безпеки. У ISA-62443-2-2 описані вимоги до безпеки, і до них відображені заходи контролю безпеки [63].

IEC/TR 62443-2-3:2015 Безпека для промислових систем автоматизації та управління – Частина 2-3: Управління патчами в середовищі IACS надає докладні рекомендації щодо безпечного встановлення програмних патчів, що є особливо критичним та специфічним для IACS. У Додатку B описано повний життєвий цикл безпечного встановлення патчів [64].

IEC/TR 62443-3-1:2009 Промислові комунікаційні мережі – Мережева та системна безпека – Частина 3-1: Технології безпеки для промислових систем автоматизації та управління повністю присвячена детальному представленню сучасних технологій безпеки, які можуть бути застосовані для захисту IACS (промислових систем автоматизації та управління). Кожен засіб захисту розглядається щодо загроз, які він усуває, його впровадження, обмежень та напрямів подальшого розвитку, а також особливостей застосування цього засобу в середовищі IACS. Оцінюється наявність спеціалізованих реалізацій для IACS, наводяться посилання на додаткову літературу, рекомендації та вказівки. Категорії засобів захисту включають автентифікацію та авторизацію, фільтрацію комунікацій та розділення мереж, шифрування та перевірку даних, ведення журналів, аналіз вразливостей, виявлення шкідливого програмного

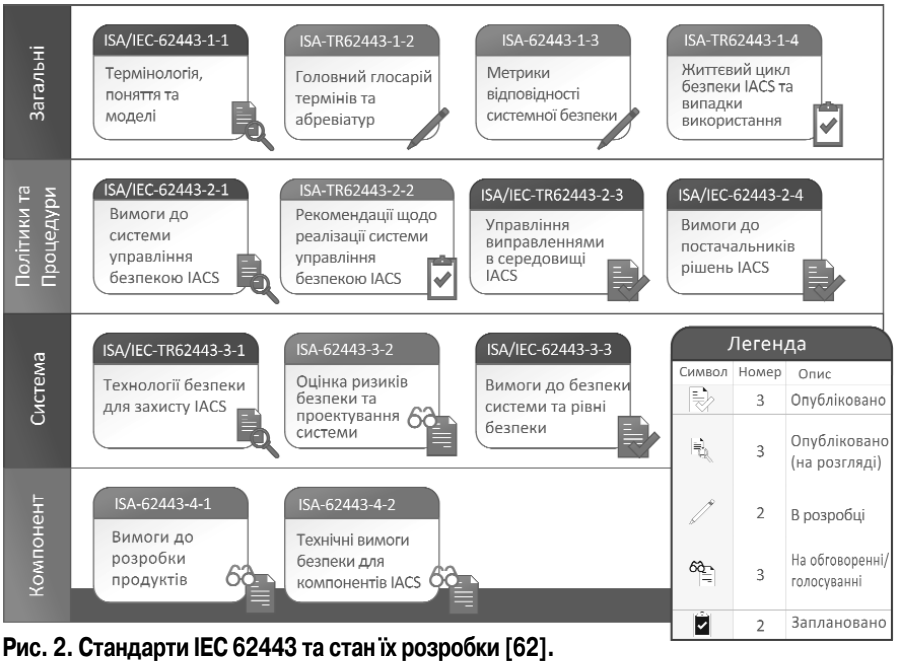


Рис. 2. Стандарти IEC 62443 та стан їх розробки [62].

забезпечення, управління безпекою або засоби фізичного захисту [65].

3.2.2 ISO/IEC 27019

ISO/IEC TR 27019 Інформаційні технології – Методи забезпечення безпеки – Настанови з управління інформаційною безпекою на основі ISO/IEC 27002 для систем управління технологічними процесами, специфічних для галузі енергетики, аналогічно до ISA-62443-2-2, адаптує ISO/IEC 27002 (настанови щодо впровадження системи управління інформаційною безпекою, див. розділ 3.3.1) для IACS. Він також наслідує структуру ISO/IEC 27002. Обидва стандарти посилаються на старшу версію ISO 27002, яка була опублікована в 2005 році, тоді як поточна (наступна) редакція норми була випущена в 2013 році (ISO/IEC 27002:2013). Для заходів безпеки, які можуть бути безпосередньо застосовані до IACS, ISO/IEC 27019 посилається на оригінальний документ для отримання додаткових настанов. Для інших заходів надаються додаткові специфічні для IACS вказівки. Крім того, визначено нові заходи безпеки, спеціально розроблені для IACS. Ці заходи описані у відповідності з іншими заходами та додатково перелічені в Додатку A 3.3.1 [66].

Хоча ISO/IEC 27019 має деякі схожості з ISA-62443-2-2 (зокрема щодо структури та підходу), ці стандарти необхідно розрізняти, оскільки вони суттєво відрізняються. Описання заходів контролю, специфічних для IACS, є різними.

Окремі заходи контролю розширені в одному стандарті, тоді як в іншому вони залишаються незмінними. ISO/IEC 27019 визначає нові заходи контролю, тоді як ISA-62443-2-2 дотримується заходів контролю ISO/IEC 27002. Нарешті, ISA-62443-2-2 досі перебуває у версії чернетки, а його аналог від IEC не існує [66].

3.2.3 NIST SP 800-82

NIST SP 800-82 «Керівництво з безпеки промислових систем управління (ICS)» — це ще одна публікація, присвячена захисту IACS. Подібно до IEC 62443-3-1, документ охоплює різні архітектури IACS (DCS, SCADA, PLC та інші) і розрахований на широке коло читачів, включаючи інженерів з управління, інтеграторів, архітекторів, дослідників та постачальників. На думку авторів, документ має технічний характер [60].

Основні цілі безпеки, визначені в NIST SP 800-82, включають:

- обмеження доступу до мереж IACS (наприклад, через розділення мереж, DMZ, багаторівневий доступ, контроль доступу);
- обмеження фізичного доступу до IACS;
- захист від експлойтів;
- виявлення інцидентів безпеки;
- створення міждисциплінарної команди з безпеки;
- ефективну комунікацію та обмін інформацією;

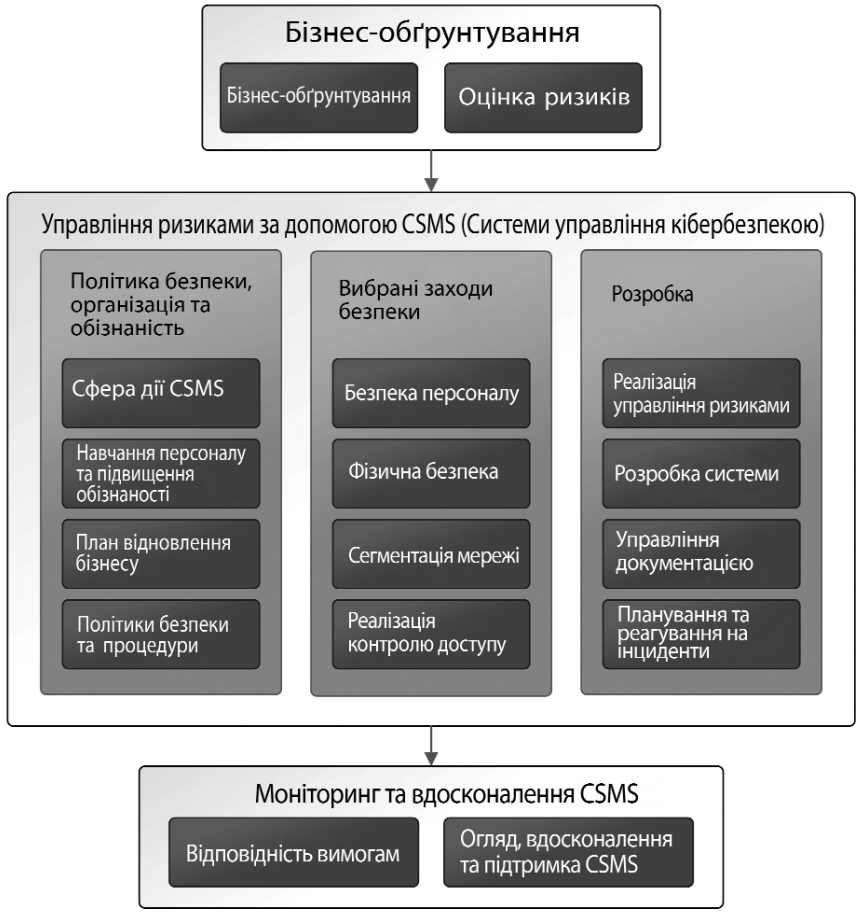


Рис. 3. Елементи системи кібербезпеки IACS, визначені в IEC 62443-2-1.

- відмовостійкість;
- плавне зниження продуктивності у разі збоїв;
- відновлення системи;
- стратегію «захисту в глибину».

Відповідно, стратегія захисту IACS повинна включати:

- політики та процедури, орієнтовані на IACS;
- підвищення обізнаності та навчання;
- забезпечення безпеки на всіх етапах життєвого циклу компонентів IACS (від проектування до утилізації);
- багаторівневу мережу, де критичні операції виконуються в найбезпечнішій підмережі;
- інші заходи, які безпосередньо випливають із цілей безпеки.

Усі ці елементи детально розглядаються в документі [60].

Процес розробки програми безпеки, описаний у NIST SP 800-82 (див. рисунок 4), відображає підхід, представлений у IEC 62443-2-1 (див. розділ 3.2.1), і включає подібні елементи. Фактично, NIST SP 800-82 посилається на IEC 62443-2-1 для отримання додаткових деталей щодо діяльності, яка становить загальний процес. Додаткові рекомендації щодо заходів безпеки для IACS наведено у Додатку G, де представлено детальний опис заходів контролю безпеки. Ці засоби контролю базуються на NIST SP 800-53, однак для кожного з них надано специфічні для IACS вказівки та покращення. Вибір засобів кон-

Рис. 4. Елементи розробки програми забезпечення безпеки IACS згідно з NIST SP 800-82.

тролю для конкретної IACS повинен ґрунтуватися на оцінці ризиків [60].

3.2.4 Каталог DHS

Каталог Міністерства внутрішньої безпеки (DHS) щодо безпеки систем управління: Рекомендації для розробників стандартів визначає великий набір із 250 заходів контролю, які можуть бути застосовані для захисту IACS (промислових систем управління та автоматизації), що використовуються в різних галузях промисловості. Для кожного заходу контролю (під, можливо, оманливим заголовком – «Вимога») надається опис рекомендованих практик безпеки та механізмів. Крім того, надається додаткове керівництво та покращення заходів контролю, де це необхідно. Заходи контролю походять із різних джерел, і їх організація відповідає структурі NIST SP 800-53, що призводить до класифікації заходів контролю на 19 категорій. Джерела заходів контролю не вказані явно, однак у Додатку А міститься таблиця перехресних посилань, де всі заходи контролю з Каталогу DHS зіставляються з 15 іншими стандартами. До цих стандартів входять AGA, FIPS, IEC 62351, ISA99, ISO 27001, ISO 17799, NERC CIP, NIST SP 800-53 та інші. Каталог DHS зосереджений на представленні заходів контролю.

Стандарт не надає додаткових рекомендацій щодо вибору заходів контролю для конкретної конфігурації системи чи галузі [67].

3.3 Загальні стандарти застосування, які описують засоби захисту та практики, які можуть бути застосовані до розумної енергосистеми.

У цьому розділі представлені універсальні стандарти кібербезпеки, які містять описи заходів кібербезпеки. Ці публікації не орієнтовані на електроенергетичний сектор чи розумну енергосистему. Однак представлені заходи та практики захисту можуть бути успішно адаптовані для захисту розумної енергосистеми.

3.3.1 ISO/IEC 27001 та 27002

Серія стандартів ISO/IEC 27000 (або скорочено ISO27k) — це давно визнаний набір стандартів, спрямованих на захист інформаційних активів у організаціях шляхом створення та функціонування системи управління інформаційною безпекою (СУІБ). ISO/IEC 27001 визначає вимоги до правильного впровадження СУІБ на всіх етапах її життєвого циклу. Процес орієнтований на управління ризиками, і його ключовою частиною є періодичне проведення оцінок ризиків. Для зменшення ризиків, виявлених під час оцінок, у Додатку А наведено перелік із 114 заходів безпеки, які охоплюють 35 цілей безпеки. Детальні рекомендації щодо впровадження цих заходів надано в ISO/IEC 27002 (кодекс практики) [68,69].

Стандарти ISO/IEC не лише широко визнані та застосовуються тисячами організацій по всьому світу, але й становлять основу для інших стандартів, керівництв, нормативних актів та рамок у сфері безпеки. Наприклад, специфічні для IACS стандарти ISO/IEC 27019 або ISA 62443-2-2 (див. розділи 3.2.2 та 3.2.1) безпосередньо базуються на ISO/IEC 27002, тоді як NIST SP 800-53 та його наступники (наприклад, NIST SP 800-82) або каталог DHS широко посилаються на них. Багато з цих похідних стандартів базуються на ISO/IEC 27001:2005 та ISO/IEC 27002:2005, тоді як у 2013 році були опубліковані нові версії цих документів, які передбачають певні зміни. Стандарти 2013 року більше не посилаються на модель Plan-Do-Check-Act, акцентують більше уваги на оцінці продуктивності системи управління інформаційною безпекою (ISMS) на основі метрик та перевизначають кілька концепцій, включаючи оцінку ризиків, вибір засобів контролю або постійне вдосконалення [68,69].

3.3.2 NIST SP 800-53

NIST SP 800-53 Редакція 4: «Заходи безпеки та захисту приватності для федеральних інформаційних систем та організацій» визначає базові набори заходів для захисту інформаційних систем у державній адміністрації США, які були розроблені на основі різних типів законодавчих та нормативних документів, стандартів і бізнес-вимог. Ці заходи, згруповані в 18 сімейств, що відображають різні аспекти безпеки, охоплюють різні аспекти захисту, включаючи розробку та управління політиками, підвищення обізнаності та навчання, планування дій у надзвичайних ситуаціях, реагування на інциденти, захист персоналу, придбання систем та інше. Хоча публікація розроблена для федеральних установ, вона отримала широке визнання у всьому світі та застосовується різними організаціями (не лише урядовими) [70].

Базові набори заходів визначені таким чином, що дозволяє їхню високу адаптацію, що сприяє розробці ефективних за вартістю стратегій та систем захисту. Визначення заходів включають параметри, специфічні для організацій, та розширення заходів. Визначено три базові набори заходів, які відповідають трьом рівням критичності систем (низький, середній та високий), визначеним у Федеральному стандарті обробки інформації (FIPS) 199. Перехід від нижчого базового набору до вищого ґрунтується на впровадженні додаткових заходів та їхніх розширень. Крім того, у новій (четвертій) версії стандарту було введено концепцію «накладок» (overlays). Накладки дозволяють визначати базові набори заходів, адаптовані до конкретних потреб організації, її місії чи бізнес-функцій, технологій або середовищ. Водночас рекомендації, специфічні для IACS, які були присутні у попередніх версіях, були перенесені до NIST SP 800-82 (див. розділ 3.2.3). Важлива частина NIST SP 800-53 присвячена поясненню процесу вибору заходів, який має бути частиною управління ризиками в організації [70].

3.3.3 NIST SP 800-64

NIST SP 800-64 «Розгляд питань безпеки в життєвому циклі розробки систем» провідно через процес інтеграції принципів і практик кібербезпеки в життєвий цикл розробки IT-систем. Ці рекомендації базуються на класичній моделі розробки програмного забезпечення – моделі водоспаду, в якій стандарти виділяють п'ять етапів. До них належать ініціація, розробка або придбання, впровадження або оцінка, експлуатація та технічне обслуговування, а також утилізація. У кожній фазі визначаються заходи безпеки, пов'язані з відповідним етапом. Описання є деталізованими і супроводжуються порадами щодо впровадження. Хоча стандарт використовує модель водоспаду як орієнтир, його принципи можуть застосовуватися і до інших підходів до розробки програмного забезпечення [71]. Однак доповнення норми вказівками щодо безпеки в умовах гнучкої розробки (agile) могло б бути корисним.

3.3.4 NIST SP 800-124

NIST SP 800-124 «Рекомендації щодо управління безпекою мобільних пристроїв у підприємствах» надає конкретні вказівки щодо забезпечення безпеки мобільних пристроїв. Стандарт описує технології управління мобільними пристроями разом із необхідними функціями безпеки та пояснює їх застосування протягом усього життєвого циклу мобільних рішень. Аналогічно до NIST SP 800-64 (див. розділ 3.3.3), за основу береться п'ятиетапна каскадна модель життєвого циклу системи [72].

4 АНАЛІЗ СТАНДАРТІВ

У цьому розділі представлено результати аналізу стандартів та засобів кібербезпеки, які вони визначають. Зокрема, досліджено взаємозв'язки між засобами захисту, а також охоплення доменів розумних мереж і сфер кібербезпеки. Ці теми описані в підрозділах [4.1, 4.2] та [4.3].

4.1 Взаємозв'язки між заходами кібербезпеки в стандартах

Взаємозв'язки між заходами кібербезпеки в ідентифікованих стандартах представлені на Рисунку 5. Односторонні суцільні стрілки вказують на те, які норми служили вхідними даними під час розробки інших специфікацій заходів і практик кібербезпеки. Наприклад, заходи, визначені в NRC RG 5.71, походять із NIST SP 800-53 та NIST SP 800-82 (див. Розділ 3.1.1). Пунктирні двосторонні стрілки показують збіжність між стандартами щодо заходів кібербезпеки. NIST SP 800-53 має високу ступінь збіжності з ISO 27001 у тому сенсі, що практично для всіх заходів,

визначених у ISO 27001, можна знайти їхні еквіваленти в NIST SP 800-53. Крім того, у Додатку H NIST SP 800-53 надає таблиці відповідностей, де представлені взаємозв'язки між окремими заходами в обох документах. Пунктирні односторонні стрілки вказують на те, що стандарт посилається на заходи або практики кібербезпеки, визначені в іншій публікації. Наприклад, IEEE 2030 рекомендує враховувати стандарти ISO 27000 під час розробки програми безпеки.

Горизонтальні лінії відображають сферу дії стандартів щодо заходів кібербезпеки, їх рівень абстракції та охоплення областей розумної енергосистеми. Наприклад, заходи кібербезпеки, визначені в ISO 27001 та 27002, є універсальними та застосовними до організацій різних типів і розмірів. З іншого боку, засоби контролю, визначені в IEC 62351, призначені для конкретних комунікаційних протоколів у розумній енергосистемі. IEEE 1686 визначає заходи для конкретних компонентів розумної енергосистеми (IED), тоді як заходи з NIST SP 800-124, NRC RG 5.71 або IEEE 1402 більш підходять для конкретних областей розумної енергосистеми (польові операції, електростанції, підстанції).

4.2 Розділи розумної енергосистеми, які охоплюються засобами контролю

На рисунку 6 представлено відображення зв'язку між розділами розумної енергосистеми та стандартами, які визначають засоби кібербезпеки для них. Розділи розумної енергосистеми відповідають архітектурі розумної енергосистеми, визначеній IEC (див. розділ 2). Усі домени розумної енергосистеми охоплені специфікаціями засобів контролю у більшій чи меншій мірі. Єдиним винятком є «Кабельні та повітряні лінії», які мають виключно фізичний характер. Стандарти, такі як IEEE 1686, NRC RG 5.71 або IEC 62443 (ISA 99), пропонують засоби кібербезпеки, спеціально призначені для вказаних розділів (підстанції, електростанції та IACS – відповідно). З іншого боку, NISTIR 7628 є публікацією широкого спектру з питань безпеки розумної енергосистеми, яка охоплює кілька доменів розумної енергосистеми. Однак деякі з них (наприклад, ринки енергії або експлуатація енергосистеми) розглядаються лише обмежено.

4.3 Напрями кібербезпеки, які охоплюють засоби контролю

Напрями кібербезпеки, які охоплюють засоби контролю, визначені в аналізованих стандартах, представлені в таблицях A1 – A4 Додатка A. Стає очевидним, що стандарти зі спільним коренем, такі як NIST SP 800-82 та DHS Catalog, які були розроблені з посиланням на NIST SP 800-53 (див. розділ 4.1), охоплюють схожі напрями кібербезпеки.

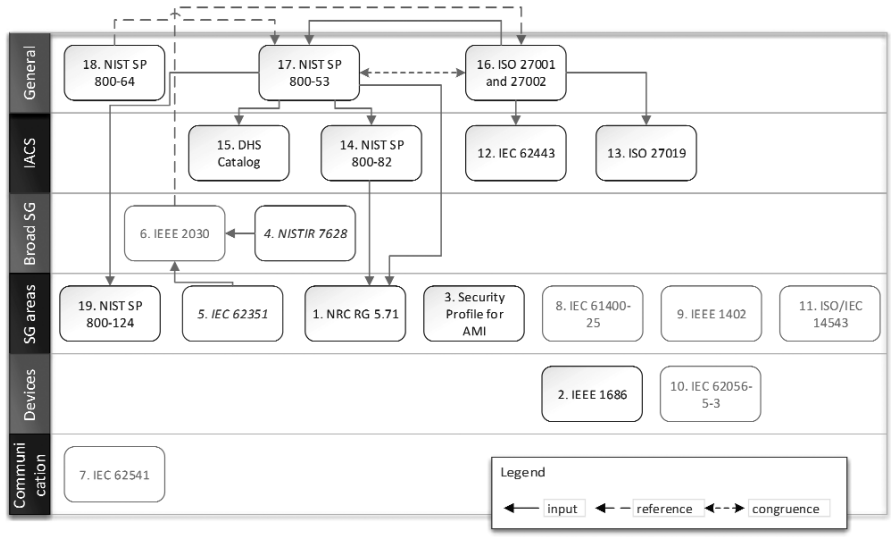


Рис. 5. Взаємозв'язки між засобами кібербезпеки в ідентифікованих стандартах. Односторонні суцільні стрілки вказують на те, які стандарти служили вхідними даними під час розробки інших специфікацій заходів і практик кібербезпеки. Пунктирні двосторонні стрілки показують відповідність між стандартами щодо заходів кібербезпеки. Пунктирні односторонні стрілки вказують на те, що стандарт посилається на заходи або практики кібербезпеки, визначені в іншій публікації. Горизонтальні смуги відображають сферу дії стандартів щодо вимог кібербезпеки, їх рівень узагальненості та/або тематичного охоплення.

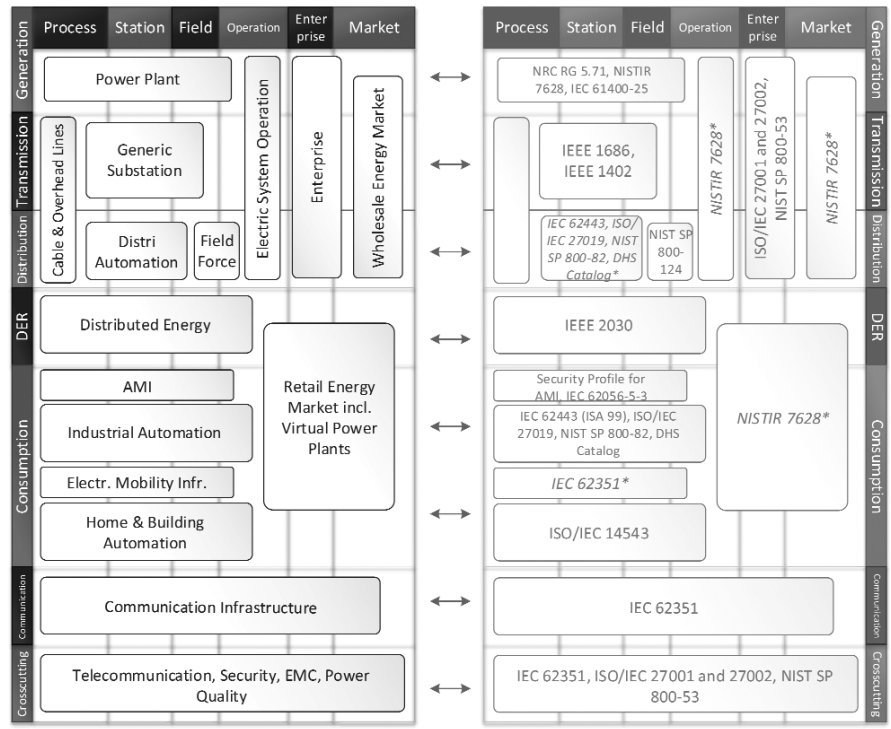


Рис. 6. Відображення відповідності між областями розумної енергосистеми та стандартами, які визначають засоби захисту для них. Стандарти, позначені зірочкою та курсивом, охоплюють зазначену область розумної енергосистеми лише у незначній мірі.

5 Пов'язані роботи

Дії з інвентаризації розумних мереж, пов'язані з ініціативами щодо стандартизації, описані в розділі 2, які були спрямовані на визнання існуючих стандартів, що стосуються кібербезпеки, мали на меті отримати загальний огляд ситуації, а не досягти наукової повноти або правильності проведення. Отже, вони не вимагали застосування та демонстрації систематичного методу дослідження. В результаті дослідження представляють різні стандарти та презентують їх з різних перспектив [73,28,74,75,15,76,77,78,79,25,24,22,17,21,23,80,27,81].

Крім того, наукові огляди, які зосереджуються на ідентифікації стандартів кібербезпеки для розумних мереж [11,12,13,14,15,16,17,18,19,20], демонструють різні рівні глибини дослідження, повноти та об'єктивності, переважно будучи лише необмеженими оглядами стандартів і специфікацій, пов'язаних із кібербезпекою розумних мереж. Жоден з них не присвячений темі заходів кібербезпеки, які можна використовувати в розумних мережах.

Серед досліджень виділяється робота Wang et al. у 12, оскільки вона ґрунтується на прозорих критеріях (джерело стандарту, релевантність до кібербезпеки розумних мереж та репрезентативність). В результаті було визнано 17 публікацій, включаючи NERC CIP, NISTIR 7628, IEEE 1686-2007, NIST SP 800-82, а також DHS Catalog12. Це єдине дослідження, яке надає деталі систематичного методу, використаного в оцінці, а також критерії відбору/оцінки.

Дослідження, описане в цій роботі, продовжує попередні дослідження автора, присвячені стандартам, що стосуються аспектів кібербезпеки розумних мереж7, вимогам до кібербезпеки для розумних мереж8 та оцінкам безпеки в розумних мережах9. Воно застосовує той самий систематичний і повторюваний метод дослідження (деталі якого відкрито надано), заснований на прозоро заявлених критеріях відбору та оцінки, щоб досягти найвищого можливого ступеня повноти.

Це дослідження присвячене заходам кібербезпеки, тобто технічним і нетехнічним заходам захисту системи або активів від кібератак, які можна використовувати в інфраструктурі розумних мереж. Наскільки відомо авторові, немає паралельних робіт, які б розглядали цю тему, незважаючи на її значущість і актуальність. В результаті цей огляд надає своєрідний посібник зі стандартів розумних мереж, які визначають заходи кібербезпеки – описано 19 стандартів і рекомендацій з точки зору заходів безпеки, які посилаються один на одного та пов'язані з критеріями оцінки. Всі вони були пов'язані з архітектурою розумних мереж IEC (див. рис. 1), щоб показати взаємозв'язки між стандартами та компонентами розумних мереж.

6 Висновки

Існує кілька стандартів, які визначають заходи кібербезпеки, що застосовуються до розумних мереж. Деякі з них, такі як NRC RG 5.71 або IEEE 1686, безпосередньо присвячені цій темі, інші розглядають її як одну з охоплюваних областей. Норми, такі як ISO 27001 або NIST SP 800-53, хоча і не присвячені розумним мережам, можуть бути легко адаптовані до них, особливо що стосується їх корпоративної частини. Деякі стандарти (NIST SP 800-82 та каталог DHS) значно перекриваються щодо визначених ними заходів контролю, інші, хоча також походять із спільного джерела, є взаємодоповнювальними (IEC 62443 (ISA 99) та ISO/IEC 27019).

Стає очевидним, що ISO 27001, ISO 27002 та NIST SP 800-53, хоча й дуже схожі, також є взаємодоповнювальними. Вони мають подібне охоплення заходів кібербезпеки та областей, але групують заходи кібербезпеки в різні категорії (див. Таблицю А4) і описують їх з різним рівнем деталізації. Для стандартів ISO доступні та встановлені процеси сертифікації. З іншого боку, NIST SP 800-53 надає більш детальні описи заходів контролю. Можливий підхід до реалізації заходів контролю може полягати в тому, щоб прагнути до задоволення вимог відповідності ISO, використовуючи публікацію NIST для отримання рекомендацій.

Серед стандартів із заходами та практиками кібербезпеки, присвяченими IACS, каталог DHS та NIST SP 800-82 демонструють видиму збіжність, оскільки обидва походять із NIST SP 800-53 і охоплюють практично ті самі області контролю. Каталог DHS повністю зосереджений на заходах контролю, тоді як NIST SP 800-82 додатково пояснює процес розробки та впровадження програми кібербезпеки для IACS. Крім того, NIST SP 800-82 періодично переглядається та оновлюється. Його найновіша версія була випущена в 2015 році, і це друга редакція оригінального випуску 2011 року. Каталог DHS, з іншого боку, датується 2009 роком, і з того часу до нього не вносилися жодні зміни чи поправки.

Аналогічно, IEC 62443 (ISA 99) та ISO/IEC 27019, які також орієнтовані на IACS, містять пересічні частини, оскільки стандарти базуються на ISO/IEC 27001. Зокрема, ISO 27019 та ISA-62443-2-2 слідують структурі ISO/IEC 27001, тоді як IEC 62443-2-1 базується на її рекомендаціях. Однак слід зазначити, що останній ще не був офіційно опублікований, а доступна чернетка є неповною. З іншого боку, IEC/TR 62443-3-1:2009 надає детальне пояснення технологій безпеки, специфічних для IACS, незалежно від ISO 27001.

Таблиця А1. Галузі кібербезпеки, які охоплюються засобами контролю, визначеними в стандартах розумних мереж або енергосистем, з високим рівнем уваги до кібербезпекових заходів і практик.

NRC RG 5.71	IEEE 1686-2013	Профіль безпеки для AMI
Контроль доступу	Журнал аудиту	Контроль доступу
Аудит та підзвітність	Доступ до комунікаційних портів	Аудит та підзвітність
Підвищення обізнаності та навчання	Електронний контроль доступу	Реагування на інциденти
Управління конфігурацією	Контроль якості прошивки	Управління інформацією та документацією
Планування дій у надзвичайних ситуаціях / безперервність безпеки, захисту та готовності до надзвичайних ситуацій	Програмне забезпечення для конфігурації IED	Життєздатність
Захист критичних цифрових активів і комунікацій	Функції кібербезпеки IED	Захист систем і комунікацій
Захист на основі глибини оборони	Наглядовий моніторинг і контроль	Цілісність систем і інформації
Захисна стратегія		Розробка та підтримка системи
Функції		
Ідентифікація та автентифікація		
Реагування на інциденти		
Обслуговування		
Захист носіїв інформації		
Безпека персоналу		
Фізичний та екологічний захист		
Оцінка безпеки та управління ризиками		
Цілісність систем і інформації		
Придбання систем і послуг		
Зміцнення системи		

Таблиця А2. Галузі кібербезпеки, які охоплюються заходами контролю, визначеними в стандартах для розумних мереж або енергосистем, що є помірно актуальними для заходів і практик кібербезпеки.

NISTIR 7628	IEC 62351
Централізований моніторинг і контроль	Запис подій (Event logging)
Централізований аналіз і управління енергосистемою	Системи виявлення вторгнень (Intrusion detection systems)
Моніторинг, аналіз і управління локальним обладнанням	Управління ключами (Key management)
Конфігурації енергосистем та інженерні стратегії	Моніторинг і управління мережами та протоколами
Тестування	Моніторинг і управління кінцевими системами
Навчання	Контроль доступу на основі ролей (Role-based access control)
	Безпека комунікаційних протоколів

Інші області розумних мереж, які добре охоплені стандартами щодо заходів кібербезпеки, — це інфраструктура AMI та атомні електростанції, для яких заходи безпеки визначені у «Профілі безпеки для AMI» та NRC RG 5.71 відповідно. Для електростанцій з меншою критичністю, ніж атомні електростанції, NRC RG 5.71, NIST SP 800-53 та NIST SP 800-82 можуть використовуватися разом як довідник, з підходом заміни високоінтенсивних заходів контролю з NRC RG 5.71 на менш інтенсивні.

IEEE 1402 присвячений фізичній безпеці електричних підстанцій, але також коротко описує вибрані заходи кібербезпеки. Щодо польової роботи технічного персоналу, NIST SP 800-124 детально пояснює заходи для захисту використання мобільних пристроїв. Специфічні області домашньої електронної системи (HES) та вітрових електростанцій охоплені специфікаціями IEC 61400-25-3 та ISO/IEC 14543. Що стосується електричних пристроїв, IEEE 1686 визначає заходи кібербезпеки для IED, а IEC 62056-5-3 охоплює вибрані області контролю електричних лічильників. IEC 62351 та IEC 62541 зосереджені на комунікаціях енергосистем та IACS.

NISTIR 7628 та IEEE 2030 охоплюють елементи всієї архітектури розумних мереж, з сильним акцентом на їхню взаємодію. Перший зосереджується на кібербезпеці, але переважно присвячений вимогам та аспектам конфіденційності, описуючи лише вибрані заходи кібербезпеки. Другий не присвячений кібербезпеці, але містить пов'язаний з нею контент. Він посилається на ISO 27001 та NISTIR 7628, але включає додаткові пояснення щодо процесу впровадження (у Додатку В) або інженерії безпеки.

Можна спостерігати певні диспропорції щодо охоплення кібербезпекою різних доменів розумних мереж. IACS та корпоративні частини розумних мереж охоплені особливо добре. Оператори атомних електростанцій та підстанцій також знайдуть корисні рекомендації щодо заходів контролю в NRC RG 5.71, IEEE 1686. Оператори інших типів електростанцій можуть адаптувати рекомендації з NRC RG 5.71 за допомогою NIST SP 800-53 та NIST 800-82.

Області, які потребують подальшого розвитку стандартизації щодо заходів кібербезпеки, включають:

- ринки,
- експлуатацію всієї енергосистеми,
- електромобілі.

Додаток

Сфери кібербезпеки, які охоплюють засоби контролю

Таблиці А1 – А4 відображають сфери кібербезпеки, які охоплюються засобами контролю, визначеними в аналізованих стандартах.

Таблиця А3. Галузі кібербезпеки, які охоплюються засобами контролю, визначеними в стандартах, що описують заходи та практики, застосовні до IACS.

IEC 62443	ISO/IEC 27019	NIST SP 800-82	DHS Catalog
Аудит	Контроль доступу	Контроль доступу	Контроль доступу
Аутентифікація та авторизація	Управління активами	Аудит та підзвітність	Аудит та підзвітність
Валідація даних	Управління безперервністю бізнесу	Підвищення обізнаності та навчання	Управління конфігурацією
Шифрування та валідація даних	Управління комунікаціями та операціями	Управління конфігурацією	Реагування на інциденти
Фільтрація, блокування та контроль доступу	Відповідність вимогам	Планування відновлення	Управління інформацією та документами
Управління	Управління людськими ресурсами	Ідентифікація та аутентифікація	Захист носіїв інформації
Вимірювання	Управління інцидентами інформаційної безпеки	Реагування на інциденти	Моніторинг та огляд
Політика безпеки систем керування	Придбання, розробка та підтримка інформаційних систем	Обслуговування	Організаційна безпека
Операційні системи	Організація інформаційної безпеки	Захист носіїв інформації	Безпека персоналу
Контроль фізичної безпеки	Фізична та екологічна безпека	Безпека персоналу	Фізична та екологічна безпека
	Політика безпеки	Фізичний та екологічний захист	Управління ризиками та оцінка
		Планування	Підвищення обізнаності з безпеки та навчання
		Управління програмами	Політика безпеки
		Оцінка ризиків	Управління програмами безпеки
		Оцінка та авторизація безпеки	Стратегічне планування
		Захист систем та комунікацій	Системи та комунікації
		Цілісність систем та інформації	Цілісність систем та інформації
		Придбання систем та послуг	Придбання систем та послуг
			Розробка та підтримка систем

Таблиця А4. Галузі кібербезпеки, які охоплюються засобами контролю, визначеними в загальних стандартах застосування, що описують заходи та практики кібербезпеки, які можуть бути застосовані до розумних мереж.

ISO 27001 та 27002	NIST SP 800-53	NIST SP 800-64	NIST SP 800-124
Контроль доступу	Контроль доступу	Оцінка впливу на бізнес	Контроль доступу
Управління активами	Аудит та підзвітність	Управління конфігурацією	Безпека додатків
Управління безперервністю бізнесу	Обізнаність та навчання	Постійний моніторинг	Аудит
Управління комунікаціями та операціями	Управління конфігурацією	Детальний план сертифікації та акредитації	Налаштування конфігурації
Відповідність	Планування відновлення після надзвичайних ситуацій	Розробка плану утилізації або переходу	Санітація носіїв
Управління людськими ресурсами	Ідентифікація та автентифікація	Утилізація апаратного та програмного забезпечення	Безпечне зберігання та передача даних
Управління інцидентами інформаційної безпеки	Реагування на інциденти	Збереження інформації	Навчання з безпеки
Придбання, розробка та підтримка інформаційних систем	Технічне обслуговування	Авторизація інформаційних систем	Політика безпеки
Організація інформаційної безпеки	Захист носіїв	Категоризація інформаційних систем	Захист систем та комунікацій
Фізичний та екологічний захист	Захист персоналу	Санітація носіїв	Цілісність систем та інформації
Політика безпеки	Фізичний та екологічний захист	Огляд операційної готовності	Автентифікація користувачів та пристроїв
	Планування	Оцінка впливу на конфіденційність	
	Управління програмами	Оцінка ризиків	
	Оцінка ризиків	Розробка безпечних інформаційних систем	
	Оцінка та авторизація безпеки	Визначення архітектури безпеки	
	Захист систем та комунікацій	Оцінка безпеки	
	Цілісність систем та інформації	Вибір та документування засобів контролю безпеки	
	Придбання систем та послуг	Документування безпеки	
		Інтеграція безпеки	
		Планування безпеки	
		Завершення роботи системи	

Література:

1. Yilin Mo, Kim Tiffany Hyun-Jin, Brancik K., et al. CyberaЪPhysical Security of a Smart Grid Infrastructure. Proceedings of the IEEE. 2012;100(1):195-209.

2. Pearson Ivan L.G. Smart grid cyber security for Europe. Energy Policy. 2011;39(9):5211-5218.

3. Tipton Harold F, Krause Micki. Information Security Management Handbook, Sixth Edition. No. c2007.

4. Von Solms R. Information security management : why standards are important. Information Management & Computer Security. 1999;7(1):50-57.

5. Kissel Richard. NISTIR 7298 Revision 2 Glossary of Key Information Security Terms. : NIST; 2013.

6. ISO/IEC . ISO/IEC 27000:2016 Information technology aЪ Security techniques aЪ Information security management systems aЪ Overview and vocabulary. 2016.

7. Leszczyna Rafa. Cybersecurity and privacy in standards for smart grids aЪ A comprehensive survey. Computer Standards and Interfaces. 2018;56(April 2017):62 - 73.

8. Leszczyna Rafa. A Review of Standards with Cybersecurity Requirements for Smart Grid. Computers & Security. 2018;.

9. Leszczyna Rafal. Standards on Cyber Security Assessment of Smart Grid. International Journal of Critical Infrastructure Protection. 2018;.

10. Webster Jane, Watson Richard T.. Analyzing the past to prepare for the future: writing a literature review. MIS Quarterly.

2002;26(2):xiii - xxiii.

11. Ruland Karl Christoph, Sassmannshausen Jochen, Waedt Karl, Zivic Natasa. Smart grid security aЪ an overview of standards and guidelines. Elektrotechnik und Informationstechnik. 2017;134(1):19 - 25.

12. Wang YuFei, Zhang Bo, Lin WeiMin, Zhang Tao. Smart grid information security - a research on standards. In: :1188 - 1194IEEE; 2011.

13. Lam Jonathan. Protecting Large and Complex Networks. IET Cyber Security in Modern Power Systems. 2016;(June).

14. Kanabar Mitalkumar G., Voloh Ilia, McGinn David. Reviewing smart grid standards for protection, control, and monitoring applications. In: :1 - 8IEEE; 2012.

15. Griffin Robert W., Langer Lucie. Chapter 7 aЪ Establishing a Smart Grid Security Architecture. In: 2015 (pp. 185 - 218).

16. Rosinger Christine, Uslar Mathias. Smart Grid Security: IEC 62351 and Other Relevant Standards. In: Springer, Berlin,

Heidelberg 2013 (pp. 129 - 146).

17. Goraj M., Gill J., Mann S.. Recent developments in standards and industry solutions for cyber security and secure remote access to electrical substations. In: :161 - 161IET; 2012.

18. Falk Rainer, Fries Steffen. Smart Grid Cyber Security - An Overview of Selected Scenarios and Their Security Implications.

PIK - Praxis der Informationsverarbeitung und Kommunikation. 2011;34(4):168 - 175.

19. Wang Yong, Ruan Da, Xu Jianping. Analysis of Smart Grid security standards. In: :697 - 701IEEE; 2011.

20. Kuzlu M., Pipattanasompom M., Rahman S.. A comprehensive review of smart grid related standards and protocols. In:

:12 - 16IEEE; 2017.

21. Hauer I., Styczynski Z. A., Komarnicki P., Stotzer M., Stein J.. Smart grid in critical situations. Do we need some standards for this? A german perspective. In: :1 - 8IEEE; 2012.

22. Kanabar Mitalkumar G., Voloh Ilia, McGinn David. A review of smart grid standards for protection, control, and monitoring applications. In: :281 - 289IEEE; 2012.

23. CEN-CENELEC-ETSI JWG . Final report Standards for Smart Grids. 2011.

24. Fan Zhong,Kulkarni Parag, Gormus Sedat, et al. Smart Grid Communications: Overviewof Research Challenges, Solutions, and Standardization Activities. IEEE Communications Surveys & Tutorials. 2013;15(1):21 - 38.

25. DKE . German Roadmap E-Energy/Smart Grid 2.0. : German Commission for Electrical, Electronic & Information Technologies of DIN and VDE; 2013.

26. Wouter Vlegels , Leszczyna (eds.) Rafal. Smart Grid Security: Recommendations for Europe and Member States. 2012.

27. Standardisation Management Board Smart Grid Strategic Group (SG3) . IEC Smart Grid Standardization Roadmap. June: Standardisation Management Board Smart Grid Strategic Group (SG3); 2010.

28. IEC . Smart Grid Standards Map. 2017.

29. Zhang Yurong, Wang Jingjing, Hu Fangfang, Wang Yuanfeng. Comparison of evaluation standards for green building in China, Britain, United States. Renewable and Sustainable Energy Reviews. 2017;68:262 - 271.

30. Metheny Matthew. Comparison of federal and international security certification standards. In: Elsevier 2017 (pp. 211 - 237).

31. Gazis Vangelis. A Survey of Standards for Machine-to-Machine and the Internet of Things. IEEE Communications Surveys & Tutorials. 2017;19(1):482 - 511.

32. ENISA . PETs controls matrix: A systematic approach for assessing online and mobile privacy tools. : ; 2016.

33. Beckers Kristian, Cote Isabelle, Fenz Stefan, Hatebur Denis, Heisel Maritta. A Structured Comparison of Security Standards. In: Springer International Publishing 2014 (pp. 1–34).

34. Sunyaev Ali.. Design and application of a security analysis method. In: Gabler 2011 (pp. 117–166).

35. Overman Thomas M., Davis Terry L., Sackman RonaldW.. High assurance smart grid. In: :1ACM Press; 2010; New York, USA.

36. Sommestad Teodor, Ericsson GoI.ranN,Nordlander Jakob. SCADAsystem cyber security a..Acomparison of standards. In: :1–8IEEE; 2010.

37. Kuligowski Christine. Comparison of IT Security Standards. PhD thesis2009.

38. Siponen Mikko, Willison Robert. Information security management standards: Problems and solutions. Information & Management. 2009;46(5):267–270.

39. Kosanke Kurt. ISO Standards for Interoperability: a Comparison. In: London: Springer-Verlag 2006 (pp. 55–64).

40. Arora Varun. Comparing different information security standards : COBIT v s . ISO 27001. Carnegie Mellon University, Qatar. 2005;:7–9.

41. Idaho National Laboratory . A Comparison of Cross-Sector Cyber Security Standards. : ; 2005.

42. Phillips T., Karygiannis T., Huhn R.. Security Standards for the RFID Market. IEEE Security and Privacy Magazine. 2005;3(6):85–89.

43. Lee Annabelle, Snouffer Stanley R., Easter Randall J., Foti James, Casar Tom. NIST SP 800-29 A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2. : ; 2001.

44. Eastaughffe K.A., Cant A., Ozols M.A.. A framework for assessing standards for safety critical computer-based systems. In: :33–44IEEE Comput. Soc; 1999.

45. IEEE Power & Energy Society. Power System Relaying Committee. , IEEE Power & Energy Society. Substations Committee., Institute of Electrical and Electronics Engineers. , IEEE-SA Standards Board.. C37.240-2014 — IEEE standard cybersecurity requirements for substation automation, protection, and control systems. : ; 2014.

46. Kreutzmann Helge, Vollmer Stefan. Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP). 2014.

47. Netbeheer Nederland . Privacy and Security of the Advanced Metering Infrastructure. : ; 2010.

48. NRC . NRC RG 5.71 Cyber Security Programs for Nuclear Facilities. : ; 2010.

49. IEEE . IEEE 1686-2013 - IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities. 2013.

50. Advanced Security Acceleration Project . Security Profile for Advanced Metering Infrastructure. : ; 2010.

51. DOE , NIST , NERC . Electricity Subsector Cybersecurity Risk Management Process. May: ; 2012.

52. The Smart Grid Interoperability Panel Cyber SecurityWorking Group . NISTIR 7628 Revision 1 Guidelines for Smart Grid

Cybersecurity. : NIST; 2014.

53. IEC . IEC/TS 62351-1: Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues. 2007.

54. Cleveland Frances. IEC TC57 WG15: IEC 62351 Security Standards for the Power System Information Infrastructure. : International Electrotechnical Commission; 2016.

55. IEEE Standards Coordinating Committee 21 . IEEE guide for the interoperability of energy storage systems integrated with the electric power infrastructure. : ; 2015.

56. IEC . IEC TR 62541-2:2016 OPC unified architecture - Part 2: Security Model. 2016.

57. IEEE-SA Standards Board . IEEE 1402 (R2008) - IEEE Guide for Electric Power Substation Physical and Electronic Security. : ; 2008.

58. IEC . IEC 62056-5-3:2016 Electricity metering data exchange - The DLMS/COSEM suite - Part 5-3: DLMS/COSEM application layer. : ; 2016.

59. ISA . ISA99, Industrial Automation and Control Systems Security. 2017.

60. Stouffer Keith, Pillitteri Victoria, Lightman Suzanne, Abrams Marshall, Hahn Adam. NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security Revision 2. : NIST; 2015.

61. IEC . IEC 62443-2-1: Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program. 2010.

62. ISA . The 62443 series of standards Industrial Automation and Control Systems Security. : ; 2016.

63. ISA . ISA 62443-2-2 Security for industrial automation and control systems - Implementation Guidance for and IACS Security Management System. 2013.

64. IEC . IEC TR 62443-2-3: Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment. 2015.

65. IEC . IEC/TR 62443-3-1: Industrial communication networks aЂ Network and system security aЂ Part 3-1: Security technologies for industrial automation and control systems. 2009.

66. ISO/IEC . ISO/IEC TR 27019:2013: Information technology aЂ Security techniques aЂ Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry. 2013.

67. DHS . Catalog of Control Systems Security: Recommendations for Standards Developers. : ; 2009.

68. ISO/IEC . ISO/IEC 27001:2013: Information technology aЂ Security techniques aЂ Information security management systems aЂ Requirements. 2013.

69. ISO/IEC . ISO/IEC 27002:2013: Information technology - Security techniques - Code of practice for information security controls. 2013.

70. National Institute of Standards and Technology (NIST) . NIST SP 800-53 Rev. 4 Recommended Security Controls for Federal Information Systems and Organizations. U.S. Government Printing Office; 2013.

71. Kissel Richard, Stine Kevin M, Scholl Matthew A, Rossman Hart, Fahlsing James, Gulick Jessica. NIST SP 800-64 Rev. 2 Security Considerations in the System Development Life Cycle. : ; 2008.

72. Souppaya Murugiah, Scarfone Karen. NIST Special Publication 800-124 Rev. 1 Guidelines for Managing the Security of Mobile Devices in the Enterprise. NIST special publication. 2013;:30.

73. IEC . Smart Grid. 2018.

74. Ontario Smart Grid Forum . Ontario Smart Grid Forum. 2017.

75. OpenSG . Security Working Group. : ; 2017.

76. IEEE Standards Association . IEEE Smart Grid Interoperability Series of Standards. 2015.

77. National Institute of Standards and Technology . NIST SP 1108r3: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. : Na; 2014.

78. CEN-CENELEC-ETSI Smart Grid Coordination Group . Smart Grid Set of Standards Version 3.1. : ; 2014.

79. CEN-CENELEC-ETSI Smart Grid Coordination Group . SG-CG/M490/H_Smart Grid Information Security. : ; 2014.

80. European Commission . M/490 Smart Grid Mandate Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment. : ; 2011.

81. State Grid Corporation of China . SGCC Framework and Roadmap to Strong & Smart Grid Standards. : State Grid Corporation of China; 2010.

27 – 29 травня 2025

XXI МІЖНАРОДНА СПЕЦІАЛІЗОВАНА ВИСТАВКА

ТЕХНОЛОГІЇ ЗАХИСТУ / ПОЖТЕХ

Генеральний медіа-партнер: Охорона праці і пожежна безпека

Генеральний інформаційний партнер: Бізнес і безпека

МІСЦЕ ПРОВЕДЕННЯ:
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

ALD
engineering company

Група компаній ALD ENGINEERING COMPANY, заснована у 2019 році, впевнено зарекомендувала себе як надійний партнер у будівельній галузі. Завдяки понад 20-річному досвіду команди у виконанні проєктів будь-якої складності, компанія займає лідируючі позиції, активно впроваджуючи сучасні будівельні технології.

Особливістю ALD ENGINEERING COMPANY є надання повного спектра будівельних послуг «під ключ»: від концепції, проєктування та будівництва до управління процесами і введення об'єкта в експлуатацію. Такий підхід дозволяє швидко реагувати на запити замовників та гарантує високу якість кінцевого результату.

З 2022 року в Україні ALD ENGINEERING COMPANY розширило свою діяльність, адаптуючись до нових викликів. Компанія почала виготовляти захисні споруди для військового та цивільного захисту, фортифікаційні об'єкти тощо. Інженери компанії розробили залізобетонні плити зі спеціальними замковими з'єднаннями, які дозволяють швидко будувати конструкції різного ступеня складності. Усі технічні рішення, включно з дизайном плит, складом бетону і армуванням, були створені спеціалістами проєктного інституту ALD ENGINEERING COMPANY, що підкреслює високий рівень інженерної експертизи.

Усвідомлюючи важливість відновлення зруйнованих міст і сіл, компанія ALD ENGINEERING COMPANY вже сьогодні готується до масштабного відбудовчого процесу. Для цього було розроблено проєкт збірних житлових будинків із залізобетонних елементів. Основними перевагами цих будинків є легкість транспортування, швидкий монтаж завдяки замковим з'єднанням та можливість адаптації до різних потреб: від гуртожитків до таунхаусів.

Виробництво залізобетонних плит відбувається на власному виробництві компанії. Товщина плит може змінюватися від 200 мм, а для підвищення рівня захисту клієнт може замовити посилене армування без зміни товщини стін. Це дозволяє створювати надійні конструкції, здатні витримувати вибухові хвилі, уламки та стрілецьку зброю. Якість усіх конструкцій підтверджена міжнародними сертифікатами ISO 9001:2015 та ДСТУ ISO 9001:2015.

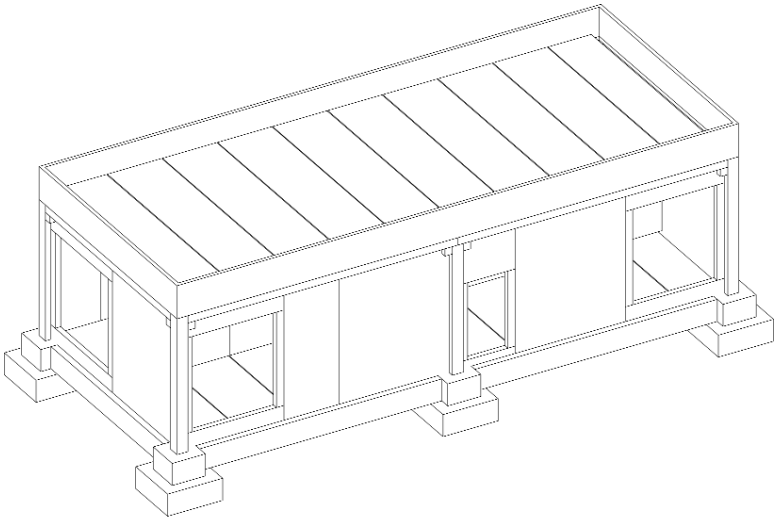
Для гарантії безпеки кожен виріб проходить подвійне тестування: на виробництві та

на полігоні у максимально наближених до бойових реальних умовах. Це забезпечує замовникам упевненість у тому, що будівлі ALD ENGINEERING COMPANY здатні витримати найскладніші загрози та забезпечити безпеку мешканців.

Збірні житлові будинки компанії є доступними за ціною, значно дешевшими за традиційне житло, і можуть бути збудовані всього за місяць. Універсальність конструкцій робить їх ідеальним рішенням для відновлення житлового фонду на звільнених територіях.

Компанія ALD ENGINEERING COMPANY переконана, що забезпечення житлом - важливий етап відновлення України. Збірні будинки здатні стати вагомим внеском у цей процес, допомагаючи тисячам людей повернутися до нормального життя у безпечних умовах.

Дотримуючись принципу «Люди важливіші за процеси», компанія завжди відкрита до співпраці з партнерами для спільної участі у відбудові країни.



Дізнатися більше про діяльність компанії можна на сайті: **https://aldholding.com/**

ALD
engineering company

ТОВ «АЛД ІНЖИНІРИНГ ТА БУДІВНИЦТВО»
Юридична, поштова адреса:
69008, Україна, Запорізька обл.,
м. Запоріжжя, Південне шосе 78А
ЄДРПОУ 43173964
+380 (67) 734-13-72
+49 (211) 176-095-11
info@aldholding.com

BunkerOK: Захищений простір для бізнесу та суспільства

У сучасних умовах війни та нестабільності безпека громадян стає ключовим фактором. Надійні захисні споруди – це вже не просто необхідність, а основа безперебійної роботи підприємств, торгових центрів, навчальних закладів та органів влади.

Українська компанія BunkerOK створює швидкоспоруджувані залізобетонні укриття модульного типу, які забезпечують високий рівень захисту, автономності та комфорту. Ці укриття сертифіковані відповідно до державних стандартів та успішно випробувані в реальних бойових умовах.

Що таке «захищений простір»?

Це не просто бункер або бетонна коробка – це повноцінне середовище, у якому люди можуть безпечно перебувати, працювати та навіть продовжувати свою діяльність у період загроз.

Захищений простір – це:

- Фізична безпека від вибухових хвиль, уламків та інших загроз.
- Автономність: електропостачання, вентиляція, запаси води та продуктів.
- Комфортні умови для тимчасового чи тривалого перебування.
- Гнучкість у використанні: укриття можна використовувати не лише у періоди загроз, але й як комерційні приміщення, склади, виробничі або адміністративні блоки.

BunkerOK пропонує три моделі укриттів, що враховують різні рівні загроз та сценарії використання: Honor, Volat та Sota.

Honor: модульні укриття нового рівня

Honor – це багатомодульні захисні споруди, які підходять як для бізнесу, виробничих підприємств, логістичних хабів, державних установ, так і для великих житлових комплексів.

Основні характеристики Honor:

- Високоміцні залізобетонні блоки з армуванням металевою фіброю.
- Товщина стін – витримує ударну хвилю 130+ кПа.
- Місткість від 15 до 100+ осіб (можливість розширення модульної системи).
- Автономна система життєзабезпечення (електрика, вентиляція, теплові завіси, аптечки).
- Можливість інтеграції у виробничі та торговельні приміщення.

Honor також може використовуватися як укриття подвійного призначення:

- У мирний час – склад, архів, холодильна камера або виробничий цех.
- У період небезпеки – захищений простір для працівників.

Volat – це готове до використання захисне укриття, яке не потребує складного монтажу. Його доставляють у готовому вигляді, і воно встановлюється протягом декількох годин.

Volat – це багатосекційна фортифікаційна споруда, яка може бути як окремо розташованою, так і інтегрованою у складні оборонні системи.

Чому Volat?

- Унікальна товщина стін – 300 мм, що витримує ударну хвилю до 849,94 кПа.

- Можливість об'єднання модулів у великі комплекси.
- Захист від уламків, високих температур, радіаційного випромінювання.
- Повна адаптація під потреби військових, промислових підприємств та стратегічних об'єктів.

Volat – це не просто укриття, а мультифункціональний комплекс, який може використовуватися як командний пункт, мобільний штаб, склад зброї або спеціального обладнання .

Sota: мобільні укриття для бізнесу та дому

Sota – це інноваційний підхід до захищеного простору в міських умовах. Ця серія укриттів підходить для квартир, офісів, складів, виробничих об'єктів, де немає можливості встановити великі конструкції.

Ключові переваги Sota:

- Компактні габарити, що дозволяють установку в будь-якому приміщенні.
- Модульна система – можна збирати укриття горизонтально або вертикально.
- Матеріали: метал + бетон, що забезпечує стійкість до уламків і вибухових хвиль.
- Місткість – від 3 до 15+ осіб.
- Зручність в установці – можна використовувати як переносний захисний модуль.

Оренда захищених укриттів Sota для бізнесу

BunkerOK пропонує унікальне рішення для підприємств – оренду захисних укриттів Sota. Це дозволяє компаніям швидко забезпечити безпечний простір для працівників без значних капітальних витрат.

Переваги оренди:

- Швидке встановлення – готові модулі розміщуються на підприємстві за кілька годин.

- Економія коштів – немає потреби у будівництві або реконструкції приміщень.
- Гнучкість – можливість орендувати укриття на будь-який термін та за потреби викупити його.

Це рішення підходить для офісних будівель, складів, торговельних центрів, автозаправних станцій та промислових об'єктів.

Чому обирають BunkerOK?

1. Реальні випробування – усі укриття протестовані в Державному науково-дослідному інституті будівельних конструкцій.
2. Модульність та масштабованість – укриття можуть бути розширені відповідно до потреб.
3. Офіційна сертифікація – відповідність ДСТУ 9195:2022.
4. Автономність – енергозабезпечення, вентиляція, запаси води та їжі.
5. Різні формати укриттів – від компактних Sota до масштабних Volat та Honor.

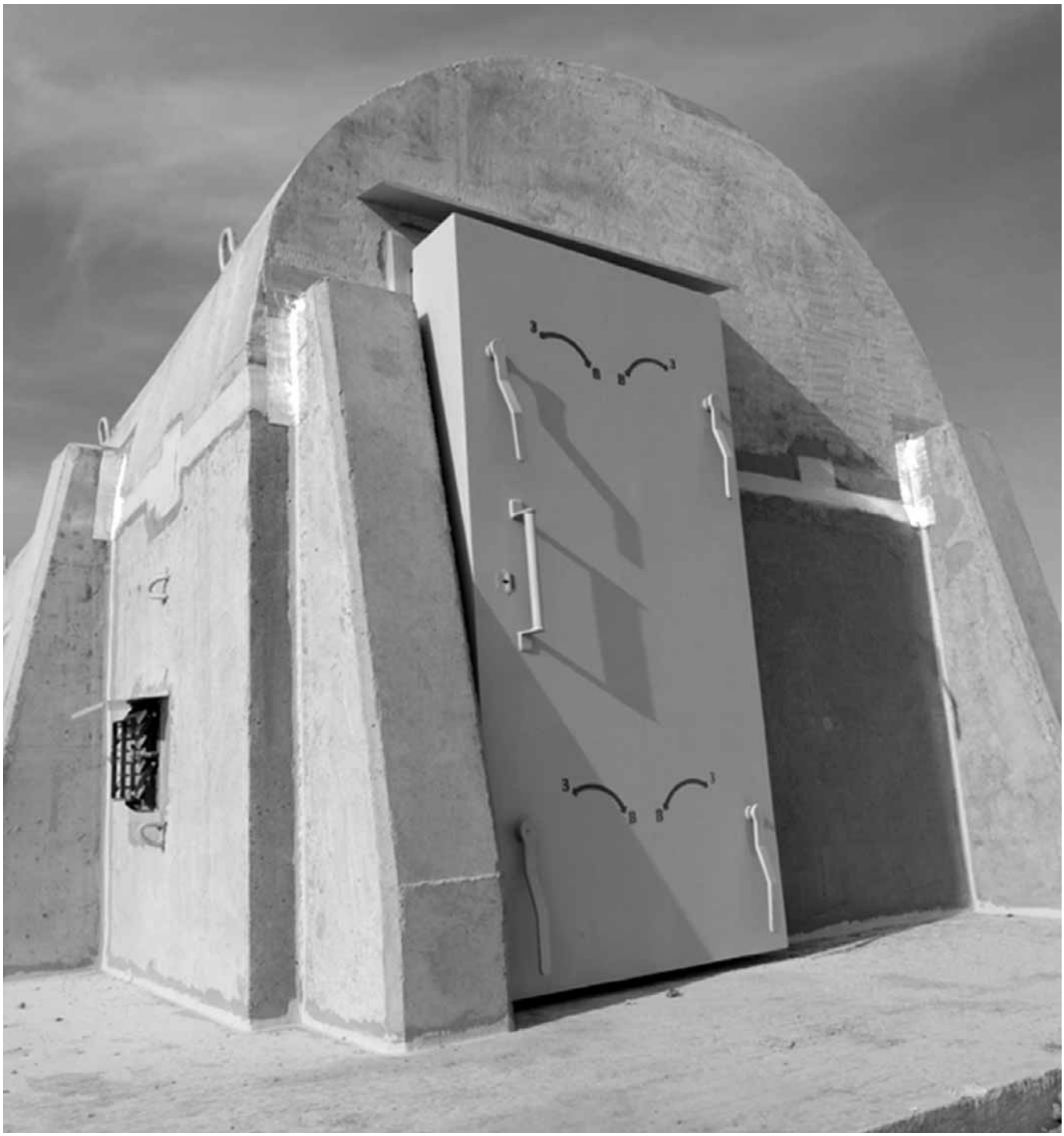
Висновок

Захисні споруди BunkerOK – це готові до використання укриття, що не лише захищають від вибухової хвилі та уламків, але й забезпечують комфортні умови всередині.

Завдяки продуманому облаштуванню – вентиляції, освітленню, ергономічним лавам – люди можуть перебувати в укритті максимально зручно навіть тривалий час. Безпека та комфорт разом – це стандарт BunkerOK.

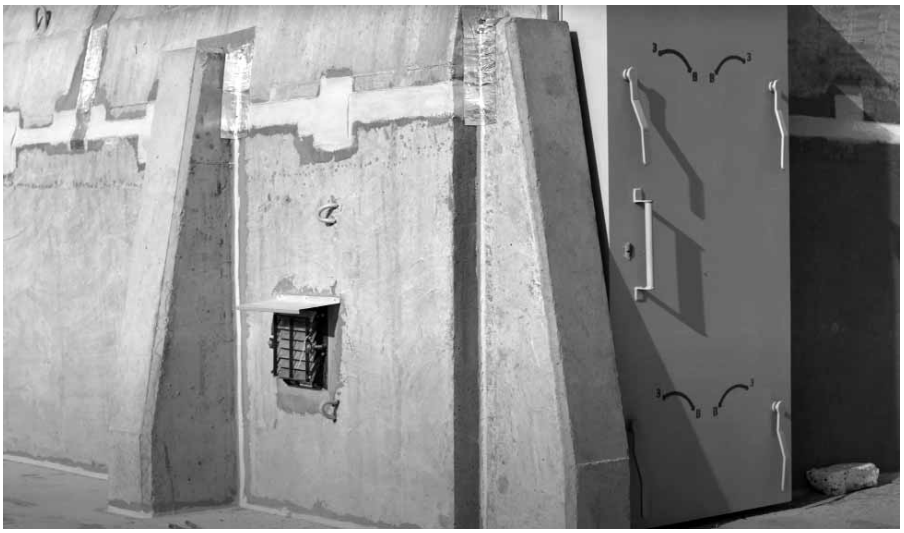
Контакти для консультації та замовлення:
bunker-ok.com.ua
+380 (93) 856 34 63

ПРУ (протирадіаційне укриття) – обов’язкове для встановлення на підприємствах критичної інфраструктури



Наземне ПРУ (протирадіаційне укриття) від компанії «Хоббіт хаус», що встановлене біля сонячної електростанції (СЕС)

До критичної інфраструктури належать: електростанції, в тому числі сонячні, котельні та склади, усі підприємства харчової промисловості, транспортні вузли, аеро та морські порти, вузли телекомунікаційних мереж, медичні установи усіх типів, а також фінансові установи та банки.



Потужні контрфорси товщиною 300 мм

Противибуховий клапан, який захищає від повітряної ударної хвилі

Арочний дах, який загальновизнано є найміцнішою конструкцією в будівництві

Згідно з Кодексом цивільного захисту, ПРУ – це негерметична захисна споруда, що гарантує безпечне перебування людей протягом не менше 48 годин. Головна перевага таких укриттів – їхній високий рівень захисту та можливість довготривалого використання.

Будівництво традиційного укриття займає до року, тоді як модульні конструкції від ТОВ «Хоббіт Хаус» дозволяють скоротити терміни будівництва у 10 разів. Вже через тиждень після початку робіт укриття може бути готове до експлуатації.

Переваги конструкцій модульних ПРУ «Хоббіт Хаус»:

- Відповідність ДБН В.2.2-5:2023 та ДСТУ;
- Захист від проникаючої радіації (Кз) 200-1000, і більше в разі заглиблення;
- Використання арочної форми як найміцнішої в будівництві;
- Швидкий монтаж без довготривалого будівництва стандартними методами.

Броньовані двері якими комплектуються споруди від ТОВ «Хоббіт хаус»

ТОВ «Хоббіт хаус» встановило понад 300 укриттів по всій Україні. Вони використовуються державними, комерційними та військовими структурами, доводячи свою ефективність у реальних умовах.

Hobbit House
https://hobbithouse.com.ua/
Телефон: +380 63 584 6394,
Пошта: k.reva@hobbithouse.com.ua

Чим небезпечний мазут для людини, водойм та ґрунту? Чи завжди є небезпечним вантажем?

Ступінь небезпеки мазуту для довкілля

Мазут - залишковий продукт переробки нафти. Це найважча фракція, що утворюється після википання всіх інших складових на зразок бензину, гасу, газойлю та ін. Як будь-який нафтопродукт мазут надає певний негативний вплив на людину та природу. Про це потрібно знати, щоб правильно перевозити та використовувати продукт, не допускаючи забруднення навколишнього середовища.

Клас небезпеки мазуту

Мазут є небезпечним вантажем, але за ступенем впливу на людину відноситься до малонебезпечних нафтопродуктів - 4-го класу небезпеки за класифікацією в п. 1.1. ГОСТ 12.1.007-76. Відповідно до цього гранично допустима концентрація шкідливих парів нафтопродукту в повітрі робочої зони починається з 10 мг/м^3. Це одна із норм для 4-го класу небезпеки. У суміші з повітрям вибухонебезпечною вважається концентрація парів мазуту від 14 до 8%. Тому при роботі з ним не допускається використовувати інструменти, які дають іскру під час удару.

Мазут утворює на поверхні води непроникну плівку, яка порушує всі види обміну

Чим небезпечний мазут та його пари для людей

Для людини високою токсичністю мають пари мазуту, які мають отруйну дію. У продуктах згоряння містяться вуглекислота, оксиди азоту, сполуки сірки, ванадію, оксид вуглецю та метан. Пари можуть потрапляти через органи дихання, іноді з їжею та водою всмоктуються у кров. Дратують слизові оболонки та очі. Пари діють як нервові отрути з наркотичною дією. Вони вражають центральну нервову систему:

- підвищують збудливість;
- викликають загальну слабкість;
- збільшують пульс;
- викликають запаморочення.

У легких випадках отруєння з'являються кашель, нежить, сльозотеча, біль у грудях та почуття сухості у горлі, у гострих – запаморочення, загальна слабкість, біль голови. При тривалому впливі спостерігається хронічне отруєння. Воно може виявлятися у вигляді бронхіту з нападами ядухи, атрофічним ринітом, ураженням зубів.

Якщо перераховувати, чим ще небезпечний мазут для людей, то треба сказати, що він несе шкоду і при попаданні на шкіру. Нафтопродукт знежирює та сушить її поверхню, що може призводити до екзем і дерматитів.

Чи небезпечний мазут для ґрунту та води

Особливу небезпеку мазут несе для водойм. При попаданні на поверхню води він утворює плівку, яка порушує волого-, енерго- та теплообмін з атмосферою.

Якщо розглядати, чим небезпечний мазут, для ґрунту, то треба сказати, що він пригнічує вплив на екологічні системи, губить живі організми і значно змінює умови їхнього проживання. Просочування нафтопродуктом ґрунтової маси веде до зміни її хімічного складу, властивостей та структури. В результаті погіршується властивість ґрунту як живильного середовища для рослин. До їхнього коріння не надходить достатня кількість вологи, через що порушуються всі фізіологічні процеси.

Ефект мазуту як тяжкої фракції проявляється пізніше, ніж від легких дистилятів. Згодом утворюється стійке вогнище забруднення, через що очищення природного середовища протікає важко. Особливо токсичні ароматичні вуглеводні, асфальтени, смоли та важкі метали, які цементують ґрунтовий простір та значно погіршують водно-фізичні властивості ґрунту.

Основні показники для вантажів різних класів небезпеки

Найменування показника	Норми для класу небезпеки			
	1-го	2-го	3-го	4-го
Гранично допустима концентрація (ПДК) шкідливих речовин в повітрі робочої зони, мг/ м^3	Менше 0,1	0,1-1,0	1,1-10,0	Більше 10,0
Середня смертельна доза при попаданні в шлунок, мг/кг	Менше 15	15-150	151-5000	Більше 5000
Средня смертельна доза при нанесенні на шкіру, мг/кг	Менше 100	100-500	501-2500	Більше 2500
Средня смертельная концентрація у повітрі, мг/м^3	Менше 500	500-5000	5001-50000	Більше 50000
Коефіцієнт можливості інгаляційного отруєння (КМІО)	Більше 300	300-30	29-3	Менше 3
Зона гострої дії	Менше 6,0	6,0-18,0	18,1-54,0	Більше 54,0
Зона хронічної дії	Більше 10,0	10,0-5,0	4,9-2,5	Менше 2,5

Чи вважається мазут небезпечним вантажем

Одним із спірних на сьогодні є питання, чи вважається мазут небезпечним вантажем чи ні. Відповідно до п. 2.2.9.1.10.6 ДОПІГ (Європейською угодою про міжнародне дорожнє перевезення небезпечних вантажів), нафтопродукт відноситься до № ООН 3082, що відповідає рідким речовинам, небезпечним для навколишнього середовища.

У п. 2.2.9 ДОПІГ йдеться про інші небезпечні речовини та вироби, які не охоплені назвами інших класів. Саме сюди включають мазут, оскільки в ін-

ших розділах документа не зустрічається. Деякі перевізники користуються тим, що цей нафтопродукт не вказаний в алфавітному переліку ДОПІГ та намагаються транспортувати його як безпечний вантаж. Але це може призвести до наслідків, оскільки підкований інспектор ДПС з посиланням на 2.2.9 ДОПІГ легко зафіксує порушення, за яким можуть наслідувати штраф і відповідальність.

За властивостями мазут справді займає почесне місце у низці нафтопродуктів та речовин із уже присвоєним класом небезпеки. Небезпечним вантажем його вважали до 25 квітня 2012 року, коли подібні вантажі транспортували відповідно до наказу Мінтрансу Росії від 08.08.1995 № 73. Згідно з цим документом, товари класифікують на небезпечні та безпечні відповідно до критеріїв ГОСТ 19433-88. По ньому мазут і бітум - безпечні, оскільки мають температуру спалаху більше 90 °С.

Але, починаючи з 25 квітня 2012 року, небезпечні вантажі стали перевозити відповідно до ДОПГ (правова підстава – постанова Уряду Російської Федерації від 15.04.2011 № 272). °С. Якщо мазут завантажується за таких умов, його відносять до небезпечних. вантажів.

Якщо ж договірних відносин на перевезення відсутні і нафтопродукт транспортується юридичною особою або ІП для власних потреб та на транспортних засобах, що належать йому на законних підставах, тоді правила ДОПІГ не застосовуються.

Висновок

Мазут – однозначно небезпечна речовина, що негативно впливає на навколишнє середовище та людину. Але при перевезенні він не завжди потрапляє до категорії небезпечних вантажів. Все залежить від умов транспортування: яка організація, на якій підставі та на чому перевозить нафтопродукт. Основні вимоги щодо перевезення мазуту наводяться у ДОПІГ. Вони пред'являються до ємностей та транспорту, а також до водія, який повинен мати свідоцтво на здійснення діяльності. Ці та інші вимоги ДОПІГ важливі для забезпечення надійності доставки та збереження вантажу.

/trader-oil/

Забутий елемент: екран протипилового фільтра в сховищах і ПРУ з електроручними вентиляторами

Актуальним питанням залишається улаштування стінки (екрану), який виключає можливість прямого опромінювання обслуговуючого персоналу, який працює на ручному приводі електроручних вентиляторів.

В проектах систем вентиляції сховищ і ПРУ інколи не передбачається влаштування захисту людей від можливого опромінювання від накопиченого у протипилових фільтрах радіоактивного пилу, пропри пряму норму, яка міститься в пунктах 7.2.1.16 та 7.2.2.6 ДБН В.2.2-5:2023 «Захисні споруди цивільного захисту».

Якщо протипиловий фільтр знаходиться в окремому приміщенні (розширювальній камері, форкамері), тоді стіна між відповідними приміщеннями повинна мати визначену нормами товщину.

Як видно з таблиці, матеріалом може бути як залізобетон (бетон), так і цегла.

Ми дослідили найбільш поширені умови, в яких будуються сховища і укриття, і склали схему, на якій зазначили можливий вигляд захисного екрану в фільтровентиляційному приміщенні.

Схематичне зображення не є рекомендацією, тому слід керуватися вимогами чинних норм, обстановкою на об'єкті та іншими чинниками, які впливають на вибір рішення.

Слід обов'язково перевірити аналогічні зони можливого опромінювання і в вертикальній площині, щоб виключити незахищені зони.

Таким чином, ми наочно побачили, що захисний екран протипилових фільтрів це не частина фільтру або електроручного вентилятора. Натомість, це може бути додатковим обладнанням, або частиною будівельних конструкцій захисної споруди.

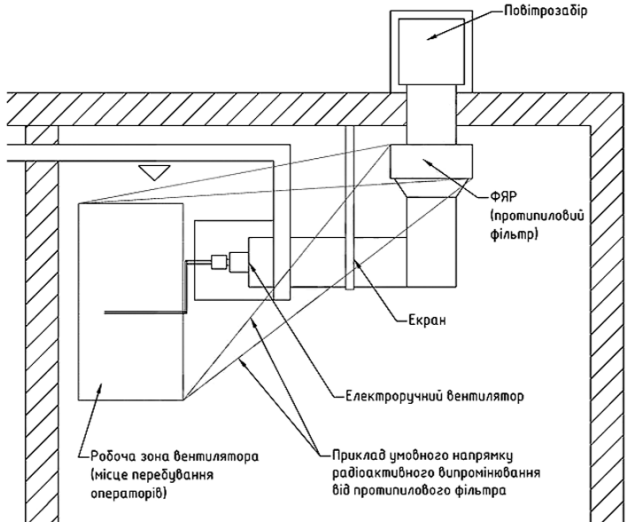
Для кріплення залізобетонної плити можна застосовувати кронштейни, підвіси, підставки тощо.

У випадку виконання екрану з цегли, його зведення не відрізняється від зведення стін, перегородок.

Найбільш доступним рішенням ми вважаємо застосування тротуарних плит потрібного розміру. Ці вироби доступні в будь-якому регіоні для застосування при будівництві, і коштують недорого.

Довідка: плита розміром 1000х1000х100 мм (1м²) буде мати вагу 240 кг.

ТОВ «ВЕБКОМ»
Сучасний Колективний Захист,
08631, Київська обл.,
Фастівський р-н, смт. Глеваха,
вул. Підприємницька, б. 8.
т. +380679353824
(технічні консультації),
+380953459920
(комерційні питання),
+380442236269
(загальні питання),
post@skz.net.ua, www.skz.net.ua



На цій ілюстрації показана можлива схема розташування захисного екрану. У фільтрі ФЯР може накопичуватися радіоактивний пил, а у робочій зоні електроручного вентилятора можуть перебувати люди. Для їх захисту слід передбачити екран, товщина якого обирається відповідно до матеріалу, з якого він зроблений, та повітроподачі, яка відбувається крізь фільтр.

Товщина стінки (екрану) для захисту персоналу

Товщина стін (екранів), мм:	Розрахункова повітроподача, м³/год					
	до 300	300-600	600-1000	1 000-5 000	5 000-10 000	більше 10 000
залізобетонних (бетонних)	50	80	100	170	200	250
армоцегляних	120	120	120	250	250	400

Найпопулярніші камери відеоспостереження 2024 року

У сучасному світі безпека будинку та офісу стає пріоритетом для багатьох. Розвиток технологій дозволяє нам забезпечувати захист за допомогою камер відеоспостереження, які можуть не лише записувати те, що відбувається, але й миттєво повідомляти власника про підозрілу активність. Відеоспостереження стало невід'ємною частиною повсякденного життя, особливо з появою розумних IP-камер, які забезпечують високу якість зйомки, надійність та додатковий функціонал, наприклад розпізнавання людини. Вибір відповідної камери для будинку чи вулиці може стати непростим завданням, враховуючи різноманітність функцій, технологій та цінових категорій на ринку.

Чому важливо вибрати правильну камеру відеоспостереження?

Камери відеоспостереження – це ваш перший засіб захисту та контролю над тим, що відбувається на території вашого будинку чи бізнесу. Незалежно від того, чи бажаєте ви стежити за своєю власністю під час відпустки або забезпечити безпеку сім'ї, якісна IP-камера забезпечить постійний моніторинг, навіть коли ви знаходитесь далеко.

На основі аналізу попиту моделей відеокамер на ринку систем відеоспостереження України в 2024 році був створений їх перелік, що ми вам і пропонуємо. При цьому враховувалось таке:

1. Висока якість зображення. У 2024 році особлива увага покупцями приділялася роздільній здатності відеокамер. Навіть бюджетні моделі тепер пропонують зйомку у Full HD, що гарантує чітку картинку як вдень, так і вночі. Пристрої з нашого рейтингу в основному забезпечують не лише високу роздільну здатність, а й деталізоване зображення, що дозволяє розглянути дрібні деталі.

2. Інтелектуальні функції. Більшість камер з ТОП-рейтингу оснащені функціями штучного інтелекту: розпізнавання облич, виявлення руху, сповіщення у реальному часі на смартфон та автоматичний запис. Все це робить системи відеоспостереження розумними та ефективнішими у питаннях безпеки.

3. Надійність та захист. IP-камери повинні бути надійними та стійкими до зовнішніх факторів, особливо якщо йдеться про зовнішнє відеоспостереження. Водонепроникність, захист від пилу та вандалізму, морозостійкість (незважаючи, що в нас мороз стає дедалі рідкісне явище) – це обов'язкові критерії для камер, які будуть використовуватися на вулиці.

4. Легкість установки та використання. Сучасні камери не потребують складного налаштування. Більшість моделей підтримують дистанційне керування через мобільні програми, що дозволяє легко підключити їх до вашої мережі Wi-Fi і відразу почати користуватися. Ця зручність заощаджує час та зусилля, особливо якщо ви вперше стикаєтеся з подібними пристроями.

5. Зберігання даних та безпека. Камери з нашого рейтингу пропонують різні варіанти зберігання відео: локальне (карти пам'яті) та хмарне зберігання. Останній варіант особливо корисний для довгострокового збереження даних та доступу до них у будь-який час. Безпека даних також важлива: більшість пристроїв підтримують зашифроване підключення, що захищає записи від стороннього доступу.

Переваги IP-камер у порівнянні з аналоговими системами

Сучасні IP-камери набагато перевершують аналогові системи за якістю зображення, функціональністю та легкістю використання. Якщо раніше відеоспостереження асоціювалося з дорогими та складними у налаштуванні системами, то зараз IP-камери забезпечують високий рівень захисту за доступні гроші. Вони пропонують такі функції, як:

– Підключення до Інтернету, що дозволяє стежити за ситуацією в режимі реального часу з будь-якого пристрою.

– Двосторонній зв'язок, що дає можливість не тільки бачити, а й чути те, що відбувається, або спілкуватися через камеру.

– Нічна зйомка з інфрачервоним підсвічуванням, що дозволяє зберігати чіткість зображення навіть у темряві.

До нашого рейтингу потрапили моделі, які продемонстрували максимальну ефективність, надійність та зручність використання у повсякденному житті і оптимальне співвідношення ціни та якості Ви отримуєте сучасні технології за розумні гроші, що робить покупку особливо вигідною.

Як вже зазначалось камери з рейтингу в основному не потребують складних технічних знань для налаштування та експлуатації.

Незалежно від того, чи ви шукаєте камеру для особистої безпеки або для бізнесу, пристрої з нашого рейтингу стануть чудовим вибором для довгострокового захисту вашого майна та близьких.

Таким чином, вибір якісної IP-камери – це внесок у безпеку та спокій. Інвестуйте у надійні рішення та забезпечте повний контроль над своєю територією за допомогою найкращих моделей 2024 року.

1. Ezviz H3C

Камера Ezviz CS-H3C регулюється по своїй осі, піднімається та опускається в межах, допустимих конструкцією, від чого спрощуються встановлення та підключення на місці використання. Особливість обладнання полягає у залученні можливостей штучного інтелекту.

Таке технологічне рішення дозволяє девайсу розрізняти людей і тварин у динаміці серед багатьох інших факторів навколишнього середовища (наприклад, опадання листя з дерева, польотів комах тощо). Завдяки вбудованому алгоритму штучного інтелекту, власнику не доведеться відволікатися на хибні сигнали системи сповіщення про тривогу.

У Ezviz CS-H3C якість відеозапису на досить високому рівні. Камера записує відео ряд у форматі Full HD, камера оснащена 2-мегапіксельним об'єктивом. Також записується і звук, причому мікрофоном, оснащеним опцією придушення шуму, що покращує акустичне відтворення. Вночі техніка здатна чітко знімати те, що відбувається на відстані до 30 метрів завдяки ІЧ-підсвічуванню.

За класом захисту від зовнішнього впливу пристрій відповідає IP67, що вказує на можливість застосування елемента системи безпеки при найскладніших кліматичних умовах – снігопадах, морозах, дощі, штормах і сонці. Атмосферні прояви не впливають на здатність камери добре бачити та передавати якісне зображення.

Передача відеоряду через мережу Wi-Fi. Керування функціями та перегляд відео здійснюється через фірмовий додаток EZVIZ. Система зберігання передбачає використання MicroSD-карток ємністю до 512 ГБ, а також доступна опція хмарного зберігання EZVIZ CloudPlay на платній основі.

Особливістю камери є інтелектуальна система виявлення людей, що суттєво зменшує кількість хибних тривог. У темну пору доби працюють вбудовані інфрачервоні прожектори з радіусом дії до 30 метрів, які забезпечують чорно-біле нічне зображення.

Особливість використаного програмного забезпечення Ezviz, що встановлення цифрового обладнання спрощено, не потребує спеціальних навичок для підключення та налаштування. Для управління технікою розроблено мобільний додаток, який вже зв'язаний з хмарним сервісом EZVIZ CloudPlay Storage, де зберігаються всі записи, і до них власник має повний та швидкий доступ із будь-якого куточка світу за наявності інтернет-з'єднання.

Переваги бюджетної IP-камери Ezviz CS-H3C полягають у:

– низькому енергоспоживання – це досягається шляхом оснащення об'єктива мікросхемою типу CMOS;

– інтелектуальних програмах – для зручності управління виробник зробив прилад сумісним із IFTTT, Alexa та Google Assistant;

– аудіопідсилювачі – він підсилює слабкі звуки, що надходять від різних джерел;

– підтримці MicroSD – об'єм карти становить до 512 ГБ, чого цілком достатньо для великої кількості знятих матеріалів;

Основні характеристики:

Матриця 1/2,7" CMOS із прогресивною розгорткою;

Мінімальне освітлення 0,01 Люкс @ (F2.0, AGC ON), 0 Люкс з ІЧ;

ІК нічне бачення до відстані до 30 м;

Вбудований мікрофон;

Самоадаптивний затвор;

Об'єктив 2,8 мм @ F2.0, кут огляду: 82° (по горизонталі), 98° (по діагоналі);

Функція 3D DNR;

Цифровий WDR;

ІЧ- фільтр перемикання день/ ніч з автоматичним перемиканням;

Максимальна роздільна здатність 1920 ? 1080 (1080p);

Максимальна частота кадрів: 30 fps;

Самоадаптація під час передачі через мережу;

Стиснення відео H.265/H.264;

Максимальний бітрейт 2 Мбіт /с;

Мережа Wi-Fi IEEE802.11b, 802.11g, 802.11n

Діапазон частот 2,4 ГГц ~ 2,4835 ГГц

Плюси: розпізнавання людей, що підтримує MicroSD до 512 ГБ.

Мінуси: висока ціна, роздільна здатність менша, ніж у конкурентів, порівняно вузький кут огляду, діапазон Wi-Fi лише 2,4 ГГц, відсутність двостороннього аудіозв'язку.

Коментар користувача

Дуже доступна ціна для камери від даного виробника.

Недоліки особливо не виявлені.

Купили кілька таких однакових камер для встановлення у заміському будинку на вулиці. Морози до мінус 20 градусів витримали, особливих нарікань немає. Виявлення людини спрацьовує, а ось автомобіля – ні, не закладено такої функції.

2. EZVIZ C8C

Основні особливості відеокамери

Камера оснащена 4-мегапіксельним об'єктивом, який забезпечує чудове зображення. Висока роздільна здатність дозволяє легко розпізнавати об'єкти та особи на записах, що є важливим фактором для систем безпеки.

Камера поворотна: має кут огляду 360 градусів по горизонталі і 114 градусів по вертикалі. Завдяки цьому широкому куту огляду камера може охопити велику площу без необхідності встановлення кількох камер. Це робить її ідеальним вибором для використання у приміщеннях або на відкритих просторах.

ІЧ-підсвічування та нічне бачення: Камера оснащена ІЧ-підсвічуванням, що дозволяє отримувати якісне зображення навіть в умовах низького освітлення. Завдяки цьому функція нічного бачення дозволяє бачити об'єкти на відстані до 30 метрів у повній темряві. Це забезпечує постійне спостереження навіть у нічний час.

Двосторонній звук: EZVIZ C8C має вбудований мікрофон та динамік, що дозволяє вести двосторонній аудіозв'язок за допомогою програми на смартфоні. Це дуже корисно, коли ви хочете спілкуватися з відвідувачами або попередити про їх неправильні дії в режимі реального часу.

Інтелектуальні функції: Камера підтримує різні інтелектуальні функції, такі як виявлення руху та звуку. При виявленні підозрілої активності камера надсилає повідомлення на ваш мобільний телефон, щоб ви могли моментально відреагувати на подію.

Запис на картку пам'яті та хмарне сховище: EZVIZ C8C підтримує запис на картку пам'яті (MicroSD) з максимальною ємністю до 256 ГБ. Вона також підтримує хмарне сховище EZVIZ Cloud, яке забезпечує додатковий захист ваших записів.

Просте встановлення та використання: Встановлення камери EZVIZ C8C не потребує спеціальних навичок або складних процедур. Вона підключається до вашої мережі Wi-Fi і може бути керована через мобільний додаток EZVIZ, доступний для iOS та Android. Мобільний додаток надає простий інтерфейс для перегляду записів, налаштування параметрів та отримання повідомлень.

Де може використовуватися камера?

Камера EZVIZ C8C може бути використана на різних об'єктах та в різних сценаріях, де потрібне надійне відеоспостереження. Нижче наведено кілька прикладів місць, де ця камера може бути застосована:

Домашня безпека: EZVIZ C8C може використовуватися для забезпечення безпеки вашого будинку чи квартири. Вона може бути встановлена на вхідних дверях, у дворі, задньому дворі або в будь-яких інших місцях, де потрібен контроль за периметром. Камера попередить вас про підозрілу активність і допоможе вам стежити за вашою власністю, навіть коли ви знаходитесь далеко від дому.

Бізнес та комерційні приміщення: Камера EZVIZ C8C може бути використана в офісах, магазинах, ресторанах та інших комерційних об'єктах. Вона може допомогти у контролі доступу, спостереженні за касовими апаратами, відстеженні руху співробітників та клієнтів, а також запобіганні крадіжкам та вандалізму.

Громадські місця: EZVIZ C8C може бути встановлена у громадських місцях, таких як парки, сквери, площі або зупинки громадського транспорту. Це допоможе забезпечити безпеку відвідувачів та відстежувати будь-яку підозрілу діяльність.

Автомобільні стоянки: Камера може бути використана для спостереження за автостоянками, де вона допоможе в ідентифікації автомобілів та реєстрації номерних знаків. Це може бути корисно для забезпечення безпеки автомобілів та запобігання крадіжкам.

Промислові об'єкти: EZVIZ C8C також може бути застосована на промислових об'єктах, складах, будівельних майданчиках та інших місцях, де потрібне спостереження за безпекою та контроль доступу.

Важливо, що перед встановленням камери на будь-якому об'єкті необхідно дотримуватися законів і правил, що регулюють відеоспостереження та захист конфіденційності.

Висновок

Камера EZVIZ C8C пропонує набір передових функцій для забезпечення

надійного відеоспостереження. З високою роздільно здатністю відеоряду, широким кутом огляду, нічним баченням та інтелектуальними можливостями вона є відмінним вибором для домашньої та комерційної безпеки.

Основні характеристики:

Вбудований мікрофон;

Матриця: 1/2.7 дюйма, Progressive Scan CMOS;

Роздільна здатність 1920?1080 пікселів, 30 fps;

Кут огляду: 87° по горизонталі, 105° по діагоналі;

Фокусна відстань: 4 мм (F1.6);

Стандарт стиснення відео: H.265 / H.264;

Чутливість: 0,2 лк @ (F1.6, AGC вкл.), 0 лк з ІЧ- підсвічуванням;

Підтримка карт пам'яті: MicroSD до 256ГБ;

Підключення до мережі : IEEE802.11 b/g/n, 2.4ГГц ~ 2.4835 ГГц

Плюси

Якісна сборка та максимальний кут огляду;

Інтуїтивно зрозумілі налаштування;

Зручно користуватися програмою.

Мінуси

Чутливий мікрофон і датчик руху, який реагує, наприклад, на комах;

Немає можливості встановити «вибрані» ракурси для швидкого повороту камери в потрібне місце;

На картинці важко розглянути дрібні деталі.

Коментар користувача

Wi-Fi поворотна камера з гарною якістю за розумною ціною. Проста в установці та підключенні. Може записувати відео на карту пам'яті. Існує функція автоматичного стеження за людиною в кадрі.

У програмі немає можливості задати «вибрані» ракурси для швидкого повороту камери в потрібне місце. Режим знімку 360 градусів має замінити цей функціонал, працює некоректно.

У камері є функція інтелектуального визначення людини. Зручно, що можна записувати саме появу людей у кадрі та отримувати повідомлення у додатку. Але в цій моделі багато хибних спрацьовувань (на сніг, наприклад). Порівнюю з іншою камерою – Ezviz C3X. У ній поява людей та машин визначається краще. Але там об'єктив подвійний, може, через це.

3. Xiaomi Outdoor Camera AW300

Xiaomi Outdoor Camera AW300 використовує 3-мегапіксельний CMOS-сенсор з підтримкою розширеного динамічного діапазону, що дозволяє демонструвати відмінну картинку в роздільній здатності 2K у будь-який час дня та ночі. У Xiaomi Outdoor Camera AW300 2 потужних білих джерела світла та 2 інфрачервоних, інтелектуальне повнокольорове нічне бачення. Коли хтось проходить повз, автоматично вмикається біле світло, тому навіть у темряві отримуємо кольорове зображення.

Xiaomi Outdoor Camera AW300 підтримує функцію інтелектуального електронного огородження. Коли вона розпізнає, що зображення змінюється або людська постать з'являється в заданій області, вона повідомить власника через мобільний телефон. Зовнішня камера Xiaomi AW300 може подавати звукові та світлові попередження, щоб відігнати непроханих гостей.

У Xiaomi Outdoor Camera AW300 вбудовані динаміки та мікрофони. Мікрофони записують якісний звук на відстані менше 7 м. Камера отримала захист IP66, вона може працювати під дощем і сонцем при температурі до 60 °C.

У Xiaomi Outdoor Camera AW300 є зовнішня антена Wi-Fi та вбудований чіп безпеки. Камера використовує технологію кодування відео H.265 та підтримує локальне та хмарне сховище.

Поставляється з кріпленням на стіну, кут повороту можливий вручну до 350° по горизонталі і 110° по вертикалі.

Існує можливість налаштування чутливості виявлення для окремих зон.

Як і більшість камер Xiaomi жорстка прив'язка до регіону, CN версії будуть працювати тільки на регіоні Китай. Глобальна ж версія працюватиме на будь-яких регіонах.

Основні характеристики

Кут огляду (FOV) 101,7°;

Роздільна здатність відео 2304 ? 1296;

Частота кадрів 30 fps;

Об'єктив F2.0;

Відеокодек H.265;

Прожектор нічного бачення: два ІЧ світлодіоди з довжиною хвилі 850 нм, два білих свілодіоди;

Робоча температура камери від -30° С до +60° С;

Бездротове з'єднання Wi-Fi IEEE 802.11b/g/n 2,4 ГГц;

Підтримка карток пам'яті до 256 ГБ;

Хмарне сховище відеоконтенту;

Плюси:

детектор руху, що настроюється;

високочутливий сенсор: камера вночі чудово працює у кольорі за наявності навіть слабкого освітлення;

потужне біле та ІЧ-підсвічування;

наявність безперебійного та «непідсанкційного» хмарного сервісу з переглядом трансляції через мобільний додаток;

гарна роздільна здатність;

кодування в H.265;

широкий робочий температурний діапазон;

доступна ціна.

Мінуси:

несумісність із обладнанням, яке підтримує стандарти ONVIF;

необхідність уточнення щодо можливості використання функцій камери в Україні.

Коментар користувача

Чудова камера за свої гроші! Дуже проста в установці та налаштуванні в додатку mi home. Мікрофон добре записує звук. Сигналізація спрацьовує при виявленні саме людини (можна відключити), так само фіксує рух загалом і зберігає окрему вкладку (у додатку). Існує додаткове світлове сповіщення при виявленні руху людини. Кут огляду досить великий.

Найголовніше забезпечити стабільний WiFi. Провід живлення дуже довгий, 2,5 метри, але з китайською розеткою.

У комплекті є qr код на папірці, щоб для повторного чи нового з'єднання не звертатися до камери. Скидання можна зробити через додаток. Флешка ємністю 64 ГБ дозволяє запис до 13 днів, а потім відбувається перезапис. Довжина файлів – по хвилині. Працює близько півроку.

4. TP-Link Tapo C310

Зовні камера виглядає досить помітно і в сірому під'їзді навряд чи зможе залишитися непоміченою. Особливо привертають увагу дві незнімні антени на корпусі, завдяки яким C310 нагадує персонажа із фантастичного мультфільму.

Корпус камери захищений від води, бруду та пилу, не боїться він і мінусових температур, завдяки чому C310 можна розміщувати навіть на вулиці або в приміщенні, що не опалюється.

На лицьовій стороні C310 розміщено два інфрачервоні світлодіоди, які дозволяють вести зйомку навіть у темний час доби або коли в приміщенні немає штучного освітлення.

Камера оснащена мікрофоном та динаміками для двостороннього зв'язку. Це дуже зручно при спілкуванні зі службами доставки, кур'єрами та просто непроханими гостями.

Є на корпусі слот для microSD-карти пам'яті, якщо не хочеться скористатися хмарним сховищем. Він розташований у важкодоступному місці та прикритий пластиною на болтах, щоб забезпечити додатковий захист.

Все керування та налаштування Tapo C310 відбувається за допомогою фірмової програми. Налаштування займає 3-5 хвилин і не потребує спеціальних навичок за рахунок покрокового майстра. Потрібно лише виб-

рати C310 зі списку обладнання. Те, що програма підтримує велику кількість різних пристроїв, можна вважати плюсом, так як вона напевно буде оновлюватися.

За допомогою додатку можна переглядати трансляцію в реальному часі, переглядати архів, слухати, що відбувається в приміщенні та спілкуватися з гостями. Якщо використовується кілька камер C310, зображення з усіх них можна виводити класичною сіткою і дивитися всі потоки одночасно.

Для використання камери в якості сигналізації передбачено режим виявлення руху. При виявленні непроханих гостей в додаток надходить PUSH-повідомлення. Якщо в зоні камери рух досить активний, повідомлення можуть стати дуже нав'язливими, тому тут кожен вибирає для себе.

Що стосується підключення до мережі, досить навіть найпростішого USB-пристрою діапазону 2,4 ГГц, із SIM-картою оператора.

Функціональні особливості

Система повідомлень про рух. Отримуйте повідомлення на смартфон під час виявлення руху, що посилює безпека вашого будинку.

3-мегапіксельна матриця та висока роздільна здатність забезпечують чудове зображення, дозволяючи розглядати навіть дрібні деталі.

Варіативні способи підключення: через Ethernet кабель або Wi Fi.

Стійкий всепогодний корпус IP66. Надійна робота в будь-яких погодних умовах завдяки захищеному корпусу.

Спілкування через двосторонній аудіозв'язок. Спілкуйтеся з кур'єрами та відвідувачами, перебуваючи в будь-якому місці, завдяки двосторонньому аудіозв'язку.

Надійне локальне сховище. Прямий запис 3 МП відео на карту MicroSD.

Високоякісне нічне бачення. Ефективне нічне бачення забезпечує чіткість огляду на відстані до 30 метрів навіть у темряві.

Автоматична сигналізація при виявленні руху. Інтегрована система попереджень із використанням світла та звуку для відлякування непроханих гостей.

Додаток Tapo для зручного управління. Легке налаштування та управління, перегляд у реальному часу, відтворення та збереження відео, все в одному додатку Tapo.

Основні характеристики

Матриця: 1/2,7 дюйма;
Роздільна здатність відео: 2304 x 1296;
Діафрагмове число об'єктива: 2,2;
Фокусна відстань: 3,89 мм;
Нічне бачення: ІЧ світлодіоди 850 нм (до 30 м);
Події: виявлення руху;
Повідомлення: Push-сповіщення;
Стиснення відео: H.264;
Частота кадрів: 15 кадрів за секунду;
Проводове або бездротове підключення: по кабелю Ethernet або Wi -Fi.

Отже камера TP-LINK Tapo C310 – це дуже простий у використанні пристрій, що забезпечує високу якість трансляції. Її можна використовувати як вдома, так і в офісі. Захист корпусу дозволяє розміщувати її навіть на вулиці, що суттєво розширює можливості з використання. Ще один суттєвий плюс – доступна ціна.

Коментар користувача

Близько року працюють дві такі камери у приватному будинку. Одна висить на вікні другого поверху для огляду машиномісця / хвіртки, друга на сараї біля будинку – для огляду території. Загалом гідне поповнення сімейства Tapo, але у вуличному виконанні. У мене всередині будинку вже працюють два побратими – Tapo C100 і C200, так що спеціально чекав виходу цією моделі, щоб можна було використовувати в одному фірмовому додатку.

Якість картинки цілком стерпна, але не чекайте чудес від камери. Щоб розглянути обличчя особи та номери авто я думаю край метрів 10, далі вже все пливе. Я її спочатку брав як суто спостережну та захист від дурня. На серйозну охоронну камеру такі іграшки не годяться – тут потрібна хороша система відеоспостереження. А подивитися за собакою/котом та іншою живністю, а так само що взагалі в окрузі відбувається саме те. Ну і думаю відлякає більшість різного виду бомжів та дрібних злодіїв.

Налаштування простіше нікуди, буквально кілька «тапів» по екрану, навіть дитина впорається. Підключити можна як по Wi-Fi так і по кабелю.

До камер відразу були куплені карти пам'яті на 128 Гб – вистачає на 8 днів циклічного запису з роздільною здатністю відео 2304 x 1296. Можна писати за розкладом, на рухи, вибирати область руху тощо.

По експлуатації у мене за дві тижня ніяких особливих проблем не виникло. Один раз тільки зглючила чи то карта пам'яті, чи сама камера – замість затирання старого запису камера почала писати що немає місця на карті (хоча стояв циклічний запис) форматнула її і почала писати наново. Можливо проблема була у картці пам'яті, оскільки купив самі дешеві.

Режим роботи заявлено від -20 градусів, але за фактом камери працювали і при -25.

Для тих, кому треба є підтримка RTSP/ONVIF – можна зняти потік кудись у сторонній додаток на сервер, хмару тощо. Мені вистачає стандартного.

Функціонал досить стандартний та збігається в принципі з іншими камерами TAPO.

Загалом вважаю дуже хороша камера вийшла, все стабільно працює і жодних «танців з бубном».

5. IP-камера TP-Link Tapo C320WS

Wi-Fi камера TP-LINK Tapo C320WS – удосконалений варіант камери моделі C310. На відміну від неї вона має чотири мегапіксельну матрицю. Об'єм локального сховища у вигляді microSD-карти подвоєний зі ста двадцяти восьми гігабайт до двох сотень п'ятдесяти шести. Відмінності торкнулися і об'єктиву – різниця у меншому фокусі. В іншому ж камери ідентичні.

TP-LINK Tapo C320WS відрізняється якісною матрицею 4 МП, що забезпечує чітке зображення з роздільною здатністю 2560x1440 з широким кутом огляду 97°. Бездротове підключення реалізовано через Wi-Fi-модуль із підтримкою частоти 2,4 ГГц, а вбудовані динамік та мікрофон забезпечують чистий двосторонній звук.

Всі функції камери доступні через зручну програму Tapo, яка відрізняється простотою налаштування та багатим функціоналом. Записи можна зберігати локально на карті MicroSD об'ємом до 256 ГБ або у хмарному сервісі за додаткову плату.

Камера оснащена інтелектуальною системою виявлення руху з можливостями розпізнавання людей, транспорту та налаштування зон детекції. Якісне кольорове нічне бачення забезпечує світлочутлива матриця та підсвітка двох типів.

Плюси: роздільна здатність відео 2560x1440, наявність LED-підсвічування та Starlight-матриці, розпізнавання людей та транспорту, двосторонній аудіозв'язок.

Мінуси: діапазон Wi-Fi лише 2,4 ГГц.

6. TP-Link TC40

TP-Link TC40 — відеокамера, що ідеально підходить для встановлення на вході в ділянку, гараж або невелику лазівку, за якою потрібен особливий контроль.

Об'єктив камери забезпечує кут огляду 85 градусів і фокусну відстань 3,9 мм, що дозволяє охоплювати невелику територію. Матриця з розділь-

ною здатністю 2 Мп забезпечує чітке зображення у Full HD-якості, на якому можна розглянути обличчя людей. Вночі, звичайно, деталізація дещо знижується, але камера підтримує нічне бачення та активується при виявленні руху у радіусі 30 метрів. Таким чином, ви зможете зафіксувати загальні риси обличчя або силует, будь то людина чи автомобіль.

Однією з особливостей цієї камери є датчик руху із підтримкою штучного інтелекту. Він розпізнає людей і надсилає повідомлення на ваш телефон. У разі потреби камера може навіть активувати сигналізацію, але це залежить від налаштувань.

Що стосується записів, то камера здійснює їх на вбудовану картку SD. Якщо використовувати карту на 256 Гб, то її вистачить приблизно на дві доби у Full HD-якості. Якщо цього недостатньо, ви можете підключити дублювання в хмару, де записи зберігатимуться до 30 днів. Однак варто врахувати, що ця опція вимагатиме додаткових витрат.

Зі зручностей варто відзначити наявність мікрофона і динаміка, що дозволяє спілкуватися, здійснюючи дзвінки в обидві сторони – ця функція нагадує домофон. Незважаючи на наявність безлічі отворів, герметичність камери не страждає. Корпус, захищений за стандартом IP65, витримує дощі, снігопади, вітер та пил.

Основні характеристики

Матриця: CMOS (1/3 дюйма);
Фокусна відстань: 3,89 мм
Діафрагма: f/2,0;
Кут огляду: по діагоналі – 85,5°; по горизонталі – 73,5°; по вертикалі – 41°;
Кут повороту: 360°, кут нахилу 130°.
ІЧ- підсвічування 850 нм (до 30 метрів);
Максимальна роздільна здатність: 1920 x 1080 пікселів;
Частота кадрів: 15 fps;
Формат стиснення відео: H.264;
Цифрове шумозаглушення;
Широкий динамічний діапазон;
Підтримка карт пам'яті до 512 ГБ;
Виявлення руху, виявлення людини;
Wi-Fi (2,4 ГГц) IEEE 802.11b/g/n.

Недоліки

Малуватий кут. Місцями «сируватий» додаток. Не можна встановити обмеження зони повороту камери. Програма не позначає переглянуті події виявлення, не вдається налаштувати свій окремий звук оповіщення на телефоні.

Коментар користувача

Моторизована вулична камера за цю ціну перекриває всі можливі недоліки. Незважаючи на інформацію на сайті виробника – людей визначає без підписки, робить це краще Xiaome AW200 у тих же умовах. У частині визначення руху – непогано, хоча спрацьовування на дивні рухи іноді є. Відстеження працює, камера повертається туди, де помітить краєм матриці рух. Після припинення руху повертається у задану раніше позицію. З непрямих мінусів – встановлену на фасаді приватного будинку камеру тролять джмелі. Можливо через слабку але схожість із вуликом. Любить дивитися на сильний дощ (точніше струмені води, що ллються з даху). Кут здався замалим. Не можна задати якісь межі для повороту, щоб при відстеженні руху камера не випускала з поля зору основний напрямок, який потрібно відстежувати, або не могла дивитися, наприклад, на сусідську ділянку, будучи встановленою на стовпі.

7. HiWatch DS-I400

Ця модель вже призначена для більш просунутих користувачів, які знаються на питаннях безпеки. Вона підключається до мережі через PoE, що дозволяє вести запис на відеореєстратор та, наприклад, переглядати її на екрані ПК.

До відеореєстратора можна підключити жорсткі диски, які зберігають записи протягом тривалого часу. Тривалість зберігання залежить від обсягу диска та роздільної здатності відео. Якщо використовувати накопичувач на 4 ТБ і встановити роздільну здатність Full HD, можна отримати більше двох місяців запису. До того ж, до цього відеореєстратора можна підключити додаткові камери, налаштувати їх в один потік і вести онлайн-спостереження за кількома об'єктами.

Якість зйомки у цієї камери на висоті. Сенсор тут 4-мегапіксельний, з фокусною відстанню 2,8 мм та кутом огляду 106 градусів. Це дозволяє камері захоплювати велику площу, що робить її придатною для встановлення як у дворі, так і на площі більшу за вхідні ворота. Запис ведеться у роздільній здатності 2560x1440 пікселів, що покращує видимість осіб на далеких відстанях і навіть номерів у денний час. Вночі, завдяки інфрачервоному EXIR-підсвічуванню, також можна розібрати загальні дані про підозрілий об'єкт.

Однак варто врахувати, що в камері немає мікрофона, ні динаміка. Є лише базовий датчик руху. Однак виконувані завдання в цієї камери дещо інші. Камера має надійний металевий корпус та захист за стандартом IP67, що забезпечує захист від снігу, спеки та зливи.

Основні характеристики

Фізичний розмір матриці: 1/3 дюйма;
Число пікселів: 4 Мп;
Фокусне відстань: 2,8 мм;
Кут огляду по горизонталі / по вертикалі / по діагоналі: 98° / 53,1° / 114,7°;
Дальність підсвічування до 30 м;
Максимальна роздільна здатність: 2560x1440;
Максимальна частота кадрів: 30 fps;
Формат стиснення відеофайлів: H.264, H.265, MJPEG;
Підтримка PoE;
Підтримувані протоколи: Bonjour, DDNS, DHCP, DNS, FTP, HTTP, HTTPS, IPv4, NTP, PPPoE, QoS, RTCP, RTP, RTSP, SMTP, SNMP, TCP/IP, UPnP.

Плюси:
- якісна матриця;
- чіткість, деталізація кадрів;
- просте встановлення;
- якісне складання.

Мінуси:
- відсутність вай-фай.

Коментар користувача

Встановив камери серії HiWatch DS-I400 з фокусною відстанню 2,8 та 4 мм по периметру будинку на дачній ділянці спільно з фірмовим відеореєстратором. Камери налаштовуються легко, працюють стабільно, картинка відмінна. Видно всю ділянку по периметру.

Що здивувало – якість картинки вночі. У чорно-білому форматі, при повній темряві дуже гарна картинка, також видно майже всю ділянку. У темряві видно світіння інфрачервоного підсвічування.

Ю. Дмитренко

За матеріалами

https://price.ru/blog/10-luchshikh-video-kamer-dlya-videonablyudeniya/#7-hiwatch-ds-i400

https://pipl.ua/ru/article/ezviz-cs-h3c-byudjetna-ip-kamera-z-velikimi-mojlivostyami?srsltid=AfmBOoquH1ekZcBU-OX1wu4betW6EV7Ie-HuN4GD3GshWlZQHH6zq

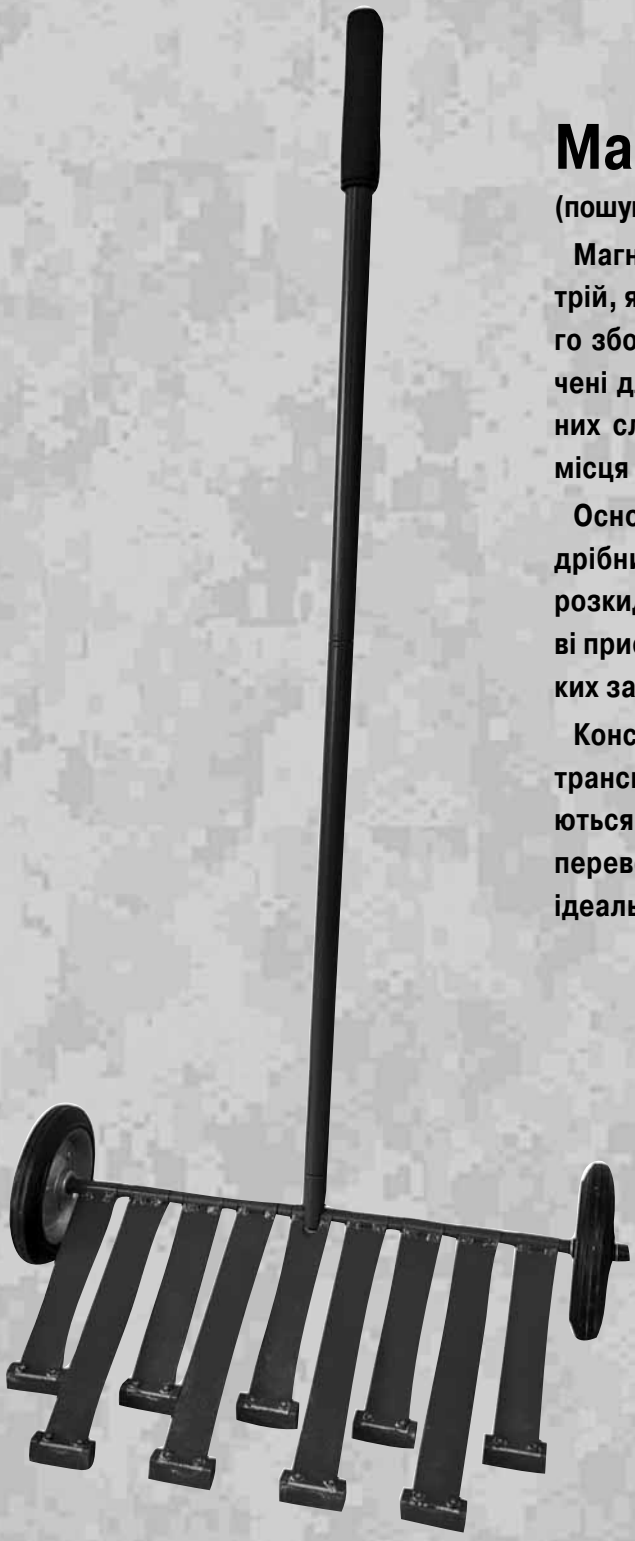
https://safetyarea.ru/articles/obzor-wi-fi-videokamery-ezviz-c8c/

https://itc.ua/articles/top-5-ulychnyh-wi-fi-kamer-vydeonablyudenyya-dlya-doma-y-malogo-byznesa/

https://dzen.ru/a/ZwNzI5smXXJGEKl5

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)

Цифровий магнітний запис

Цифровим називається запис, при якому сигнальний опис інформації, що записується, перетворюється в каналі запису в цифрову форму або перекодується з однієї цифрової форми в іншу. Техніка цифрового магнітного запису налічує декілька десятиліть. Її виникнення та розвиток на перших етапах були пов'язані з потребами електронно-обчислювальної техніки у зовнішніх запам'ятовуючих пристроях (ЗЗП), що володіють досить великим обсягом пам'яті і низькою вартістю зберігання інформації. Зовнішні запам'ятовуючі пристрої ЕОМ у вигляді накопичувачів на магнітних стрічках (НМС) і дисках (НМД) і зараз є найбільш поширеними пристроями цифрового запису, причому існує велика кількість різних типів НМС і НМД, зокрема НМД з рухомими або фіксованими головками, зі змінними або стаціонарними макетами дисків, зі змінними блоками пам'яті та ін.

Апаратура точного магнітного запису цифрова

Апарати цифрового магнітного запису (АЦМЗ), що використовуються в обчислювальній техніці, мають ряд специфічних особливостей у плані розміщення інформації на носії запису, режимів роботи, вимог до достовірності та ін. У зв'язку з цим, а також через виняткове використання у ті часи у звуко- і відеозапису аналогових методів, цифровий запис протягом тривалого часу застосовувалася майже виключно в НМС та НМД, що входять до складу ЕОМ.

Досягнення мікроелектроніки та пов'язаний з ними наприкінці 70-х – на початку 80-х рр. минулого сторіччя майже повсюдний перехід до цифрових методів обробки та передачі сигналів з'явилися поштовхом до широкого впровадження цифрової техніки у всі пристрої магнітного запису, включаючи запис аналогових сигналів. При цьому вхідні аналогові сигнали за допомогою аналого-цифрових перетворювачів (зазвичай за методом ІКМ) перетворюють на цифрові. Цифрові сигнали записують на магнітну стрічку, а після їх відтворення здійснюють зворотне цифро-аналогове перетворення, так що на вихід АЦМЗ надходить аналоговий сигнал [3].

Цифрові методи використовуються для запису звуку, сигналів телебачення, телеметрії та управління, в автоінформаторах, системах зв'язку та документування та багатьох інших випадках, коли потрібно накопичення інформації з метою її подальшого відтворення.

Багатоканальна апаратура точного магнітного запису (АТМЗ) для реєстрації інформації як аналогової, так і цифрової розроблялася для використання у важких кліматичних і вібраційно-ударних навантаженнях від підводно-морського, наземного до аерокосмічного застосування.

Слід зазначити, що АТМЗ в цілому являє собою прецизійний вимірювальний інструмент, а не як часто існуюче уявлення про магнітофони, як про пластмасову коробку, яку можна взяти із собою на пікнік. Це і визначило технічні вимоги до АТМЗ, до їх стрічкопротягувальних механізмів (СПМ) і до їх конструкції для виконання завдань замовників по реєстрації відповідних обсягів і часу інформації, що надходить на запис.

Під час створення АТМЗ і цифрової, зокрема, інженерно-технічні робітники та науковці НДІ ЕМП окрім звичайної інженерної роботи активно займалися науково-технічною творчістю - винахідницькою роботою, результати якої потім впроваджувалися у реальні вироби. Це дозволяло отримувати високі технічні характеристики виробів на рівні та вище аналогічних закордонних.

Найбільш активними винахідниками по відомостям, зокрема, на початок 1985р. (до 25-річчя інституту) були вже згадані вище Головні конструктори: Зволинський В.М. (мав 34 наукових праці та 36 авторських свідоцтв - а. с. - на винаходи, 16 з яких були впроваджені в АТМЗ з економічним ефектом 240 474 руб.), Орлович Ю.П. (14 а.с., впроваджено 10 з економічним ефектом 167 256 руб.); інженерно-технічні робітники та науковці Муравйов Г.Г. (80 а. с., впроваджено 53 з економічним ефектом 613 564 руб.), Дорошенко В.І. (82 а. с., впроваджено 48 з економічним ефектом 593 501 руб.), Кукла В.П. (65 а. с., впроваджено 28 з економічним ефектом 308 038 руб.), Травніков Є.М. (112 а. с., впроваджено 24 з економічним ефектом 394 549 руб.), Чуманов І.В. (63 а. с., впроваджено 11 з економічним ефектом 279 255 руб.), Савчук В.П. (19 а. с., впроваджено 17 з економічним ефектом 293 644 руб.) та інші.

Апаратура магнітного запису, зберігання та відтворення спеціальних цифрових сигналів

Розробка апаратури магнітного запису, зберігання та відтворення спеціальних цифрових сигналів розпочалася у далекому 1960р. з розробки бортових апаратів запису імпульсної, як тоді говорили інформації та її відтворення, зберігання і аналізу на стаціонарних наземних апаратах, а саме бортового виробу «Агат» і наземного виробу «Корунд» **(Головний конструктор Супруновський І.В.).**

Виріб «Агат» (за ДКР «Агат»)

Виріб «Агат» – бортова апаратура магнітного запису імпульсних сигналів.

Призначений для запису імпульсних сигналів позитивної полярності на борту літака в складі системи радіотехнічної розвідки «Куст-12М» [2]. Запис виконується одночасно по 4 каналам. В якості носія використовується попередньо розмагнічена стрічка типу РЕ-41 (фірма «Agfa») завширшки 6,25 мм. Середня швидкість руху носія 4,76 см/с. Тривалість безперервного запису 5 год. при запасі носія 1000 м.

Конструктивне виконання – носимий портативний апарат з співвісним розташуванням котушок з магнітним носієм.

Виріб «Агат» розроблено у таких модифікаціях:

«Агат-1» - швидкість транспортування носія 4,76 см/с;

«Агат-2» - швидкість транспортування носія 9,5 см/с;

«Агат-А» - відсутній обігрів та генератор, використовувався на штучних супутниках Землі (див. «Бізнес і безпека» №4, 2020р.).

Виріб «Агат»

Основні технічні характеристики виробу «Агат»: кількість каналів – 4; параметри імпульсних сигналів: амплітуда 4,5 ± 0,5 В; тривалість 40 – 50 мс; максимальна частота слідування 900 Гц; вихідний опір по всім каналам 100 кОм; відношення сигнал/шум при відтворенні 20 дБ; час запису – 5 годин (при швидкості 4,76 см/с); керування апаратом дистанційне; живлення – 24 - 31 В постійного струму; вага – 4,5 кГ; габарити – 280 х 280 х 100 мм.

Рік створення виробу – 1960. Виріб «Агат» серійно вироблявся заводом «Маяк» (м. Київ) з 1961 р., виріб «Агат-А» для космосу – з 1963 р.

Виріб «Корунд»

Виріб «Корунд» – чотириканальна апаратура «Корунд» призначена для відтворення та візуального аналізу імпульсних та синусоїдальних сигналів, які записано на бортовому магнітофоні «Агат» [2].

До складу апаратури окрім стаціонарного апарату запису, який виконано у вигляді настільного апарату, входять блок аналізу та три електронні осцилографи (див. на фото).

Анзіна Т.М.

Апаратура забезпечує:

- одночасний перегляд та індикацію результатів запису по 4 каналам;
- визначення каналу, в якому виявлено сигнал;
- в режимі циклічного відтворення – періодичне зчитування даних по обраному каналу з дільниці стрічки не менше 100 мм;
- вимірювання часових інтервалів між сигналами, які зчитуються, при циклічному відтворенні;
- в режимі циклічного відтворення індикацію часових калібрувальних міток, які відтворюються зі стрічки спільно з сигналом, що досліджується.

Апаратура має покажчик довжини магнітної стрічки, що оглянуто, проградуйований в одиницях часу, що відповідає швидкості запису.

Апаратура стаціонарна, розміщується в наземних та підземних спорудах, які опалюються.

Основні технічні характеристики виробу «Корунд»: кількість каналів – 4; динамічний діапазон амплітудних співвідношень 10 дБ; похибка вимірювань часових інтервалів: тривалістю 0,5 мм ±40 %; 1,0 мс ±20 %; 2,5 мс ±10 %; керування виробом місцеве; живлення від мережі змінного струму – 220 В 50 Гц; споживана потужність 2 кВА; вага – 560 кГ; габарити – 2 м^3 .

Рік створення виробу - 1960.

В розробці виробів «Агат» та «Корунд» брали участь заступники Головного конструктора: з радіоелектронної частини Рубан І.М., з технологічної частини Кучеренко Б.І., з конструкторської частини Данилевський В.Ф.; інженерно-технічні робітники: Йолкін В.І., Конрад Г.А.,Тищенко В.П., Дорошенко Р.Т., Співак А.Г., Дмитрієв Є.П., Спільник А.О., Анзіна Т.М., Алексєєва М.Є., Тарасова Г.П. – у тому числі в частині оформлення документації та багато інших.

Отриманий досвід розробки як перших зазначених виробів так і інших АТМЗ був в подальшому використаний при її розвитку і був втілений у вироби «Агат-1» та «Корунд-1».

Виріб «Агат-1» (за ДКР «Агат-1»)

Виріб «Агат-1» (**Головний конструктор Ціос В.М.**) – бортова авіаційна апаратура магнітного запису та автоматичного відтворення цифрової інформації отриманої від станції радіотехнічної розвідки «Вираж-1» та наступного введення цієї інформації в радіолінію «борт носія – наземний командний пункт». На 15 доріжках дискретна інформація записується у двійковому коді і на одній доріжці записуються вигнали управління роботою апарата [6]. Апаратура розрахована на безперервну роботу протягом 10 годин з 3-х разовою зміною магнітного носія.

Конструктивне виконання – возимий портативний апарат.

Основні технічні характеристики та приклади застосування наведено у [8].

На фото варіанти виробу «Агат-1» - вигляд, який він мав за результатами створення в НДІ ЕМП, а вид за результатами впровадження у серійне виробництво на київському заводі «Маяк» під назвою МР-1 наведено у [8].

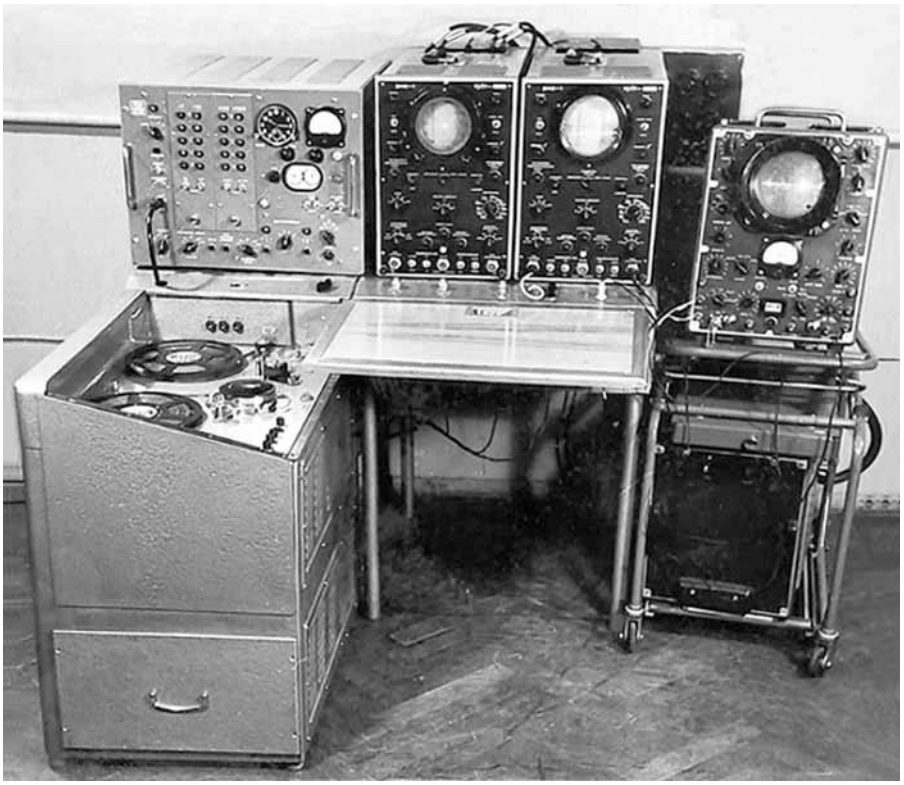
Виріб «Корунд-1»

Виріб «Корунд-1» (**Головний конструктор Ціос В.М.**) – наземна апаратура магнітного запису та відтворення цифрової інформації, що була записана на апаратурі «Агат-1» [6].

Конструктивно виконано у вигляді стійки з вертикальним стрічкопротягувальним механізмом (СПМ) та електронним блоком із застосуванням базових несучих конструкцій.

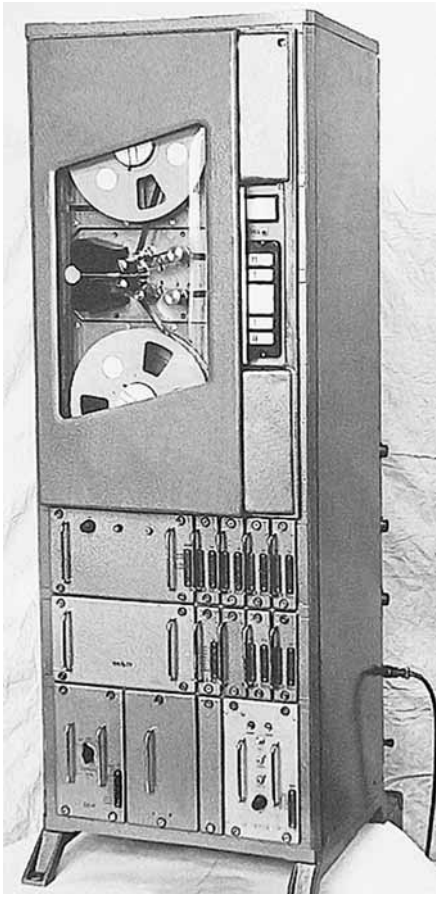
Основні технічні характеристики та приклади застосування наведено у [8]. На фото виріб «Корунд-1» - вид, який він мав за результатами створення в НДІ ЕМП, а вид за результатами впровадження у серійне виробництво на київському заводі «Маяк» під назвою УРВ-1 наведено у [8].

В розробці виробів «Агат-1» та «Корунд-1» брали участь заступники Головного конструктора: з радіоелектронної частини Рубан І.М., з технологічної частини Кучеренко Б.І., з конструкторської частини Гоменюк А.К.; інженерно-тех-



Виріб «Корунд»

Варіанти виробу «Агат-1»



Виріб «Корунд-1»

нічні робітники: Броваренко В.Ф., Співак А.Г., Дмитрієв Є.П., Тарасова Г.П., Богданова Н.Ф., Теремецька А.І., Гловацька Л.К., в частині оформлення документації – Тарасова Г.П. та багато інших.

Апаратура магнітного запису імпульсних сигналів в складі комплексів аналізу повітряної обстановки

Виріб «АМЗ-92»

Виріб «АМЗ-92» (**Головний конструктор Тищенко В.П. к.т.н. Орлович Ю.П.**) – універсальна апаратура магнітного запису та відтворення цифрової інформації для застосування в комплексі 9К 37. Апаратура призначена для застосування в складі виробів 9С470 та 9С18 при бойовій (документування повітряної обстановки та інформації з бортового обчислювача командного пункту) та навчально-тренувальній роботі [1]. Записана інформація в подальшому вводилась до стаціонарної ЕОМ для оцінки правильності дій обслуговуючого персоналу, а також використовувалась для покращення алгоритмів роботи та ТТХ комплексу.

Конструктивне виконання – возимий портативний апарат з двох блоків (блок СПМ «АМЗ-92РК» та блок електроніки контроля достовірності реєстрації інформації «АМЗ-92ТО», який використовувався в процесі експлуатації як для контролю, так і

Гоменюк А.К.

Гловацька Л.К.

для налаштування та ремонту блока «АМЗ-92РК») та пульта дистанційного керування.

В якості носія інформації використовується стрічка типу И-4414 шириною 25,4 мм.

Основні технічні характеристики виробу «АМЗ-92» [6]: кількість каналів – 30; вид запису цифрових сигналів вперше у НДІ ЕМП – ФМ, що дозволило подвоїти щільність запису, яка складала 50 імп/мм; швидкість руху стрічки при запису/відтворенні – 2,38; 19,05 см/с; тривалість запису 10 год; швидкість руху стрічки при перемотуванні – 3м/с; достовірність – 10^{-6}; обсяг інформації, що записується – $5x10^{7}$ біт; керування апаратом дистанційне; електроживлення – трифазне 220 В 400 Гц; 27 В постійного струму; споживана потужність – 500 Вт; вага – 130 кГ; габарити – 706х506х560 мм.

В розробці брали участь заступники Головного конструктора: з радіоелектронної частини Фомкин Л.В., з технологічної частини Кучеренко Б.І., з конструкторської частини - Старовatов А.О., Гоменюк А.К.; інженерно-технічні робітники: Ягічев О.М. - провідний розробник блоку «АМЗ-92-ТО»; Гончарук В.О., Чехлай І.О., Осовець Б.Л., Боброва Л.П., Лисак В.І., Фесай О.П., Панченко В., Мовчун М.Я. – відповідав за зборку та регулювання СПМ виробу та інші.

Дослідні зразки пристрою виготовляло дослідне виробництво НДІ ЕМП і постачало Замовнику (НДІ приладобудування ім. Тихомирова В.В у м. Жуковському). В подальшому серійне виробництво було налагоджено на підприємстві поштова скриня (п/с) Р-6813 у м. Самара.

Умови експлуатації: 17 група нормалі НО 005.026/с.

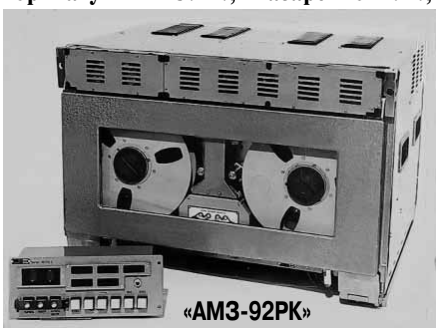
Рік створення – 1973 – 1976 рр.

Використовувався свого часу в складі ЗРК «Бук» для запису (з наступним аналізом) сигналів телеметрії роботи комплексу від моменту виявлення повітряної цілі до моменту її знищення.

До речі, в складі кожного транспортного засобу (в кабіні водія) зазначеного комплексу використовуються також магнітофони «МС-61», створені у НДІ ЕМП (див. «Бізнес і безпека» №5, 2019 р.), для запису перемовин водіїв транспортних засобів під час бойової роботи. До речі, у 2017 р. в Повітряних силах ЗС України виникла потреба в модернізації зазначених виробів і НДІ ЕМП мав отримати шанс повернутися до тематики робіт, для якої він, власне, і був створений колись у 1959 р. Нашими фахівцями було розроблено технічне завдання на модернізацію кожного з виробів з застосуванням сучасної елементної (твердотільної) бази, а потім почалася довготривала епопея його узгодження з Замовником і питання у підсумку було спущено на гальмах взагалі.

Виріб «КОД»

Виріб «КОД» (**Головний конструктор Ратушняк Є.М., Назаренко А.В.,**



«АМЗ-92РК»

«АМЗ-92ТО»

Виріб «АМЗ-92»

Кучеренко Б.І.

Ситник О.Т.) – багатоканальна апаратура реєстрації цифрової інформації в автоматизованій системі керування (АСК) спеціального призначення для систем «ОСНОВА» та «БАЙКАЛ» [6].

Виріб забезпечує: тривалий, безперервний (без зміни носія) запис імпульсної інформації, що надходить для документування та тривалого зберігання; відтворення раніше задокументованої інформації і видачу її до апаратури обробки з метою аналізу інформації, виготовлення звітних документів та тренажу особового складу об'єкту експлуатації. Запис цифрової інформації відбувається по 23 доріжкам в режимі послідовного та паралельного кодів [1].

В якості носія інформації використовується стрічка типу И-4406-25 завширшки 25,4 мм.

Основні технічні характеристики виробу «КОД»: кількість каналів – 24; вид запису цифрових сигналів – КІМ; частотний діапазон 1,2 – 30,4 кГц; швидкість руху стрічки при запису/відтворенні – 4,76 -76,2 см/с; тривалість запису 5 год при швидкості 4,76 см/с; швидкість руху стрічки при перемотці перемотуванні – 3,3 м/с; достовірність – 10^{-5}; обсяг інформації, що записується – $5x10^7$ біт; керування апаратом дистанційне; електроживлення – 27 В постійного струму; споживана потужність – 500 Вт; вага – 220 кГ; габарити – 500х600х1200 мм.

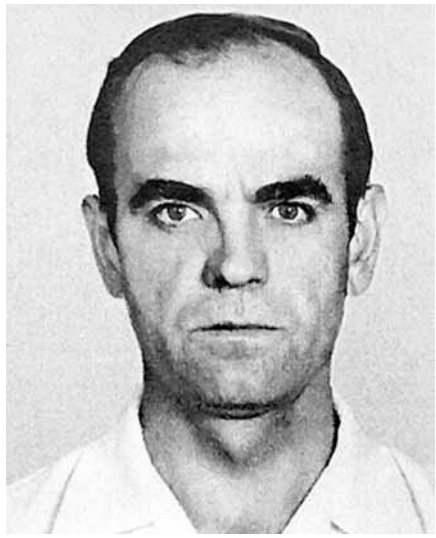
Умови експлуатації: 15 група нормалі НО 005.026/с.

Рік створення – 1974 – 1976. Замовник п/я с А-3706. Підприємство-виробник п/с А-7706.

В розробці брали участь заступники Головного конструктора: з радіоелектроніки Згура В.С., Іваненко Б.М., з технологічної частини Кучеренко Б.І., з конструкторської частини Гоменюк А.К., Проскурко В.М. в частині оформлення документації - Сперанська Р.В. та інші.

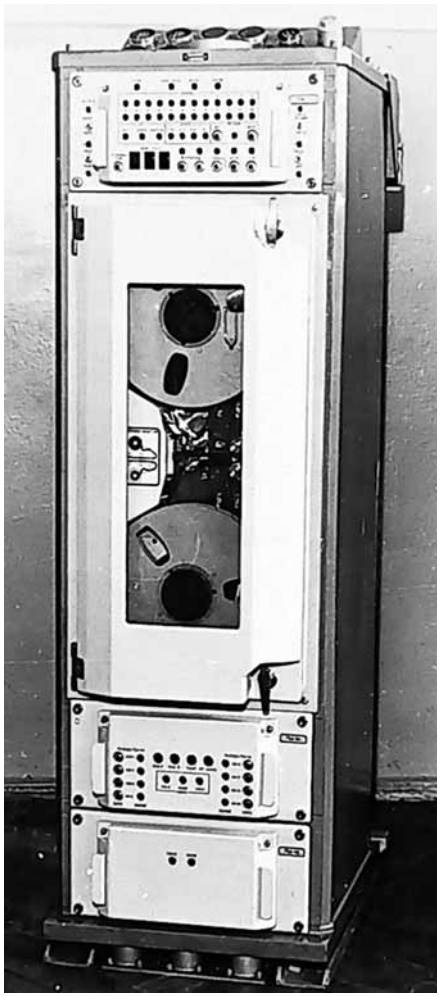
Дослідні зразки пристрою спочатку виготовляло дослідне виробництва, оскільки потреба у виробі була значною і треба його було організувати оптимальним чином. Як згадував один з Головних конструкторів виробу «КОД» Ситник О.Т., «керівництво МРП вирішило передати документацію різним підприємствам: магнітні головки були передані Єреванському об'єднанню «Ферріт», СПМ – Мінському електромеханічному заводу (МЕМЗ), а електроніка і весь виріб Кімовському заводу Тульської області. На нараді в Міністерстві представник Кімовського заводу мовчав, а головний інженер МЕМЗ Осипенко І.Г. зацікавлено поставився до освоєння СПМ і запропонував через тиждень після наради зустрітись в Мінську, де ми детально обговорили всі проблеми, дали детальні вказівки, що потрібно для освоєння виробу. Через місяць в Мінську уже був організований складальний цех і проблем з виготовленням і зборкою механізму з биттям вала < 1 мкм не було.

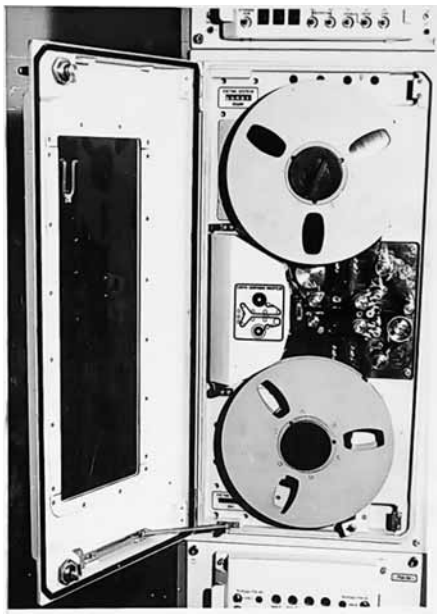
Ще більше приємно здивували головний інженер об'єднання «Ферріт» з Єревану Мусаелян Е.Г. і головний технолог Арутюнян Ш.Є., які направили групу своїх спеціалістів в НДІ ЕМП, що протягом місяця вивчали технологію виготовлення 24-канальних магнітних головок, отримали документацію і приступили до виготовлення. Яке ж було здивування, коли мене і Кабака О.А. – начальника відділу головок, викликали через 2 місяці в Єреван, бо партія головок, яка була виготовлена не відповідала ТУ. По приїзді, коли ми перевірили параметри декількох головок, виявилось, що віддача їх на 30 % більша ніж за ТУ, а допуск був вказаний в ТУ тільки в мінус.



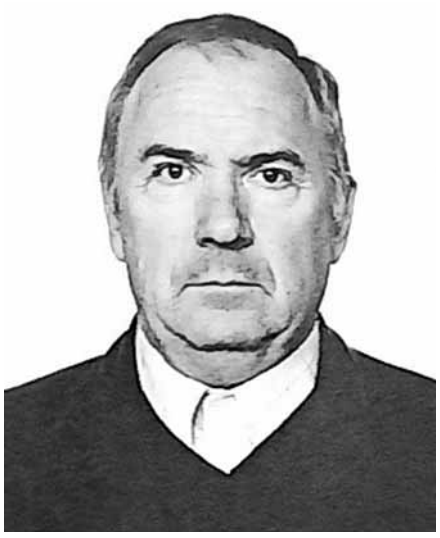
Назаренко А.В.

Виявилось, що спеціалісти «Ферріта» замінили матеріал сердечника на той, що виготовлявся в них на підприємстві, а він мав кращі параметри і ідентичність між каналами була такою, якої ми в НДІ ЕМП досягти не могли. Так що проблем з головками, СПМ і налагодженням виробу ми не мали. Мали тільки великі проблеми з небажанням керівництва Кімовського заводу освоювати нову техніку, що закінчилось звільненням директора, після цього завод довгі роки випускав виріб «КОД» і був задоволений, бо він ішов без проблем і працівники отримували і 13-у зарплату і премії, яких до цього давно не отримували.





Виріб «КОД» (ліворуч) та його блок стрічкопротягувального механізму (СПМ, праворуч)



Чуманов І.В.

Проскурко В.М.

Під час впровадження мені часто доводилось зустрічатись з Осипенко І.Г., Арутюняном Ш.Є. і в Москві в МРП, де контролював цю роботу прекрасний спеціаліст, морський офіцер у відставці Мальцев М.І., і в Києві. Я ці зустрічі пам'ятаю до цього часу і вдячний їм усім за активну допомогу в нашій роботі. Зазначу, що головну роль зіграли у випробуваннях, коригуванні документації і впровадженні у виробництво провідні спеціалісти НДІ ЕМП Чуманов І.В., Чехлай І.О., Петриченко В.І., Міщенко Е.Г., Пейков У.П., Проскурко В.М.».

Виріб «ФД-92»

Виріб «ФД-92» (**Головний конструктор Ратушняк Є.М., Андрущенко В.Ф.**) – возима прецезійна багатоканальна апаратура магнітного запису цифрової інформації для комплексу 5Ж15.

В якості носія інформації використовується стрічка типу 6Л шириною 25,4 мм.

Короткий опис побудови виробу «ФД-92» [10]: принцип дії – запис та відтворення інформації за допомогою радіоелектронних блоків. Керування стрічкопротяжним механізмом електричне (місцеве та дистанційне); схемні рішення: схеми побудовані функціонально-вузловим та блочним методами. Схеми виконано друкованим монтажем на напівпровідниках та інтегральних мікросхемах. Складові частини виробу з'єднуються монтажними дротами та міжблочними кабелями.

Зовнішнє оформлення відповідало сучасним на той момент вимогам естетики та вимогам організації-замовника В-2431.

Конструктивно виріб «ФД-92» виконано у вигляді шафи, до складу якої входять:

- блок автоматики ФД-962;
- блок лічильника метражу ФД-963;
- стрічкопротягувальний механізм (СПМ) ФД-964;
- блок живлення ведучого електродвигуна ФД-965;
- блок живлення бокових електродвигунів ФД-966;
- блок живлення загальний ФД-9201;
- блок живлення 27 В постійного струму ФД-9202.

Блок ФД-964 зібрано на литій плиті, яка має можливість обертатись відносно основної стійки, що відкриває доступ до елементів, що розташовані на зворотній стороні плити;

На плиті встановлено: приймальний та подавальний вузол з підкотушниками; вузли регулювання натягу в подавальній та приймальній гілці стрічки; рушійний механізм з електроприводом, ведучим валом та притискним роликом і магнітними головками;

Зовні блок ФД-964 закрито кришкою з резиновим ущільнювачем, що запобігає потраплянню в блок пилу;

Блоки ФД-962; ФД-963; ФД-965; ФД-9201; ФД-9202 зібрані на литих рамках, що з'єднуються між собою лицевими панелями з елементами управління та задніми стінками з роз'єднувачами. Кожен з блоків має можливість висуватись. При цьому забезпечується доступ до кожної з друкованих плат, що входять до складу блоку. Між собою блоки з'єднуються пласкими кабелями.

Виріб має ЗІП та комплект інструментів та приналежностей.

Основні технічні характеристики виробу «ФД-92» [6, 10]: кількість каналів – 24; вид запису цифрових сигналів – ОФМ; щільність запису 50 імп/мм; швидкість руху стрічки при запису/відтворенні – 9,53; 19,05; 38,1, 76,2 см/с; відхилення швидкості від номінальної не більше 1 %; тривалість запису 12 год при швидкості 9,53 см/с; швидкість руху стрічки при перемотуванні – 5 м/с; динамічний перекіс не більше 25 мк; достовірність – 10^{-5}; обсяг інформації, що записується – $5x10^7$ біт; час запису – 3 години; керування апаратом місцеве та дистанційне; електроживлення – 220 В 400 Гц, 27 В постійного струму; споживана потужність 650 Вт; вага – 120 кГ; габарити – 525x450x1795 мм. Надійність – наробіток виробу на відмову 400 год. Кількість обслуговуючого персоналу – 1 люд. Річний випуск: по першому року 15 шт, по третьому року 60 шт. Гуртова ціна при серійному виробництві по першому року випуску - 39100 руб, по третьому - 35450 руб.

Умови експлуатації: 13 група нормалі НО 005.026/с.

Рік створення - 1973. Дослідні зразки виробу виготовило дослідне виробництво НДІ ЕМП і відправило Замовнику п/с В-2431. Державні випробування, в яких брали участь провідні фахівці НДІ ЕМП, відбувались на Центральному ракетному полігоні у м. Приозерськ в Казахстані, а також на полігоні «Емба-5» в Оренбурзькій обл. Згодом, конструкторська документація на виріб була передана для серійного виробництва підприємству п/с М-5514 (м. Львів, завод об'єднання «ЛОРТА»), яке його випускало протягом багатьох років.

В розробці брали участь заступники Головного конструктора: з радіоелектроніки Андрущенко В.Ф., з технологічної частини Кучеренко Б.І., з конструкторської частини Іонін М.А.; інженерно-технічні робітники: Йолкін В.І., Реденський О.А., Назаренко А.В., Маслакова Л.С., Котов Г.В., Спичка В.С., Шаповаленко Б., Кукла В.П., Старовatов А.О., Гловацька Л.К. та інші.

Виріб «ФД-92»

Староватов А.О. за проєктуванням

Андрущенко В.Ф.

Виріб «Бирюса-МЗ»

(Головний конструктор Тищенко В.П.)

Виріб «Бирюса-МЗ» («АМЗ-91») - багатоканальна апаратура точного магнітного запису, що призначена для реєстрації звукових частот та цифрової інформації, в складі пристрою магнітного запису «АМЗ-91», що входить до складу шафи документування «ФА-91» для застосування в складі комплексу 5Ж15 [1].

Розробка виконувалась шляхом доопрацювання двох дослідних зразків апаратури «ФД-92» за додатковими вимогами Замовника.

Технічні характеристики виробу «АМЗ-91» в цілому відповідали технічним характеристикам виробу «ФД-92». Основна відміна – наявність певної кількості каналів запису-відтворення мовної (звукових частот) інформації.

В розробці брали участь в основному ті ж самі фахівці, що і в розробці виробу «ФД-92».

Умови експлуатації: 13 група нормалі НО 005.026/с.

Рік створення -1970 -1974. Організація Замовник п/с В-2431. У 1971р. виготовлено 2 дослідних зразка, які були після держвипробувань передані Замовнику.

Виріб «Служебник-Ц»

(Головний конструктор к.т.н. Орлович Ю.П.) – багатоканальна апаратура цифрового магнітного запису та відтворення в системі документування інформації.

Апаратура забезпечує запис та відтворення паралельно по 13 каналам цифрових сигналів, що представлені у формі БПН («без повернення до нуля»).

В апаратурі здійснюються необхідні, специфічні для апаратури точного магнітного запису, перетворення вхідних сигналів перед їх записом на магнітну стрічку.

Основні технічні параметри та приклади застосування наведено у [8]. Згідно технічнимх умовам [11] виріб мав два виконання (інші ТТХ в основному співпадають):

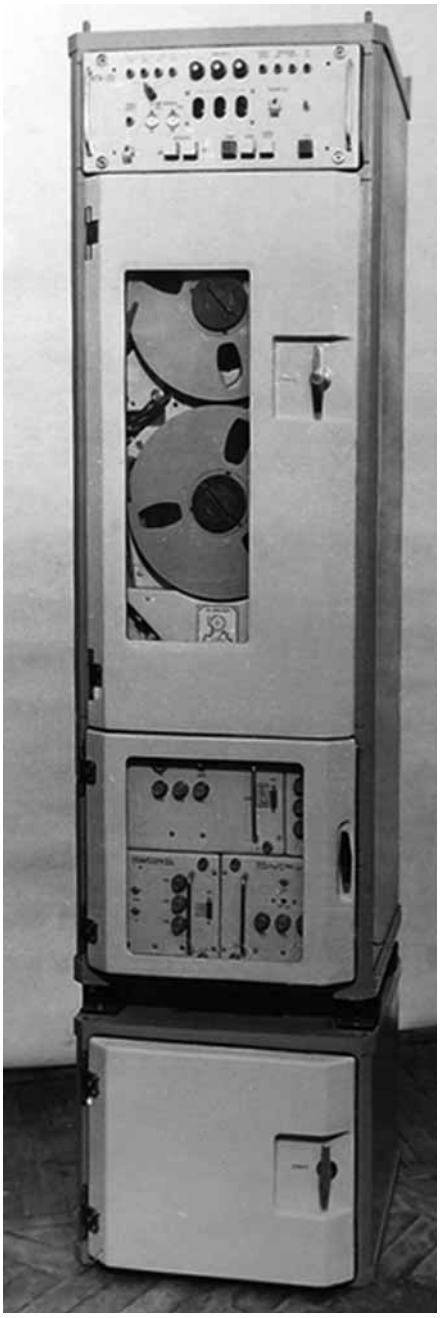
- «Служебник-Ц1» - електроживлення трифазне 200 В частоти 400 Гц; швидкість транспортування магнітної стрічки 2,38; 4,76; 9,52; 19,05 см/с; час безперервної роботи не менше 10 год; маса 140 кг.
- «Служебник-Ц2» - 220 В частоти 50 Гц; швидкість транспортування магнітної стрічки 4,76; 9,52; 19,05; 38,1; 76,2; 152,4 см/с; час безперервної роботи не менше 20 год; маса 180 кг.

Зовнішній вигляд повного комплекту виробу наведено на фото нижче, а динаміку розвитку АТМЗ цифрових сигналів в процесі їх створення в НДІ ЕМП, зокрема в складі комплексів аналізу повітряної обстановки для авіаційної та ракетної техніки наведено нижче в табл. 1.

Розробка 1984 – 1988 рр. Відомо, що апаратура пройшла успішні випробування на одному з радянських авіаційних полігонів в Казахстані.

В розробці брали участь заступники Головного конструктора: по загальним питанням Ковінченко М.М., з розробки апаратури обробки цифрової інформації Реденський О.А., з технологічної частини Романова С.Х., з конструкторської частини Проскурко В.М., з надійності Середа А.Ф.; інженерно-технічні робітники: с.н.с. Смірнов Ю.М., Чехлай І.О., Гончарук В.О. (керував випробуваннями апаратури на авіаційному полігоні в Казахстані), Кравченко В.В. та Самелюк В. – в частині електроприводу, Василевський В.О.; в частині оформлення документації (в тому числі і виробів «ФД-92», «АМЗ-92», «Бирюса-МЗ», «КОД») Сперанська Р.В. - керівник, Міщенко Е.Г., Сніжко Г.К., Тернова Т.М., Іванова Т.П., Алексеєнко В.В., Коротчук Є.С., Михайлова Т.Н., Величковська Є.В., Хмель В.Г., Круть Л.П., та інші.

Варто відмітити, що директора НДІ ЕМП починаючи з першого директора Каменєва В.М. та кінчаючи Антоновим В.І. завжди і всіляко підтримували творчу молодь, сприяли її професійному зросту. Оскільки Київський політехнічний інститут (КПІ)



Виріб «Бирюса МЗ»

Бобарчук О.А.

Професор Геранін В.О.

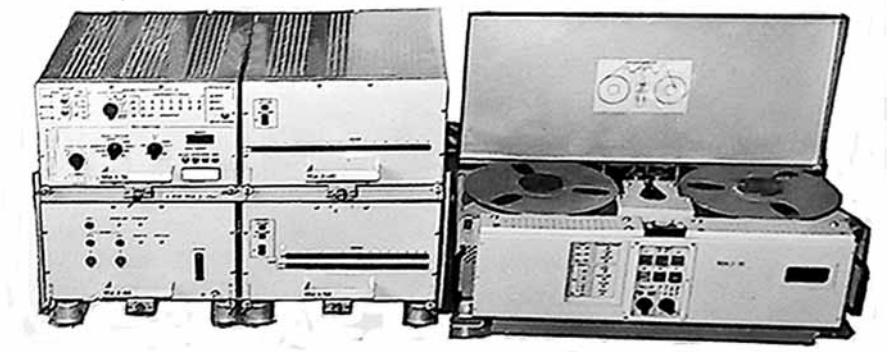
був базовим Вишем НДІ ЕМП у підготовці інженерів для інституту, у 1984р. за підтримки директора НДІ ЕМП Антонова В.І., була створена спільна «Лабораторія з дослідження цифрових методів запису та обробки інформації в АТМЗ» під керівництвом д.т.н., професора КПІ Гераніна В.О., в якій проходили підготовку студенти старших курсів КПІ, зокрема Горошко С.П., Дележа Б.В., Бобарчук О.А., Берман Г.В., Іголкін В., Дяченко О.Б. та які після закінчення навчання були прийняті на постійну роботу в НДІ ЕМП і внесли певний позитивний внесок в створення унікальної апаратури «Служебник-Ц».

Згодом Бобарчук О.А. та Дяченко О.Б. захистили кандитатські дисертації і успішно працювали далі. Сьогодні Бобарчук О.А. – завідувач кафедри комп'ютерних мультимедійних технологій Державного університету «Київський авіаційний інститут». Під його проводом студенти старших курсів успішно готують під час виконання курсових та дипломних робіт презентації, каталоги музею техніки магнітного запису НДІ ЕМП, створили сайт зазначеного музею в Інтернеті – все це допомагає у справі збереження багатючої історії НДІ НМП (див. публікації автора у журналах «Бізнес і Безпека» за 2019 -2024рр.), зокрема для прийдешніх поколінь радіоінженерів.

Після розпаду Радянського Союзу в спробі вижити інститут у 1992-1993 рр. проваджував рекламу даного виробу для широкого загалу користувачів з заявленою вартістю одного комплекту апаратури «Служебник-Ц» в 1 млн. радянських рублів [7]. Потенційно зазначений комплект міг бути застосованим не тільки для документування цифрової інформації для військових користувачів, але й міг застосовуватись для обробки цифрової інформації при наукових дослідженнях, на виробництві, в медицині тощо. Проте не склалося...

Слід окремо зазначити, що при розробках АТМЗ (АЦМЗ зокрема) взагалі було тісно налагоджене спільне співробітництво з підприємствами оборонних галузей промисловості СРСР. Зокрема, через технічний відділ інституту поставлялася нова елементна база Міністерства електронної промисловості на етапі експериментальних зразків, які проходили дослідну експлуатацію й апробацію при проектуванні нових видів апаратури. Якщо перші АТМЗ (зокрема серії «Астра», «Корунд») були побудовані на радіолампах, то в наступних (серії «Агат-1», «Василек», «Сепия», «Звук» тощо) вже широко застосовувались напівпровідникові елементи, зокрема транзистори, а потім додалися інтегральні мікросхеми - ІМС (вироби серії «Остров», «МУЗ-6», «АМЗ-92», «МУЗ-10» тощо. В апаратурі «Служебник-Ц» застосовувались також унікальні спеціалізовані ІМС попередніх підсилювачів власної розробки та виробництва - цим займався відділ мікроелектроніки інституту, зокрема к.т.н. Герасимук Л.М.).

АЦМЗ «Служебник-Ц»

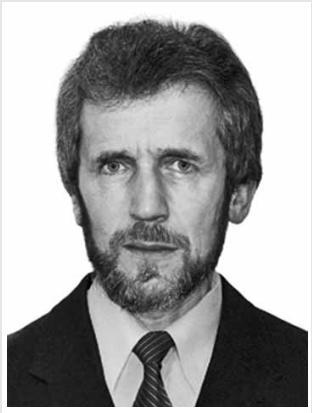


Таблиця 1

Технічні характеристики		Апаратура запису-відтворення спеціальних цифрових сигналів		Апаратура запису імпульсних сигналів у складі комплексів аналізу повітряної обстановки			
		«Агат» «Корунд»	«Агат-1» «Корунд-1»	АМЗ-92	«КОД»	«ФД-92»	«Служебник-Ц»
Кількість доріжок	інформаційних	4	16	28	23	23	13
	службових		16	2	1	1	1
Швидкість надходження цифрових сигналів, кбіт/с		900 Гц	4,8	19,2	15,2	152,0	10,0 за швидкості 4,76 см/с; 320 за швидкості 152,4 см/с
Достовірність			$1,5x10^{-4}$	10^{-6}	10^{-6}	10^{-5}	10^{-5}
Час запису, год.		5	0,3	12 за швидкості 2 см/с	6 за швидкості 4,76 см/с	3 за швидкості 19 см/с	20 за швидкості 4,76 см/с

Щиро вітаємо!

Колектив Кафедри інформаційної та кібернетичної безпеки імені Володимира Бурячка Київського столичного університету імені Бориса Грінченка щиро вітає Провозіна Олександра Петровича з Днем народження!



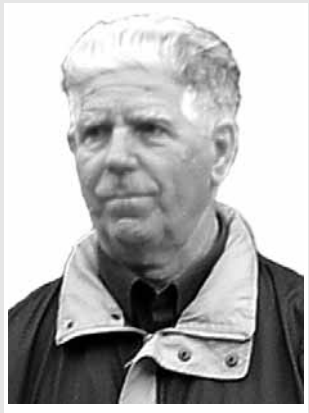
Шановний Олександре Петровичу! Дякуємо Вам за вагомий внесок у підготовку фахівців у сфері кібербезпеки та захисту інформації, які нині успішно працюють в установах і організаціях України підтримуючи безпеку держави на належному рівні.

Зазначаємо, що завдяки Вашому досвіду та невтомній праці у сфері розробки новітніх засобів технічного захисту інформації, в Україні було сформовано основні засади забезпечення захисту інформаційного простору держави та залучено творчу молодь до навчання і наукових досліджень.

Зичимо Вам доброго здоров'я, творчої наснаги, подальших успіхів і плідної співпраці на благо України!

Щиро вітаємо!

Щиро вітаємо Літвинова Валентина Івановича – непересічну людину та радіоінженера, Головного конструктора авіаційних бортових мовних реєстраторів («чорних скринь») та бортових мовних інформаторів (аварійних сповіщувачів) – **з 90-річним Ювілеєм!** (1січня 2025 р.)



Ви є одним з фундаторів НДІ ЕМП, успішно працювали і творили з часу його утворення 1 жовтня 1959 р. і до виходу на заслужений відпочинок. На всіх посадах по життю, на яких працювали, Ви проявили себе як грамотний організатор, принциповий, відповідальний, творчий фахівець і винахідник, який свої винаходи впроваджував у серійні вироби залучаючи при цьому творчу молодь до навчання, винахідництва та науково-технічних досліджень.

Розроблені вперше в СРСР під Вашим проводом вироби «МС-61» та «МН-61», «Арфа-М», «РИ-65» та «Алмаз-9» широко серійно вироблялись для авіації Радянського Союзу, створені Вами унікальні вироби «Арфа-Р» для надзвукового літака Ту-144 та «Арфа-К» для космічних станцій успішно працювали і вирішували завдання безпеки авіаційних польотів на належному рівні.

Зазначені вироби розроблені десятки років тому і були успішно впроваджені у виробництво та й до теперішнього часу затребувані (зокрема «МС-61» та «МН-61», «РИ-65») - це чи не гарантія найвищих здібностей їхніх творців під Вашим керівництвом?!

Не дивлячись на похилий вік, Ви зуміли зберегти тверезість розуму та ясність думки, плідно сприяєте у справі збереження історії НДІ ЕМП.

Зичимо Вам, Валентине Івановичу, доброго здоров'я і наснаги, до ста років дожити без старості, подальшої плідної співпраці з музеєм техніки магнітного запису НДІ ЕМП, успіхів у Ваших добрих починаннях і справах!

З глибокою повагою, колеги та ветерани АТ «НДІ ЕМП», редакція журналу «Бізнес і безпека».

«Чорна скриня» «МС-61». Аварійний сповіщувач «РИ-65»

Під керівництвом Головного науково - технічного управління нашого Міністерства формувалися довгострокові програми розвитку підприємств об'єднання «Маяк» (НДІ ЕМП, НДІ ім. Мануїльського, заводу «Маяк» тощо), апаратурні комплексні цільові програми (АКЦП) створення нових АТМЗ і взаємодії з підприємствами суміжних галузей (див. вище приклад при створенні виробу «КОД»).

У такий спосіб в інтересах замовників успішно вирішувалися завдання по створенню АТМЗ різноманітних видів для різних умов експлуатації, зокрема таких важливих характеристик як діапазони реєструємих частот (швидкість надходження цифрових потоків) і час безперервної роботи на об'єкті застосування.

Потреби забезпечення Замовників у апаратурі, що розроблялась у НДІ ЕМП, задовольнялись власним дослідним виробництвом на рівні одиночного та дрібносерійного виробництва. Наприклад, протягом 1979 р. [1] виготовлено і відправлено Замовникам наступну апаратуру (дрібні серії): «Строб-МЗ» - 8 приладів підприємству п/с М-5440; «Гранит-2» - 12 зразків п/с Г-4810; «Пигмей» - 8 блоків 9С-20И, 8 блоків 9С30И п/с В-8828; «Арфа-К» - 1 блок 33А-10, 3 блока 27А-30 п/с В-8828; «Лилипут-Р» - 4 бортових апарата, 16 касет, 4 пульта індикації п/с В-8828; «Квадрат-3БС» - 5шт., 5 касет п/с Р-6510; «Квадрат-НУ» - 3 апарата в/ч 25966-Б; «Квадрат-УС» - 3 апарата в/ч 25966-Б; «Стенд-17И» - Белорецькому металургійному комбінату; «Остров-РК» - 2 компл. п/с Г-4429; «Остров-РМ» - 4 компл. (1- Г-4173, 3 - в/ч 30882); «Остров-К» - 1 компл. в/ч 30882; «Агат-68» - 3 компл. п/с А-1965; «КАМЗ-023» - 3 компл. п/с А-1129.

В інших випадках, які зазначено вище, конструкторська документація передавалась на серійні підприємства, розташовані на території Радянського Союзу – у Києві, Львові, Кімовську, Самарі, Мінську, Кишиневі, Вільнюсі, Єревані.

(Далі буде).

Олександр Провозін
Заст. Голови правління АТ «НДІ ЕМП»

Література.

1. Річні звіти діяльності та накази по підприємству за 1960 – 1991 рр.

2. Альбом изделий, разработанных в организации п/я 231, Министерство радиопромышленности СССР, экз. №1, инв. №910, 1965.

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

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

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

6. Перечень специальной аппаратуры магнитной записи, разработанной (разрабатываемой) и выпускаемой малыми сериями (планируемой к освоению производства) на предприятиях , организации п/я Г-4965, а также планируемой к освоению производства на предприятиях других министерств. Инв. №10, Киев, 1975.

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

8. Провозин А. Обеспечение безопасности полетов в авиации. Краткая история «черных ящиков» в Украине, «Бизнес и безопасность», №1, 2020.

9. Травников Е.Н. Механизмы аппаратуры магнитной записи. Киев, «Техніка», 1976.

10. Изделие «ФД-92». Технико экономическая характеристика. ЛЩ3.060.125 Д9. 1978.

11. ЛЩ1.750.061 ТУ. Технические условия «Служебник-Ц». 1986.

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

ufi Approved Event

27–29 травня

Генеральний інформаційний партнер:

Обладнання та інструмент для професіоналів

МІСЦЕ ПРОВЕДЕННЯ:
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

Капітал будівництво | Бетон і асфальт | 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

Впровадження автоматизованих систем централізованого оповіщення територіальних громад

Стаття 30 розділу IV Кодексу цивільного захисту населення України регламентує забезпечення оповіщення шляхом автоматизації процесу передачі сигналів і повідомлень про загрозу або виникнення надзвичайних ситуацій та функціонування сигнально-гучномовних пристроїв і електронних інформаційних табло для передачі інформації з питань цивільного захисту, встановлення яких покладене на органи місцевого самоврядування та суб'єкти господарювання.

У відповідності до Кодексу та Постанови КМУ від 27.09.2017 №733 органи місцевого самоврядування за кошти територіальних громад створюють місцеві автоматизовані системи централізованого оповіщення, які, у тому числі, забезпечують оповіщення всередині приміщень лише комунальної власності.

При цьому сотні тисяч виробничих, торгівельно-розважальних, торгівельних, лікувальних та інших закладів, що належать суб'єктам господарської діяльності, нажаль залишаються не обладнаними засобами оповіщення про надзвичайні ситуації. У теперішній час це унеможливлює гарантоване оперативне доведення повідомлень про повітряну тривогу до мільйонів глядачів та персоналу наведених вище закладів. Виправлення цієї ситуації, вкрай неприпустимої в умовах ведення повномасштабної війни на всій території України, можливе шляхом використання спеціалізованих програмно-апаратних засобів оповіщення.

У теперішній напрацьований досвід впровадження місцевих автоматизованих систем централізованого оповіщення (МАСЦО) на базі програмно-технічних засобів виготовлених компанією «ОЗОН С». У багатьох областях України впроваджено більше п'ятдесяти автоматизованих систем централізованого оповіщення, які у теперішній воєнний час сповіщають понад 4 млн. людей про повітряну тривогу.

Впровадження систем виконується «під ключ»: від проектування до технічного забезпечення гарантованого використання систем за призначенням, включаючи виготовлення обладнання, його монтаж та налагодження. Проєктування здійснюється з урахуванням рекомендацій гармонізованого в Україні європейського стандарту ETSI TS 102 182 та з безумовним виконанням всіх вимог діючих в Україні нормативно-правових актів та нормативно-технічних документів, а саме Кодексу цивільного захисту України, Постанови КМУ від 27.09.2027 р. №733, відповідних наказів та рекомендацій ДСНС України. Всі проєкти розробляються у повній відповідності до погодженого ДСНС України Технічних завдань та мають позитивний висновок уповноваженої експертної організації. Обладнання для систем виготовляється за Технічними умовами ТУ У 27.9-32723765-003:2017 погодженими Українським науково-дослідницьким інститутом цивільного захисту, Державною службою України з надзвичайних ситуацій та перевіреними на відповідність діючому законодавству Державним науково-технічним центрі стандартизації, метрології та сертифікації в установленому порядку.

До складу комплекту місцевої автоматизованої системи централізованого оповіщення (МАСЦО) входять: автоматизовані робочі місця оперативних чергових пунктів керування цивільним захистом, пристрої централізованого керування мережами телерадіомовлення та рекламно-інформаційними табло, пристрої керування електромеханічними сиренами, електропневматичні сирени, сигнально-гучномовні пристрої для оповіщення всередині приміщень і на відкритих територіях, у тому числі, аеромобільна система оповіщення на базі безпілотних летальних апаратів, що була презентована та мала успіх на Міжнародному форумі MUNI EXPO 2019, м. Тель-Авів.

Практично всі складові систем виробляються в Україні й тому мають оптимальні техніко-економічні показники. В залежності від кількості та величини населених пунктів, що входять до складу об'єднаної територіальної громади, вартість впровадження МАСЦО складатиме 4 – 10 млн грн для міст районного значення або територіальних громад з 10-15 населеними пунктами та 10 – 25 млн грн для міст обласного значення або великих територіальних громад.

Окремо слід зазначити, що, в умовах безперервних ракетно-артилерійських обстрілів, особливого значення набуває наявність захисних споруд цивільного значення, а також ефективність їх використання. У теперішній час проєктування, будівництво, пристосування захисних споруд відповідно до п. 6 Глави 7 Кодексу цивільного захисту України регламентується ДБН В.2.2-5:2023 «Захисні споруди цивільного захисту». З метою виконання вимог п. 11.7 цього ДБН та з урахуванням реальних проблем, що виникають при використанні захисних споруд за призначенням, розроблений спеціалізований програмно-апаратний комплекс «ОЗОН ЗС», що інтегрується в МАСЦО.

Незважаючи на постійні повітряні атаки та обстріли, наразі виконуються роботи по впровадженню МАСЦО в громадах Херсонської та Дніпропетровської областей.

Висловлюємо готовність бути надійними партнерами громад у забезпеченні безпеки життєдіяльності населення в умовах широкомасштабної війни. Завдяки нашим економічно доступним та якісним рішенням кожна громада зможе бути впевнена у своєчасному й ефективному оповіщенні про повітряну тривогу.

До кінця другого кварталу 2025 року для передплатників журналу «Бізнес і безпека» пропонується 20% знижка на розробку проєктів МАСЦО.

ТОВ «БЕЕСОФТ»
м. Київ, вул. Соловцова Миколи, будинок 2, офіс 38/3
info@beesoft.work
+380931978495

ТОВ «ФАЛЬКОН-М»
м. Миколаїв, вул. Робоча, 2 А, оф. 711
evfalconm@gmail.com
тел. 067-512-57-07

ТОВ «НАУКОВО-ВИРОБНИЧЕ ПІДПРИЄМСТВО «ОЗОН С»
м. Дніпро, вул. Ливарна, б. 9, кв. 44
office@ozons.com.ua
+380567900579
+380567900580

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

- СПІВПРАЦЯ ГРОМАД ТА ДСНС - ПРАВИЛА ЕВАКУАЦІЇ НАСЕЛЕННЯ - «НАБІР ДЕМІНЕРА НД-4» -
- ПРОТИДІЯ ОНЛАЙН-ШАХРАЙСТВУ - ФІШИНГ ФАЙЛОМ, АБО РОСІЙСЬКА КІБЕРМАТРЬОШКА -
- ЯК МАЄ ЗМІНИТИСЯ УКРАЇНСЬКА АРМІЯ, ЩОБ ВИГРАТИ ВІЙНУ - ШТУЧНИЙ ІНТЕЛЕКТ У ВІЙСЬКУ -
- «ЛИПЯВКА ТА ПАРТНЕРИ» ПІДТРИМУЮТЬ БІЗНЕС ПІД ЧАС ВІЙНИ - ТАКТИЧНА МЕДИЦИНА ВІД ПРАТ «АВ-ФАРМА» -
- БЕЗПЕКА В TELEGRAM - НАВЧАЛЬНА ПРОГРАМА ПІДГОТОВКИ ОСОБОВОГО СКЛАДУ З ОХОРОНИ -
- РОСІЯНИ ОТРУЇЛИ РІЧКУ СЕЙМ - ДИТЯЧІ ПРОТИГАЗИ - ТЕПЛОВІЗІЙНІ СИСТЕМИ - ЯК ЗАГАСИТИ ЕЛЕКТРОМОБІЛЬ - ВИХОВАННЯ ДОБРОЧЕСНОСТІ ТА БОРОТЬБА З КОРУПЦІЄЮ В ОБОРОННОМУ СЕКТОРІ -

більш детально, читайте на стор. <None>

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

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

+38 (095) 268-05-87
plast@iec-expo.com.ua,
helen@iec-expo.com.ua
www.iec-expo.com.ua

Виховання доброчесності та боротьба з корупцією в оборонному секторі

В основному ДКЗС зосереджує увагу на регіонах Західних Балкан та нових незалежних держав, що утворилися після розпаду Радянського Союзу, однак, останнім часом все більше уваги приділяється Близькому Сходу, Південній Америці та Азії.

Організація Транспаренсі Інтернешнел (ТІ) є позапартійною глобальною мережею, яка забезпечує поєднання міжнародної присутності глобальних НУО з місцевими можливостями своїх понад 90 національних представництв. Ці представництва займаються тим, що заохочують контакти між відповідними представниками від уряду, громадянського суспільства, бізнесу та ЗМІ з метою забезпечення прозорості під час виборів, у діяльності установ державної влади, під час закупівель та бізнесових операцій. Вони також іноді здійснюють програми стимулювання урядів до імплементації антикорупційних реформ.

Глобальними пріоритетами для ТІ є боротьба з корупцією у сфері політики, державних закупівлях та приватному секторі. Вони також підтримують дотримання міжнародних антикорупційних конвенцій і працюють над подоланням бідності й підтримкою розвитку. ТІ не займається проведенням розслідувань за підозрою в корупції або оприлюдненням інформації про її окремі прояви, однак, іноді співпрацює з тими організаціями, які це роблять.

Починаючи з 2000 року, представництво ТІ у Сполученому Королівстві почало працювати над питаннями корупції у сфері оборони. Спочатку основна увага приділялася сфері збройового експорту, і ТІ зібрала разом представників урядів-експортерів зброї та оборонної промисловості, щоб обговорити можливі конструктивні заходи, які б допомогли знизити рівень корупції у цій сфері. Ці ідеї включають можливість створення оборонного консорціуму проти корупції, покращення стану імплементації Конвенції ОЕСР, пактів доброчесності щодо закупівель і більш тісного співробітництва з іншими міжнародними організаціями.

Останнім часом ТІ почала співпрацювати з НАТО в рамках Трастового фонду з метою розв'язання проблеми корупції та корупційних ризиків у сфері оборони. Вона також розпочала ініціативу, направлену на краще оцінювання ефективності зусиль в рамках програм доброчесності у сфері оборони.

Використання потенціалу міжнародних організацій для сприяння змінам

Величезна кількість міжнародних організацій, міжурядових організацій та глобальних інститутів громадянського суспільства беруть участь у боротьбі з корупцією. За таких обставин для прихильників реформ з числа офіційних осіб міністерства оборони або громадян виклик полягає у тому, як використати цей потенціал для започаткування позитивних змін. Наступні три підходи вже підтвердили свою успішність:

1. Міжнародні стандарти: Національна інституція, зацікавлена у реформах, починає співпрацювати з міжнародною інституцією, яка забезпечує дотримання міжнародного стандарту. Це може бути антикорупційний стандарт під егідою ОЕСР, або це може бути етичний стандарт на зразок Керівництва ООН з питань конфлікту інтересів для державних посадових осіб, або стандарт доброчесності якогось процесу, наприклад, аудиту. Метою є дотримання стандарту з використанням будь-яких механізмів зворотного зв'язку для того, щоб отримати престиж, гордість за виконану роботу та покращення ефективності – все те, що може дати дотримання міжнародних стандартів. У тісній співпраці з групою оцінки інспекції створюють відмінні можливості не лише для отримання зворотної інформації, але й для того, щоб включати важкі реформи до порядку денного вищого керівництва.

2. Спільні проекти: Національна інституція зацікавлена в отриманні допомоги від міжнародної організації для вирішення специфічного питання, важливого для керівництва цієї інституції, але на його вирішення не вистачає місцевих ресурсів. Для цього створюється спільна програма з об'єднаним механізмом менеджменту, тобто, виконавчі групи, спостережні структури для забезпечення керівництва, спільного оцінювання і спільних доповідей тому органу, в рамках якого регулярно зустрічається вище керівництво обох сторін. Такий підхід дозволяє національним інституціям закріпитися в рамках дотримання в своїй роботі міжнародних стандартів доброчесності, прозорості та підзвітності. Спільні проекти також можуть бути ефективними механізмами для передачі норм, цінностей і методів роботи. Прозорість поліпшується паралельно з тим, як вільні інформаційні потоки «західної» частини проекту змушують місцевих партнерів дотримуватися такого ж рівня точності й чесності у своїх доповідях (див., наприклад, Вставку 22.4).

3. Будівництво «мостів»: Часто в національних інституціях або десь у суспільстві можна виявити таких прихильників у питанні виховання доброчесності, які мають і мотивацію, і ресурси (принаймні – людські ресурси). Водночас, можливість їх зустріти може бути обмеженою через саму природу бюрократії або суспільства, наприклад, через взаємну підозру чи бюрократичні правила. Міжнародні організації можуть допомогти зустрітися цим природним союзникам, поділитися знаннями і досвідом, сформувати довіру один до одного та працювати разом у спільній мережі. У цьому випадку буде корисним, якщо національний уряд заохочуватиме міжнародні організації до створення широких зв'язків з суспільством і в державному апараті для того, щоб мати відповідну інформацію й контакти, які дозволять грати паритетно. Міжнародні організації, як правило, мають хороші можливості для організації спілкування офіційних осіб держави і неурядових експертів чи активістів з їхніми іноземними партнерами. Розвиток подібних мереж може мати суттєвий результат принаймні у двох напрямках: 1) створення професійного та добре інтегрованого експертного класу; 2) зростання професійного рівня громадянського суспільства, який дозволить здійснювати більш ефективний незалежний моніторинг.

Вставка 22.4. Програма професійного розвитку НАТО-Україна

У 2005 році НАТО й Україна спільно визнали недостатнім рівень підготовки цивільних державних службовців міністерства оборони та інших структур оборонного сектору. Військові офіцери мали можливість регулярно отримувати підготовку як вдома, так і за кордоном, але їх цивільні колеги таких можливостей не мали. Це протиріччя вело до розбалансування системи управління обороною.

Україна звернулася за допомогою у вирішенні цієї проблеми й у 2006 році НАТО й Україна створили спільну Програму професійного розвитку для підготовки цивільних службовців з сектора оборони. Було визначено відповідальних з української сторони і створено спільну керівну групу програми на базі Офісу зв'язку НАТО в Україні. Представника Департаменту кадрової політики Міністерства оборони було визначено для допомоги менеджеру програми з числа співробітників офісу. На додаток, було створено робочу групу з питань менеджменту програми, до якої увійшли представники від основних зацікавлених сторін: керівництва Міністерства оборони (помічник міністра), Департаменту кадрової політики Міністерства оборони, Апарату Ради національної безпеки і оборони, а також спеціальний оборонний радник від Сполученого Королівства (Сполучене Королівство стало провідною державою у цьому проекті), голова

Офісу зв'язку НАТО та менеджер програми. Від імені цієї менеджерської групи менеджер програми 3-4 рази на рік робив доповідь для основних спонсорів програми у Брюсселі.

Підготовка й освіта за кордоном є важливою частиною програми і на момент написання цього розділу понад 1000 українських офіційних осіб отримали підготовку на відповідних курсах. Однак, з огляду на високу зацікавленість у таких курсах, виник суттєвий корупційний ризик (який був розповсюджений у внутрішній системі відбору). І для того, щоб дотриматися стандартів доброчесності у цій програмі, було запроваджено такі процедури:

1. Потреба у підготовці подавалася за рік до початку курсів на основі трансформаційних цілей Міністерства оборони. Це допомагало забезпечити мотивацію менеджерів до направлення тих людей, які дійсно могли добре виконувати поставлені завдання.

2. Потреби у підготовці мали відповідати вибраним курсам та перспективам потенційних кандидатів (або принаймні їх займаним посадам) і відображені у річному плані, який затверджує вище керівництво міністерства.

3. Менеджери програми, у взаємодії з Міністерством оборони, визначають резерв можливих кандидатів з огляду на відповідність вимогам та посаді, а також за умови погодження керівництва. Відібрані кандидати беруть участь у конкурсі, проходять мовне тестування, а також інтерв'ю у менеджерській групі, до якої входять представники України і НАТО.

4. Спільний менеджмент і відповідальність за результати, а також регулярні звіти для вищого керівництва заінтересованих сторін.

Стосовно останнього пункту необхідно зазначити, що підтримка з боку керівництва міністерства мала вирішальне значення для забезпечення доброчесності рішень, що приймалися, й у декількох випадках винних осіб було суворо покарано за спроби обійти встановлені правила.

У всіх зазначених випадках ключовим чинником є люди: їх відданість справі, порядність та добрі стосунки з партнерами є визначальними для успіху справи. Для міжнародних організацій першочерговою передумовою успіху є наявність національного партнера, здатного терпляче працювати з усіма заінтересованими відомствами, допомагати у врегулюванні протиріч, виступати з принципових позицій, коли це потрібно, та, в решті решт, брати на себе відповідальність за процес, спочатку разом, а потім, в ідеалі, поступово перебирати зростаючу відповідальність за виконання проекту. Тому можна допустити шанс того, що читач, який зміг дочитати так далеко у цьому компендіумі, може виявитися якраз придатною для цього особою.

Частина IV. Імплементація програм виховання доброчесності

Ця заключна частина компендіуму розглядає практичні аспекти формування і виконання програм виховання доброчесності у сфері оборони. У цьому контексті важливе значення має визнання наявності культурних особливостей конкретної оборонної структури в конкретній країні та посилення тих рис організаційної культури, які сприяють вихованню індивідуальної та організаційної доброчесності і стримують корупційні прояви. Такий передовий досвід пізніше можна буде поширити на інші органи державної влади в країні.

Розділ 23
Практична робота над змінами

Не існує двох оборонних організацій, які мають однакові проблеми з доброчесністю та корупцією. Відповідно, ініціативи з питань виховання доброчесності можуть потребувати різного рівня і типу зусиль – від незначних вдосконалень у певних процедурах, наприклад, підвищення прозорості і доброчесності у процедурі закупівель, до всеохоплюючих заходів реформування, метою яких є підвищення рівня доброчесності у всіх основних процедурах оборонної економіки, а також зміна загального ставлення і поведінки персоналу організації.

У цьому розділі основну увагу зосереджено на останньому випадку. Він має дати читачеві розуміння суті уже випробуваних менеджерських стратегій і процесів, з усіма їх перевагами і недоліками. В ньому також дається інформація стосовно можливих несподіванок і пропозиції щодо подолання викликів формування й виконання програм виховання доброчесності.

Загальна структура таких програм ґрунтується на твердому розумінні поточного стану й динаміки змін доброчесності у сфері оборони та корупційних ризиків, а також на належному рівні відповідальності і стратегічному баченні.

Оцінка поточного стану

Часто трапляється так, що керівництво оборонних організацій ініціює зміни під тиском парламентських слухань або громадської думки стосовно якогось конкретного випадку або корупційної поведінки. Доволі часто вони хочуть продемонструвати швидкі результати, в той час, як запропоновані зміни можуть мати лише тимчасовий позитивний ефект, якщо взагалі його матимуть.

Тому потрібно наполегливо рекомендувати спочатку оцінити стан доброчесності, перш ніж починати формувати програму виховання доброчесності. Така оцінка повинна в результаті дати:

- ідентифікацію сфер оборонної діяльності з найвищим рівнем корупційного ризику;
- розуміння причин дійсної або потенційної корупційної поведінки;
- розуміння ставлення військових та іншого персоналу міністерства оборони, а також суспільства до проблем корупційної поведінки;
- оцінку готовності сприйняти заходи виховання доброчесності та необхідні зміни.

На додаток, всеохоплюючий і добре структурований огляд стану доброчесності у сфері оборони за участі всіх заінтересованих сторін сприятиме:

- розумінню причинно-наслідкових зв'язків і взаємозалежності між заходами виховання доброчесності та різними варіантами передового досвіду;
- формуванню бачення того, хто може бути вірогідними союзниками або опонентами заходів виховання доброчесності;
- виявленню потенційних активістів у справі запровадження змін.

Вставка 23.1. Інструмент самооцінки НАТО

Співробітництво між країнами-членами НАТО і Трансперенсі Інтернешнел, лідером якого виступає Польща, дало можливість створити Процес самооцінки з питань доброчесності у сфері оборони і безпеки. Він доступний будь-якій країні, що бажає ним скористатися, і це вже зробили декілька країн-членів НАТО та країн-партнерів.

Процес самооцінки з питань доброчесності дає можливість країнам скористатися готовою формулою для перевірки можливостей власних систем виховання доброчесності. Він приділяє основну увагу тим відповідям, які дають міністерство оборони та інші опитувані під час детального опитування, а пізніше вивчаються зовнішньою експертною групою оцінки. Запитальник звертається до основних складових системи доброчесності в оборонному відомстві та відповідних корупційних ризиків у кожній із них. Він також пропонує рекомендації стосовно того, як заповнювати запитальник і як діяти далі, плануючи реформи та втілюючи плани виховання доброчесності й зниження рівня корупції. Група експертів оцінює відповіді й організує відвідування, щоб на місці оцінити основні сильні й слабкі сторони процесу, а також готує ряд висновків і пропозицій для подальших дій. Процес може бути або одноразовим заходом, або частиною циклу, який повторюється декілька разів.

Процес самооцінки з питань доброчесності включає такі питання:

1. Демократичний контроль і співробітництво.
2. Національне антикорупційне законодавство та політика.
3. Антикорупційна політика у сфері безпеки і оборони.
4. Персонал – поведінка, політика, підготовка, дисципліна.

5. Планування й бюджетування.
6. Операції.
7. Закупівлі.
8. Зв'язки з оборонними компаніями та іншими постачальниками.
9. Специфічні питання для конкретної держави.

Джерело: Mark Pyman, Building Integrity and Reducing Corruption Risk in Defence Establishments: Ten Practical Reforms, з передмовою Лорда Джорджа Робертсона (UK: Transparency International, April 2009); Повне описання запитальника можна знайти за адресою: Transparency International, "Integrity Self-Assessment Process", http://www.defenceagainstcorruption.org/tools-and-techniques/ selfassessment-tool.

Для оцінки поточного стану використовують дослідження внутрішніх і публічних джерел, сфокусовані дискусії з людьми з середини оборонного відомства та з-поза його меж, структуровані запитальники та інтерв'ю. Створення інструменту самооцінки та запитальника НАТО – тобто перших результатів у рамках ініціативи НАТО з виховання доброчесності – може бути особливо корисним під час цих попередніх оцінок. У Вставці 23.1 дається попередня інформація та посилання щодо цих інструментів, доступних будь-якій країні чи оборонному відомству, що прийняли антикорупційний порядок денний.

Формування міцної коаліції

Серед найбільш корисних результатів оцінки ризиків корупції у сфері оборони є такий, як створення відчуття терміновості. *(Ця думка, а також декілька наступних грунтуються на публікації: John P. Kotter, Leading Change*

(Boston: Harvard Business School Press, 1996). Цілеспрямовані інтерв'ю і дослідження часто приносять переконливі свідчення та якісні дані, які можуть збуджувати реакцію людей, що без цього знання могли бути байдужими до проблеми корупції або до її ширшого й довгострокового впливу на результати діяльності організації та її етос.

Це також створює атмосферу, в якій легше забезпечити залучення вищого керівництва, як військового, так і цивільного, у всіх підрозділах оборонної структури, а не лише у тих, що вважаються найбільш слабкими проти корупції.

Важливо вже на цьому етапі визначитися стосовно того, хто буде головним провідником змін, а також почати шукати підтримки з боку представників парламенту й громадянського суспільства, зокрема, оборонних мозкових трестів, груп активістів та ЗМІ. Представники постачальників оборонних технологій, продуктів і послуг також можуть розглядатися серед потенційних союзників ініціатив, направлених на боротьбу з корупцією.

Будь-яка спроба виховання доброчесності й зниження рівня корупції у сфері оборони може бути успішною, у першу чергу, за умови наявності міцної коаліції у складі політичного керівництва міністерства оборони, вищого військового керівництва, парламентарів та провідних представників громадянського суспільства, за підтримки основних постачальників оборонної продукції і використовуючи переваги постійного моніторингу з боку незалежних, критичних ЗМІ.

Формування та доведення до учасників задуму і стратегії

Складні проекти на зразок виховання доброчесності та скорочення рівня корупції у сфері оборони потребують людей із стратегічним баченням, які можуть також успішно працювати над його втіленням і для цього передавати іншим причетним у зрозумілій формі свої бачення і стратегію.

Вставка 23.2. Формулювання бачення

Берт Нанус визначає бачення таким, що виглядає як «реалістичне, правдиве, привабливе майбутнє організації». Це коротке визначення підкреслює наступні ключові характеристики формулювання бачення:

- Реалістичність: бачення має ґрунтуватися на реаліях, щоб відповідати потребам організації.

- Правдивість: бачення повинне викликати довіру, щоб воно сприймалося. У кого бачення повинне викликати довіру? Це найбільш важливо для членів організації. Якщо у членів організації це бачення не буде викликати довіру, то воно не буде ними сприйматися і мети не буде досягнуто. Одна з цілей бачення – надихнути членів організації на досягнення належного рівня доброчесності, а також вказати на мету і напрям роботи для всіх співробітників. Бачення, що не викликає довіри, не дозволить досягти жодної з цілей.

- Привабливість: якщо бачення має надихати членів організації, то воно повинне бути привабливим. Люди повинні хотіти бути частиною цього майбутнього, яке пропонується для організації.

- Майбутнє: бачення стосується не того, що існує зараз, – воно стосується майбутнього. Бачення говорить про те, де ми хочемо бути у цьому майбутньому.

Таке формулювання бачення може забезпечити вирішення ряду питань життєдіяльності організації:

- Сприяє формуванню в людей відданості справі й заряджає їх. Однією з головних причин того, що потрібно мати бачення для організації, є його мотиваційний ефект. Коли люди бачать, що організація віддана своєму баченню, – і це полягає у чомусь більшому, ніж просто наявність формулювання бачення – то це генерує ентузіазм стосовно курсу, яким треба пройти, і підтримує в людях відданість своїй роботі щодо досягнення цього бачення.

- Додає сенсу в життя членів організації. Бачення дозволяє людям відчувати себе частиною чогось більшого й таким чином наповнює змістом їхню роботу. Правильне бачення означатиме щось важливе для кожного в організації, якщо вони бачитимуть реальний внесок своєї роботи у здійснення цього бачення.

- Встановлює високий рівень стандартів. Бачення слугує дуже важливій функції встановлення передових стандартів. Фактично, добре бачення у своїй суті повністю зорієнтоване на найвищі стандарти. Якщо бачення не передбачає жагу до найкращого, то в ньому не буде достатньої мотивації або захоплення для будь-кого в цій організації. Найвищі стандарти також можуть виступати постійною метою і стимулювати програми виховання доброчесності, а також служити мірою оцінки значимості організації.

- З'єднує сьогоднішній день з майбутнім. Правильне бачення переносить організацію з сьогоднішнього дня і зосереджує її увагу на майбутньому. Дуже легко бути завантаженим поточними кризами й подіями та втратити відчуття напряму подальшого руху. Добре бачення може дати орієнтир у майбутнє і забезпечити позитивне цілеспрямування.

Джерела: *Bert Nanus, Visionary Leadership: Creating a Compelling Sense of Direction for Your Organization (San Francisco: Jossey-Bass, 1992); "Strategic Vision", in Strategic Leadership and Decision Making (Washington, DC: National Defense University Press, 1997).*

По-перше, керівництво оборонної структури має правильно сформулювати проблему виховання доброчесності та основні підходи до суттєвого скорочення потенціалу корупції в оборонній сфері. Завузьке обмеження рамок проблеми навряд чи дозволить мати довгостроковий і системний вплив на стан корупції. З іншого боку, зашироко розсунуті рамки, наприклад «розбудова демократичних і підзвітних оборонних інституцій», може призвести до втрати фокусу і не дозволить створити необхідний для забезпечення успіху рівень підтримки. Розділ 2 цього компендіуму дає приклад того, як сама проблема та підхід до її розв'язання можуть бути раціонально обмежені.

Після цього настає черга оформлення перспективного бачення (концепції, задуму, прим. перекладача). Воно повинно бути сформульовано з урахування конкретики кожної країни та її оборонного відомства, а також відповідати реальному стану доброчесності та рівню загрози корупції. Дехто хоче бачити корумпованих посадових осіб ув'язненими у в'язниці, в той час, як інші будуть закликати до «вільного від корупції» оборонного відомства. Не існує загальноприйнятого рецепту того, як саме потрібно формулювати бачення, однак, воно повинно бути конструктивним і давати картину майбутнього хай нелегкого, але досяжного. Вставка 23.2 дає рекомендації щодо формування й формулювання бачення.

Коллінз та Поррас (Collins and Porras) пропонують дещо інший підхід до того, як визначати бачення. Концептуально вони розглядають його як таке, що має дві головні складові: керівну філософію та реалістичний імідж, де керівна філософія визначається як «система фунда-

ментальних мотиваційних оцінок, принципів, цінностей і традицій», що походять від ключових переконань, цінностей і цілей організації, а імідж забезпечується яскравим описанням місії організації. *(James C. Collins and Jerry I. Porras, "Organizational Vision and Visionary Organizations", California Management Review 34:1 (Fall 1991), 30–52.)*

Одного лише бачення недостатньо для того, щоб просувати організацію від її сьогоднішнього стану до бажаного майбутнього. Цей перехід від сучасного до майбутнього вимагає стратегії, яка буде адекватною організаційній культурі і здійсненною. Вставка 23.3 пропонує огляд стратегій менеджменту загальних змін та чинників, які обумовлюють вибір тієї чи іншої стратегії виховання доброчесності.

Вставка 23.3. Стратегії менеджменту загальних змін

Досвідчені практики з питань менеджменту організаційних змін визначають чотири основні стратегії менеджменту змін, головний зміст яких полягає в наступному:

1. Емпірично-раціональна: люди по своїй суті раціональні і будуть переслідувати свої власні інтереси з того моменту, коли вони їх усвідомлять. Зміни ґрунтуються на передачі інформації та заохоченнях.

2. Нормативно-(пере)навчальна: люди є соціальними істотами і будуть дотримуватися культурних норм і цінностей. Зміни ґрунтуються на перевизначенні та переосмисленні існуючих норм і цінностей та створенні стимулів дотримуватися нових.

3. Владно-залякувальна: люди загалом покірні і будуть в основному робити те, що їм скажуть або можуть змусити робити. Зміни ґрунтуються на застосуванні владних повноважень і накладенні санкцій.

4. Середовищно-адаптивна: люди не хочуть втрат і різких радикальних змін, але вони з готовністю пристосовуються до нових обставин. Зміни ґрунтуються на створенні нової організації та переведенні людей зі старої в нову.

Не існує однієї найкращої стратегії змін; лідери змін найкращий результат отримують у разі суміші стратегій. Вибір однієї або більше з цих стратегій залежить від ряду чинників, зокрема:

- Суть і масштаб. Цей чинник може змінюватися від незначного, наприклад, пристосування процесу всередині підрозділу, до повного трансформування всієї організації. Чим значніші суть і масштаби змін, тим більш вірогідним буде суміш стратегій, у якій владно-залякувальна стратегія відіграватиме центральну роль.

- Рівень протидії. Сильний опір закликає до поєднання владно-залякувальної та середовищно-адаптивної стратегій. Слабкий спротив або погодження свідчать на користь комбінації емпірично-раціональної та нормативно-(пере)навчальної стратегій.

- Цільова аудиторія. Велика кількість населення – це аргумент на користь суміші всіх чотирьох стратегій, так би мовити «для всіх потроху».

- Ставки. Високі ставки потребують суміші усіх чотирьох стратегій. Коли ставки дуже високі, тоді нічого не можна залишати на відкуп випадковості.

- Часові обмеження. Короткі терміни свідчать на користь владно-залякувальної стратегії. На довші терміни доцільно використати суміш емпірико-раціональної, нормативно-(пере)навчальної та середовищно-адаптивної стратегій.

- Наявний досвід. Маючи адекватний експертний рівень з питань менеджменту змін, доцільно вибирати якусь суміш зазначених вище стратегій. Якщо ж цього немає, то це говорить на користь владно-залякувальної стратегії.

- Залежність. Це класична ситуація двосічного меча. Якщо організація залежить від своїх людей, то менеджерська спроможність командувати чи вимагати є обмеженою. І навпаки, якщо люди залежать від організації, то їхня здатність ставати в опозицію або чинити опір є обмеженою. Взаємозалежність майже завжди сигналізує про необхідність певного рівня переговорів.

У підсумку, люди управляють організаційними змінами майже таким самим чином, як би вони управляли будь-чим іншим, що має швидкоплинний, нестійкий або хаотичний характер – насправді, вони не зовсім навіть управляють змінами, вони скоріше долають наслідки цих змін.

Тому цей процес є справою настільки ж лідерських якостей, наскільки й менеджерського вміння.

Джерела: *Fred Nickols, Change Management 101: A Primer (Distance Consulting, 2007), www. managementhelp.org/misc/reqs-for-successful-change.pdf; Стратегії адаптовано з: Warren G. Bennis, Kenneth D. Benne and Robert Chin, eds., The Planning of Change, 2nd Edition (NY: Holt, Rinehart and Winston, 1969).*

І бачення, і стратегія, спрямовані на виховання доброчесності й скорочення корупційних ризиків, мають бути зрозуміло доведені до всіх членів оборонної структури. Оскільки міцні антикорупційні коаліції включають учасників з-поза меж оборонної структури, то бачення і стратегічний підхід також мають бути доведені до більш широкого кола сектору оборони і безпеки, а також до громадськості.

Принципова важливість комунікації у справі менеджменту змін неодноразово підкреслювалася з того часу, коли це питання було вперше сформульоване та отримало розвиток. Ясність, послідовність і постійність комунікації дають найбільший ефект для досягнення успіху. Комунікація повинна бути двосторонньою, тобто керівники й активісти змін повинні й слухати так само, як і говорити. Сприяння і спонсорство також важливі у питанні комунікації. *(Gregory R. Guy and Karen V. Beaman, Eff ecting Change in Business Enterprises: Current Trends in ChangeManagement, Research Repot R-1371-05-RR (NY: The Conference Board, 2005).)*

Роль міністра оборони як провідного комунікатора є чіткою ознакою особистої відданості і, само по собі, посилає потужний сигнал всім членам оборонної структури й суспільства, зокрема, коли міністр передає свої власні бачення пріоритетів і досягнень у справі покращення стану доброчесності у сфері оборони.

Для імплементації стратегії виховання доброчесності активісти змін можуть вирішити за доцільне розробити менш формальний план чи програму. У цьому питанні досвід суттєво відрізняється. Робилися спроби використовувати формалізовані програми з чітко визначеними цілями, зі створенням відповідальних організацій, що мають чіткий мандат, наприклад, антикорупційні бюро у міністерствах оборони Польщі та України, а також із виділенням визначених ресурсів. Чи це є ефективним підходом, чи ні – потрібно ще подивитися.

Яким би не був рівень формалізації, ці та інші ознаки програмного менеджменту, такі, як особиста й організаційна відданість справі, регулярні доповіді стану прогресивних змін за визначеними індикаторами прогресу і результатів, притаманні більшості зусиль з виховання доброчесності.

Інші риси добре спланованого, системного процесу організаційних змін представлені у Вставці 23.4.

Вставка 23.4. Приклад спланованого, системного процесу змін

Типовий спланований, системний (і систематичний) процес організаційного розвитку часто відбувається згідно із загальним підходом, описаним нижче. Буває багато варіацій, наприклад, об'єднання різних етапів та/або розділення певних етапів на декілька фаз. У цьому прикладі мається на увазі, і це зазвичай так і буває, що керівництво організації ставить завдання відповідальному за зміни – у складі організації або з-поза її меж – як саме здійснювати менеджмент процесу змін.

Етап 1: З'ясування очікувань і ролей у процесі змін

Цей етап іноді називають «початковим» або «вхідним». Це той етап, на якому починаються стосунки між вами (першим відповідальним за зміни) та вашими замовниками, незалежно від того, чи ви є зовнішнім, чи внутрішнім консультантом. Експерти вважають, що цей етап

є одним з найбільш важливих (якщо не найважливішим) етапів у процесі змін в організації. Результати діяльності на цьому етапі закладають підвалини успішних організаційних змін. Якість виконання завдань цього етапу зазвичай є принциповим показником того, як ініціатива розвиватиметься далі. Цей етап дає відповіді на ряд запитань, зокрема, таких як:

- Хто є дійсним замовником?
- Як визначається «успіх»?
- Як оцінити готовність замовника до змін?

Етап 2: Спільна розвідка для визначення пріоритетів змін

Чим тісніше співробітництво відповідального за зміни з членами організації замовника, тим більша вірогідність успіху зусиль, направлених на зміни. Відповідальний за зміни і замовник працюють разом протягом цього етапу для того, щоб краще зрозуміти загальну пріоритетність реформаторських зусиль та як ефективніше їх докласти. Це може бути або головною проблемою в організації, або захоплюючим баченням, якого треба досягти. Разом ви зберете інформацію, проаналізуєте її з метою визначення ключових моментів та висновків, а потім на основі цього запропонуєте рекомендації.

Іноді збір інформації відбувається дуже швидко, наприклад, з метою підготовки до одного засідання учасників планування. В інших випадках потрібно буває докласти набагато більших зусиль, зокрема, для оцінки стану всієї організації та розробки плану змін, проведення інтерв'ю, тощо.

Іноді дехто применшує важливість або взагалі пропускає цей важливий етап спільної розвідки і починає менеджмент змін з доведення амбіційного і всеохоплюючого бачення майбутніх змін.

Багато хто вважає, що починати проект організаційних змін без повноцінної оцінки (проведення розвідки) поточної ситуації в організації замовника просто неетично. Фокусуючи більшу частину уваги на доповіді про необхідність досягнення амбітного бачення, без проведення хоча б окремих ретельних досліджень, часто буває шкідливим для справи і ви можете закінчити тим, що матимете справу з симптомами поточних проблем, а не з їх корінням. Так само, проект може перетворитися у спроби реалізувати прекрасне бачення, яке спершу виглядає захоплюючим і мотивуючим для багатьох, однак, пізніше виявляється абсолютно нереалістичним, особливо тоді, коли перед організацією вже стоять декілька важливих завдань.

Цей етап включає:

- формування керівного ядра проекту;
- спільне планування й збір необхідної інформації;
- спільну підготовку ключових висновків;
- спільне поширення рекомендацій в організації замовника.

Етап 3: Спільне планування діяльності з розвитку організації та врахування пріоритетів

На цьому етапі основна увага зосереджується на подальшому доопрацюванні рекомендацій стосовно того, як краще забезпечити пріоритети, а також розробці на їхній основі окремих планів дій. Різні плани іноді інтегрують у єдиний план менеджменту змін. Таким чином, початкова діяльність на цьому етапі часто перетинається і є продовженням дій кінця попередньо розглянутого етапу. Взяті разом плани дій тепер можуть забезпечити чітке й реалістичне бачення змін. Вони формують «дорожню карту» для менеджменту переходу від поточного стану до бажаного майбутнього стану.

Цей етап також включає:

- вибір заходів розвитку організації на основі результатів попереднього аналізу;
- спільну розробку планів дій;
- спільну розробку планів оцінки;
- спільну розробку планів вивчення.

Етап 4: Менеджмент змін та спільні оцінки

На цьому етапі основна увага приділяється підтримці й оцінюванню заходів змін, включаючи дії у відповідь на спротив, який з'являється з боку членів організації, а іноді й з боку відповідальних за зміни. Цей етап включає:

- зв'язок зі споживачем стосовно планів дій;
- виконання споживачем планів дій;
- підтримку споживачем разом з відповідальним менеджером стабільного темпу змін;
- спільне оцінювання виконання заходів проекту й бажаних результатів.

Джерело: *Carter McNamara, "Organizational Change and Development", Free Management Library, www.managementhelp.org/org_chng/org_chng.htm#anchor556912.*

Не принижуючи специфіки кожного конкретного випадку, досвідчені професіонали з питань менеджменту змін виділяють такі спільні ознаки успішних ініціатив з менеджменту змін:

- увага до прибирання з дороги перепон на шляху змін;
- демонстрація успіху на якомога ранніх етапах;
- використання перших успіхів для розвитку змін;
- закріплення нових запроваджених підходів у організаційну культуру. *(Kotter, Leading Change.)*

Прибрати перепони на шляху змін

Як правило, дуже рідко можна зустріти відкритий опір ініціативам з будівництва доброчесності.

Частіше можна спостерігати випадки прихованої опозиції, а також перепони різного характеру.

Активістам змін рекомендується прибирати з дороги такі перешкоди для прогресивних змін, звертаючи при цьому особливу увагу на: *(Jeanne Dininni, "Guide to Management Theory of John Kotter", Work.com How-to Guides to Your Business (2009).*

1. Незадоволення, зумовлене зарозумілістю.
2. Реакцію самозахисту, спричинену страхом.
3. Несприйняття, спричинене страхом.
4. Коливання, спричинені зневірою.

Добра стратегія комунікації із залученням більшості вищого керівництва оборонного відомства є потужним інструментом прибирання перепон на шляху змін. Більш специфічні підходи можна буде застосовувати, коли справа торкається конкретної цільової групи.

Посилення повноважень членів організації є ще одним інструментом, за допомогою якого можна усувати перешкоди. Воно передбачає цілий ряд способів – від простого заохочення людей доповідати про конфлікти інтересів та інші корупційні ризики, через делегування відповідальності й ресурсів, заради досягнення конкретних цілей доброчесності, до призначення членів організації виконувати роль керівників груп, які мають завдання контролювати стан справ і всі процеси у цілих сферах значного корупційного ризику, наприклад, у оборонних закупівлях, офсетах тощо.

Наділення повноваженнями може бути особливо ефективним, коли вище керівництво оборонного відомства привселюдно визнає досягнення особистостей і груп, а також продемонструє тривалу відданість справі виховання доброчесності.

Нарешті, усунення всіх перепон як передумови для вжиття заходів не є обов'язковим.

Керівники й особи, відповідальні за зміни, можуть вирішити усунути окремі потенційні перепони, зменшити вплив інших та навіть ігнорувати деякі бар'єри, якщо вони вірять, що позитивні очікування від змін є більш важливими, ніж обструкції, що можуть іноді з'являтися.

Демонструвати швидкі досягнення

Важливе значення має питання підтримання темпу змін та переконання скептиків у серйозності намірів і здійсненності стратегії виховання доброчесності. Відповідно, відповідальні за зміни особи перебуватимуть під тиском щодо початку імплементації стратегій або програм виховання доброчесності одразу ж після їх оголошення і від них очікуватимуть демонстрації того, що програми працюють.

Досвідчені практики дають пораду відповідальним за зміни (і керівникам оборонного відомства також) стосовно того, що недоцільно втягуватися у деструктивні дії, такі, як зосередження надмірної уваги на деталях, негативне реагування на критику, упередженість висновків та мікроменеджмент співробітників, тому що всі такі прояви знижують шанси на успіх.

«Швидкі досягнення» не обов'язково означають суттєві зміни у порядку діяльності організації.

Вони також можуть не мати значного впливу на кількісні показники корупційного ризику. Те, що дійсно є важливим, так це демонстрація відданості на практиці, демонстрація рішучості у відповідь на спротив, а також підтвердження дієвості антикорупційної стратегії, яка ґрунтується на вихованні доброчес-

ності, підвищенні рівня прозорості та покращенні звітності.

Наприклад, коли застосовується незалежний моніторинг випадків оборонних закупівель як частина стратегії виховання доброчесності (див., зокрема, Розділ 7 цього компендіуму), то необхідно чекати випадків великих за обсягом закупівель, наприклад, закупівель літаків або кораблів. Реалістичність цього підходу може бути випробувана у менших за обсягом випадках – можливо навіть вартістю в декілька сотень тисяч євро – бо це також буде відмічено у профільних ЗМІ та неурядових організаціях. Успіх такого нетрадиційного підходу сприятиме підтриманню темпу реформ та, з іншого боку, допоможе відповідальним за зміни побачити майбутні перепони і відповідно уточнити стратегію виховання доброчесності.

Використання початкових успіхів для прискорення змін

Початкові успіхи у вихованні доброчесності та зниженні ризиків корупції хоч і можуть бути несуттєвими, однак у кожному випадку їх потрібно закріплювати, а потім розширювати для запровадження більш бажаних змін.

Водночас, обриси бажаного майбутнього також можуть змінюватися. Виконання програм виховання доброчесності – це динамічний процес, який передбачає постійне врахування й упровадження уроків отриманого досвіду. Тому може трапитися так, що основні параметри ініціативи пізніше виявляться занадто амбіційними або, навпаки, недостатньо глибокими.

Окрім цього, менеджмент змін, як і будь-який інший менеджмент, повинен передбачати можливість уточнення планів або прийняття змін на основі отриманого досвіду. У повній відповідності з відомим військовим афоризмом про те, що «жодний план бойових дій не може вціліти після контакту з ворогом», *(Це висловлювання приписують фельдмаршалу Гельмуту фон Мольтке (Field Marshall Helmuth von Moltke) (1800-1891). Якщо фразу перекласти з німецької мови, то вона виглядатиме наступним чином: "Жодний план операції не може напевне передбачити далі, ніж відбудеться перша сутичка з головними силами ворога")* жодний план реформ не може вціліти після сутичок з реаліями повсякденної імплементації. *(Guy and Beaman, Eff ecting Change in Business Enterprises.)*

Однак, існують і певні постійно діючі чинники, які обумовлюють успішну імплементацію, зокрема, потрібно:

- помічати й відзначати успіхи в роботі по досягненню цілей програми виховання доброчесності;
- продовжувати пояснювати суть і причини змін;
- забезпечити зворотній зв'язок від персоналу оборонного відомства та заінтересованих зовнішніх представників;
- продовжувати зусилля з визначення потенційного опору та його причин;
- визначати й інвестувати у знання і вміння, які потрібні для прискорення та інституціалізації виховання доброчесності.

Упроваджувати нові підходи у організаційну культуру

На заключному етапі, згідно з твердженням Коттера щодо менеджменту змін, потрібно забезпечити, щоб бажані зміни, а у цьому випадку мова йде про виховання доброчесності й зниження рівня корупції, стали незворотними.

Цього можна досягти, коли нові стандарти і (що більш важливо) нова поведінка, що характеризується доброчесністю та нетерпимістю до корупції, стануть частиною загального ставлення, переконань і традицій оборонної структури та зовнішніх заінтересованих представників, зокрема, парламенту, оборонної промисловості, ЗМІ, тощо.

Підготовка майбутніх лідерів оборонного сектору має важливе значення для інституціалізації такої організаційної культури. Вставка 23.5 описує підготовчий курс, який НАТО пропонує в рамках Ініціативи з будування цілісності та виховання доброчесності для майбутніх лідерів сектору оборони у НАТО та країнах-партнерах. Вставка 23.6 пропонує приклад використання рольової гри, яку було успішно використано у підготовці лідерів наступного покоління у секторі оборони та безпеки у багатьох країнах-партнерах.

Підсумовуючи сказане, можна стверджувати, що компендіум дає багато прикладів того, що потрібно робити з конкретними проявами корупції та практичними підходами до покращення доброчесності. Цей розділ розглядав національні процеси менеджменту змін. Однак, не існує заздалегідь повністю готового варіанту вирішення проблеми для кожного оборонного відомства. Застосування зазначених тут ідей та передового досвіду до конкретної ситуації потребує розвиненої уяви і стратегічного мислення, лідерських якостей та наполегливості, які поєднуються із застосуванням принципів ефективного врядування у сфері оборони.

Вставка 23.5. Навчальний курс НАТО з питань будування цілісності та виховання доброчесності

Ініціатива з підготовки майбутніх лідерів оборонних відомств (провідну роль в якій відіграє Сполучене Королівство) дала можливість провести п'ятиденний курс підготовки з питань виховання доброчесності в рамках Ініціативи НАТО з будування цілісності та виховання доброчесності.

Цей курс було створено для міністерств оборони, персоналу збройних сил та призначено для посадовців рівня полковника. Лекції проводяться персоналом Оборонної академії Сполученого Королівства, Женевського центру політики безпеки, НАТО, Оборонного коледжу Швеції, Транспаренсі Інтернешнел, а також іншими запрошеними лекторами від різних урядових і міжнародних інституцій.

Зміст лекцій включає типи корупції та слабкі місця у секторі оборони, питання корупції під час військових операцій та миротворчих місій, а також роль ЗМІ й менеджерські аспекти стосовно боротьби з корупцією. Лекції приділяють першочергову увагу практичним питанням, різним прикладам національного досвіду та ролі офіцерів і цивільних середньої ланки в успішному проведенні змін.

Головними цілями цього навчального модулю є допомогти учасникам:

1. Зрозуміти суть корупції взагалі.
2. Зрозуміти суть корупції у секторі оборони.
3. Зрозуміти шляхи успішного виховання доброчесності та боротьби з корупцією на політичному рівні, виконавчому рівні та в індивідуальній поведінці.
4. Переконатися у тому, що питання може бути вирішено.

Учасники курсу також досліджують концепції прозорості та ефективного врядування, а також підходи до взаємодії з оборонними постачальниками і громадянським суспільством.

Вони обмінюються особистим досвідом і вчаться один в одного. Найважливішим етапом курсу є підготовка кожним слухачем особисто презентації на тему: «Що я робитиму для виховання доброчесності».

Перший пілотний курс було проведено у липні 2008 року в Оборонній академії Сполученого Королівства. Його учасниками стали вісімнадцять представників з України, Грузії, Азербайджану, Вірменії, Румунії, Албанії, Боснії-Герцеговини, Чорногорії, Польщі, Сполученого Королівства, Норвегії та Швейцарії.

Станом на початок 2010 року цей курс відвідали учасники з понад 20 країн у Школі НАТО в Обераммергау, Навчальному центрі миротворчих операцій у Сараєво та Національній академії оборони в Києві. Він був з ентузіазмом прийнятий близько 30 військовими і цивільними високого рангу, при цьому до 15 додаткових лекторів та міжнародних експертів з питань боротьби з корупцією брали участь у кожному з курсів.

Джерело: *Навчальний курс НАТО з питань будування цілісності та виховання доброчесності (NATO Building Integrity Training Course): http://www.defenceagainstcorruption.org/tools-and-techniques/ training-module.*

Вставка 23.6. Рольові ігри – важливі інструменти навчання

В якості інструменту політичних реформ навчальні курси повинні отримати повну підтримку органів влади, залучати необхідних осіб і покращити їхні знання та вміння, а також їхнє ставлення до справи. Водночас, впливати на людське ставлення ніколи не було легкою справою, оскільки в цьому доводиться торкатися глибоко прихованого і навіть підсвідомого. Якщо ми хочемо, щоб слухачі змінили свої ставлення, ми спочатку повинні дати їм можливість усвідомити природу

цих ставлень. Після цього нам треба допомогти їм з'ясувати, на чому саме ґрунтуються певні ставлення. Наприкінці ми повинні заохотити їх спробувати й попрактикувати різні ставлення. Нічого із зазначеного не можна досягти звичними методами навчання.

Марно сподіватися, що це можна зробити за допомогою презентації з використанням слайдів.

А тепер спробуйте уявити рольову гру, в якій опозиційний член парламенту критикує плани закупівлі реактивних винищувачів, а міністр оборони аргументовано пояснює, навіщо повітряним силам потрібен цей літак. У реальному житті один з виконавців насправді бере участь в опозиційній політичній діяльності, в той час, як інший учасник гри працює в оборонному відомстві, але у цій грі кожен з них грає роль когось іншого. Таким чином вони ставлять себе на місце інших людей і в результаті вони краще бачать свою власну роль через призму цієї гри. Окрім цього, виконавці мають можливість відчути аспекти питання закупівель у драматичний, безпосередній, майже реальний спосіб. Це може служити доповненням до того, що вони попередньо вивчили під час більш традиційних занять.

Наприкінці першого дня один з слухачів, коментуючи ввідну сесію про демократичне врядування, заявив: «Я знаю цей матеріал. Нам давали його в університеті.» На другий день він грав провідну роль у рольовій грі. Після цього він сказав: «Вчора я думав, що я розумію все, про що ви говорите, однак це було не так. ТЕПЕР я це розумію.»

Під час рольової гри інший учасник, який грав роль члена парламентської слідчої комісії, сказав інструктору гри, що він збирається повернутися додому. Захоплений зненацька інструктор запитав про причину такого рішення. «Я не можу стерпіти такого зухвалого міністра оборони», – відповів учасник. Інструктор вказав, що це гра, хоча вона дійсно була дуже реалістичною і учасник з цим погодився. Інструктор також зауважив, що така зарозуміла поведінка була потрібна, щоб досягти навчальних цілей, і учасник з цим також погодився. «Це настільки реалістично, що я не можу цього стерпіти, незважаючи на те, що ми багато чому вчимося», – сказав він і поїхав додому.

На підведенні підсумків після закінчення рольової гри учасник, який виконував роль корумпованого міністра, сказав: «Мені дуже не сподобався характер, який я грав. Я ніколи не думав, що можу зіграти такого злодія.» А інший виконавець, якого спитали, чи його правдива гра була завдяки його обдарованості, чи його надихнули обставини гри, відповів: «Я жахливий актор. Це була саме гра.»

Іншим позитивним наслідком рольової гри є те, що вона допомагає зміцнити колектив, а це пізніше створить переваги під час роботи в класі. Нарешті, збудження від гри також має довготривалий ефект. Через багато часу, коли слухачі забудуть про інструкторів і про курс, вони будуть пам'ятати гру. Інструктор може лише забезпечити певні реалістичні умови, однак ми твердо переконані, що рольова гра є невід'ємною частиною «передового досвіду» у навчальних програмах, які прагнуть досягти більшого, ніж просто передати знання та покращити вміння.

Джерела: *Sami Faltas, Centre for European Security Studies, www.cess.org; Sami Faltas and Merijn Hartog, "The Starlink Program: Training for Security Sector Reform in Armenia, Azerbaijan, Georgia, Moldova, and Ukraine", Connections: The Quarterly Journal, 7:2 (Summer 2008), 81–91.*

Розділ 24

Врахування культурної специфіки конкретної організації під час реалізації заходів з будування цілісності й виховання доброчесності

Успіх діяльності з розробки і реалізації ефективної стратегії та програм будування цілісності і виховання доброчесності залежить від того, чи знайде в них відображення специфічний вплив конкретних організаційних культур та чи будуть вони сприяти посиленню тих особливостей організаційної культури, які культивують цілісність і доброчесність поведінки на індивідуальному й організаційному рівнях і, у той же час, запобігають проявам корупційної поведінки.

Важливість культурного контексту

У багатьох державах посткомуністичного світу, державах, що розвиваються, і державах, що тільки знаходяться на шляху до реальної демократії, корупція досягла таких масштабів та завдала такої великої шкоди цим державам з точки зору їх політичного й економічного розвитку, а також інтересів їх суспільств та рядових громадян, що є всі підстави розглядати корупцію у цих державах як загрозу для їх національної безпеки.1 Кожний новий уряд цих країн часто приходить до влади під антикорупційними гаслами та завдяки обіцянкам «зламати хребет корупції». Проте на практиці нікому з них так і не вдалося знайти ефективного рішення цієї проблеми, хоча б з точки зору захисту інтересів національної безпеки. По закінченні терміну перебування при владі будь-якого з урядів, об'єктивні дані та соціологічні опитування свідчать, що рівень корупції не тільки не зменшився, але, навпаки, її тенета поширились іще більше та укорінились іще глибше в усі сфери діяльності держави і суспільства. Наслідками такої ситуації є підрив довіри людей до демократії, послаблення тканини суспільства, поглиблення напруги у суспільстві та створення нових каналів для здійснення олігархічними й кримінальними колами безпосереднього чи прихованого впливу на структури і механізми державного управління. У таких умовах корупція перетворюється на загрозу інтересам національної безпеки, а боротьба з корупцією стає найголовнішим завданням політики національної безпеки держави.

Проблема корупції значною мірою стосується й оборонного сектору та починає займати все більше місця у діяльності оборонної організації. З одного боку, збройні сили, за результатами останніх соціологічних досліджень Трансперенсі Інтернешнел, входять до трійки найменш корумпованих державних інституцій, що само по собі обумовлює високий рівень довіри суспільства до оборонних організацій. Але, з іншого боку, оборона

традиційно була і залишається закритою сферою для нагляду й контролю з боку суспільства і навіть парламенту. Таким чином, за умов відсутності ефективних механізмів демократичного нагляду й контролю, а також культури, де таке явище, як корупція, вважається недопустимим і неприйнятним, сфера оборони легко перетворюється на осередок брудних інтересів та на експериментальний майданчик, де створюються і проходять апробацію нові корупційні схеми.

У попередніх главах ми розглядали приклади позитивного досвіду з підвищення стандартів цілісності й доброчесності оборонної організації, процесів та поведінки членів оборонної організації, а також зниження корупційних ризиків в оборонному секторі. Однак, намагання застосувати такий позитивний досвід по відношенню до деяких країн часто не дають бажаного ефекту та, незалежно від щирості намірів, тільки імітують відповідні моделі діяльності, які просто не відповідають місцевим умовам.

Невдале застосування позитивного досвіду по відношенню до деяких країн пояснюється, у тому числі, фундаментальними культурними відмінностями. У багатьох випадках застосування конкретної моделі діяльності, яка успішно імітується на початкових етапах діяльності, у кінцевому рахунку закінчується повним провалом або дає результати, що не відповідають визначеним цілям відповідної діяльності. Це відбувається тоді, коли зразкові моделі діяльності починають впроваджуватись без урахування специфічних особливостей конкретної країни, її традицій, досвіду, а також організаційної та людської культури.

Тобто це означає, що впровадження будь-якої зразкової моделі не матиме бажаного ефекту, якщо при цьому не буде враховуватись культурний контекст країни, де вона впроваджується.

При реалізації зовнішніх моделей і позитивної практики необхідно адекватно перекласти їх на мову відповідної країни, що дасть змогу врахувати місцеві особливості, традиції, тенденції та стереотипи. Також необхідно переконати-

ся в тому, що зразкові моделі та позитивна практика, які рекомендуються ззовні, отримують належну інтерпретацію та не спотворюються місцевими настроями чи ідеологією.

Чому люди чи організації відрізняються одні від одних?

Культурні відмінності проявляються щонайменше на семи різних рівнях:

1. Відмінності між Заходом та Сходом, наприклад, між індивідуалістичними суспільствами західного світу та колективістськими суспільствами Сходу. Крім того, існують і перехідні типи суспільств по лінії індивідуалізм/колективізм, до яких можна віднести деякі слов'янські та/чи православні країни.

2. Відмінності між країнами, що знаходяться по обидві сторони Північної Атлантики (США і Канада, з одного боку, та країни Західної Європи, з іншого боку). Між цими двома суспільствами немає радикальних відмінностей, але після закінчення епохи «холодної війни» деякі з їх стратегічних поглядів та пріоритетів почали розвиватись у дещо відмінних напрямках.

3. Відмінності між країнами Західної та Східної Європи, які раніше розділяла Берлінська стіна, а згодом – віртуальна «залізна завіса». Незважаючи на дуже активні, а у багатьох випадках колосальні зусилля, яких докладали і продовжують докладати країни колишнього соціалістичного табору для повернення у русло європейської демократії, політичні і соціальні стереотипи попередніх часів встигли пустити глибоке коріння у свідомості, поглядах та світовідчутті громадян східноєвропейських країн та їх суспільств в цілому. Після падіння у 1989 році Берлінської стіни, країни Східної Європи почали активно запроваджувати у себе (у більшості випадків без попереднього критичного аналізу) норми, процедури та правила своїх колег із Західної Європи. Проте реалії сучасного життя свідчать, що західноєвропейські суспільства намагаються не помічати відмінностей у конкретних моделях поведінки, зокрема, на рівні спілкування та самоорганізації місцевих спільнот; соціальних контактів; стосунків між батьками й дітьми та між сусідами; турботи про старих та зв'язків поколінь; моделей взаємодопомоги в родині та між друзями; а також моделей поступового просування вперед невеликими кроками заради досягнення спільних цілей. Існують і поведінкові моделі неформальних спільнот, які розташовані на рівні між окремою особистістю – соціальне та функціональне значення якої у тоталітарних суспільствах було зведено до мінімуму – та державою, яка намагалася регулювати і втручатися в усі сфери життя суспільства.

4. Відмінності між інститутами державної влади та рядовими громадянами країни.

У суспільствах східноєвропейських країн ставлення громадян до влади існує у двох вимірах. З одного боку, громадяни в усьому покладаються на владу, вважаючи, що саме влада повинна займатись вирішенням якщо не усіх, то хоча б найважливіших з їх проблем.

Влада є активним суб'єктом державного управління, у той час, як рядові громадяни є пасивними об'єктами. З іншого боку, рядові громадяни добре бачать і розуміють, що ті, хто при владі, мають власні цілі й амбіції, наприклад у сфері підвищення рівня свого життя та отримання привілеїв і пільг, які дає перебування при владі.

5. Відмінності між силовими структурами (тобто тими, які мають законне право на застосування сили) та іншими державними інституціями. Силові структури продовжують вважати себе структурами вищого порядку, заради яких суспільство має терпіти злидні й обмеження, тому що «той, хто не хоче годувати власну армію, буде годувати чужу». Тобто це фактично означає, що адекватне ресурсне забезпечення діяльності силових структур має бути гарантованим, незалежно від рівня ефективності та продуктивності використання цих ресурсів.

Мілітаризована ідеологія намагається підтримувати у суспільстві уявлення про те, що національна безпека є священною, що захист суверенітету та незалежності держави навіть за відсутності адекватних загроз є важкою й у той же час найважливішою справою держави та її збройних сил, які мають забезпечуватись усім необхідним, навіть за рахунок фінансування таких важливих для суспільства сфер діяльності, як охорона здоров'я, освіта, наука чи захист навколишнього середовища. Вставка 24.1 наводить два із загальноприйнятих тлумачень терміну «організаційна культура» та її складових.

6. Відмінності між оборонним сектором та іншими силовими структурами держави. Дуже багато представників оборонного сектору продовжують вважати, що – на відміну від, наприклад, органів охорони правопорядку чи цивільної оборони – військова організація не зобов'язана звітувати перед суспільством про результати та наслідки своєї діяльності.

7. Відмінності між цивільним і військовим персоналом збройних сил. Держави Центральної та Східної Європи досягли значного прогресу у впровадженні демократичних цивільно-військових стосунків. Тим не менше, військові та цивільні представники збройних сил дуже рідко вважають себе єдиною командою, коли йдеться про боротьбу з корупцією, а, навпаки, часто обвинувачують одні одних у порушенні стандартів цілісності й доброчесності.

Відмінності національної та організаційної культури на усіх цих рівнях вимагають особливої уваги та зусиль з точки зору будування цілісності й виховання доброчесності, належної підготовки перекладачів і контактних осіб та створення систем профілактики і раннього попередження порушень, які будуть органічно інтегровані у загальну антикорупційну діяльність. У залежності від обраних критеріїв та параметрів, відмінностям на кожному з цих семи рівнів буде приділятись увага відповідно до їх пріоритетності, а потім будуть здійснюватись цілеспрямовані заходи з метою мінімізації негативного впливу «відхилень» при впровадженні позитивного досвіду та підвищення до максимально можливого рівня їх позитивного впливу.

Культурні нашарування та сприйняття корупції

При розгляді різних ініціатив і проектів з будування цілісності й виховання доброчесності місцеві активісти, які будуть опікуватись впровадженням змін, мають враховувати стереотипи та ставлення до корупції, що формувались внаслідок впливу культурних нашарувань чотирьох основних видів. Це особливо важливо у випадку, якщо вони бажають пов'язати конкретні поведінкові моделі з культурними особливостями, що впливають на ставлення до корупції та її сприйняття, і якщо вони бажають упровадити в організації робочу стратегію боротьби з корупцією та змінити ставлення членів організації до цього явища.

Вставка 24.1. Про тлумачення терміну «організаційна культура»

Одне із загальноприйнятих тлумачень терміну «організаційна культура» визначає її як:

- Комплекс уявлень, цінностей і норм, разом з такими символами, як драматичні події та особистості, які відображають унікальний характер організації та складають загальний контекст, у якому організація здійснює свою діяльність.

Інші провідні вчені, які спеціалізуються на дослідженнях організаційної культури, віддають перевагу більш загальному визначенню, що враховує чинники, які фактично є частиною корпоративної культури:

- Сукупність спільних базових поглядів і уявлень, які сформувались в організації в процесі та у результаті вирішення її проблем, пов'язаних із зовнішньою адаптацією та внутрішньою інтеграцією, та які виявились достатньо дієвими для того, щоб бути визнаними ефективними і, відповідно, для того, щоб культивуватись серед нових членів як належний спосіб сприйняття, мислення та відчуття по відношенню до цих проблем.

Ці два визначення майже нічим не відрізняються за змістом. Іншими словами, коли організації з часом розвиваються, вони весь час змушені вирішувати дві головні проблеми – це інтеграція окремих індивідів в єдине й ефективне ціле та ефективна адаптація до зовнішнього середовища, яка дозволить організації вижити та ефективно працювати. У міру того, як організації шукають і знаходять рішення цих двох головних проблем, вони здійснюють процес «колективного навчання». У результаті цього процесу створюється комплекс спіль-

них поглядів і уявлень, який, по суті, і формує організаційну культуру.

Організаційна культура може складатись з таких елементів:

- задекларовані та незадекларовані цінності;
- писані і неписані правила поведінки членів організації;
- традиції, звичаї та ритуали;
- розповіді, реальні чи вигадані, про історію організації;
- організаційний сленг – мова, яка зазвичай використовується при спілкуванні всередині організації та у розмовах про організацію;
- клімат – відчуття, що виникають при спостереженні процесів взаємодії членів організації з іншими членами організації, зовнішніми суб'єктами та оточуючим середовищем, у тому числі з фізичним простором, який вони займають;
- образи і символи, які можуть існувати на підсвідомому рівні, але їх присутність може відчуватись одразу в декількох елементах організаційної культури.

Джерела: *Гарет Морган, Образи організації (Gareth Morgan, Images of Organization (Thousand Oaks, Каліфорнія: Sage Publications, 1997 р.); Едгар Шейн, «Організаційна культура та лідерство» у класичній теорії організації, під редакцією Джея Шафрітца та Дж. Стівена Отта (Edgar Schein, "Organizational Culture and Leadership" in Classics of Organization Theory, Jay Shafritz and J.Steven Ott, eds) (Fort Worth: Harcourt College Publishers, 2001 р.); Організаційна культура», www.soi.org/reading/change/culture.shtml.*

Історичні нашарування, які є результатом впливу різних чинників, що формувались у процесі довгого історичного і культурного розвитку. Впродовж багатьох століть своєї історії народи Центральної та Східної Європи перебували під гнітом різних імперій, центри яких знаходились далеко за межами територій цих народів. Люди постійно контактували з традиціями і законами, які формували в них сприйняття корупційної поведінки як головної чи навіть єдиної умови спілкування з представниками імперій на місцях. Наприклад, за часів Оттоманської імперії, це була єдина можлива модель поведінки, оскільки у ті часи корупція була синонімом влади та формою її існування. Такий віковий історичний досвід не міг не залишити свого довготривалого й глибокого сліду у стереотипних уявленнях та поведінкових моделях на рівні як суспільств, так і окремих особистостей. Цей слід, у свою чергу, впливав на вибір життєвої стратегії людей і суспільства в цілому. Виправлення такого роду «відхилень», завдяки яким корупція сприймається як нормальне явище, вимагає великого терпіння і наполегливості. Головними інструментами подолання таких «відхилень» мають бути так звані «м'які» заходи, як-от: діяльність активістів (лідерство), освіта й виховання, впровадження кодексів етичної поведінки та особистий приклад. Відповідно, перевага має надаватись позитивним заходам, тобто не боротьбі з корупційною поведінкою як такою, а створенню стимулів етичної поведінки. З цієї точки зору, велика відповідальність лежить на політичному керівництві країни, оскільки кожний черговий випадок корупції тільки підсилює у свідомості суспільства уявлення про корупцію як про цілком природне, а отже й нормальне явище.

Нашарування епохи комуністичного правління складаються з наслідків та різних факторів впливу, сформованих у часи існування тоталітарних однопартійних систем радянського типу, де майже не існувало такого поняття, як «приватна власність», де управління економікою здійснювалось командно-адміністративними методами і де права людини були дуже обмеженими. Комуністична система створила власну модель корупції, яка існувала завдяки тотальному дефіциту товарів, послуг та можливостей, отримання яких було можливим тільки через застосування «альтернативних», а по суті корупційних шляхів. Різноманітні монополії час від часу відтворювали самі себе і, як логічний результат менталітету суспільства та неприродної монополії однієї єдиної політичної партії, завжди залишались при владі.

Стереотипні уявлення про корупцію, що виникли внаслідок перебування народів у складі імперій, можуть розглядатись як такі, що були нав'язані ззовні, а також як символи домінування іноземної сили. На відміну від них, корупція у тоталітарному суспільстві має внутрішнє походження. У таких суспільствах корупційна практика створювалась самим суспільством. Тобто корупційна поведінка є добровільною і свідомою, та є результатом особистого вибору, який робиться з метою досягнення певних цілей, не обов'язково пов'язаних з виживанням. Ось чому корупція у тоталітарному суспільстві є певною мірою більш шкідливою для суспільства та його окремих представників. Це проявляється в уявленнях типу «я засуджую корупційну поведінку інших, але сам при нагоді не збираюсь відмовлятися від такої можливості». З корупційними поглядами, що сформувались в епоху тоталітаризму, необхідно боротися не час від часу, а системно і впродовж довгого часу. Найбільш дієвими у даному випадку видаються заходи негативного спрямування – нагляд і контроль, переслідування з боку правоохоронних органів, звільнення та інші види покарань.

Перехідні нашарування складаються з наслідків і чинників впливу, що сформувались на перехідному етапі від тоталітаризму до демократії, тобто впродовж відносно короткого та дуже динамічного періоду історії окремих країн. Вважається, що це період, у який відбувається перехід від тоталітарного суспільства до суспільства, що функціонує відповідно до принципів демократії і ліберально-ринкової економіки. Проте цей період часто характеризується таким негативним явищем, як брутальний перерозподіл власності, де етика і моральність, а також такі поняття, як чесність, справедливість і законність відкидаються на задній план окремими обмеженими колами осіб у їх активному прагненні до самозбагачення за рахунок решти суспільства. Майже усі члени суспільства змогли скористатися плодами свободи і демократії, але кількість постраждалих у результаті перерозподілу власності значно перевищує кількість тих, хто залишився у виграші. Подібні явища негативно впливають на сприйняття суспільством реформ перехідного періоду та підривають довіру людей до процесів демократизації. З цим пов'язане і таке явище, як поширення серед широких верств суспільства переважного уявлення про владу і політику як шляхів до власного збагачення та посилення власного впливу.

За таких умов корупція сприймається як ефективна, прагматична і раціональна модель поведінки, яка повністю відповідає змісту й природі перехідного періоду. Таким чином, якщо «історичні» та «комуністичні» культурні нашарування приводять до формування уявлень про корупцію, які можна визначити як «реактивні», тобто як необхідність прийняття «правил гри», у даному випадку спостерігається якісна відмінність у ставленні до корупції, яке стає «проактивним». Це означає, що корупція відтворює сама себе, і що вона все частіше набуває «інноваційного» характеру, а участь у корупційних діях пояснюється тим, що «усі так роблять» і що у цьому немає нічого надзвичайного (тобто це є нормальним).

Боротьба з поглядами та моделями поведінки, які утворились на перехідному етапі демократичного розвитку, вимагає системних багатовекторних зусиль у політичному, законодавчому, інституційному та дисциплінарному напрямках. Це вимагає чіткого політичного бачення, політичної волі та щирого бажання побороти корупцію, модернізації законодавства у відповідності з вимогами сучасності, спільних зусиль різних відомств та організацій, а також жорстких санкцій до порушників, не виключаючи кримінальної відповідальності і позбавлення волі.

«Імплантоване» нашарування складається з наслідків та різних чинників впливу, сформованих у процесі реалізації моделей і практик, запропонованих ззовні. «Імплантовані» моделі та практики знаходять своє відображення у свідомості людей, змінюючи цінності, норми, правила та міжлюдські стосунки. Сьогодні у глобальному масштабі поширюється модель ліберальної економіки, яка будується на принципах вільного ринку й приватної власності. Але світову економіку, через її масштаби, важко контролювати, а міжнародні корпорації при здійсненні своєї діяльності, як правило, не враховують інтересів суспільств та держав, де розташовані їх потужності. Надмір-

на увага до приватних і корпоративних інтересів може негативно впливати на морально-етичні погляди суспільств і людей, а також сприяти поширенню корупції та інших порушень, пов'язаних із зловживанням владними повноваженнями. Бувають випадки, коли міжнародні корпорації використовують корупційні канали з метою виходу на нові ринки, у тому числі й у сфері торгівлі озброєннями. Негативний вплив на місцеві політичні та економічні еліти, а також на органи державного управління значно посилюється, коли до подібної практики вдаються західні компанії. Факти корупційної поведінки з боку західних компаній та усвідомлення того, що «вони поводяться так само», часто приводять до ліквідації останніх етичних перешкод на шляху до корупції.

Підходи до вирішення проблем адаптації до культурної специфіки

Коли ми говоримо про необхідність адаптації антикорупційних програм до культурної специфіки окремого конкретного суспільства, таку діяльність необхідно розглядати у чотирьох головних вимірах:

На міжнародному рівні

Стратегія діяльності на цьому рівні складається з наступних базових елементів:

- розробка міжнародних стандартів цілісності й доброчесності та використання еталонних показників для визначення «найкращих» стандартів і прикладів позитивного досвіду, які будуть рекомендуватись для впровадження в інших країнах. При цьому має забезпечуватись певний баланс між загальною ефективністю «найкращих» стандартів і прикладів позитивного досвіду, з одного боку, та необхідністю їх адаптації до конкретного культурного середовища, з іншого боку;

- уникнення практики використання подвійних стандартів по відношенню до урядів і компаній держав, де впроваджується позитивний досвід, та західних держав;

запровадження практики оцінки й порівняння підприємств з точки зору стандартів цілісності й доброчесності та складання відповідних рейтингів; відмова від започаткування контрактних стосунків з підприємствами, які не відображені у відповідному рейтингу або мають низький рейтинг за показниками цілісності й доброчесності;

- запровадження й поширення практики укладення «пактів про доброчесність» та антикорупційних союзів у сфері оборонних закупівель;

- поширення на сферу оборони вимог Світового банку щодо обліку державних витрат та фінансової звітності (PEFA);

- суворе дотримання антикорупційних вимог у сфері закупівель;

- прозорість військового бюджету та запровадження антикорупційних стратегій в оборонному секторі;

- значне збільшення фінансування програм з підготовки, освіти, виховання та наукових досліджень у сфері будування цілісності, виховання доброчесності й підвищення ефективності державного управління.

Крім того, у більшості з країн, що останнім часом приєдналися до НАТО та Європейського Союзу, а також в інших державах, що обрали шлях реформ, таке поняття, як «цілісність і доброчесність» не завжди чітко сприймається як протилежність корупції. Тому, окрім заходів з будування цілісності та виховання доброчесності, боротьба з корупцією має постійно перебувати на першому плані як стратегічний пріоритет, щоб питання корупції не опинились у тіні балачок про «цілісність і доброчесність».

На національному рівні

Стратегії на цьому рівні мають максимально враховувати культурні та інші особливості конкретної країни. Тобто стратегії мають будуватись на точному діагнозі «захворювання», а не тільки на його симптомах.

У багатьох країнах необхідність виживання в умовах драматичних подій створює ситуацію, коли адаптація запропонованих норм і практики тільки імітується, а насправді ніякої реальної адаптації не відбувається. Тобто зовнішньому спостерігачеві може здаватись, що запропоновані ззовні норми і стандарти активно сприймаються і підтримуються, хоча у дійсності національна специфіка фактично залишається «за кадром». Органи державної влади і політики можуть говорити й демонструвати Європі те, що, з їх точки зору, вона хоче від них почути і побачити.

Саме таку ситуацію можна бачити на прикладі боротьби з корупцією. Для боротьби з корупцією іноді створюються безліч стратегій, законів та відповідних органів, а європейські організації отримують бездоганні звіти, незалежно від практичних результатів антикорупційної діяльності, навіть якщо реального прогресу у цій сфері не відбувається. За цих умов такі живучі явища, як кумівство, стосунки за принципом «ти – мені, я – тобі» та фаворитизм (просування по службі завдяки особистим зв'язкам, а не діловим якостям) легко відтворюють самі себе та отримують подальше поширення.

З іншого боку, у місцевих культурах часто превалює так званий «високий контекст» (коли велика увага приділяється символам, які іноді можуть бути навіть більш важливими, ніж явища чи речі, які вони символізують; висококонтекстна культура характерна для таких країн, як Росія, а також африканських, азіатських та арабських країн – прим. перекладача): тобто усе, що говориться або робиться, необхідно інтерпретувати у конкретному культурному контексті та в залежності від конкретних обставин. У таких культурах дуже велике, якщо не найбільше, значення мають статус, повага та репутація, які необхідно підтримувати за будь-яких обставин.

Поведінкові моделі у висококонтекстних культурах відрізняються високою адаптивністю, коли поведінка модифікується відповідно до зовнішніх умов і характеризується намаганням уникати прямої конфронтації та не демонструвати відкрито свого справжнього ставлення до того чи іншого питання.

На цьому рівні, європейські або євроатлантичні організації мають запровадити практику публічного оголошення та засудження держав, не здатних ефективно боротися з корупцією. Це має бути практика відкритого і дозованого тиску, поєднаного з постійним зовнішнім наглядом і моніторингом, періодичними ревізіями і санкціями та демонстраціями «неповної довіри». У той же час, для того, щоб місцеві еліти не втрачали довіри суспільства та не відокремлювались від нього, необхідно періодично відзначати їх успіхи та досягнення у впровадженні позитивного досвіду.

Така стратегія має передбачати заходи з метою:

- запровадження механізмів систематичного раннього попередження та запобігання порушенням;

- створення перешкод на шляху до корупції системного характеру;

- запровадження дисциплінарних санкцій за корупційну поведінку, у тому числі у вигляді повернення державі грошових коштів чи майна, отриманих незаконним шляхом;

- упровадження сучасних методів аудиту діяльності в усіх сферах державного/публічного сектору;

- створення нової, синхронізованої політичної й економічної культури.

На рівні сектору безпеки

Стратегії на цьому рівні обмежуються культурною специфікою сектору оборони конкретної країни, особливо, коли мова йде про традиційну та іноді дуже потужну культуру закритого, «секретного» характеру.

Навіть у найбільш прозорій формі правління – демократії – існують окремі сфери, де прозорість обмежується, наприклад, коли йдеться про питання національної безпеки. Тим не менше, держави, що знаходяться на перехідному етапі демократичного розвитку, мають визнати необхідність впровадження практики парламентського нагляду й контролю за сферою безпеки. Замість культури закритості і секретності має бути створена культура прозорості і відповідальності, що повинна поступово трансформуватись у культуру прозорості і звітності, яка, у свою чергу, стане запобіжником корупції, а також запобіжником неефективного державного управління.

Стратегії на цьому рівні мають вирішувати три завдання у сфері підвищення ефективності й результативності державного управління, будування цілісності та виховання доброчесної поведінки:

Першим завданням повинно бути формування розуміння того, що сфера національної безпеки більше не має того ексклюзивного статусу «недоторканості», який вона мала у тоталітарному суспільстві. На початку 21-го століття та у відповідності з принципами демократії, сектор безпеки має конкурувати за правові, людські, фінансові, матеріальні та інші ресурси на рівні з іншими сферами державної діяльності, наприклад, освітою, охороною здоров'я, соціальним забезпеченням і т. ін.

Друге завдання полягає у формуванні розуміння того, що сфера національної безпеки не є сферою гарантованого ресурсного забезпечення за будь-яких умов і будь-якого рівня загроз, і що витрати на утримання сектору безпеки не є обов'язковими. Замість такого підходу має запроваджуватись новий підхід, згідно з яким витрати на сферу безпеки розглядаються як інвестиції, які мають приносити добрі прибутки та служити на користь суспільству, а не бути для нього лише важким тягарем.

Третє завдання полягає у формуванні розуміння того, що національна безпека та сектор безпеки не є питаннями тільки обмеженого й ізольованого від рядових громадян кола експертів. Навпаки, це сфера діяльності, яка належить до сфери законних інтересів кожного громадянина та представляє ці інтереси.

Стратегії на цьому рівні спрямовані на підвищення прозорості силових структур та створення нормативно-правової бази, відповідно до якої інформація, створена органами державного управління або в інтересах цих органів, має бути максимально публічною і відкритою.

Ці стратегії мають вирішувати й таку проблему, як страх перед силовими структурами, який сформувався у свідомості народів за довгі роки їх історії. З цієї точки зору, у рамках стратегій з підвищення стандартів прозорості бажано було б передбачити такі допоміжні інструменти, як «гарячі лінії», поштові скриньки, громадські приймальні й т. ін., які б працювали на умовах гарантованої анонімності.

На рівні сектору оборони

Стратегії на цьому рівні мають розроблятися з урахуванням особливостей оборонного сектору конкретної країни, традиційної для країни моделі цивільно-військових стосунків, статусу й іміджу збройних сил у суспільстві та ролі військово-промислового комплексу в житті країни.

У країнах колишнього соціалістичного табору військова організація була «державою в державі» завдяки унікальній ролі, яка відводилась збройним силам у системі безпеки цих країн. У перехідний період суспільству продовжують часто нагадувати про цей особливий статус військової організації. Військові дуже часто пояснюють втрату довіри з боку суспільства і скорочення їх бюджету, «тиском ззовні» та зрадою політиків. Таким чином, питання військової організації набуває політичного характеру, коли збройні сили намагаються здійснювати непрямий тиск на виборних посадових осіб або безпосередньо впливати на політичні процеси, розглядаючи при цьому цивільний контроль за їх діяльністю як зазіхання на їх інтереси.

За часів правління комуністичних партій оборона також вважалася справою надзвичайної державної важливості. Навіть через багато років після падіння комуністичних режимів, збройні сили та сфера оборони досі користуються статусом привілейованих отримувачів бюджетних коштів, поглинаючи левову частку державних ресурсів, часто за рахунок інших важливих сфер державної діяльності. Такі умови створювали сприятливе середовище для функціонування різного роду корупційних схем та неефективних методів управління.

Крім того, багато з колишніх соціалістичних держав підтримували окремі режими силою зброї – через продаж озброєнь чи так звану «братерську допомогу» – практику, яка сьогодні підпадає під обмеження міжнародного законодавства. На цьому фоні сформувалася культура таємних і нелегальних операцій, які часто здійснювались за підтримки розвідувальних служб.

Усі ці явища, які дійшли до сьогоднішнього дня з комуністичних часів, ще й досі не подолані; вони заважають суспільству здійснювати нагляд і контроль за збройними силами, їх бюджетом та діяльністю.

Ситуація ускладнювалась і постійними змінами уряду, кожна з яких приводила до зростання напруги всередині керівництва оборонної організації. На посади міністрів оборони іноді призначались особи, які не мали необхідної професійної кваліфікації й досвіду, але уміло користувалися можливостями міністерства оборони з метою власного збагачення та збагачення своїх політичних союзників. Міністри, разом з вищим керівництвом міністерств оборони, часто займались не питаннями формування й реалізації відповідних напрямків державної політики, а корупційною діяльністю, перетворюючи міністерства оборони на розсадники корупції.

Стратегії на цьому рівні повинні мати багатовекторне спрямування та охоплювати широке коло проблем, питань і недоліків. Незважаючи на зусилля, які докладають міністерства оборони для впровадження систем планування, програмування та бюджетування на зразок американської системи PPBS, сучасних механізмів планування сил і засобів та принципів менеджменту оборонних закупівель й т. ін., у багатьох випадках спостерігається відсутність серйозного глибокого підходу та реальної зацікавленості в успішності відповідних реформ, а загальні принципи діяльності залишаються на рівні радянських часів. Найбільше занепокоєння викликають проблеми, пов'язані з плануванням, реалізацією програм і звітуванням у сфері фінансового та матеріально-технічного забезпечення діяльності військової організації, де й досі превалюють старі підходи, побудовані на управлінні бюджетними надходженнями й видатками, а не управлінні результатами, і де рішення дуже часто приймаються не відповідно до визначених стратегічних цілей і завдань, а виходячи з сьогохвилинних потреб чи інтересів.

Надмірна централізація процесів прийняття рішень у сфері розподілу ресурсів, у поєднанні з низьким рівнем прозорості, створюють сприятливе середовище для безконтрольності і корупції. Ситуація ускладнюється ще більше у випадку відсутності парламентського нагляду й контролю за процесами оборонних закупівель та утилізації надлишкового військового майна чи інфраструктури, відсутності можливостей для відкритого публічного обговорення реальних оборонних потреб та їх бюджетного забезпечення, а також відсутності ефективного контролю й аудиту бюджетних витрат. У державах посткомуністичного простору майже неможливо знайти прикладів об'єктивних оцінок результативності бюджетних витрат з точки зору їх впливу на стан оборони і національної безпеки.

Однак у деяких країнах можна спостерігати й ознаки певного прогресу. Наприклад, при перевірці діяльності Міністерства оборони у 2007 році Державне контрольно-ревізійне управління Болгарії оцінювало не тільки відповідність бюджетних витрат вимогам законодавства, але й ефективність їх використання по відношенню до отриманих результатів.

У підготовленому за результатами перевірки звіті Контрольно-ревізійне управління вказувало на відсутність стратегічних документів, де були б чітко визначені реалістичні цілі й завдання та параметри вимірювання їх ефективності/результативності, а також відсутність чітко визначених оборонних потреб. Звіт також констатує існування у міністерстві оборони занадто громіздкої і складної системи менеджменту, яка складається аж з п'яти рівнів, а також відсутність чіткого розподілу функцій і повноважень, коли за планування, розробку і реалізацію напрямків діяльності та за аналіз/оцінку програм і бюджетів відповідають занадто багато працівників.

У таких зауваженнях не було б нічого дивного чи надзвичайного, коли б йшлося про країну з усталеними і добре розвиненими механізмами державного

управління у сфері оборони. Але для даного культурного середовища, враховуючи його певні специфічні особливості, такі зміни, з точки зору деяких експертів, можна вважати дійсно революційними. Інші приклади цілісності діяльності на різних рівнях наведені у тексті Вставки 24.2.

Вставка 24.2. Зміцнення цілісності у сфері оборони однієї з посткомуністичних країн

Досвід Болгарії дає нам декілька прикладів успішних реформ, побудованих на зміцненні цілісності діяльності на самих різних рівнях – політичному, міжнародному, на рівні реалізації стратегічних концепцій та рівні будівництва інституційної інфраструктури.

Оборонна доктрина в редакції 1999 року: приклад цілісності на політичному рівні Уряд, що прийшов до влади у Болгарії в результаті виборів 1997 року, поставив перед собою чітке завдання: привести країну до членства в НАТО і Європейському Союзі. У відповідності з цією стратегією парламент країни затвердив нову редакцію Концепції національної безпеки, а рік потому була затверджена й нова Оборонна доктрина, де Болгарія фактично розглядається як член НАТО і ЄС, і де чітко визначені політичне бачення, стратегія та базові принципи розробки й планування заходів у цьому напрямку. Для затвердження цих важливих документів знадобилося більше року активних зусиль, завдяки яким вдалося розпочати процес реального реформування сектору оборони – попри спротив з боку консервативної частини військового керівництва, яке намагалося підмінити реальні реформи їх замаскованою адаптацією до місцевих умов, та тільки після звільнення з посад деяких членів політичного і військового керівництва держави та призначення на їх місце представників нової формації. Згодом активному реформуванню оборонного сектору сприяли спільні зусилля представників збройних сил і політиків, консультації й поради експертів та відкриті публічні дискусії з відповідних питань. Під час відкритих дискусій, де обговорювалися положення Оборонної доктрини перед її поданням на затвердження парламенту, аргументи деяких консервативно налаштованих представників збройних сил повністю губилися на фоні переконливої аргументації прибічників реформ.

Косовська криза 1999 року: приклад цілісності на міжнародному рівні Криза у Косово дає нам переконливі свідчення важливості і значення цілісності як головної передумови успіху спільної діяльності. По-перше, операція НАТО у Косово була чудовим зразком цілісності діяльності, який дозволив болгарському народові побачити й оцінити значення політичної цілісності на міжнародному рівні. По-друге, той же принцип цілісності був ключовим критерієм, яким керувались різні держави при прийнятті рішень стосовно цього конфлікту, особливо в контексті можливої участі у спільній військовій операції. Рішення уряду Болгарії повністю відповідали положенням Концепції національної безпеки і Оборонної доктрини. Вони створили прецедент застосування базових ідей, які згодом були покладені в основу програми оборонних реформ, що розроблялась якраз у цей період. Узгодженість політичної стратегії і фактичної діяльності стала тим міцним фундаментом, який забезпечив широку підтримку відповідних процесів з боку суспільства та дозволив успішно проводити усі консультації з керівництвом НАТО та окремих держав-членів альянсу. На підтвердження цілісності своєї політики і діяльності Болгарія відхилила прохання керівництва Російської Федерації про надання її повітряного простору для польотів бойових літаків російських ВПС.

План 2004: Цілісність на рівні реалізації Оборонної доктрини Процес розробки програми оборонних реформ, відомої як «План 2004», дуже відрізнявся від аналогічних процесів, що відбувались у Болгарії до 1999 року. По-перше, ця програма базувалась на положеннях Концепції національної безпеки і Оборонної доктрини та розроблялась під чітким керівництвом глави уряду і за активної підтримки президента й парламенту держави. По-друге, вона базувалась на об'єктивному оперативному аналізі різних можливих варіантів структури, чисельності, складу технічного парку та стандартів бойової підготовки, а також можливих оперативних планів збройних сил. По-третє, діяльність з розвитку сил і засобів була узгодженою з програмами освіти, виховання й підготовки особового складу, розвідувальної і контррозвідувальної діяльності, медичного забезпечення, тилового забезпечення, соціальної підтримки, закупівель та наукових досліджень, передачі певних функцій і структур стороннім організаціям, трансформації у цивільні структури військових формувань, підпорядкованих іншим силовим відомствам (не Міністерству оборони) й т. ін. Усі ці заходи здійснювались з використанням ефективних механізмів реалізації та за організаційної підтримки відповідних органів, а їх бюджетне забезпечення планувалося на основі об'єктивних прогнозних розрахунків на період до 2004 року. «План 2004» передбачав не тільки скорочення та реструктуризацію збройних сил, але й заходи зі створення відповідної організаційної інфраструктури і підвищення ефективності усіх процесів за рахунок впровадження Системи планування, програмування і бюджетування (PPBS), реалізації механізмів прозорості, звітності, відповідальності та вимірювання результативності діяльності, а також використання даних оперативних аналізів при прийнятті рішень у сфері оборони.

Оборонний менеджмент, цілісність та будівництво організаційної інфраструктури Реалізація Оборонної доктрини та «Плану 2004» проводилась паралельно із запровадженням механізмів PPBS та здійсненням спеціальних досліджень з питань керівництва і менеджменту оборонної сфери. З 1998 року в Болгарії проводились дослідження з питань цивільно-військових стосунків та парламентського контролю. Після затвердження у 2004 році «Плану 2004» розпочався новий дослідницький проект, який реалізовувався спільно з Управлінням консультаційної та менеджерської діяльності (DCMS) Міністерства оборони Сполученого Королівства і мав на меті подальше офіційне впровадження сучасних методів державного управління й оборонного менеджменту, у тому числі, через зміни положення про Міністерство оборони та зміни і доповнення до Закону «Про оборону». З метою підвищення стандартів прозорості, звітності й відповідальності та вдосконалення спроможностей для вимірювання ефективності/результативності процесів оборонного менеджменту, міністр оборони підписав розпорядження про створення рад з питань програмування, інтеграції і модернізації, які будуть діяти спільно з новоствореними управліннями з питань оборонного планування, євроатлантичної інтеграції та політики у сфері озброєнь, а також новим управлінням планування політики і програм у складі Генерального Штабу збройних сил та аналогічними структурами у складі керівництва окремих видів збройних сил.

На завершення зазначимо, що, оскільки культурні особливості виходять своїми коріннями з глибини історії оборонної організації та її колективного досвіду, зусилля з адаптації та змінення цих особливостей вимагають великих інвестиції часу і ресурсів. З цієї точки зору, дуже бажаною і корисною була б допомога з боку активістів реформ або, іншими словами, агентів змін, які діятимуть зсередини системи. Без такої підтримки учасникам системи буде важко сприймати реалії сектору оборони як речі, які створили вони самі, а також зрозуміти істинний зміст звичайних речей чи явищ, над якими вони раніше ніколи не замислювались або сприймали як належне. З іншого боку, агент змін, який має зовнішнє походження по відношенню до оборонної організації або відповідної країни, повинен добре ознайомитись з особливостями культурної специфіки оборонної організації, з якою він буде працювати. Проект НАТО з будування цілісності і виховання доброчесності, за підтримки пов'язаного з ним Трастового фонду, міг би стати корисним інструментом реформування культурного середовища у секторі оборони і таким чином сприяти підвищенню стандартів прозорості, ефективності та результативності діяльності оборонної організації.

Додаток 1: Вибрані джерела

Офіційні документи:

Конвенція ООН проти корупції (United Nations Convention Against Corruption (2004). www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf. Офіційний переклад також доступний арабською, китайською, французькою, російською та іспанською мовами. www.unodc.org/unodc/en/treaties/CAC/index.html

Кримінальна конвенція Ради Європи про боротьбу з корупцією (Criminal Law Convention on Corruption). Council of Europe, ETS No. 173 (1999). http://conventions.coe.int/treaty/en/treaties/html/173.htm

Цивільна конвенція Ради Європи про боротьбу з корупцією (Civil Law Convention on Corruption)

Council of Europe, ETS No. 174 (1999). http://conventions.coe.int/treaty/en/treaties/html/174.htm

Конвенція Ради Європи про відмивання, пошук, арешт і конфіскацію кримінальних доходів (Convention on Laundering, Search, Seizure and Confi scation of the Proceeds from Crime and on the Financing of Terrorism) Council of Europe (2005) http://conventions.coe.int/Treaty/EN/Treaties/HTML/198.htm

Міжамериканська конвенція про боротьбу з корупцією. (Inter-American Convention Against Corruption). Organization of American States (1996) www.oas.org/juridico/english/Treaties/b-58.html

Міжнародний кодекс поведінки державних посадовців. (International Code of Conduct for Public Offi cials) UN General Assembly Resolution 51/59 (1996). http://www.un.org/documents/ga/res/51/a51r059.htm

Настанови й посібники:

Антикорупційний інструментарій ООН

Глобальна програма проти корупції, Офіс ООН з питань боротьби з наркотиками та злочинністю (UN Anti-Corruption Toolkit, The Global Programme Against Corruption, United Nations Offi ce of Drugs and Crime (3rd edition, 2004)) www.unodc.org/pdf/crime/corruption/toolkit/corruption_un_anti_corruption_toolkit_sep04.pdf

Передовий досвід боротьби з корупцією, ОБСЄ. (Best Practices in Combating Corruption, OSCE (2004)). Оригінал англійською мовою; текст також доступний вірменською, азербайджанською, македонською, російською та сербською мовами. www.osce.org/item/13568.html

Парламентський контроль за сектором безпеки: принципи, механізми і практичні аспекти. Посібник для парламентарів. Міжпарламентський союз та ДКЗС. (Parliamentary Oversight of the Security Sector: Principles, Mechanisms and Practices, IPU-DCAF. Handbook for Parliamentarians (2003)). Оригінал англійською мовою, також доступний у перекладі понад 35 мовами. www.dcaf.ch/publications/kms/details.cfm?lng=en&id=25289&nav1=4

Реформування та врядування у системі безпеки. Серія настанов та довідників Комітету допомоги розвитку ОЕСР (Security System Reform and Governance, OECD DAC Guidelines and Reference Series, Organisation for Economic Co-operation and Development (2005). www.oecd.org/dataoecd/8/39/31785288.pdf

Посібник з реформування системи безпеки: підтримка у сферах безпеки та судової влади

Серія настанов та довідників Комітету допомоги розвитку ОЕСР (Handbook on Security System Reform: Supporting Security and Justice, DAC Guidelines and Reference Series, Organisation for Economic Co-operation and Development (2007) www.oecd.org/dataoecd/43/25/38406485.pdf

Антикорупційний досвід: національна система виховання доброчесності в дії. Транспаренсі Інтернешнел (Anti-Corruption Handbook: National Integrity System in Practice Transparency International, project ACH). www.transparency.org/ policy_research/ach

Антикорупційний довідник простою мовою

Транспаренсі Інтернешнел. (The Anti-Corruption Plain Language Guide, Transparency International (2009). www.transparency.org/content/download/45306/725785/fi le/TI_Plain_Language_Guide_280709.pdf.

Посібник по боротьбі з корупцією

Агентство міжнародної допомоги США, Центр демократії та врядування (A Handbook on Fighting Corruption, USAID Center for Democracy and Governance, February 1999). www.usaid.gov/our_work/democracy_and_governance/publications/pdfs/pnace070.pdf

Виховання доброчесності та зниження ризику корупції в оборонних відомствах: десять практичних реформ. Марк Пайман, Транспаренсі Інтернешнел (Building Integrity and Reducing Corruption Risk in Defence Establishments: Ten Practical Reforms. Mark Pyman, Transparency International (2009) www.defenceagainstcorruption.org/publications

Методології

Інструменти Світового Банку з питань урядування та боротьби з корупцією

Інститут Світового Банку, взаємодіючи з іншими підрозділами Світового Банку, надає підтримку країнам у покращенні врядування та протидії корупції. На основі багатодисциплінарного підходу він застосовує активно-навчальні методи, поєднуючи емпіричні діагностичні дослідження, практичне застосування рекомендацій досліджень, колективні дії та попередження. Він періодично випускає Індикатори врядування у світі (Worldwide Governance Indicators (WGI)) та результати діагностики по окремих країнах. Такий комплексний підхід грунтується на оперативних дослідженнях та потужній базі даних. www.worldbank.org/wbi/governance

Посібник з питань оцінювання рівня корупції

ПРООН та Глобальна Доброчесність (A Users' Guide to Measuring Corruption, UNDP and Global Integrity, www.globalintegrity.org), забезпечує уряд, громадянське суспільство та практикуючих експертів прикладами передового досвіду з питань оцінювання рівня корупції. В наявності англійською, іспанською та французькою мовами. www.undp.org/ oslocentre/flagship/users_guide_measuring_corruption.html

Фінансовий менеджмент в органах державної влади: аналітичні інструменти. (Public Financial Management: Performance Measurement Framework PEFA Secretariat, World Bank (2005). В наявності англійською, французькою, іспанською, португальською, російською, арабською, китайською, українською, турецькою, вірменською, сербською та в'єтнамською мовами. www.pefa.org/pfm_performance_frameworkmn.php

Посібник з питань оцінки боротьби з корупцією

Підготовлено Агентством міжнародної допомоги США (Anticorruption Assessment Handbook USAID, Bertram I. Spector, Michael Johnston and Svetlana Winbourne (February 2009). www.usaid.gov/our_work/democracy_and_governance/technical_areas/anticorruption_handbook/ index.html

Оцінка прозорості оборонних бюджетів і процесу бюджетування

(Assessing the Transparency of Defence Budgets and Budgeting, Todor Tagarev, "A Means of Comparing Military Budgeting Processes in South East Europe," Information & Security. An International Journal 11 (2003): 95-135.

Доступні бази даних:

Індекс сприйняття рівня корупції Транспаренсі Інтернешнел (Transparency International's Corruption Perceptions Index) Починаючи з 1995 року, Транспаренсі Інтернешнел оцінює Індекс сприйняття рівня корупції. До 2008 року було накопичено дані на 180 країн. Ця інформація доступна в Excel на сайті: http://www.icgg.org/corruption.cpi_2008.html або на сайті www.transparency.org/content/download/38703/612764.

Барометр світової корупції (Global Corruption Barometer) Це дослідження проводиться з 2003 року. Оцінюється загальне ставлення суспільства до питань корупції у десятках країн світу. Дослідження 2009 року проведено у 69 країнах. Відповідні доповіді Транспаренсі Інтернешнел наявні англійською, французькою та іспанською мовами. www.transparency.org/policy_research/surveys_indices/gcb

Індекс хабародавців. (Bribe Payers Index)

Цей Індекс Транспаренсі Інтернешнел дає оцінку тій стороні корупції, яка дає хабарі – оцінюється вірогідність дачі хабара фірмами з індустріалізованих країн за кордоном. Повні доповіді за 1999, 2002, 2006, та 2008 роки в наявності на сайті www.transparency.org/ policy_research/ surveys_indices/bpi.

Індикатори врядування у світі

(Worldwide Governance Indicators, World Bank)

Станом на 2009 рік доповіді по проекту «Індикатори врядування у світі» накопичили загальні та індивідуальні індикатори врядування за 212 країн і територій за період 1996-2008 років по шести показниках врядування, включно з таким, як «контроль корупції». http://info.worldbank.org/governance/wgi/index.asp

Індекс відкритості бюджету

(Open Budget Index)

Індекс відкритості бюджету проводить дослідження кожні два роки. Рейтинги бюджетів за 2008 рік вільно доступні арабською, китайською, англійською, французькою, португальською та іспанською мовами. Повна версія доповіді англійською мовою доступна на сайті http://openbudgetindex.org/fi les/FinalFullReportEnglish1.pdf. www.openbudgetindex.org

Державні витрати та фінансовий контроль

(Public Expenditure & Financial Acountability (PEFA), www.pefa.org. PEFA робить оцінки стану державного фінансового менеджменту в країні. Доповіді наявні на сайті www.pefa.org/assesment_reportmn.php.

Вибрані доповіді та монографії

Виховання доброчесності та будівництво оборонних інституцій, матеріали конференції

(Building Integrity and Defence Institution Building, Conference Report (Monterey, CA: 25–27 February 2009)).

Виховання доброчесності та зниження рівня корупції у сфері оборони, матеріали семінару

(Mark Pyman, Peter Foot and Philipp Fluri, eds., Building Transparency and Reducing Corruption in De-

fence, Workshop Proceedings (Geneva & Lugansk: May 2008)), www.nps.edu/GovIndustry/Conferences/NATO/ Documents/Transparency International Geneva workshop on building integrity May 2008.pdf.

Nils Roseman, Code of Conduct: Tool for Self-Regulation for Private Military and Security Companies, Occasional Paper #15 (Geneva: DCAF, 2008).

Rasma Karklins, The System Made Me Do It. Corruption in Post-Communist Societies (New York: M.E. Sharpe, 2005).

Світовий Банк. The World Bank, "Measuring Corruption: Myths and Realites," Findings 273 (April 2007).

Контрольний офіс уряду США. United States Government Accountability Offi ce, Defense Contracting Integrity (Washington, D.C.: GAO, 2009).

Додаток 2:
Транспаренсі Інтернешнел. Міжнародна програма з питань оборони та безпеки

Корупція у сфері оборони

Транспаренсі Інтернешнел (ТІ), це організація громадянського суспільства, яка очолює боротьбу проти корупції у всьому світі. Через понад 90 своїх представництв по всьому світу, а також міжнародний секретаріат в Берліні, Німеччина, Транспаренсі Інтернешнел поширює знання про негативний вплив корупції, а також працює з партнерами в органах влади, бізнесі та громадянському суспільстві з метою застосування заходів боротьби з корупцією. Для отримання більш повної інформації про Транспаренсі Інтернешнел, звертайтеся до сайту : www.transparency.org.

Глобальна програма Транспаренсі Інтернешнел у секторі безпеки і оборони «Оборона проти корупції» ("Defence Against Corruption" (DAC)) спрямована на скорочення корупції та зміну ставлення до проблем корупції у сферах оборони та безпеки на благо всіх громадян. Ця міжнародна оборонна програма очолюється представництвом Транспаренсі Інтернешнел у Сполученому Королівстві від імені всього руху Транспаренсі Інтернешнел.

Оборонна програма Транспаренсі Інтернешнел почалася шість років тому, звівши разом органи влади, оборонні компанії, наукові заклади та громадянське суспільство з метою визначення найкращих підходів до вирішення проблеми оборонної корупції. Програма DAC широко відома у міністерствах оборони, службах безпеки, оборонних компаніях та організаціях у всьому світі. На сьогодні вона фінансується Міністерством міжнародного розвитку Сполученого Королівства і НАТО.

DAC співпрацює з країнами, що проводять реформи, від Колумбії до Польщі та Афганістану, а також з міжнародними організаціями з метою зниження рівня корупції у сферах оборони і безпеки. З органами влади, міжнародними організаціями, громадянським суспільством та обороною DAC конструктивно співпрацює щоб підвищити рівень доброчесності у сфері торгівлі зброєю. А для того, щоб досягти незворотніх змін у всьому світі, організація підтримує експертів і активістів антикорупційних реформ, організує дискусії та розповсюджує знання з питань боротьби з корупцією.

В результаті активного співробітництва з НАТО було розроблено два антикорупціних інструменти:

І. «Процес самооцінки з питань доброчесності у сфері оборони і безпеки» було розроблено у 2008 та 2009 роках у взаємодії з Польщею і робочою групою представників десяти країн. Успішна апробація пройшла в Норвегії, Україні та Боснії і Герцеговині. Сьогодні цей інструмент є широкодоступним для використання.

ІІ. Інноваційний навчальний курс «Виховання доброчесності та зниження ризику корупції». Цей п'ятиденний курс розрахований на досвідчених посадовців міністерства оборони, міністерства внутрішніх справ та офіцерів збройних сил рівня підполковника і вище. Цей курс вже проводився шість разів за участю двадцяти країн і очевидно буде розширюватися.

Як курс самооцінки, так і навчальний курс призначені для допомоги країнам у підвищенні рівня знань і отриманні досвіду боротьби з корупцією у сфері оборони.

Програма DAC також активно працює з країнами Африки з питань корупції у сферах безпеки і оборони, а також підтримує переговори з питань підписання Договору ООН про торгівлю зброєю.

Важливе значення у боротьбі з корупцією у сферах безпеки і оборони грають дослідження, які проводить DAC. Їх результати розповсюджуються серед зацікавлених структур з метою розповсюдження передового досвіду і заохочення до впровадження сучасних антикорупційних методів. Також DAC публікує раз у два місяці дайджест новин про випадки корупції у сфері оборони.

Поточна інформація про діяльність Транспаренсі Інтернешнел у сферах оборони й безпеки, включно з статистикою, оглядами поточних та минулих проектів та публікаціями доступна на сайті DAC: www.defenceagainstcorruption.org.

Контакти:
Transparency International-UK
Defence Against Corruption programme
London

Director
Mark Pyman
Tel.: +44 207 785 6359
E-mail: mark.pyman@transparency.org.uk

Programme Manager
Anne Christine Wegener
Tel.: +44 207 785 6358
E-mail: anne-christine.wegener@transparency.org.uk

Додаток 3: Основні скорочення

ГІ . . . . . .Гуманітарна інтервенція
РЄ . . . .Рада Європи
ДКЗС . .Женевський центр демократичного контролю над збройними силами
РЄАП . .Рада євроатлантичного партнерства
ЕОА . . .Європейське оборонне агентство
ЄС . . . .Європейський Союз
ЖЦПБ .Женевський центр політики безпеки
ВВП . . .Валовий внутрішній продукт
МКЧХ .Міжнародний комітет Червоного Хреста
МУО . .Міжурядова організація
ІПП . . .Індивідуальна програма партнерства
МССБ .Міжнародні сили сприяння безпеці (Афганістан)
NAMSA Агентство НАТО з питань утримання і поставок (NATO Maintenance and Supply Agency)
НУО . . .Неурядова організація
ОЕСР .Організація економічного співробітництва та розвитку
ОБСЄ .Організація з безпеки та співробітництва в Європі
ОПОК .Озброєні приватні охоронні компанії
PAP-DIB . . .План дій партнерства щодо будівництва оборонних інституцій (Partnership Action Plan on Defence Institution Building
ПВК . . .Приватні військові контрактори
ПДП . .Приватно-державне партнерство
СППБ (PPBS) Система планування, програмування та бюджетування (Planning, Programming, and Budgeting System)
ГРП (PRT) .Група реконструкції провінції (Provincial Reconstruction Team)
ТІ . . . . .Транспаренсі Інтернешнел
ООН . .Організація Об'єднаних Націй
USAID .Агентство міжнародного розвитку США (US Agency for International Development)

www.skz.net.ua

ТОВ «ВЕБКОМ»

Ексклюзивний дистриб'ютор в Україні продукції Arconik (Ізраїль), MineARC (Австралія), ПРО ЗАХИСТ (Україна). Ми виробляємо, імпортуємо та постачаємо спеціальне обладнання для сховищ та протирадіаційних укриттів

Сучасний Колективний Захист

Наша історія почалась в 2010 році, коли Україна готувалася до Чемпіонату Європи з футболу 2012 року. Ми здійснили постачання обладнання для першої захисної споруди цивільного захисту, збудованої за часів незалежності України.

Більше десяти років ми набували досвід в сфері обладнання та технологій в сфері захисних споруд цивільного захисту. Зараз ми готові ділитися нашими знаннями. Ми впевнені, від цього виграє кожна сторона партнерства. Але головне це захист та безпека, які отримають кінцеві споживачі наших продуктів - власники та користувачі сховищ, протирадіційних укриттів, приватних бункерів, бомбосховищ та захищених кімнат. Не важливо, потрібен вам лише один фільтр-поглинач, одна ФВУ чи захисно-герметичні двері, ми в будь-якому випадку забезпечимо вас обладнанням.

Зараз ми працюємо міцною командою з підприємств та підприємців, об'єднаних однією метою - працювати в сфері цівільного захисту задля забезпечення безпеки українців.

Наша Компанія є ексклюзивним офіційним дистриб'ютором в Україні:

- Всесвітньо відомого та найбільш досвідченого виробника спеціальної продукції для колективного захисту від ЯРХБ загроз, компанії ARCONIK (Ізраїль);
- Українського виробника спеціального обладнання для захисних споруд цивільного захисту, під торгівельною маркою ПРО ЗАХИСТ (Україна);
- Компанії Atmas (Фінляндія);
- Світового лідера у виробництві продукції для захисту і рятування людей під час аварій та катастроф, для добувної і нафтохімічної промисловості, MineARC Systems Pty Ltd (Австралія);
- Компанії KIBO (Греція);
- Компанії BiroSAFE (Північна Македонія);
- Компанії G.G. Defense Systems Ltd. (Ізраїль)

Наша спеціалізація включає постачання такої продукції та послуг:

- обладнання для захисних споруд цивільного захисту (двері, противибухові пристрої, вентилятори тощо);
- засоби колективного захисту від ЯХБ загроз;
- системи автономного життєзабезпечення;
- рішення «під ключ» для приватних сховищ і незахищених об'єктів (проектування та комплектація);
- системи протиепідемічного захисту.

Запрошуємо до співробітництва підприємців та компанії

ТОВ «ВЕБКОМ» Сучасний Колективний Захист, 08631, Київська обл., Фастівський р-н, смт. Глеваха, вул. Підприємницька, б. 8. т. +380679353824 (технічні консультації), +380953459920 (комерційні питання), +380442236269 (загальні питання), post@skz.net.ua, www.skz.net.ua

Hobbit House

МОДУЛЬНІ УКРИТТЯ ЦИВІЛЬНОГО ЗАХИСТУ

Гарантована відповідність
відповідають ДБН В.2.2-5:2023 та ДСТУ 9195:2022

Максимальна міцність
витримують вибухові хвилі до 300 кПа

Перевірено в реальних умовах
тестуються обстрілами на полігонах

Швидке рішення
оперативне виробництво та монтаж

Укриття — вимога Кодексу цивільного захисту України!

Усі підприємства та установи мають облаштовувати укриття для захисту людей у разі надзвичайних ситуацій. Одним із найбільш ефективних рішень є використання модульних залізобетонних укриттів, які поєднують високу міцність, швидкість будівництва та відповідність державним стандартам.

вебсайт:
hobbithouse.com.ua

телефон:
+38 063 584 6394

пошта:
k.reva@hobbithouse.com.ua