Бізнес і безпека

№ 6/2024 (159)

ISSN 1819-9429

00159

40226 - передплатний індекс в Укрпошті

www.bsm.com.ua

Бізнес і безпека

АРМІЇ ПОТРІБЕН ВІЙСЬКОВИЙ КОДЕКС - УКРАЇНЦІ ЗНИЩИЛИ ПОЛОВИНУ ПАРКУ РОСІЙСЬКИХ ВЕРТОЛЬОТІВ КА-52 - ЯК ПЕЙДЖЕРИ «ХЕЗБОЛЛИ» ПЕРЕТВОРИЛИСЯ НА БОМБИ - ШТУЧНИЙ ІНТЕЛЕКТ НА БОРТУ ВІДЕОКАМЕРИ -ВПРОВАДЖЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ ЦЕНТРАЛІЗОВАНОГО ОПОВІЩЕННЯ ТЕРИТОРІАЛЬНИХ ГРОМАД - ВІСІМ ДОКАЗІВ НЕБЕЗПЕКИ ТЕЛЕГРАМУ - КОМПЛЕКТ ЗАСОБІВ ДЛЯ РОЗМІНУВАННЯ ТА ДИСТАНЦІЙНОГО ДЕАКТИВУВАННЯ ПРОТИТАНКОВИХ МІН «КЛЮЧ» - БЕЗПЕКА ЕЛЕКТРОННОЇ ПОШТИ - ХТО ЗУПИНИТЬСЯ, ТОЙ ПРОГРАЄ. ЯК БПЛА ВПЛИВАЮТЬ НА ВІЙНУ - ЯК ВИЯВИТИ ШПИГУНСЬКЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НА СМАРТФОНІ - ЗАХИСНІ СПОРУДИ ВІД КОМПАНІЇ «ALD ENGINEERING COMPANY» - ДИТЯЧІ ПРОТИГАЗИ - БОРОТЬБА З КОРУПЦІЄЮ В ОБОРОННОМУ СЕКТОРІ

An ALLIED UNIVERSAL Company

There for you™

AMAG TECHNOLOGY
An ALLIED UNIVERSAL Company

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

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

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

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

G4S Україна

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

An ALLIED UNIVERSAL Company

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

ІНДИВІДУАЛЬНИЙ ЗАХИСТ ОРГАНІВ ДИХАННЯ

ІЗОД

www.izod.com.ua

ЦИВІЛЬНІ ПРОТИГАЗИ

ПРОМИСЛОВІ ПРОТИГАЗИ

ІЗОЛЮЮЧІ ПРОТИГАЗИ

ФІЛЬТРИ ПРОТИГАЗОВІ

ПРОТИГАЗОВІ МАСКИ

НАПІВМАСКИ ПРОТИГАЗОВІ

САМОРЯТІВНИКИ

ПРОТИПОЖЕЖНЕ ОБЛАДНАННЯ

СПЕЦІАЛЬНИЙ ЗАХИСНИЙ ОДЯГ

ДИТЯЧІ ПРОТИГАЗИ

ПРИВАТНЕ ПІДПРИЄМСТВО «СЕЛЛ`КОМ» працює на українському ринку засобів індивідуального захисту більше 10 років і займає лідируючі позиції серед компаній, що займаються виробництвом та постачанням засобів індивідуального захисту органів дихання. Наша компанія є ексклюзивним дистриб'ютором компанії **«TRAYAL CORPORATION»** та **«SIGMA s.r.o.»** які є провідними виробниками протигазів, фільтрів і масок.

ПРИВАТНЕ ПІДПРИЄМСТВО «СЕЛЛ`КОМ» має реєстрацію та дозвіл на імпорт в Україну продукції військового та подвійного призначення. Наша компанія виготовляє, комплектує та постачає засоби індивідуального захисту (протигази різних типів) для найбільших підприємств України, Збройним Силам України та ДСНС України.

TRAYAL KORPORACIJA

SIGMA

ПРИВАТНЕ ПІДПРИЄМСТВО «СЕЛЛ`КОМ» +38 067 640 80 10, +38 066 400 66 85, www.izod.com.ua

КОМПЛЕКТ ЗАСОБІВ ДЛЯ РОЗМІНУВАННЯ ТА ДИСТАНЦІЙНОГО ДЕАКТИВУВАННЯ ПРОТИТАНКОВИХ МІН «КЛЮЧ»

Комплект засобів призначений для розмінування, дистанційного знешкодження (деактивування) та викручування підривників протитанкових мін типу (далі ПТМ) «ТМ-62» та аналогів.

Комплект служить для технічного забезпечення саперів інженерно-саперних підрозділів під час виконання ними робіт по розмінуванню ПТМ «ТМ-62» та аналогів. За допомогою пристроїв та комплектуючих даного комплекту можна виконувати роботи по дистанційному вилученню та перевертанню ПТМ, по переводу підривників з робочого в неробоче положення, викручувати та вкручувати в ПТМ підривники типу «МВЧ» та «МВП», вилучати вкопані ПТМ за допомогою допоміжного важілю дистанційної деактивації мін, дистанційно викручувати підривники типу «МВЧ» та «МВП» з мін, які заходяться в грунті, при цьому виявляючи вибухонебезпечні пастки, які можуть бути встановлені під ПТМ. Паракорд, загальною довжиною 100 м та товщиною 6 мм забезпечує достатню відстань та зусилля, для безпечної роботи саперів. Набір розташований в наплічному рюкзаку, що робить його ефективним при використанні та застосуванні.

Набір розміщений в сумці у вигляді ранцю, має невеликі розміри та мінімальну вагу, що робить його зручним у використанні спеціалістами під час проведення пошукових робіт.

ТЕХНІЧНІ ХАРАКТЕРИСТИКИ

1. Габаритні розміри сумки, мм, не більше . .. . - 550 x 330 x 130
2. Загальна вага, кг, не більше. . . . . .- 6,5

Комплектація:

Дистанційний універсальний викручувач для підривачів типу «МВЧ» та «МВП» з ПТМ . . . . . - 1 шт.

Універсальний спеціальний ключ для підривачів типу «МВЧ» та «МВП» - 1 шт.

Екстрактор - гак для вилучення ПТМ «ТМ-62» зі спорядженням. . . . . - 1 шт.

Гак для вилучення ПТМ «ТМ-62» з грунту. . . . . - 1 шт.

Зачіп-хомут для вилучення ПТМ з підривниками типу «МВП» з грунту - 1 шт.

Зачіп для вилучення ПТМ з підривниками типу «МВЧ» з грунт . . . . . .- 1 шт.

Захват мотузковий . . . . . .- 1 шт.

Універсальний ключ для переводу підривників ПТМ . . . . . .- 1 шт.

Паракорд 6 мм довжиною 50 м з карабіном . . . . . .- 2 шт.

Ласо з паракорду довжиною 1,5 м з карабіном . . . . . .- 5 шт.

Допоміжний важіль для дистанційної деактиваці ПТМ . . . . . .- 1 шт.

Рюкзак спеціальний . . . . . .- 1 шт.

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

Бізнес і безпека

№ 6/2024 (159)

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

Видається з 10 квітня 1996 року.

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

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

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

☆ ☆ ☆

Надруковано у **ТОВ «Друкарня «Літера»** Адреса друкарні: м. Київ, вул. Сім'ї Хохлових, 8.
Замовлення № 165 від 20.11.2024 р.

Друк офсетний.
Папір крейдований.
Формат 60 х 84 1/8.
Обсяг 10 ум. др. стор.
Підписано до друку 20.11.2024 р.
Наклад 12 000 екз.
Передплатний індекс – 40226.
Періодичність: 6 на рік.
Ціна договірна.
м. Київ – 2024

☆ ☆ ☆

ISSN 1819-9429

АКТУАЛЬНО

ФІЗИЧНИЙ ЗАХИСТ. ОХОРОНА. ТЕХНІЧНІ ЗАСОБИ БЕЗПЕКИ

ПОЖЕЖНА БЕЗПЕКА

ПОРАДИ

Армії потрібен Військовий кодекс. Як законодавчо змінити «совкові» порядки, що породжують зловживання

Як реформувати армію, щоб позбавити її «совковості» й «затягів», врахувати сучасні воєнні реалії? Юрист, правозахисник, а нині військовослужбовець Алі Сафаров пропонує реформувати армійське право — систему керівних документів, що регулюють існування та повсякденну діяльність ЗСУ, відмовитися від застарілих статутів, ухваливши натомість Військовий кодекс та узгодивши його з іншими законодавчими документами.

Адже формувалася ця система спочатку на основі радянських документів, згодом додавалися вже сучасніші норми, проте в старі акти не завжди вносилися необхідні зміни. Або ж певні норми бездумно копіювалися з попередніх наказів.

Фантомні поршневі літаки

Наприклад, в Інструкції з організації обліку особового складу в системі Міноборони України в Аркуші обліку льотної роботи розмежовується наліт на літаках із реактивними двигунами і на літаках із поршневими двигунами. Але в Збройних силах України немає поршневих літаків. І взагалі останні поршневі літаки, окрім навчально-тренувальних, були зняті з озброєння в Радянському Союзі у 50-х роках минулого сторіччя. Натомість є, наприклад, турбогвинтові літаки, які мають реактивний двигун, але рушій у них гвинт, як у поршневих літаків, тож цікаво, куди саме зараховують наліт таких пілотів?

Якщо простежити історію цієї норми, то вона залишається незмінною від появи наказу міністра оборони СРСР від 01.11.1982 № 0200/ДСК «О введении в действие Наставления по учету личного состава Советской Армии и Военно-Морского Флота».

Висота літер і відстань між наметами

Або ж, наприклад, Статут внутрішньої служби ЗСУ. Він затверджується законом України і регулює купу аспектів військового життя — від обов'язків командира роти до графина зі склянкою в приміщенні чергового.

Цим Статутом імперативно визначаються розміри покажчиків і зразки написів на дверях приміщень у сантиметрах, висота літер, висота розміщення від підлоги. Статут встановлює вимоги до розбивки табору, знову ж таки імперативно регулюючи відстань між наметами та інші фактори, які взагалі-то мають бути індивідуальними залежно від місцевості та ситуації.

І водночас Статут геть не регулює правила військового життя під час війни, розосередження особового складу тощо. Також положення Статуту в багатьох моментах перетинаються з іншими нормативними актами, зокрема із Законом України «Про військовий обов'язок та військову службу», «Про соціальний та правовий захист військовослужбовців та членів їх сімей» тощо, що призводить до виникнення правових колізій.

Це створює величезні можливості для переviряльників або для зловживання владою командирами, адже, хай там як військовослужбовець старатиметься, він усе одно щось порушить просто через суперечливість керівних документів. Причому правила накладання стягнень також не врегульовано належним чином.

Алі Сафаров. Фото з особистої фейсбук-сторінки

За однакові вчинки комусь буде зауваження, а комусь сувора догана

Наприклад, Дисциплінарний статут ЗСУ не визначає, за що саме може бути зроблено зауваження, накладено догану чи сувору догану. Це визначає особисто командир залежно від своїх переконань, а часом навіть від свого настрою в конкретний момент. За одинакові вчинки одному військовослужбовцю може взагалі нічого не бути, а іншому прилетить сувора догана, що тягне за собою позбавлення премії. Ці концептуальні моменти, закладені в армійську нормативну базу, дуже демотивують.

Потрібен Військовий кодекс

Якби можна було пофантазувати на тему реформування війська, то, мабуть, перше, що я запропонував би, — це розробка й ухвалення Військового кодексу, який об'єднав би в собі Закони України «Про Збройні сили України», «Про військовий обов'язок і військову службу», «Про соціальний і правовий захист військовослужбовців та членів їх сімей» тощо з узгодженням положень та уніфікацією термінології.

У Кодексі мають визначатися основні засади функціонування армії як структури, взаємодія армії з Міноборони та іншими органами виконавчої влади (нарешті варто чітко визначити, що Міноборони — то не армія, а армія — то не Міноборони). Водночас Кодекс визнав би такими, що втратили силу, статути Збройних сил України, визначивши, що питання, які вони регулювали, мають регулюватися наказами Міністерства оборони України та іншими підзаконними нормативними актами.

Закони «Про національну безпеку України», «Про оборону», «Про мобілізацію та мобілізаційну підготовку» тощо не повинні включатися до Військового кодексу, натомість мають узгоджуватися між собою та зводитися в єдиний нормативний документ.

Визначаються Статус і коло регулювання питань наказами Генерального штабу ЗСУ. Наприклад, такий документ, як наказ № 73 про взаємодію з журналістами, має ухвалюватися на рівні Міноборони, а не ГШ і реєструватися в Мін'юсті, адже він стосується не тільки військових. Ну й дається час Кабінету Міністрів України та Міноборони привести свої підзаконні нормативні акти у відповідність до Кодексу.

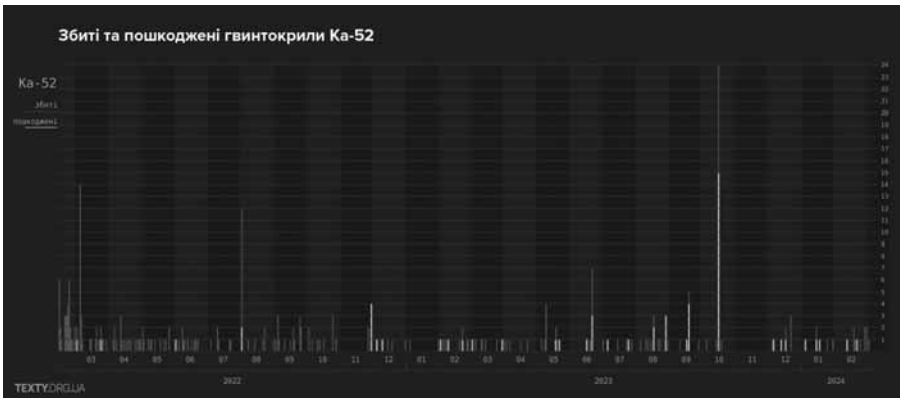
Додатково Військовий кодекс має узгоджуватися з іншими українськими законодавчими актами, зокрема із Законом України «Про доступ до публічної інформації». Бо, з одного боку, зрозуміло, що армійська система закрита, а інформація зсередини чутлива і впливає на обороноспроможність країни, а з другого — така закритість призводить до зарахування до інформації з обмеженим доступом навіть відкритої за своєю суттю інформації.

Міноборони України як розпорядник публічної інформації має оприлюднювати свої нормативні документи, що, на превеликий жаль, не завжди робиться.

З одного боку, зрозуміло, що в умовах війни є нагальніші потреби, ніж реформування армійського законодавства. А з другого — без реформування підвищити ефективність війська та бажання в ньому служити не вийде.

Алі Сафаров
texty.org.ua

Долітались. Українці знищили близько половини парку потужних російських вертольотів Ка-52



З графіки видно, що після цієї вдалої атаки майже два місяці минуло без втрат таких машин. Це означає, що росіяни їх або не використовували, або використовували мінімально.

Російський гелікоптер Ка-52 «Алігатор» — грізна зброя, здатна завдавати чималої шкоди. За різними оцінками, до початку повномасштабного вторгнення ПКС РФ мали від 140 до 160 бойових вертольотів «Алігатор». Ще кілька одиниць випустили в ході війни. За час війни ЗСУ знищили або пошкодили близько половини цієї техніки.

Вдалий жовтень

Особливо вдалим було 17 жовтня 2023 року. За даними ініціативи ORYX, яка відстежує військові втрати, на аеродромах поблизу Бердянська та Луганська того дня було уражено п'ятнадцять бойових гелікоптерів Ка-52 і дев'ять багатоцільових гелікоптерів Мі-8. Аналітики ідентифікували як повністю знищені сім Ка-52 й два Мі-8. Тоді на аеродроми прилетіли надані союзниками ракети.

З графіки видно, що після цієї вдалої атаки майже два місяці минуло без втрат таких машин. Це означає, що росіяни їх або не використовували, або використовували мінімально.

Початок

Також бачимо, що багато гелікоптерів ми знищили на початку війни.

Ка-52 брали участь в атаці на аеропорт у Гостомелі, який захищали нацгвардійці 4-ї бригади НГУ.

Перший Ка-52 збив ракетою з ПЗРК «Ігла» молодший лейтенант Сергій Фалатюк, гелікоптер згорів вщент. Ще один пошкодили вогнем із зенітної автоматичної гармати ЗУ-23М. Інший Ка-52 приводнили над Київським морем. А загалом того дня наші військові збили шість російських вертольотів різних марок.

Загальні втрати

За даними української розвідки, за весь час війни росіяни втратили близько 80 вертольотів Ка-52, але точну інформацію наразі отримати неможливо.

Як розповів один з офіцерів ЗСУ, «якщо ти бачиш, що за Ка-52 тягнеться чорний дим, це ще не означає, що він знищений. Він може сісти десь на окупованій території, і потім його відремонтують. У нього можуть бути пошкоджені лопаті, але сам вертоліт залишиться майже цілим. І після нескладного ремонту знову літатиме. Навіть у Міноборони РФ не завжди володіють повною статистикою, бо не про всі пошкодження доповідають нагору. До того ж росіяни приховують свої втрати і від нас. Але загалом, думаю, близько половини «Алігаторів» ми приземлили остаточно».

Чому це грізна машина?

Російська пропаганда дуже вихваляла ці гелікоптери. Він і «всепогодний», і броньований, і озброєний всім, чим тільки можна.

Отже, що вміє Ка-52 (Hokum B за класифікацією НАТО, також відомий як «Алігатор»)?

Його можна використовувати як командирську машину армійської авіації. Він здатен здійснювати радіорозвідку місцевості, давати цілевказівки, а також координувати дії групи бойових вертольотів.

Спроєктований для того, щоб уражати броньовану й небронюванну техніку, живу силу й повітряні цілі на полі бою.

Є продовженням розвитку моделі Ка-50 «Чорна акула». У 1990-ті роки ця машина відзначилася в Чечні, й пілоти були задоволені її бойовими якостями. Ка-52 — це, по суті, наступна ітерація «Чорної акули».

Екіпаж — два льотчики. Озброєний рухомою гарматною установкою з автоматичною гарматою калібру 30 мм і боєкомплектом 460 снарядів, протитанковим ракетним комплексом «Вихрь» із лазерною променевою системою наведення. Також здатен нести авіабомби, гарматні контейнери та іншу зброю загальною масою до 2000 кг. Додатково Ка-52 може брати

на борт керовані ракети класу «повітря-повітря» малого радіуса дії Р-73 та «Ігла-В», а також некеровані ракети «повітря-земля».

Ка-52 обладнаний радарною системою «Арбалет». Має броньовану капсулу для екіпажу. Катапультування капсули можливе від 0 до 4100 м. Ведення вогню і керування (зокрема, одночасне) може здійснювати будь-який із пілотів.

Льотно-технічні характеристики

Екіпаж . . . . . - 2 пілоти.
Максимальна злітна маса .- 10 800 кг.
Крейсерська швидкість .- 250 км/год.
Максимальна швидкість у горизонтальному польоті . . . . . -310 км/год
Максимальна швидкість . -350 км/год
Дальність польоту практична -520 км
Дальність польоту перегоночна -1200 км
Статична стеля . . . . . .- 3600 м
Динамічна стеля . . . . . .- 5500 м

Перше бойове застосування Ка-52 було здійснене в Сирії — там росіяни втратили кілька машин.

Перша зустріч українських військових із Ка-52 сталася 25 листопада 2018 року під час захоплення в Азовській протоці наших малих броньованих артилерійських катерів «Бердянськ», «Нікополь» та рейдового буксира «Яни Капу», які здійснювали плановий перехід із порту Одеси до порту Маріуполя в Азовському морі.

Нагадаємо, що вночі окупанти атакували наші катери поблизу Кримського мосту, під яким вони мали пройти, щоб дістатися до Маріуполя.

Катери зазнали вогневого ураження й втратили можливість самостійно продовжувати рух. У результаті орієнтовно о 20:50 за київським часом їх захопили спецпідрозділи ФСБ.

За офіційними російськими даними, до атаки на українські катери було залучено вертольоти Ка-52. Один із них випустив по наших кораблях дві некеровані ракети. Окрім вертольотів до атаки з повітря був залучений винищувач Су-30.

Олександр Шульман
Тексти.org.ua

Як пейджери «Хезболли» перетворилися на бомби

17 вересня в Лівані вперше почали вибухати сотні пейджерів, які належали членам підтримуваного Іраном угруповання «Хезболла». Загинули щонайменше десяток людей, а понад 2700 отримали поранення, багато виявилися тяжкими. Наступного дня знову сталися вибухи – тепер детонували рації, що призвело до загибелі ще 20 людей та численних поранень. Серед загиблих були члени «Хезболли», але також і цивільні, зокрема четверо дітей. За даними ЗМІ, посол Ірану в Лівані також серйозно постраждав під час вибухів пейджерів «Хезболли». Відомо, що ізраїльська розвідка перед вибухами пейджерів відправила повідомлення арабською мовою, що виглядало як інформація від вищого керівництва «Хезболли», які супроводжувалися звуковим сигналом. Внаслідок цього у багатьох є ушкодження очей, аж до сліпоти.

За оцінками експерта Бі-бі-сі, смертельними виявилося менше 1% вибухів пейджерів, проте сотні людей зазнали серйозних поранень, і інцидент став значним психологічним ударом для «Хезболли».

Після повторних вибухів міністр оборони Ізраїлю Йоав Галант оголосив про перенесення основних військових зусиль на північ, заявивши про початок «нової фази» війни. На півночі Ізраїль межує з Ліваном, де активно діє «Хезболла».

У свою чергу прем'єр-міністр Ізраїлю Беньямін Нетаньяху 18 вересня оприлюднив коротке відеозвернення, в якому пообіцяв повернути жителів північних регіонів країни до своїх будинків. Враховуючи події, що відбулися в Лівані, ізраїльська влада, ймовірно, планує розпочати нову військову операцію проти цього угруповання.

Ізраїльський військовий експерт Ігаль Левін вважає, що масові вибухи пейджерів є результатом високоточних дій ізраїльських спецслужб. Він казав, що вибухи могли стати наслідком заміни цілої партії девайсів під час централізованих закупівель, які здійснювали бойовики.

Як все починалось

Доставляти пейджери до Лівану почали влітку 2022 року невеликими партіями.

Ізраїль створив підставну компанію з виробництва пейджерів, які почали масово вибухати в Лівані. Девайси постачалися членам ліванського угруповання «Хезболла». Зокрема, йдеться про угорську компанію B.A.C. Consulting.

Про це повідомляє The New York Times посилаючись на джерела в розвідці. Ізраїль не підтвердив і не спростував свою причетність до вибухів, проте 12 нинішніх та колишніх чиновників оборони та розвідки, ознайомлених із ситуацією, стверджують, що за цим стоять ізраїльтяни.

За їхніми даними, угорська фірма отримала контракт на виробництво пристроїв від тайванської компанії Gold Apollo. Ізраїль інвестував мільйони у цю розробку, створивши дві інші підставні компанії, щоб приховати імена офіцерів своєї розвідки, залучених до виробництва пейджерів.

Хоча B.A.C. обслуговувала і звичайних клієнтів, основним споживачем була «Хезболла». Пейджери, що поставлялися угрупованню, містили батареї з вибуховою речовиною PETN. Вони почали надходити до Лівану влітку 2022 року, але виробництво різко зросло після заяви лідера «Хезболли» Саїда Насралли, який закликав членів угруповання уникати використання мобільних телефонів.

Хто може стояти за організацією вибухів?

«Хезболла» звинуватила у вибухах пейджерів Ізраїль, погрозивши йому «суворим покаранням» у відповідь. Ізраїль поки не прокоментував подію.

Як повідомляє Reuters з посиланням на високопоставлене джерело в ліванських службах безпеки, ізраїльська розвідка «Моссад» встановила вибухівку у 5 тисячах пейджерів, ввезених ліванським угрупуванням «Хезболла» за кілька місяців до вибухів.

«Моссад» впровадив усередину пристрою вибухову речовину та електронну схему її активацію на яку надходить код. Його дуже важко знайти навіть за допомогою будь-якого приладу чи сканера», – цитує Reuters слова із їй відомого джерела.

Джерело, близьке до «Хезболли» попросило не називати його імені, повідомило AFP, що «пейджери, що вибухнули, відносяться до нещодавно ввезеної «Хезболлою» партії з 1000 пристроїв».

Згідно з Reuters, високопоставлене джерело в ліванських службах безпеки ідентифікувало за фотографією модель пейджера – AP924, який, як і інші пейджери, приймає та відображає текстові повідомлення, але не може використовуватися для телефонних дзвінків. За даними джерела, ці пейджери виготовила тайванська компанія Gold Apollo.

Однак у заяві тайванської фірми йдеться про те, що пейджери, використані під час вибуху, були виготовлені будапештською компанією B.A.C. Consulting, яка мала ліцензію на використання бренду Gold Apollo.

«Продукт був не наш. На ньому був лише наш бренд», – заявив у середу засновник та президент Gold Apollo Хсу Чинг-Куанг журналістам в офісі компанії у тайванському місті Новий Тайбей.

Інше джерело в службі безпеки повідомило Reuters, що в нових пейджерах було заховано до трьох грамів вибухівки, яка залишалася непоміченою для «Хезболли» протягом кількох місяців.

Колишній аналітик ЦРУ Майк Діміно вважає, що ізраїльська розвідка заздалегідь визначила, хто постачає комунікаційні пристрої для «Хезболли» та які типи пристроїв використовуються.

«Це була класична диверсійна операція. Робота розвідки у кращому вигляді», – написав Діміон у X (колишній твіттер).

Телеканал Sky News Arabia з посиланням на джерела повідомив, що розвідувальна служба «Моссад» заволоділа комунікаційними пристроями «Хезболли» ще до того, як їх було передано угрупованню, яке Ізраїль та країни Заходу вважають терористичною.

Як вибухові пристрої могли бути наведені в дію?

За словами джерела, на яке посилається телеканал Sky News Arabia, агенти «Моссада» помістили на батареї пристроїв деяку кількість PETN (Пентаеритриттетранітрат) – потужної вибухової речовини, і підірвали їх, підвищивши температуру батарей на відстані.

Пентаеритриттетранітрат – це бризантна вибухова речовина. У чистому вигляді вона використовується для спорядження капсул-детонаторів, а у флегматизованому вигляді – для спорядження кумулятивних запасів, детонуючого шнура. Це хімічно стійка речовина.

PETN є білим кристалічним порошком. При нагріванні він розкладається із сильним самоприскоренням, часто із вибухом.

Представник угруповання повідомив Wall Street Journal, що деякі люди відчули, як пейджери нагрівалися перед вибухами. Перегріті літій-іонні батареї можуть спалахнути, але експерти кажуть, що зламування пейджерів та їх перегрів зазвичай не призводять до таких сильних вибухів.

Як передає кореспондент Бі-бі-сі з питань безпеки Френк Гарднер, який посилається на неназваного екс-співробітника британської армії, у пейджери могло бути закладено від 10 до 20 грамів бойової сильнодіючої вибухової речовини.

Вибухівку могли заховати у фальшивому електронному компоненту. Потім вибухові пристрої мали активуватися за допомогою спеціального буквено-цифрового повідомлення. Перша ж людина, яка після цього починала користуватися пейджером, приводила пристрій у дію – і він вибухав, припускає експерт.

Експерт зі зброї в Атлантичній раді Алекс Плітсас також вважає, що йдеться про невеликий заряд вибухівки у пейджерах. «Загоряння літій-іонної батареї – це одне, але я ніколи не бачив, щоб вона так вибухала. Це схоже на невеликий заряд вибухівки», – сказав Плітсас. «За час своєї служби я побачив чимало програм та операцій, але сьогодні у світі диверсій було щось нове», – написав у X Плітсас.

Експерт з безпеки літій-іонних батарей з Університету Ньюкасла Пол Крістенсен зазначив, що рівень збитків, завданих вибухами пейджерів, не відповідає відомим випадкам виходу з експлуатації таких батарей у минулому.

«Ми говоримо про те, що відносно невелика батарея спалахнула. Не йдеться про смертельний вибух. Мені потрібно знати більше, але інтуїція підказує мені, що це малоймовірно», – цитує Крістенсена видання Times of Israel.

Експерти з вибухових речовин стверджують, що кілька пейджерів, які не вибухнули, були виявлені та вивчаються в рамках розслідування, до якого можуть бути залучені щонайменше шість країн.

Як відреагували у світі?

Прем'єр-міністр Лівану Наджіб Мікаті звинуватив Ізраїль у вибухах, які є «серйозним порушенням суверенітету Лівану і злочином за всіма стандартами».

Тегеран назвав дії Ізраїлю терористичним актом та прикладом масового вбивства.

Найближчий союзник Ізраїлю – США закликав Іран не нагнітати напруженість і додав, що штати не мають відношення до того, що сталося.

«США не були залучені до подій. США не знали про цей інцидент заздалегідь, зараз ми збираємо інформацію», – заявив представник Держдепартаменту Метью Міллер на прес-брифінгу у вівторок.

Глава дипломатії ЄС Жозеп Боррель засудив напади, «які ставлять під загрозу безпеку та стабільність Лівану та підвищують ризик ескалації у регіоні».

«Навіть якщо ці атаки здавалися цілеспрямованими, вони призвели до тяжких, невиборних, побічних жертв серед цивільного населення, зокрема серед дітей», – заявив Боррель.

Він зазначив, що Європейський союз хоче запобігти тотальній війні, оскільки вона матиме «важкі наслідки для всього регіону та за його межами».

Представник ООН заявив, що останні події в Лівані «викликають крайнє занепокоєння, особливо з огляду на те, що вони відбуваються в умовах крайньої нестабільності».

Що це означає для Ізраїлю та «Хезболли»?

Ізраїль, швидше за все, здійснив таку масштабну операцію для того, «щоб посилити стримування «Хезболли» та переконати ізраїльських громадян, у тому числі тих, хто був евакуйований на північ, що вони перебувають у безпеці», вважає арабський експерт Мурад Шишані – «Але це може призвести до абсолютно протилежних результатів, якщо «Хезболла» посилить свої атаки як відповідь».

Якщо до вибухів пейджерів причетний Ізраїль, це матиме глибокі наслідки для «Хезболли» та її керівництва, пише австралійський генерал-майор у відставці Мік Райан.

«Ізраїльтяни продемонстрували, що вони мають доступ до комунікаційних мереж «Хезболли» та ланцюжків її постачання. Це дасть кожному члену «Хезболли» привід переглянути свою думку про те, чи варто довіряти засобам зв'язку та іншому устаткуванню, яке постачається організацією», – пише Райан.

«Але загалом ізраїльтяни показали, що вони можуть перехоплювати та фальсифікувати постачання, призначені для «Хезболли». Що ще вони могли підробити?

Міжнародний редактор Бі-бі-сі Джеремі Боуен вважає, що хоча «Хезболла» буде якийсь час приголомшена нападом, угруповання «швидко збереться з силами та знайде інший спосіб зв'язку. Ліван – маленька країна, повідомлення можна легко передавати навіть вручну».

Крім того, згідно з звітом Al Monitor, запланована атака пішла не за планом: вибухи пейджерів мали стати першим залпом у великій ескалації, але «Хезболла» почала виявляти підозрілість, що змусило Ізраїль розпочати проведення операції завчасно.

Хоча ізраїльтяни показали, що можуть проникнути в комунікації «Хезболли», і продемонстрували, що можуть принизити їх (членів угруповання), ця операція ні на йоту не віддаляє регіону від повномасштабної війни, а скоріше навіть наближає її, підсумовує Боуен.

Чи може в Україні повторитись подібний сценарій?

На деякі питання з цього приводу відповість експерт з питань кібербезпеки Віталій Якушев.

– Чи може в Україні повторитися історія, аналогічна тій, що сталася з бойовиками Хамаса в Лівані – вибухами пейджерів, мобільних телефонів, планшетів, комп'ютерів та інших електронних гаджетів зв'язку та отримання інформації?

Це питання одночасно і легке і складне. Легке, бо теоретично-технічно відповідь: так, можливо у будь-якій країні світу – в Україні, Сполучених Штатах, Зімбабве, Лівані, де завгодно.

Якщо казати, наскільки це легко зробити, – це дуже складна операція. Цей тип атак називається supply chain attack, або атака через довіреного постачальника.

Можливо, пам'ятайте атаку 2017 року, коли використовували M.E.doc (програмне забезпечення для звітності та документообігу). Це якраз приклад supply chain attack, коли довіреного постачальника програмного забезпечення зламали і через нього завантажували шкідливе програмне забезпечення на комп'ютери українських компаній. Тому відповідь так, можливо.

У Лівані була багатокрокова, багаторічна програма: спочатку треба було взяти обладнання. По-друге, в це обладнання додати вибухівку та після цього запрограмувати спрацювання вибухівки під якісь умови.

Хтось пише, що була відправлено якась фраза. Хтось пише, що була діяльність, яка призвела до нагрівання батареї та вибуху поміщеного біля неї речовини. Можливо, правди ми і не дізнаємося. А можливо, і буде якась інформація.

Але щоб у ворога з'явилася можливість доступу до обладнання, яке буде продаватися (в Україні), або взагалі його продати – необхідно, щоб були фахівці, які вирішать це питання дуже грамотно. Питання не просто розмістити вибухівку, а щоб вона спрацьовувала «розумно». Ворог повинен точково знати, чого він хоче.

Ну, і по-третє – це щоб воно спрацювало у потрібний час, щоб нічого не збило, щоб вибухівка не висохла, не намокла, щоб із нею нічого не сталося.

Тому на практиці це напівфантастичний приклад, коли така складна операція була успішна. І це буде в підручниках по дуже складним гібридним операціям. Тому що тут був і фізичний доступ до обладнання, і айтішна частина.

А статися це може, якщо у держоргані, приватній або державної компанії не ведуться роботи з протидії supply chain attack через надійного постачальника, тобто не перевіряють, що закуповують, тому, відповідно, така атака можлива.

– А могли б наші спецслужби провести таку операцію?

У теорії могли б, але, по-перше, це дуже дорого фінансово. Наші спецслужби мають фахівців належного рівня, і можуть залучати для консультацій фахівців ззовні. Але ось реалізувати подібний сценарій...

Чому я говорю про фінанси? Тому що, крім закупівлі обладнання, вибухівки, щоб ніхто не дізнався, установки, основи підставних компаній, треба мати можливість це точково продати. Дуже багато факторів. Теоретично так, але на практиці ... Я б дуже хотів, щоб наші спецслужби такі операції не тільки теоретично могли проводити, а й реально проводили.

– У жовтні 2022-го наші спецслужби влаштували операцію з підриву вантажівки на Кримському мосту. Транспорт проїхав через Болгарію, Грузію Вірменію, Північну Осетію та Краснодарський край і жодна собака не почула, що там 21 тонна вибухівки.

Тут одна вантажівка і багато вибухівки. Тому, на мою думку, менше потрібно було залучати людей, які це здійснювали. Відповідно, менше каналів витоку. У таких операціях головне не технічна реалізація, а щоб не «витекла» інформація.

Або така операція, як підрив пропагандиста Владлена Татарського, коли за допомогою жінки пронесли вибухівку в статуетці.

А ось у Лівані була дуже складна операція з тисячами пристроїв, декількома підставними фірмами і не сталося витоку інформації. Ось найбільш складний момент у таких операціях, на мою думку.

Але якщо згадати про Кримський міст – так, це дуже класний кейс.

Ю. Дмитренко

https://news.telegraf.com.ua/mir/2024-09-19/5872211-nashi-spetssluzhbi-takozh-mozhut-provesti-analog-peydzhernoi-ataki-fakhivets-ozvuchiv-nyuansi

https://informator.ua/ru/ukraincy-mogut-byt-bez-sveta-zimoy-do-18-chasov-v-sutki-prognoz-oon

https://www.bbc.com/russian/articles/c23k82gylkno

Виставки по всьому світу - Безпека

Виставка безпеки та здоров'я
December 02, 2024 until December 04, 2024
Лондон - ExCeL Лондон, Англія, Великобританія Виставковий центр ExCel Categories: Краса і здоров'я Ключові слова: здоров'я, Безпека

Шоу добробуту на робочому місці
December 02, 2024 until December 04, 2024
Лондон - ExCeL Лондон, Англія, Великобританія Виставковий центр ExCel Categories: Краса і здоров'я, Освітні послуги Ключові слова: Безпека

SECURA North Africa - Expo & Conference
December 03, 2024 until December 05, 2024
Mohammadia - Safex - Foire d'Alger, провінція Алжир, Алжир Categories: Служба безпеки, Охоронне та охоронне обладнання Ключові слова: Кібербезпека, Рятувальне обладнання, Аварійний, Безпека

Пожежа та безпека Азія
December 24, 2024 until December 26, 2024
Карачі - Карачі Експо Центр, Сінд, Пакистан Карачі Categories: Служба безпеки, Охоронне та охоронне обладнання Ключові слова: Аварійний, Безпека

ШОУ ІНСТРУМЕНТІВ ТА БЕЗПЕКИ
January 22, 2025 until January 25, 2025
Сеул - Конференц-центр COEX, Сеул, Корея Середземне море Categories: Інженерний сектор Ключові слова: Інструменти, Безпека

Безпека Здоров'я та благополуччя Live
January 22, 2025 until January 23, 2025
Манчестер - Центральний конференц-комплекс Манчестера, Англія, Великобританія Windmill Street, Manchester Central, Манчестер, Ланкашир, Англія, M2 3 Categories: Краса і здоров'я Ключові слова: здоров'я, Безпека

Промислова виставка запобігання катастрофам
January 29, 2025 until January 31, 2025
At Koto - Koto, Токіо, Японія Koto, Токіо, Японія Categories: Екологічні послуги, Служба безпеки Ключові слова: Безпека

Конференція та виставка IADC з охорони здоров'я, безпеки, навколишнього середовища та навчання
February 19, 2025 until February 20, 2025
Х'юстон - Конференц-центри Hoppica - Х'юстон/CityCentre, Техас, США Kendra scott Categories: Краса і здоров'я, Освітні послуги Ключові слова: Навколишнє середовище, Навчання, здоров'я, Безпека, подача

Індіана Безпека та здоров'я Конференція & Експо
February 24, 2025 until February 26, 2025
Індіанаполіс - Конференц-центр Індіана, Індіана, США Конференц-центр Індіани Categories: Інженерний сектор, Наукове дослідження, Охорона здоров'я та фармацевтика Ключові слова: ліжко, Нафтохімічні речовини, Літієва батарея, Безпека, Нафта

Індіана Конференція з безпеки та охорони здоров'я та виставка
February 24, 2025 until February 26, 2025
Індіанаполіс - Конференц-центр Індіана, Індіана, США Конференц-центр Індіани Categories: Наукове дослідження, Охорона здоров'я та фармацевтика Ключові слова: Газети, Безпека

Construction Expo & Safety Conference
March 03, 2025 until March 04, 2025
Oakbrook Terrace - Оукбрук Террас, Іллінойс, США O Categories: Будівельний сектор Ключові слова: будівництво, Безпека

Шоу безпеки - Японія
March 04, 2025 until March 07, 2025
Koto - Tokyo Big Sight, Токіо, Японія Categories: Технологічний сектор, Служба безпеки, Охоронне та охоронне обладнання Ключові слова: Безпека, Безпека

Казахстанська міжнародна виставка захисту, безпеки, рятування та пожежної безпеки
March 12, 2025 until March 14, 2025
Алмати - Міжнародний виставковий центр "Атакент", Алматинська область, Казахстан Categories: Служба безпеки, Охоронне та охоронне обладнання Ключові слова: Безпека, Безпека

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

Штучний інтелект на борту відеокамери

У світі штучного інтелекту, що постійно розвивається, можна змигнути і пропустити інновацію. З кожним днем з'являються нові технології, здатні кардинально змінити звичні методи ведення бізнесу, забезпечення безпеки та аналізу даних.

У сфері відеоспостереження штучний інтелект (ШІ) вже не просто доповнення – це необхідний інструмент, який дозволяє компаніям не лише захищати свої активи, а й оптимізувати багато процесів. Сучасні камери з ШІ не просто фіксують те, що відбувається, вони допомагають бачити більше, реагувати швидше та діяти передбачувано, автоматично адаптуючись до поточних умов та вимог. Враховуючи швидкість розвитку цифрових технологій, вкрай важливо вибирати рішення, які не застаріють відразу після впровадження, а слугуватимуть надійною основою для подальшого розвитку та вдосконалення. Розглянемо, як саме штучний інтелект може примножити можливості систем відеоспостереження для бізнесу.

Цінність ШІ у відеоспостереженні

Розвиток штучного інтелекту привніс еволюційні зміни в індустрію відеоспостереження значно розширюючи можливості традиційних систем. Сучасні системи на основі ШІ здатні не лише записувати відео, а й аналізувати його в режимі реального часу, що сприяє досягненню нового рівня безпеки та ефективності.

Використання алгоритмів глибокого навчання дає можливість телекамерам точно класифікувати об'єкти в кадрі, будь то людина, транспортний засіб чи тварина. Це значно скорочує кількість хибних тривог, які часто виникають через нерухомі об'єкти або рухи, викликані природними факторами. Крім того, ШІ може ефективно визначати аномальні ситуації, такі як залишені без нагляду предмети у громадських місцях чи незвичайна поведінка людей, що може вказувати на потенційні загрози чи екстрені ситуації.

Глибока інтеграція розумних камер відеоспостереження з іншими системами безпеки, такими як системи контролю доступу та сигналізації, створює складну та багаторівневу систему захисту. У разі виявлення загрози ШІ-камери можуть автоматично активувати певні процедури безпеки, наприклад, блокування доступу або оповіщення служби охорони. Це забезпечує більш ефективну та швидку відповідь на можливі проблеми.

Для бізнесу використання ШІ у телекамерах відкриває нові можливості: від аналізу поведінки клієнтів до оптимізації роботи персоналу та керування ресурсами. Ці дані допомагають підвищувати рівень продажів, покращувати клієнтський досвід та оптимізувати операційну ефективність, роблячи бізнес більш конкурентоспроможним та прибутковим.

Інтеграція ШІ в системи відеоспостереження надає не лише підвищений рівень безпеки, а й цінні дані для стратегічного аналізу та управління, роблячи інвестиції у такі технології важливим далекоглядним рішенням для будь-якої компанії.

Безпека і конфіденційність даних

Впровадження штучного інтелекту в системи відеоспостереження викликає питання, пов'язані з безпекою та конфіденційністю даних, що збираються. У міру збільшення обсягів та деталізації відеоданих зростає ризик їх несанкціонованого використання, що ставить на порядок денний завдання щодо захисту та обробки персональної інформації.

Однією з критично важливих аспектів є забезпечення захисту даних всіх етапах їх життєвого циклу, від збору до зберігання та використання. Розробка та впровадження надійних механізмів шифрування та автентифікації допомагає запобігти зламуванню та витоку даних. Крім того, необхідне суворе дотримання законів та правил захисту даних, що особливо важливо в різних країнах та регіонах з різними вимогами до конфіденційності.

Питання, пов'язані з моральними питаннями застосування відеоспостереження зі штучним інтелектом, також мають велике значення. Потрібно стежити за тим, щоб відеоспостереження застосовувалося так, щоб не порушувати права та свободи людей та не вторгатися у їхній особистий простір.

Переваги відкритих платформ

Відкриті платформи у системах відеоспостереження пропонують низку значних переваг, які сприяють покращенню інноваційної екосистеми та полегшують адаптацію технологій під специфічні потреби користувачів. Ці платформи забезпечують більш гнучкий підхід до розробки та впровадження нових функцій, оскільки вони підтримують взаємодію безлічі розробників та виробників обладнання.

Головна перевага відкритих платформ полягає в їх масштабованості та модульності. Користувачі та розробники мають можливість додавати та інтегрувати нові функції без обмежень, що накладаються пропрієтарними системами. Це відкриває двері для інновацій і дозволяє системам постійно еволюціонувати і адаптуватися до вимог безпеки та технологій, що змінюються.

Відкритість платформ також сприяє кращій сумісності між різними видами обладнання та програмного забезпечення, що суттєво спрощує інтеграцію нових пристроїв та додатків до існуючих систем. Це зменшує залежність від одного виробника та дає можливість організаціям вибирати найбільш підходящі та ефективні технології для їх конкретних потреб.

Прозорість відкритих платформ також призводить до підвищеної безпеки. З відкритим доступом до коду спільнота може брати активну участь у виявленні та виправленні вразливостей, підвищуючи загальну надійність системи. Крім того, відкриті платформи зазвичай супроводжуються активною спільнотою розробників, яка підтримує користувачів та сприяє розвитку спільної інфраструктури.

Відкриті платформи відеоспостереження надають більше можливостей для налаштування, об'єднання пристроїв та спільної роботи, що робить їх чудовим варіантом для розробки стабільних та гнучких систем, здатних адаптуватися до майбутніх вимог. У наш час, коли гнучкість та інновації мають велике значення, вони допомагають забезпечити високий рівень безпеки та ефективності.

Edge Computing

Edge Computing, простими словами, є децентралізованою архітектурою обчислень, яка наближає обробку даних до джерела даних. На відміну від традиційного хмарного обчислення, де дані відправляються до центральних центрів обробки даних для аналізу, Edge Computing обробляє дані на краю мережі там, де вони генеруються. Це дозволяє аналізувати дані в режимі реального часу, зменшує затримку та підвищує продуктивність додатків.

Локальна обробка даних має кілька ключових переваг. По-перше, вона прискорює реакцію системи на події, що відбуваються, що критично важливо для систем безпеки. По-друге, зниження залежності від центральних серверів та хмарних систем значно підвищує надійність роботи відеоспостереження, особливо в умовах нестабільного інтернет-з'єднання або при атаках на мережну інфраструктуру. Використання Edge Computing також суттєво скорочує витрати на передачу та зберігання даних. Так, як більшість даних обробляється і аналізується на місці, необхідність передачі всіх зібраних даних на віддалені сервери для подальшої обробки мінімізується. Це знижує споживання інтернет-трафіку та зменшує навантаження на хмарні сервери, що веде до оптимізації витрат на зберігання даних.

Обробка даних на периферії допомагає підвищувати рівень конфіденційності та безпеки інформації, оскільки чутливі дані можуть оброблятися і зберігатися локально, не залишаючи території, що охороняється. Це важливо для організацій, які працюють з конфіденційною інформацією або підпорядковуються суворим нормативам захисту даних.

Edge computing ідеально підходить для інтеграції з ШІ в системах відеоспостереження. Алгоритми ШІ, що працюють на периферійних пристроях, можуть миттєво аналізувати вхідне відео, виявляти події, що цікавлять, і вживати заходів без затримок, пов'язаних з необхідністю звернення до центральних серверів.

Технологія Edge Computin є не тільки способом підвищення ефективності відеоспостереження, але це ще й метод зниження операційних витрат, покращення безпеки та підвищення швидкості обробки даних. Це робить цю технологію незамінним інструментом у сучасній інфраструктурі відеоспостереження, адаптованої до вимог цифрової доби.

Одним із варіантів впровадження технології Edge Computin у галузь відеоспостереження є смарт камери.

Смарт камери

Смарт камери відеоспостереження – це сучасні пристрої, які об'єднують функції традиційних камер з додатковими можливостями завдяки підключенню до Інтернету та використанню штучного інтелекту. Ось кілька ключових особливостей смарт камер:

Віддалений доступ: Ви можете переглядати відео в реальному часі або записи з будь-якого місця через мобільний додаток або веб-браузер.

Датчики руху: Камери можуть автоматично починати запис або надсилати сповіщення, коли виявляють рух.

Нічне бачення: Завдяки інфрачервоним світлодіодам, камери можуть знімати у темряві.

Двосторонній звук: Деякі моделі дозволяють не тільки чути, що відбувається, а й говорити через камеру.

Інтеграція з іншими пристроями: Смарт камери можуть працювати разом з іншими розумними пристроями, такими як системи безпеки, освітлення та голосові помічники.

Розглянемо більш детально функціонал смарт відеокамер.

Нові можливості камер та відеореєстраторів: PID, LCD, PD/VD, FD, SOD, CC, HM, CD, QD, RSD, LPD – що приховується за латинськими літерами позначень?

Застосування IP технологій у системах відеоспостереження значно розширило обрії можливостей для автоматизації контролю безпеки та моніторингу бізнес-процесів.

Алгоритми машинного навчання, крім відомих та популярних функцій IP камер та відеореєстраторів (висока роздільна здатність, деталізація зображення, якісна нічна зйомка, віддалене керування з телефону тощо), забезпечують системи наступними функціональними можливостями:

PID – виявлення вторгнень по периметру;

LCD – виявлення перетину ліній;

SOD – пошук залишених чи втрачених предметів;

PD – виявлення пішоходів;

VD – виявлення транспорту;

FD – розпізнавання облич;

CC – підрахунок відвідувачів;

HM – теплова карта;

CD – виявлення щільності скупчення людей;

QD – визначення довжини черги;

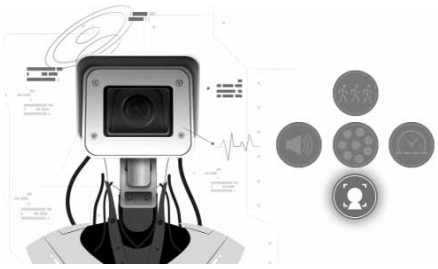
RSD – виявлення гучних звуків;

LPD – розпізнавання номерних знаків автотранспорту.

Можливості камери відеоспостереження з функцією розпізнавання обличчя (FD)

Камера виявляє обличчя людини, яка рухається в запрограмованій зоні і при спрацюванні датчика виконує такі дії:

– порівняння виявленої особи зі знімком, збереженим у базі даних;



–ведення бази даних за білим та чорним списком відвідувачів;

– налаштування сумісності із системою контролю доступу.

Як функцію розпізнавання обличчя можна використовувати для бізнесу?

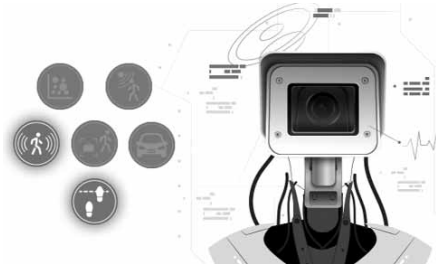
Підвищення якості обслуговування клієнтів. Наприклад, до офісу прийшов VIP клієнт, якому необхідно приділити

максимум уваги. Камера фіксує обличчя, звіряє фото з базою даних та повідомляє відповідального співробітника про прихід важливого відвідувача. Співробітник зустрічає гостя та забезпечує йому відповідний прийом, підвищуючи лояльність клієнта до бізнесу.

Забезпечення надійної захисту від злодіїв чи порушників громадського порядку. Камера зафіксує зловмисника, навіть якщо його не вдалося піймати «на гарячому», і занесе його до списку небажаних відвідувачів. У майбутньому, як тільки ця людина з'явиться у полі зору камери, тривожне повідомлення повідомить охорону щодо потенційної загрози.

Функції виявлення вторгнень по периметру PID та перетину ліній LCD: як це працює?

Функція PID виявляє людей, транспортні засоби чи інші об'єкти в зоні камери (встановлюється у налаштуваннях).



Порушенням вважатиметься не перетин віртуальної лінії, а проникнення об'єкта всередину периметра. Він також позначається віртуально за допомогою інтерфейсу камери, як правило зеленим прямокутником.

Рух транспортного засобу фіксується в будь-якому напрямку (ліворуч, праворуч, вперед, назад).

Камера виявляє автомобілі, автобуси, вантажні машини, мотоцикли, мопеди, велосипеди, що припарковані всередині периметра або рухаються зі швидкістю до 15 км/год.

Де рекомендовано встановлювати камери відеоспостереження з функцією виявлення вторгнення по периметру?

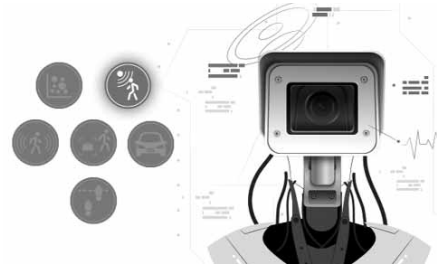
– міжквартальні проїзди;
– внутрішні двори офісних будівель;
– двори багатоквартирних будинків;
– паркінги;
– вуличні парковки, тощо.

Застосування функції виявлення перетину ліній (LCD) дозволяє відстежувати людей, транспорт чи інші рухомі об'єкти при перетині віртуальної лінії. У налаштуваннях можна встановити різні конфігурації:

– в одному напрямку A-> B, B-> A;
– у двох напрямках A <-> B.

Які завдання функцій виявлення пішоходів (PD) та виявлення транспорту (VD)?

Камера відеоспостереження з інтелектуальними функціями PD та VD – чудовий помічник під час досліджень дорожньо-транспортних пригод.



Камери та відеореєстратори з функцією виявлення транспорту/пішоходів можна налаштувати на фіксування чітко визначених цілей. У меню можна встановити параметри відстеження: лише статичний чи рухомий об'єкт.

Кількість одночасних розпізнавань залежить від моделі камери чи реєстратора.

Користувач може запрограмувати систему так, щоб вона фокусувалася тільки на людях чи автомобілях, за винятком іншого зі списку подій.

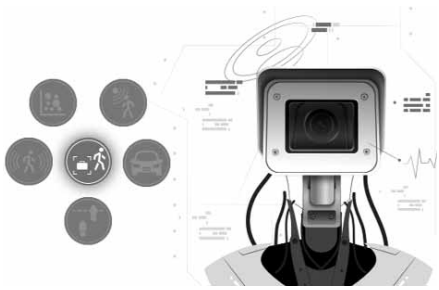
Алгоритми побудовані таким чином, щоб не було хибних спрацьовувань. Наприклад, поява в зоні дії камер тварин, комах, птахів, сильного вітру та інших перешкод, через які охоронна сигналізація надсилає повідомлення користувачеві про рух пізно вночі.

Функція виявлення стаціонарних об'єктів (SOD) – можливість виявляти забуті чи втрачені предмети

Функція допомагає виявити стаціонарні об'єкти на запрограмованій ділянці біля зони дії камери відеоспостереження.

Камера розпізнає забуті або спеціально залишені предмети, наприклад:

– багаж;
– гаманець;
– сумка;
– пакети;
– небезпечні матеріали та інше.



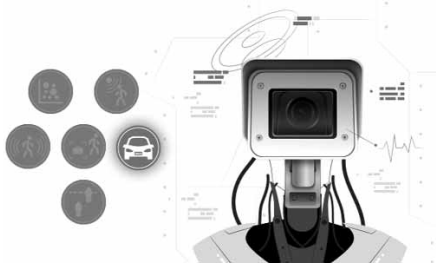
У налаштуваннях камери можна встановити надсилання тривожного сигналу при виявленні статичного об'єкта.

Крім того, камери з інтелектуальною функцією можна використовувати на автостоянках та в паркінгах. Наприклад, для виявлення незнайомого автомобіля.

Камери з функцією LPD – визначення номерних знаків

Відеокамери з цією функцією, як правило встановлюють на в'їзді/виїзді:

– у паркінг;
– на СТО;
– на гаражну стоянку;
– на паркування для відвідувачів магазину чи бізнес-центру;
– на територію житлових корпусів чи котеджних селищ тощо.

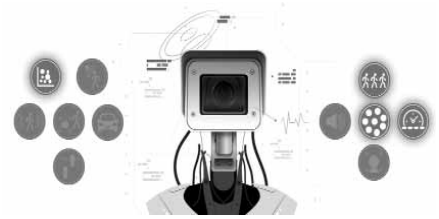


Встановлення інтелектуальних камер відеоспостереження підвищує ефективність контролю безпеки на вказаних об'єктах.

Інтелектуальні можливості систем відеоспостереження, які можна використовувати у торгівлі чи сфері послуг

– **СС** підрахунок відвідувачів. Використовує алгоритм перехресного рахунку для виявлення часу переміщення об'єктів чи людей віртуальними лініями.

Штучний інтелект розпізнає об'єкти, що рухаються на зображенні та підраховує їх кількість.



ВАЖЛИВО! У зоні дії камер не повинно бути автоматичних або обертових дверей та інших рухомих деталей інтер'єру.

– **HM** теплова карта – зручний інструмент для аналізу бізнес-процесів або проведення слідчих дій чи експертиз. Виявляє зони із найбільшою концентрацією людей. Інформація експортується до спеціального звіту. У меню керування можна налаштувати параметри звіту.

– **CD** виявлення щільності натовпу, чим можна вирішити проблему магазинів із обслуговуванням покупців у години пік. Камера надсилає повідомлення про скупчення людей у черзі, що дозволяє своєчасно розвантажувати обслуговуючий персонал та покращувати якість сервісу.

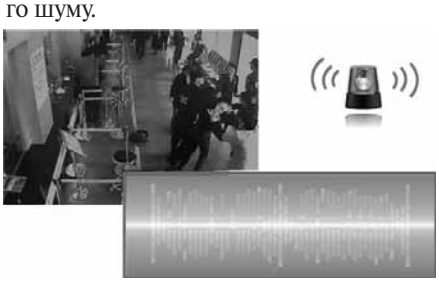
– **QD** визначення довжини черги, визначає кількість об'єктів, що детектуються в черзі, що потрапляють у поле зору IP-відеокамер, та відправляє повідомлення при перевищенні заданого порога кількості об'єктів. Аналітичний модуль формує звіти, групує виникнення черг по зонах та зберігає відео з часовими відрізками, що фіксують момент утворення черги.

Які ще інтелектуальні можливості мають IP камер відеоспостереження нового покоління?

RSD – виявлення та аналіз звуків

За наявності мікрофона (вбудованого або підключеного до аудіо виходу) фіксує та записує на картку пам'яті/жорсткий диск події, що перевищують допустимий рівень звуку (встановлюється користувачем у налаштуваннях) або подає сигнал тривоги. Наприклад, крики, вибухи тощо.

Хибна тривога є малоймовірною, оскільки сучасні SMART IP-камери обладнані передовими фільтрами фонового шуму.



Функція ActiveDeterrence

Активна тривога – покращує охоронні функції системи відеоспостереження. При виникненні небезпеки включається світлове (синя/червона лампочка) та звукове (вбудована сирена) оповіщення.

Передача архівів відеозаписів на хмарне сховище Dropbox\Googledisk

Використовується на об'єктах, де потрібне довгострокове та безпечне зберігання даних. Крім того, це чудова можливість мати доступ до архівів у режимі віддаленого доступу.

Функція ANR

Розшифровується як AutoNetworkResume, розроблена для IP систем відеоспостереження, що працюють у нестабільній мережній інфраструктурі.

Функція дозволяє зберегти та відновити відеозапис при обриві з'єднання між реєстратором та відеокамерою. При обриві з'єднання відео записується на SD карту, встановлену у відеокамері, а після відновлення з'єднання дані з SD карти копіюються в архів реєстратора.

Антитуман

Антитуман – це дуже корисна функція для вуличних SMART IP-камер, яка дозволяє в автоматичному режимі покращувати якість зображення в умовах низької видимості, туману, запиленості, або невеликого снігопаду. Якість зображення покращується шляхом регулювання рівня контрастності та компенсування задимлення картинки.

Автостеження

Функція автостеження є необхідністю для IP-камер, що встановлюються в місцях великого скупчення людей, таких як аеропорти, вокзали, великі супермаркети та автомобільні паркування. Камера стежить за пересуванням об'єктів у кадрі, відстежує траєкторію руху, фіксує нестандартну поведінку, а також визначатиме залишені предмети. Залежно від заданого сценарію поведінки, камера самостійно обробить подію та подасть, у разі потреби, сигнал тривоги.

Область інтересу (ROI – Region of Interest)

Функція ROI дозволяє змінювати якість зображення в окремих областях. Оператор відеоспостереження може самостійно встановити до чотирьох областей у кадрі, в яких буде деталізоване зображення, при цьому, у невиділеній області кадру якість зображення знизиться. Функція «Область інтересу» дозволяє покращувати якість зображення, не збільшуючи швидкості потоку передачі даних, що дозволяє оптимально використовувати пропускну здатність каналу та зменшити необхідний дисковий простір для зберігання відео.

Детектування зміни якості відео (VQD – Video Quality Detection)

Детектування зміни якості відео є функцією, що безпосередньо впливає на якість зображення, а також на безпеку відео. При зміні сцени зйомки, розфокусуванні, фальсифікації відео, а також при розриві з'єднання з камерою подається сигнал тривоги на пульт оператора відеоспостереження.

Режим коридору

Функція «Режим коридору» призначена для відеоспостереження в довгих

коридорах. Режим коридору активується в налаштуваннях камери і зображення змінює орієнтацію з 16:9 на 9:16, при якому в кадр потрапляє тільки вертикальна область коридору, з мінімальним включенням в кадр стін.

Розумне ІЧ-підсвічування (Smart IR)

Функція розумного інфрачервоного підсвічування дозволяє камері автоматично налаштовувати інтенсивність свічення інфрачервоного підсвічування залежно від відстані до об'єкта, що потрапив у кадр. Розумне ІЧ-підсвічування прибирає недолік IP-камер зі звичайним ІЧ-підсвічуванням, де, при наближенні об'єкта до камери на близьку відстань, можливе засвічення зображення.

Виконання SMART IP-камер

SMART IP-камери випускаються у двох виконаннях: внутрішньому, для використання всередині приміщень, та вуличному, для встановлення поза приміщеннями. IP-камери, призначені для ву-

личного використання, мають пиловологозахищений корпус, а також можуть мати вандалозахист. Моделі, призначені для використання в зимових умовах, мають спеціальний внутрішній підігрівач, який забезпечує нормальне функціонування камери в суворі зимові морози.

Економічна вигода та рентабельність інвестицій

Економічна вигода від впровадження систем відеоспостереження зі штучним інтелектом виражається через різні аспекти, що впливають на загальну рентабельність інвестицій. Використання передових технологій сприяє не лише підвищенню рівня безпеки, а й суттєвому зниженню витрат на експлуатацію та обслуговування систем.

Один з основних економічних ефектів – це зниження витрат на працю. Автоматизація процесів моніторингу та аналізу даних зменшує потребу у великих оперативних командах. Системи з ШІ здатні обробляти великі обсяги даних швидше та точніше, що знижує ризик людських помилок та прискорює процес прийняття рішень.

Додатковою економічною перевагою є підвищення ефективності обслуговування та технічної підтримки систем. Сучасні системи відеоспостереження можуть самостійно діагностувати неполадки та визначати необхідність у технічному обслуговуванні, що мінімізує простої та запобігає дорогому ремонту.

Застосування відеоспостереження також впливає на зниження операційних ризиків та втрат від непередбачених подій, таких як крадіжки, вандалізм чи виробничі аварії. Системи з ШІ можуть попереджати про потенційні загрози та автоматично активувати заходи щодо їх запобігання, що суттєво підвищує рівень захищеності об'єктів.

Інвестиції в інтегровані системи відеоспостереження окупаються не лише за рахунок прямої економії, а й через підвищення загальної цінності підприємств завдяки покращенню якості обслуговування та рівня безпеки.

Інновації і майбутнє відеоспостереження

Майбутнє систем відеоспостереження обіцяє бути насиченим новизною завдяки розвитку технологій штучного інтелекту і машинного навчання, що продовжується. Постійне вдосконалення ШІ покращує не тільки існуючі функції, а й відчиняє двері для створення нових, більш інтелектуальних та автономних систем відеоспостереження.

Одним із напрямків інновацій є покращення алгоритмів розпізнавання та аналізу відеозображення для більш точної ідентифікації об'єктів та аналізу моделей поведінки в реальному часі. Це значно підвищить ефективність моніторингу та дозволить прогнозувати різні ситуації на основі аналізу одержуваної відеоінформації.

Розвиток Edge Computing продовжить посилювати тенденцію до децентралізації обробки даних, що зробить системи відеоспостереження більш надійними та швидкими за умов, коли кожна секунда на рахунку. Впровадження більш розвинених технологій шифрування та забезпечення анонімності на рівні пристроїв зміцнить захист приватності та забезпечить більш високий рівень захисту даних.

У найближчому майбутньому можна очікувати появи біометричних технологій, таких як розпізнавання за ходою або аналіз жестів, що відкриє нові можливості для систем безпеки та персоналізованих послуг. Штучний інтелект дозволить аналізувати складні ситуації та пристосовуватися до змін у навколишній обстановці, завдяки чому відеоспостереження стане не лише засобом забезпечення безпеки, а й способом покращити якість життя.

Інтеграція відеоспостереження з іншими технологіями, такими як інтернет речей (IoT) та розумні міські системи, забезпечить створення багатофункціональних, взаємодіючих та автоматизованих систем, які можуть бути застосовані в різних областях, від управління міським трафіком до екологічного моніторингу.

Амбіції та технології в галузі відеоспостереження розвиваються, якість та функціональність систем покращуються з кожним новим поколінням. Завдяки цьому ми можемо бути впевнені, що майбутнє відеоспостереження стане ще більш інтегрованим, безпечним і продуктивним.

Підсумки

Системи відеоспостереження з інтеграцією штучного інтелекту на борту відеокамер є важливим інструментом в арсеналі сучасних технологій безпеки. Впровадження ШІ у системи відеоспостереження не тільки розширює їх функціональні можливості, роблячи їх ефективнішими і розумними, а й відкриває нові перспективи їх застосування у різних галузях. Значні переваги, такі як покращення якості моніторингу, оптимізація ресурсів, підвищення безпеки даних та збільшення економічної вигоди роблять інвестиції в ці технології дуже привабливими.

Завдяки здатності до адаптації під різні вимоги та можливості інтеграції з іншими системами відеоспостереження на базі ШІ стає міцною складовою розумних міст, виробничих комплексів, роздрібної торгівлі та інших сфер. Це сприяє зміцненню не тільки фізичної, а й інформаційної безпеки, забезпечуючи захист персональних даних.

Відкритість платформ та постійне впровадження інновацій надають ґрунт для подальшого розвитку та вдосконалення технологій відеоспостереження. Передові підходи в області ШІ призводять до створення все більш розумних, ефективних і автономних систем, здатних набагато більше, ніж просто реєстрація зображень. Вони стають справжніми помічниками у прийнятті рішень та управлінні безпекою, що робить їх невід'ємною частиною сучасної інфраструктури будь-якого масштабу.

Ю. Дмитренко

За матеріалами:

https://securtv.ru/presscenter/3884.html

https://greenvision.ua/blog/iskusstvennii-intellekt-IP-kameri?srsltid=AfmBOoqA50SeceYjLpOm-mDdSGXqAI-Up8hpDtATqlFu7bEhEbTENr4cX

https://www.vtkt.ru/articles/network_security/SMART_IP-cameras.php

Впровадження автоматизованих систем централізованого оповіщення територіальних громад

Науково-виробниче підприємство «ОЗОН С» більш 20 років спеціалізується на організаційно-технічному забезпеченні безпеки життєдіяльності населення у надзвичайних ситуаціях техногенного, природного, екологічного, соціального, терористичного та воєнного характеру.

Серед наших замовників: Кабінет Міністрів України, ДСНС України, обласні, міські та районні державні адміністрації, органи місцевого самоврядування територіальних громад, Головні управління та військові частини Міністерства оборони, Міністерства внутрішніх справ та Служби безпеки України, об'єкти НАК «Нафтогаз України», підприємства Держрезерву, найбільші підприємства хімічної, машинобудівної та гірничо-металургійної галузей, енергогенеруючі компанії, об'єкти виготовлення, збереження, ремонту та утилізації боєприпасів, морські порти, нафтобази й інші об'єкти підвищеної небезпеки.

Станом на сьогоднішній день у багатьох областях України впроваджено більше п'ятдесяти автоматизованих систем централізованого оповіщення, які у теперішній воєнний час сповіщають понад 3,5 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 27.09.2017 р. №733, відповідних наказів та рекомендацій ДСНС України. Всі проєкти розробляються у повній відповідності до погоджених 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 НДІ цивільного захисту, ДСНС України та у встановленому порядку зареєстрованими у державному центрі стандартизації, метрології та сертифікації.

До складу 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.

Наша команда має багаторічний досвід розробки і виробництва МАСЦО та для підвищення ефективності й надійності експлуатації впроваджує новітні технології захищені патентами на винахід, які підтверджують їх світову новизну. Кінцеві технічні засоби оповіщення населення на відкритих територіях мають у своєму складі автономні сонячні електростанції з вбудованими акумуляторами, що забезпечує їх працездатність при цілодобових відключеннях в мережах електроживлення.

На кожному етапі виробництва від вибору комплектуючих виробів до вихідного контролю складових системи здійснюється багатоступінчасте тестування. Усе обладнання перевіряється на відповідність стандартам якості та безпеки. Окрім виробництва обладнання забезпечується його повний технічний супровід, а також проводиться навчання відповідального персоналу для ефективної експлуатації систем. При проєктуванні та введені систем в експлуатацію враховується унікальність кожної громади та пропонуються рішення, що максимально відповідають специфічним умовам та вимогам.

У теперішній час, незважаючи на постійні повітряні атаки в місті Херсоні та в громадах Херсонської області, виконуються роботи по впровадженню МАСЦО.

Окремо слід зазначити, що наші підприємства мають успішний досвід співпраці з іноземними партнерами. В рамках спільної донорської програми Уряду України та восьми держав-партнерів, що реалізує проєкти в деокупованих і прифронтових громадах, а також на національному рівні - «Партнерство за сильну Україну», впроваджено МАСЦО в чотирьох прикордонних громадах Чернігівської області, що потерпають від обстрілів агресора. До кінця поточного року планується впровадження МАСЦО м. Чернігова.

Компанія «ОЗОН С» висловлює готовність бути надійним партнером 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 першого кварталу 2025 року для передплатників журналу «Бізнес і безпека» пропонується 20% знижка на розробку проєктів МАСЦО.

Вісім доказів небезпеки телеграму — одного з найуспішніших російських проєктів

Сьогодні телеграм є одним із найпопулярніших застосунків по обидва боки українсько-російського фронту, про що свідчать дані Similarweb по Україні та Росії. Станом на кінець 2023 року він обслуговував 25 мільйонів росіян і 7 мільйонів українців. Більшість наших міністерств, держадміністрацій, новинних сайтів і лідерів думок є його активними користувачами. Те саме можна сказати й про Росію.

Телеграм — один із найуспішніших російських проєктів XXI століття. Хоча представники месенджера і його власник Павло Дуров роблять все, щоб їх перестали асоціювати з Росією, це й досі російський застосунок. У нього російські розробники, він має сервери в Росії, і є численні докази його співпраці з Кремлем.

Телеграм з'явився у 2013-му й протягом 11 років встиг перетворитися зі звичайного месенджера на потужну соцмережу з анонімними каналами, новинами, ботами й криптовалютою, де можна купити що завгодно.

Дуров і компанія змогли переконати багатьох українців у незалежності від Росії, але ця незалежність існує лише в заявах, тоді як на практиці телеграм — потужна інформаційна й розвідувальна зброя Кремля. Розповідаємо, що відомо про цю платформу.

700 мільйонів

Після повномасштабного вторгнення українці стали у вісім разів більше часу проводити в телеграмі. Пік популярності припав на 28 лютого — 6 березня 2022 року, коли ми щодня проводили в телеграмі годину. Волонтери й держава навчилися використовувати цю платформу для координації роботи. Завдяки анонімним ботам біженці в перші місяці великої війни могли знаходити місця для ночівлі й дізнаватися про умови перебування за кордоном. Нині телеграм сповіщає про повітряну тривогу там, де не чути сирен. У ньому працюють боти для збору інформації як про російські, так і про українські техніку та війська.

У червні 2022-го телеграм мав 700 мільйонів користувачів і контролював 4% ринку месенджерів, ставши найпопулярнішим застосунком для спілкування в Білорусі, Казахстані, Молдові, Азербайджані, Киргизстані, Йорданії та Камбоджі. У 2023-му він посів четверте місце за популярністю серед застосунків для спілкування на планеті. Це якщо не зважати на китайські WeChat та QQ, відомі лише в КНР. На першому місці за чисельністю аудиторії Індія, де живе 70 мільйонів його користувачів.

Телеграм також став основним джерелом новин і місцем для спілкування в Ірані. 2016 року 20 із 83 мільйонів (20%) іранців були його користувачами. Але Міжнародний комітет із захисту журналістів порекомендував іранським журналістам не користуватися телеграмом через проблеми з безпекою.

Через майже цілковиту відсутність цензури в телеграмі можна знайти буквально все. Окрім новинної стрічки він також працює як величезний маркетплейс. Це чимось схоже на напівананімний даркнет, зайти в який можна в один клік.

Вистава

У грудні 2013-го в російських ЗМІ з'явилася інформація про те, що ФСБ вимагала від соцмережі «ВКонтакте» надати дані про учасників груп, пов'язаних із Євромайданом (зокрема, «Ми патріоти України», «Фьодорич — гарант Конституції», «Український наступ», «Козацький цитатник» та багатьох інших). Дуров заявив, що відмовився це робити.

Далі Дуров писав: «Захист особистих даних людей того вартий і коштує значно більше. З грудня 2013 року я не маю власності, але в мене лишилося дещо важливіше — чисте сумління та ідеали, які я готовий захищати».

Після продажу частки Дурова у «ВКонтакте» та звільнення з посади директора він повідомив, що емігрував із Росії. Хоча, за інформацією його колишнього колеги Антона Розенберга, восени 2014 року Дуров без зайвого шуму й піару повертався жити до рідного Санкт-Петербурга.

З 2014 року основним проєктом братів Дурових є телеграм. Вони створили його, коли працювали у «ВКонтакте». І деякий час (принаймні до вересня 2017-го) розробники як телеграму, так і ВК, до якого з 2014-го Дуров уже начебто не мав стосунку, працювали разом у будинку Зінґера на Невському проспекті в Петербурзі.

Далі ми розглянемо факти, які свідчать про те, що телеграм і зараз тісно пов'язаний із Росією.

1. Російське фінансування

Телеграм ніколи не був прибутковим. За приблизними оцінками, станом на кінець цього року загальні борги компанії мали перетнути позначку 530 млн доларів. Перші вісім років телеграм офіційно нічого не заробляв, а 2021-го на каналах стали з'являтися рекламні публікації.

Щоб розміщувати рекламу на каналах, замовник мав покласти на рахунок щонайменше 2 млн євро. Перші оголошення рекламували криптовалюту, іпотеки, жовті новини та сумнівні курси.

З червня 2022 року працює преміум-підписка для користувачів, яка коштує 5 доларів на місяць. Дуров каже, що до 2021-го розробку й сервери він оплачував із власних коштів. Російський «Форбс» оцінив тодішню частку Дурова у «ВКонтакте» в 400 млн доларів.

Але фінансова історія телеграму має й цікавіші сторінки: у 2018 та 2021 роках Дуров залучив 2,5 млрд доларів на запуск криптовалюти і покриття боргів компанії. Після невдалої спроби отримати дозвіл на фінансові операції від Комісії з цінних паперів та бірж США Дурову довелося повернути ці гроші з відсотками.

У 2018 році в документах для Комісії Дуров звітував, що отримав 850 млн доларів від 81 інвестора. Імен інвесторів він не називав, але частина з них самі заявили про свої інвестиції. Серед перших офіційних інвесторів телеграму були:

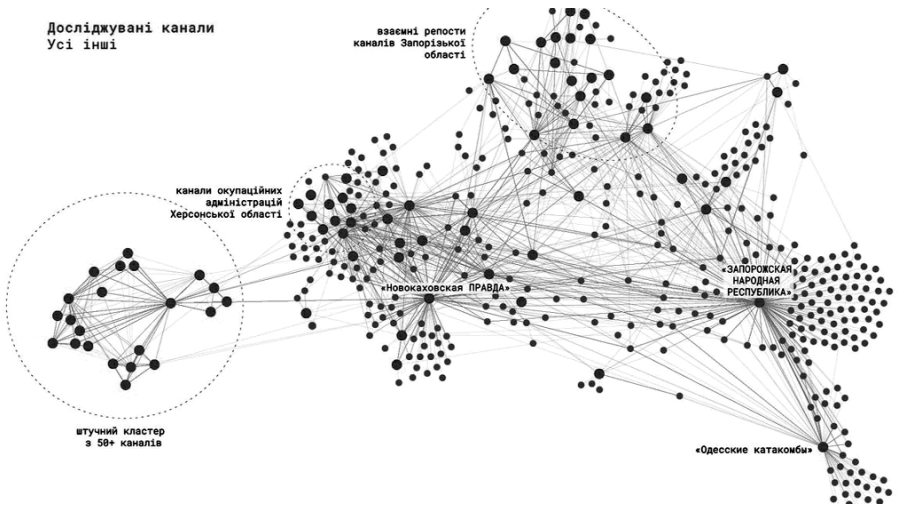
- російський мільярдер Роман Абрамович (вклад 17 млн доларів);
- засновник російської платіжної системи Qiwi Сергій Солонін (10 млн доларів);
- колишній власник компанії «Вімм-Білль-Данн» російський олігарх Давид Якобашвілі, проти якого Україна ввела санкції за наближеність до путінського режиму.

Втративши гроші на ідеї криптовалют, у 2021-му представники Дурових розмістили облігації на Санкт-Петербурзькій фондовій біржі. Зазвичай вибір біржі залежить від місцезнаходження потенційних інвесторів. Отже, Дуров розраховував саме на російські активи.

У 2021 році компанія «ВТБ-капітал» витратила понад 1 млрд доларів на облігації телеграму. Ця компанія на 60% належить російській державі, нею понад 20 років керує партнер Путіна Андрій Костін.

Ще одним покупцем облігацій став «Альфа-Капітал», що належить російському олігархові львівського походження Михайлові Фрідману, підсанкційній особі в Україні та Євросоюзі. Старша донька Путіна Марія деякий час керувала благодійним проєктом «Альфа-Ендо», який фінансував Фрідман. Це свідчить про тісні стосунки між олігархом і диктатором.

До націоналізації в липні 2023 року Фрідману також належали український Сенс Банк (колишній Альфа-банк Україна), мобільний оператор «Київстар» і виробник Моршинської мінеральної води. Російська компанія Фрідмана «АльфаСтрахование» станом на травень 2023-го співпрацювала з Росгвардією, страхуючи російських окупантів.



2. Блокування і розблокування

Легенда, що телеграм не здає даних владі, дістала розвиток 2017 року. Внаслідок теракту в петербурзькому метро загинуло 16 лю-

дей. ФСБ заявила, що злочинці координували дії в телеграмі, й вимагала від Дурова надати їй так звані ключі шифрування. За легендою, вони дали б змогу ФСБ читати листування підозрюваних. Тим часом Роскомнагляд подав на соцмережу до суду, обіцяючи заблокувати її в Росії у разі відмови надати ключі. Дуров заявив, що спецслужби не отримають такої інформації.

Телеграм програв суд, і в квітні 2018 року Роскомнагляд постановив заблокувати месенджер. Але це «блокування» було максимально неефективним, бо Роскомнагляд блокував адреси, що не стосувалися телеграму. У результаті месенджер працював і далі, а сервіси Google, Microsoft та Amazon час від часу були недоступними, коли Роскомнагляд блокував доступ до їх серверів. Рекордом було блокування 20 млн IP-адрес за один день. Телеграм продовжив роботу, але жоден із сервісів Google тоді не працював.

Для порівняння: для успішного блокування фейсбуку та інстаграму в Росії знадобилося кілька днів (зараз ці соцмережі доступні лише через VPN).

Можна зробити висновок, що російська влада й не планувала блокувати телеграм і лише вдавала боротьбу з ним та незалежність Дурова. Здійснити таке блокування нескладно. Так, під час протестів 2021 року на Кубі заблокували основні месенджери, серед яких був і телеграм.

2020 року журналісти Wired попросили колишнього спікера Роскомнагляду прокоментувати блокування. Відповідь була така: «Я ватнік, а в нинішній ситуації брати участь в американських розслідуваннях — це западло. Бережіть себе». Кінець цитати.

Як і в історії з гучним виїздом і тихим поверненням Дурова, на відміну від широко обговорюваного блокування «розблокування» телеграму пройшло майже непомітно.

Заступник голови Мінкомзв'язку РФ Олексій Волін заявив, що Роскомнагляд і прокуратура припинили блокування, оскільки воно «технічно неможливе», а сама команда месенджера вже співпрацює з владою. Отже, тоді було офіційно визнано, що принаймні з літа 2018-го телеграм співпрацював із російськими спецслужбами.

У березні 2022 року заступник керівника Комітету з інформаційної політики, інформаційних технологій і зв'язку Росії Олег Матвєйчев заявив: «Дуров знайшов компроміс із ФСБ... Телеграм установив обладнання, щоб можна було стежити за всіма небезпечними суб'єктами».

Згідно із законом про захист приватних даних РФ усі великі компанії, що мають на своїх серверах приватні дані росіян, зобов'язані тримати ці сервери на території Росії. Телеграм успішно працює на території цієї країни, дотримуючись її законів. Що не раз підтверджували представники місцевої влади. Отже, сервери з нашим листуванням і приватними даними телеграм тримає там само, у Росії.

3. Співпраця з урядами

За даними російської «Новой газеты», 2011 року, невдовзі після перших мітингів на Болотній площі в Москві, Павло Дуров у листуванні з Владиславом Сурковим, одним із ідеологів нападу на Україну та спроб створення «Новоросії», писав про свою соцмережу «ВКонтакте»: «Як ви знаєте, ми вже кілька років співпрацюємо з ФСБ та відділом «К» МВС, оперативно видаючи інформацію про тисячі користувачів нашої мережі у вигляді IP-адрес, номерів мобільних телефонів та іншої інформації, необхідної для їх ідентифікації».

Далі Дуров писав, що не треба блокувати опозиційні спільноти, адже це призведе до відпливу користувачів на західні платформи, які Росія вже не зможе контролювати. Такого підходу Дуров дотримується й нині, тому канали в телеграмі майже ніколи не блокуються, незважаючи на контент.

У 2017 році у відповідь на прохання іранської влади Дуров заблокував один із основних опозиційних каналів Ірану. У 2019-му під час протестів у Москві Роскомнагляд вимкнув увесь мобільний інтернет, а анонімний телеграм-канал «Товарищ майор» опублікував архів особистих даних 3000 учасників мітингу. У метаданих файла було зазначено, що його створено в Головному управлінні МВС Росії в Москві. До речі, цей канал теж ніхто не блокував.

Але з демократичними урядами телеграм не поспішає співпрацювати. Єдиним публічним випадком співпраці телеграму із західними країнами є Німеччина. Після численних проігнорованих росіянами запитів щодо блокування екстремістських груп у німецькій урядовій газеті вийшло відкрите звернення до Дурова, і той відповів. Після переговорів німецька поліція оголосила про блокування 81 каналу й 90 груп. За даними видання Spiegel, телеграм створив для поліції електронну пошту для комунікації.

4. В Україні

В Україні велику популярність телеграм здобув наприкінці 2018 року, перед доленосними виборами президента. Тоді тут з'явилося близько 15 анонімних новинних каналів, які багато хто пов'язував із Росією. Вони стрімко набрали популярність і почали впливати на громадську думку, поширювати фейки та пропаганду.

Як писали Texty.org.ua, найпопулярнішими каналами, які читали 2020 року депутати Верховної Ради від «Слуги народу», були такі (всі вони проросійські):

- Легитимный, анонімний;
- Резидент, анонімний;
- Темный рыцарь, анонімний;
- Макс Бужанский — канал нардепа Максима Бужанського;
- Dubinsky.pro — канал нардепа Олександра Дубінського.

Анонімний проросійський канал «НачШтабу» навіть рекламували на київських білбордах. СБУ викрила керівника антиукраїнської мережі каналів, який отримував вказівки з Росії. Ним виявився одесит, один із організаторів заворушень під час одеського Антимайдану.

5. Шифрування

Наскрізне шифрування (End-to-end або E2E-encryption) — надійний спосіб захисту даних, зокрема текстового листування. Ключі для розшифровки таких даних містяться лише на пристрої, що надіслав ці дані, і на пристрої отримувача. Будь-хто інший, якщо навіть дістане доступ до зашифрованого листування, не зможе його розшифрувати без отримання ключів із будь-якого з цих пристроїв. Отже, дані, зашифровані наскрізним шифруванням, можна розшифрувати лише на пристроях відправника й отримувача.

У 2015 році Дуров в інтерв'ю заявив, що великою проблемою WhatsApp є приватність, а телеграм значно захищеніший. Але це, м'яко кажучи, неправда.

У телеграмі наскрізне шифрування відсутнє за умовчанням, його можна вмикати вручну лише для секретних чатів. Їх можна створювати тільки зі смартфона, з комп'ютера цих чатів не видно. Для кожного співрозмовника треба вручну створити окремий секретний чат.

Крім того, незалежні аналітики не можуть провести аналіз коду телеграму. Вихідний код застосунків для смартфонів і комп'ютера справді відкритий, але серверний код телеграму закритий. Тому достеменно невідомо, що відбувається з листуванням, коли воно опиняється на серверах, але зрозуміло одне: таке листування в більшості випадків не зашифроване наскрізним шифруванням.

Щоб побачити, як телеграм може розшифровувати збережені на своїх серверах контакти, файли та всі отримані й надіслані повідомлення, достатньо взяти новий смартфон, встановити на нього телеграм і увійти у свій акаунт. Ви побачите все своє попереднє листування. Про цю проблему писали 2016 року дослідник кібербезпеки Німа Фатемі й засновник месенджера Signal Моксі Марлінспайк.

Це підтвердив виданню Wired Еліес Кампо, який п'ять років працював у телеграмі. Після публікації представники телеграму заявили, що це неправда й що Кампо ніколи там не працював, лише недовго був волонтером. У відповідь Кампо передав журналістам документи за кілька років роботи в компанії (2016–2021), а також скриншоти листування зі своєї електронної пошти на домені телеграму з керівниками Apple, Spotify і Stripe від імені компанії.

Також він надав копії контрактів між телеграмом та іншими компаніями зі своїм підписом. Ще одне підтвердження того, що дані зберігаються на серверах у незашифрованому вигляді, журналісти Wired отримали в приватній бесіді з одним із колишніх розробників месенджера, який попросив не називати його імені. Керівник служби підтримки телеграму Маркус Ра підтвердив, що несекретні чати на серверах телеграму можуть розшифрувати працівники компанії.

І до наскрізно зашифрованих секретних чатів також є питання: коли користувач надсилає адресу сайту в телеграмі, у чаті з'явиться скриншот цього сайту. У 2021 році німецький дослідник виявив, що телеграм створює попередній перегляд посилань на своїх серверах як для звичайних, так і для секретних чатів, а отже, має доступ і до так званого секретного листування.

Хоча це суперечить самому сенсу секретного чату, адже як може сервер зробити скриншот, не маючи адреси сайту?

6. Сервери в Росії

У 2014 році, коли Дуров ненадовго покинув Росію, з'явилася легенда, що розробники, сервери й офіс розташовані за кордоном. Відкритий 2014 року офіс у Лондоні було закрито 2019-го і врешті оголошено про переїзд офісу до Дубая (ОАЕ) в хмарочос Kazim Towers.

Ці заяви виявилися неправдою. Після того як влада Німеччини довгий час не могла отримати від Дурова відповіді на запити, у 2021-му журналісти видання Spiegel відвідали офіс телеграму в Дубаї. Він виявився порожнім, а консьєрж будівлі розповіла журналістам, що не бачила, щоб хтось заходив до офісу, вже більш як три роки.

За інформацією Антона Розенберга, який багато років працював у «ВКонтакте» й згодом у

телеграмі, станом на вересень 2017-го офіс компанії «Телеграм» містився на Невському проспекті в будинку Зінґера в Санкт-Петербурзі.

Для передачі даних телеграм використовує послуги двох партнерів: GlobalNet LLC і RETN. Обома компаніями керують росіяни, обидві зареєстровані в Росії й мають філії в ЄС та Британії.

Раніше ми з'ясували, що листування користувачів зберігається на серверах телеграму. Де саме містяться сервери, представники компанії очікувано не говорять, але для того, щоб листування передавалося без затримок, сервери треба розмістити якомога ближче до користувачів.

Одним із ключових ринків для телеграму є Росія, де компанії GlobalNet і RETN мають свої сервери й канали передачі даних.

Компанія GlobalNet зареєстрована в Нідерландах, і телеграм використовує її потужності для роботи в Європі. Хоча цей провайдер також має канали зв'язку в Казахстані, Україні, Німеччині, Росії та інших країнах, але завдяки реєстрації трафік телеграму в ньому юридично вважається європейським. При цьому 2020 року GlobalNet вказував телеграм як одного з ключових партнерів і мав сервери в кількох російських містах.

У 2022 році із сайту GlobalNet зникла російська мова й прибрали всі згадки про Москву та Петербург

У 2022 році із сайту GlobalNet зникла російська мова, натомість додали українську версію й прибрали всі згадки про Москву та Петербург. Цим провайдером керує росіянин Олексій Закревський, який вказує два поточних місця роботи: Амстердам і Санкт-Петербург. Також щонайменше шестеро з одинадцяти працівників компанії станом на серпень 2023-го досі жили в Росії.

Ймовірно, саме там, на російських серверах партнерів, телеграм і зберігає листування своїх користувачів. Це опосередковано підтверджувалося і його «розблокуванням», після чого всі претензії до компанії зникли, а отже, вона діє згідно із законодавством РФ, що зобов'язує компанії тримати дані росіян у Росії.

Українські дослідники знайшли й сервери, які належать безпосередньо телеграму в Росії. За даними сервісу GeoLite2, що показує географічну належність IP-адрес, станом на вересень 2023 року принаймні один із серверів telegram.org досі містився в Санкт-Петербурзі. Отже, просто зараз, під час війни, частина серверів телеграму, у якому ви спілкуєтеся з друзями й читаєте новини, розміщена в Росії.

Треба зауважити, що виявити за IP-адресою, у якій країні розміщений сервер, не завжди можливо й різні сервіси можуть вказувати на різні країни.

7. Працівники в Росії

Під час «блокування» телеграму та судового процесу з Роскомнаглядом віцепрезидент компанії Ілля Перекопський, третя особа в топ-керівництві, публічно відвідує Росію. У липні 2020 року, за місяць після «розблокування» телеграму, Перекопський виступав на форумі перед прем'єром РФ Михайлом Мішустіним, де критикував податкову систему США, а ще за місяць відпочивав із губернатором Вологодської області в лісі.

Росіянка Альона Соф'їна живе в Москві й працює в студії українофоба Артемія Лебедєва. Вона авторка одних із найпопулярніших стикерів телеграму.

Влітку 2023-го я розшукував працівників телеграму, які вказали в LinkedIn місцем проживання Росію. Із 41 знайденого працівника щонайменше троє жили в Росії. Тихон Давидов, один із працівників, який начебто жив і працював в Еміратах, протягом 2018–2022 років водночас читав лекції в Московському державному університеті.

«Привіт, мене звати Тихон Давидов, я живу в Москві»

До того ж Тихон грає в шахи й у своєму профілі на Chess.com у червні 2022 року писав: «Привіт, мене звати Тихон Давидов, я живу в Москві». Згодом у телеграмі ввели non-linkedin policy, яка забороняє працівникам мати акаунти в цій соцмережі.

8. Доказ для ФСБ

У серпні 2022 року херсонський журналіст Ігор Бондаренко потрапив у російський полон під час спроби виїхати з міста. За два місяці до цього він видалив зі своїх месенджерів усе листування, зокрема й у телеграмі. Але на допит російські військові, за словами Ігоря, принесли його листування в секретному чаті з представниками «Правого сектору» за пів року. І такі випадки непоодинокі.

Такі випадки можна було б пояснити роботою спеціальних програм, що збирають інформацію з відкритих чатів, аналізують публічні дані, можуть деанонімізувати користувачів і збирати їхній цифровий портрет. Але ці програми не можуть відновлювати видалене листування, тим паче із секретних чатів, які начебто зашифровані й зберігаються виключно на двох пристроях співрозмовників. Принаймні так стверджують у телеграмі.

У чому небезпека?

Згідно з дослідженням групи «Рейтинг» за 2023 рік протягом 15 місяців частка українців, які читають новини в телеграмі, зросла вчетверо (з 11% до 41%), а питання небезпеки телеграму не раз порушували різні лідери суспільної думки. Водночас кожен із нас, користуючись телеграмом, робить його важливішим для інших користувачів.

Багато хто думає «я не пишу нічого секретного, тож і приховувати мені нічого», але навіть у такому разі дані з наших смартфонів допомагають телеграму аналізувати інформацію й отримувати з неї важливі розвідувальні дані.

Наприклад, багато волонтерів, які допомагають ЗСУ, у телеграмі проводять збори, тримають зв'язок із військовими та між собою. Хоча живуть у Львові чи Києві, й, здавалося б, їхнє листування та геопозиція не можуть завдати шкоди військовим «на нулі».

Дехто навіть обмежує передачу приватних даних у телеграмі, але не відмовляється від нього, «бо зручно». При цьому телеграм може аналізувати на лише власне листування й передані файли, а й метадані, а саме час активності, кількість дзвінків і співрозмовників, найактивніші співрозмовники, список контактів.

Останній дуже важливий момент. Маючи списки контактів мільйонів людей, телеграм може аналізувати зв'язки між ними, виявляти справжні імена людей, сферу їхньої діяльності («Олександр СБУ», «Микола розвідка» або «Сергій Генштаб»), знаходити додаткові номери телефонів, на які можуть бути зареєстровані «анонімні» телеграм-акаунти тощо.

Телеграм може створювати в себе цифровий портрет навіть тих людей, які не мають телеграм-акаунтів, але є в когось у списках контактів

Таким чином, телеграм може створювати в себе цифровий портрет навіть тих людей, які не мають телеграм-акаунтів, але є в когось у списках контактів. І що більше таких згадок у контактах різних людей, то більша точність.

Signal — хороша альтернатива

У телеграмі є більшість активних українців, тож видалитися звідти непросто, але можливо. Для цього насамперед зверніть увагу на альтернативи, зокрема на Signal. Це справді захищений і безплатний месенджер, створений у США, який шифрує все без винятку листування та дзвінки. Нічого з того, що написано в чаті або сказано під час дзвінків, працівники Signal не зможуть дізнатися.

Запропонуйте вашим контактам перенести листування в цей месенджер. Спробуйте вести все важливе листування в ньому, а не в телеграмі. Замість читання новин у телеграм-каналах підпишіться на потрібні вам видання та лідерів думок в інших соцмережах, якщо ви ними користуєтеся, або переглядайте новинні сайти. Згадайте, врешті, що таке RSS. Це перевірений часом і зручний спосіб читати новини в програмах-читалках на кшталт Inoreader, Feedly та Reeder.

Те саме можуть зробити й видання. Так, команда Ukraïner у лютому 2023 року опублікувала матеріал «Що не так із телеграмом», а в червні повністю відмовилася від спілкування в ньому й закрила свій канал. Відмовитися від телеграму спочатку може бути незручно, але врешті йому можна знайти альтернативу.

Український бізнесмен Ярослав Ажнюк опублікував матеріал «Чому варто видалити телеграм зі свого мобільного». Як пише Ярослав, мобільні застосунки з доступом до камер, мікрофона та локації — це складні системи, і ніхто не може гарантувати, що вони непомітно не шпигуватимуть за власниками.

Піти з телеграму

Поки ви почнете процес переходу, зробіть прості й важливі кроки, щоб зменшити кількість даних, яку може отримувати про вас телеграм.

1. Насамперед вимкніть на смартфоні доступ для телеграму до контактів, файлів, камери, мікрофона та локації.
2. Не пишіть у телеграмі нічого важливого, не передавайте паролів, чутливих і приватних даних.
3. На комп'ютері користуйтеся вебверсією в браузері, вона має значно менше можливостей для стеження за вашою системою.

Ми платимо за зручність телеграму нашими особистими даними: повідомленнями, геолокацією, контактами, фото та відео. Будь-яка платформа сама по собі нічого не варта без своїх користувачів. Цінність телеграму з усіма його зручностями була б нульовою, якби в ньому не було нас із вами.

Ми платимо за зручність телеграму нашими особистими даними

Поки що майже будь-який наш чат у телеграмі — це груповий чат, який також читають працівники месенджера. І частина з них досі живе в Росії. Тому намагайтеся звести до мінімуму всю активність у телеграмі або й узагалі видаліть його. Не обирайте зручність, нехтуючи безпекою.

Назар Токар
Тексти.org.ua

Офіційно персональні. У чому полягає проблема з офіційними телеграм-каналами обладміністрацій

Одним з класичних аргументів на користь читання новин у телеграмі є наявність у ньому офіційних джерел інформації. Ніби крім російської дезінформації та анонімних каналів-сміттярок, на платформі присутні якісні медіа та офіційні державні інституції, які доносять перевірену інформацію. І це начебто робить телеграм «допустимим» і навіть «бажаним» джерелом новин для українців. Та тільки на обласному рівні значна кількість офіційних державних телеграм-каналів більше схожа на персональні блоги.

З'ясовуємо, що не так із державною комунікацією в телеграмі на прикладі рекомендованого Кабміном списку телеграм-каналів голів обласних адміністрацій.

Як ми взагалі дізнаємося, що якийсь телеграм-канал є офіційним?

Є два варіанти. **Перший — «синя галочка»** (верифікація з боку самої платформи, її видають через верифіковані акаунти в інших соціальних мережах і публікації в медіа).

Другий — офіційна комунікація з боку держави. Як це, наприклад, було 1 березня 2022 року, коли Кабмін опублікував перелік офіційних телеграм-каналів голів облдержадміністрацій — «щоб уникнути фейків» та щоб українці знали, яким джерелам у телеграмі можна довіряти.

← Новини

Щоб уникнути фейків, користуємось офіційними джерелами

Департамент комунікацій Секретаріату Кабінету Міністрів України, опубліковано 01 березня 2022 року о 17:03

НАДЗВИЧАЙНІ СИТУАЦІЇ

Задум вдалий, але від самого початку він мав довгострокові ризики. І сьогодні ми бачимо їхнє втілення.

По-перше, ставку одразу було зроблено не на офіційні сторінки інституцій, тобто облдержадміністрацій, а на персональні канали голів ОДА (ОВА). Близько половини всіх каналів не мали прізвища тодішнього голови у своєму посиланні. У телеграмі назва каналу й посилання на нього можуть відрізнятися.

І тут, звісно, можна спробувати знайти пояснення: персоналізована інформація викликає більше довіри.

Щоправда, лише в короткостроковій перспективі — принаймні допоки голова ОДА обіймає свою посаду. А що відбувається зі зміною голови? Бачимо на характерних прикладах.

Португальське онлайн-казино

Сьогодні з усього списку (24 канали) лише на трьох (Київської, Хмельницької та Херсонської областей) за вказаними адресами ведуться безособові офіційні інформаційні сторінки (та лише 5 з 24 мають синю галочку верифікації від платформи).

Решта — або персональні канали нинішніх і колишніх очільників ОДА. Один взагалі перетворився на португальське онлайн-казино. Це сталося з каналом колишнього голови Донецької ОДА Павла Кириленка.

Він пішов на підвищення і став головою Антимонопольного комітету України та змінив посилання на особистий телеграм-канал зі @pavlokyrylenko_donoda на @pavlokyrylenko_amcu. Платформа дає змогу це робити, зберігши свою аудиторію.

А старий лінк (той, на який досі веде посилання з офіційної сторінки КМУ) залишився

«безхозним», тобто його може використати будь-хто. У нашому й кращому випадку, це португальське онлайн-казино, в гіршому — може бути псевдоукраїнським інформаційним каналом з російськими адмінами.

TOSHKENT АНДИЖОН

Проте не завжди зміну посади супроводжує зміна посилання. А тому офіційна комунікація Кабміну вже в день публікації замість промоції офіційного каналу голови Черкаської ОДА промотувала персональний канал Олександра Скічка — звільненого з посади голови точно в день публікації цього списку, 1 березня 2022 року. А офіційний канал за один день перетворився на персональний блог. Дуже надійне офіційне джерело інформації від держави, хіба ні?

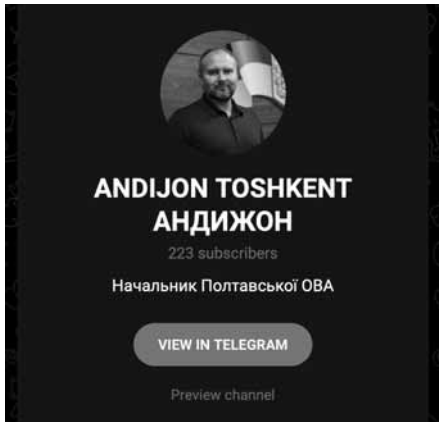
Офіційний канал голови Кіровоградської ОДА протримався трохи довше — 6 днів. Саме стільки після публікації списку обіймала свою посаду Марія Чорна (звільнена 7 березня 2022 року, але залишається активною в телеграмі за поширеним на сайті КМУ лінком @chornamary, де, як і Скічко, веде вже свій персональний блог).

Ще довше проіснував офіційний канал голови Запорізької ОДА — посилання КМУ веде на персональний канал Олександра Старуха (@starukhofficial), який утратив свою посаду 26 січня 2023 року. У новопризначеного голови Юрія Малашка вже новий телеграм-канал із нейтральнішим посиланням @zoda_gov_ua. Але чи залишиться цей канал офіційним джерелом інформації в Запорізькій області після зміни голови — невідомо.

Бо, наприклад, у Полтавській ОДА вирішили зберегти профіль у телеграмі зі зміною голови.

Тепер за адресою каналу @DMYTROLUNIN (названого на честь попереднього голови) — вже профіль нового очільника ОВА — Філіпа Проніна. Його призначили 10 жовтня й через тиждень після призначення він у телеграмі опублікував одне привітання та видалив всю попередню стрічку новин. З незрозумілих причин канал (на який веде посилання в з офіційної сторінки Кабміну) тепер називається «ANDIJON TOSHKENT АНДИЖОН».

Дивлячись на всю цю спробу «офіційної комунікації» в телеграмі, хочеться кричати від



недбалості та безглуздості затії. Навіть призначені президентом голови ОДА сприймають себе як місцевих лідерів і щосили піарять себе особисто. Хоча після відставки про них мало хто згадує. Це дивна поведінка, адже вони обіймають навіть не виборні посади, тож і комунікувати мають не від свого імені, а від імені держави й від посади, яку обіймають.

Приватизація аудиторії

У результаті цього хаосу немає зрозумілої та чіткої інструкції з відокремлення офіційних телеграм-каналів від фейкових двійників. А відсутність єдиного стилю посилання та більшменш надійного оновлюваного списку офіційних локальних телеграм-каналів доповнює можливістю «приватизувати» аудиторію після втрати державної посади.

І така приватизація можлива не тільки на рівні областей. Наприклад, хоча на загальнонаціональному рівні майже всі офіційні телеграм-канали деперсоналізовані, проте телеграм-канал прем'єр-міністра України має промовисте посилання @Denys_Smyhal. Себто в разі зміни його на посаді доведеться заново налагоджувати офіційну комунікацію в телеграмі. Особливо за умови, коли офіційного телеграм-каналу Кабміну взагалі немає.

І вбудована на платформі можливість змінити адресу посилання на канал (себто зберегти всіх підписників зі зміною персони) насправді не найкращий можливий вихід — Павло Кириленко з португальським казино яскраво продемонстрували чому.

P.S. Окремо варто написати, що всі посилання на телеграм з цієї офіційної комунікації КМУ спочатку ведуть на фейсбук. Але це вже тема для окремого розлогого тексту про якість офіційних документів та, наприклад, відсутність навіть базових знань з редагування посилань і видалення зайвих параметрів.

Юлія Дукач
Texty.org.ua

Телеграм-окупація

Як Росія вибудовувала медіамережу, а вийшло потьомкінське село

На початку березня, одразу після повномасштабного вторгнення, російські інформаційні війська націлилися на українські райцентри — і для кожного обраного міста чи громади створили власний телеграм-канал. Кожен з них декларував, що повідомлятиме місцевим жителям локальні новини. А насправді взявся поширювати російські тези та сприяти підтримці окупантів. Або імітувати таку підтримку місцевими.

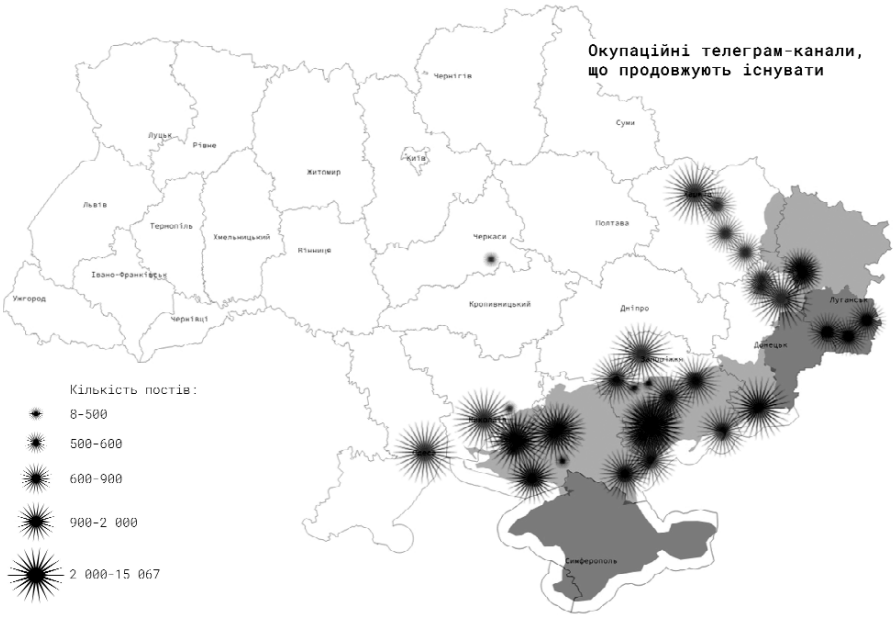
Сама стратегія створення локальних джерел пропаганди є доволі ефективною. Принаймні теоретично. Адже на противагу центральним рупорам російської пропаганди, локальні ресурси можуть легше завойовувати місцеву аудиторію та здобувати її довіру, оскільки змішують свої тези з місцевими новинами, іноді корисними.

Системний підхід щодо створення телеграм-каналів у всіх окупованих населених пунктах підтвердив захоплений у березні в полон російський підполковник, начальник відділення інформаційного протиборства та оперативного маскування 58-ї армії Південного військового округу ЗС РФ. На допиті він назвав 10 таких каналів. Ми виявили їх 120. З них 68 було створено в перші два тижні війни, а решту запустили після посилення й поглиблення окупації, потім частину з них припинили оновлювати.

Ми розташували ці канали на карті, щоб оцінити початкові воєнні амбіції Росії. Цікаво, що ця карта схожа на карту плану вторгнення, яку ще до початку війни опублікувало німецьке видання Bild

Щоправда, відступ на київському напрямку та припинення просування російської армії на інших фронтах зменшили амбіції й на інформаційному фронті – від березня нові російські тг-канали з'являлися вже лише на півдні України. А від травня — тільки в Херсонській області.

У результаті бачимо нерівномірність інформаційної агресії: поки Херсонська й Запорізька області густо засівали окупаційними інформаційними телеграм-каналами, нещодавно звільнена Харківська область залишалася майже «непокритою» за межами самого Харкова. Можливо, це свідчить про більш і менш пріоритетні території окупації. І такий розподіл інформаційної активності корелює з воєнними зусиллями. Це стало помітно під час вересневого українського наступу: на Харківщині росіяни виставили менш боєздатні частини, а найбільш підготовлені сконцентрували на Херсонщині.



Водночас на початку літа відбулося зменшення масштабів мережі (а з нею — й остаточне зменшення російських воєнних амбіцій).

Відтоді активні місцеві телеграм-канали залишилися лише в Херсонській і Запорізькій областях. До того ж загальна їх кількість поступово зменшилася до 80.

Російська телеграм-імперія в Україні

Розбудовою мережі (про)російських інформаційних пропагандистських джерел, які начебто працюють в Україні, Росія займається вже багато років. На відміну від офіційних рупорів Кремля, їхнє основне завдання — транслювати підтримку Росії та «зсередини» критикувати українську владу. І робити це, використовуючи максимально можливу багатоканальність: сайти, телебачення, соціальні мережі й навіть друковані видання.

Поступово одним з основних інструментів російської пропаганди став телеграм, який уже здобув статус найпопулярнішої в Україні соціальної мережі та найнебезпечнішого джерела російського впливу. Адже телеграм абсолютно не модерує контент і російські пропагандисти там почуваються вільно. До того ж в умовах поганого інтернету телеграм завантажується на телефон швидше, ніж сайти медіа чи соцмережі.

Ще на початку лютого 2021 року СБУ звинуватила 12 загальноукраїнських телеграм-каналів у тому, що їх ведуть агенти впливу спецслужб РФ. Їхня цільова аудиторія — мешканці великих міст, які цікавляться політикою, а також чиновники й політики.

Як із їхньою допомогою Росія намагалася маніпулювати українськими парламентарями, читайте тут.

Ці канали поширювали панічні настрої та намагалися (й досі намагаються) дестабілізувати суспільно-політичну ситуацію. Половину з них створювали прицільно для жителів найбільших міст сходу й півдня України. Саме їх створення наприкінці 2018 року можна вважати стартом розбудови регіональних проросійських інформаційних телеграм-осередків.

Кульмінації ця розбудова досягла після початку війни, коли телеграм став основним інструментом для імітації локальної новинної стрічки й місцевої підтримки окупантів. СБУ встановила осіб, які керували каналами, декого навіть арештували, але основні фігуранти мешкали за межами України.

Централізований російський контент і «накручені» підписники

Зважаючи на ідентичне оформлення й синхронність стрічки російських телеграм-каналів, створених після 24 лютого 2022 року, які мімікрували під українські, можна зробити висновок, що принаймні половину з усіх 120 каналів централізовано створили російські інформвійська. І вели їх теж, вочевидь, з єдиного штабу.

Найяскравіший приклад — мережа з 51 каналу, створена 5–7 березня. Кожен канал — з назвою міста в заголовку та російським або українським прапором опісля. Кожен з однаковою кількістю накручених підписників у перші дні створення. А також з ідентичним описом, у якому пропонують, у разі чого, звертатися до того самого адміна. Усі канали публікували однакові тексти про російські гуманітарні коридори й гуманітарну допомогу.

Як свій перший пост 43 канали обрали цитату зі звернення російського воєначальника, керівника Національного центру управління обороною РФ Михайла Мізінцева. Змінювали лише назву міста:

«Жители [підставити назву міста]!

Розбудова паралельної реальності

Очікуючи на радісну зустріч російської армії, усі згадані канали від моменту створення або відкрито заявили про свою проросійську позицію в описі чи російським прапором на аватарці, або активно перепощували новини з великих російських пропагандистських ЗМІ, таких як «РИА Новости» чи «ТАСС». А кожен третій пост на досліджуваних каналах мав у

тексті слово «Россия», «россиянин» або «русский». Жоден з них навіть не намагався зайняти «нейтральну» позицію. Що, очікувано, не сприяло їх популярності серед українців.

Усі їхні дописи можна розділити на дві великі групи: російська офіційна пропаганда й місцеві новини.

Російська пропаганда в локальних телеграм-каналах загалом дублює офіційну кремлівську й зосереджена на таких темах:

- російська допомога українцям і роздача російської гуманітарки (одна з найпопулярніших тем навесні);
- успіхи на фронті й могутність російського озброєння;
- класичні пропагандистські російські тези про «братські народи», «спільну історію», «повернення в рідну гавань» та «Велику Росію»;
- спроби поєднати ці тези з аргументацією необхідності проведення референдумів;
- демонізація ЗСУ та агресивна антиукраїнська риторика.

Рецепт успіху такого тг-каналу доволі простий: максимум локальних новин, мінімум пропаганди. Що більше корисного місцевого контенту, то більше справжніх підписників. Що

краще завуальовано «паркетні» новини, то ефективніша реальна пропаганда й вища ймовірність довіри до окупаційної влади. Але й то складніше вести такий канал.

Зразковий пропагандист

Більшість каналів ідуть простим шляхом: репостять російські новини й місцевих колаборантів, збільшують свою аудиторію завдяки фальшивим користувачам (про що свідчить різке одноразове зростання їх кількості та значно менша кількість переглядів). Але є й ті, що зуміли ефективніше використати доступ до окупаційної влади. Найяскравіший приклад — «Официальный канал Каховской военно-гражданской администрации».

Це один з перших «адміністративних» каналів, запущених у травні. У ньому все зробили так, як, вочевидь, планували для всієї мережі. Хто саме його веде — невідомо.

Серед типового контенту — оголошення від Каховської ДЮСШ, шкіл і дитсадочків, новини про початок видачі автономерів російського зразка, радощі від постачань рязанських шкільних підручників, залякування перевірками підприємців, які відмовляються виставляти цінники в рублях, і зовсім мало постів суто пропагандистського змісту на кшталт новини про те, як «Укронацисты пообещали убить Кирилла Стремоусова».

Певний зразковий окупаційний інформаційний телеграм-канал. Має 4500 підписників і середній перегляд посту — 4000 разів. Це високий показник. І цей канал має один з найвищих показників оригінальності контенту серед усієї мережі.

Репости VS оригінальний контент

Репости є невіддільною складовою більшості каналів. У середньому кожен третій пост на окупаційних каналах є репостом. Проте більшість намагається балансувати між репостами та власними публікаціями.

У телеграм-каналі «Запорожская Народная Республика» 85% контенту — репости з 370 інших каналів. Понад 1000 з них — з каналу «Военкоры Русской Весны» та майже 800 — з російського пропагандистського каналу «Рыбарь». Цей канал створили на початку березня, за 5 місяців на ньому опублікували понад 15 тис. повідомлень.

Створені окупантами тг-канали, намагаючись зберегти локальність своєї стрічки, активно репостили з «братніх» телеграм-каналів регіону. А тому кожен третій репост походить з самої мережі окупаційних каналів регіону.

Тому, наприклад, канали Бердянська й Мелітополя (а для цих міст створювали 8 і 6 каналів відповідно) виокремлюються на мережі в окрему групу. Також неозброєним оком видно штучну мережу з 51 каналу для різних міст України, які репостили лише один одного й мало цікавилися, що відбувається за межами їхньої бульбашки.

Українські військові в приватних розмовах стверджують, що їхні противники на полі бою не повідомляють своєму керівництву про реальний стан справ. Були навіть свідчення, що молодші офіцери інсценували події для фотозвітів начальству. У цій порушеній комунікації, яку російська мова описує словом «очковтерательство», — одна з причин нинішньої слабкості російської армії. Також російська армія має жорстку управлінську культуру, в якій не місце імпровізації, а є лише сліпе й формальне виконання наказу.

Схоже, така сама проблема роз'їдає й армію пропагандистів.

Матеріал створено в межах проєкту Fight For Facts!, який фінансує Федеральне міністерство економічного співробітництва та розвитку Німеччини (BMZ). Погляди, висловлені в цих публікаціях, належать незалежним авторам і не обов'язково відбивають погляди BMZ.

Texty.org.ua

Безпека електронної пошти

Визначення безпеки електронної пошти

Безпека електронної пошти є важливою сферою кібербезпеки, яка присвячена захисту електронної пошти та облікових записів від кібератак. Він охоплює широкий набір технологій, найкращих практик і стандартів, призначених для захисту каналу зв'язку.

На практиці це охоплює захист вхідних повідомлень електронної пошти, захист зв'язку, який покладається на електронну пошту як канал, і захист облікових записів від несанкціонованого доступу, компрометації або навіть повного захоплення облікового запису. Більше ніж просто захист самого облікового запису електронної пошти, безпека електронної пошти також включає захист посилань у вмісті електронної пошти, виявлення зловмисних чи спам-повідомлень і навіть класифікацію електронних листів за підкатегоріями, такими як інформаційні бюлетені чи квитанції.

Загальні протоколи безпеки електронної пошти

Протоколи безпеки електронної пошти включають протоколи передачі, шифрування, політики та автентифікації. Нижче наведено деякі з найпоширеніших протоколів, які використовуються для захисту електронної пошти:

SPF (Sender Policy Framework)

SPF — це протокол автентифікації, який дозволяє адміністраторам призначати відправників, яким дозволено доставляти електронні листи з домену. Авторизовані відправники додаються до запису DNS для домену. Теоретично SPF повинен блокувати несанкціоновані IP-адреси від надсилання електронних листів із домену; однак SPF обмежений і вимагає додаткових протоколів, щоб бути ефективним.

DKIM (DomainKeys Identified Mail)

DKIM — це протокол автентифікації, який може виявляти підроблені або підроблені адреси електронної пошти. DKIM створює цифровий підпис, прив'язаний до доменного імені для вихідних повідомлень. Цей підпис підтверджує для одержувача, що домен не було змінено.

DMARC (автентифікація повідомлень домену, звітування та відповідність)

Крім того, протокол автентифікації DMARC дозволяє власникам доменів перевіряти свої домени, публікуючи запис DMARC у записі DNS. Політика DMARC публікується в записі DNS і вказує, які дії слід вжити, якщо електронний лист не проходить автентифікацію SFP або DKIM.

При спільному використанні SPF, DKIM і DMARC забезпечують більш повну систему безпеки електронної пошти. SPF запобігає використанню домену неавторизованими відправниками, DKIM перевіряє цілісність і автентичність електронної пошти, а DMARC забезпечує структуру політики для обробки невдалої автентифікації. Ця комбінація допомагає захистити від спуфінгу електронної пошти, фішингових атак і уособлення домену.

Національний інститут стандартів і технологій (NIST) рекомендує організаціям, у тому числі малому та середньому бізнесу (SMB), прийняти протоколи SPF, DKIM і DMARC для покращення безпеки електронної пошти.

Хоча DMARC є безкоштовним і відкритим стандартом, його впровадження залишається повільним. За деякими даними, лише приблизно половина відправників електронної пошти використовує протокол, а серед тих, хто використовує, лише 14% встановили для нього політику застосування. Політики примусового виконання визначають, як оброблятимуться електронні листи, якщо вони проходять або не автентифікуються. Без них DMARC доставляє всі електронні листи незалежно від їх статусу автентифікації.

Хоча організації можуть запроваджувати стандарти DMARC самостійно, багато організацій покладаються на сторонніх постачальників для цієї послуги. Такі організації, як Global Cyber Alliance, надають список постачальників, а також інструменти та ресурси для впровадження DMARC.

Хоча SPF, DKIM і DMARC є ефективними протоколами безпеки електронної пошти, вони не надійні. Вони покладаються на належне впровадження та налаштування адміністраторами домену. Вони також не захищають від кіберзагроз, які не включають пряме видавання себе за законного відправника. Ось чому найкраща практика полягає в тому, щоб доповнити ці протоколи іншими заходами, такими як розширений захист електронної пошти та навчання користувачів.

Чому безпека електронної пошти є важливою для бізнесу?

Як головний вектор кіберзагроз, електронна пошта становить значні ризики для кібербезпеки. За даними Deloitte, 91 відсоток усіх кібератак починається з фішингового електронного листа. Електронна пошта також є основним каналом для деяких із найпоширеніших і дорогих типів кіберзагроз, таких як фішинг і фішинг.

Без спеціального рішення для безпеки електронної пошти організації ризикують стати жертвами різноманітних кіберзагроз. Традиційні платформи електронної пошти часто не мають надійних функцій безпеки, що робить їх сприйнятливими до фішингових атак, шахрайства з компрометацією бізнес-електронної пошти (BEC), зараження шкідливим програмним забезпеченням тощо. Ці ризики можуть мати серйозні наслідки, зокрема фінансові втрати, репутаційну шкоду та юридичну відповідальність.

Співтовариство безпеки та авторитетні установи, такі як Gartner, рекомендують організаціям використовувати інтегроване стороннє рішення безпеки електронної пошти . Ця технологія доповнює власні функції безпеки платформ електронної пошти, одночасно забезпечуючи більш розширений і багаторівневий захист від кіберзагроз.

Типи загроз безпеці електронної пошти

Організації стикаються з численними загрозами безпеці електронної пошти, які можуть мати руйнівні наслідки, якщо їх не вирішити належним чином.

1. Фішинг: фішинг — це практика видавання себе за відомі та визнані бренди, щоб обманом змусити одержувачів натиснути зловмисне посилання або завантажити вкладений файл, заражений шкідливим програмним забезпеченням. Фішинг можна використовувати для збору облікових даних, захоплення облікових записів (ATO) тощо.

2. Фішинг: спеціальний фішинг, також відомий як компрометація ділової електронної пошти (BEC), — це цілеспрямована загроза електронною поштою, яка видає себе за особу, відому передбачуваній жертві. На відміну від фішингових електронних листів, які містять шкідливі посилання або вкладення, фішингові атаки зазвичай покладаються на текстовий вміст для використання жертв. З цієї причини шахрайство з фішингом часто важче виявити та захиститися від нього.

3. Шкідливе програмне забезпечення: шкідливе програмне забезпечення відноситься до шкідливого програмного забезпечення. Електронна пошта є найпоширенішим способом розповсюдження зловмисного програмного забезпечення, яке хакери можуть вставляти у вкладені файли електронної пошти або цільові фішингові сторінки. Загроза може скомпрометувати системи, викрасти дані чи облікові дані тощо.

4. Атаки Man-in-the-middle (MitM): атаки MitM відбуваються, коли хакери перехоплюють законне листування електронної пошти двох сторін, дозволяючи зловмисникам підслуховувати або маніпулювати інформацією. Атаки MitM можуть скомпрометувати інформацію користувача та дозволити хакерам обійти засоби безпеки, такі як MFA.

5. Програми-вимагачі: програми-вимагачі – це інвазивний тип зловмисного програмного забезпечення, призначене для шифрування файлів, щоб хакери могли вимагати викуп за їх випуск. Електронна пошта залишається найпо-

пулярнішим способом розповсюдження програм-вимагачів.

Фішинг

Одна з найстаріших форм ризиків для безпеки електронної пошти, яку часто називають шахрайством нігерійського принца. Хоча фішинг також можна доставляти за допомогою текстових повідомлень, чату та інших методів, зазвичай фішинг доставляється електронною поштою. Сучасні фішингові електронні листи видають себе за відомий бренд з метою обману змусити одержувача натиснути шкідливу URL-адресу. URL-адреса веде на фішингову сторінку, яка виглядає законною та містить форму, призначену для отримання облікових даних користувача. Коли користувач заповнює форму, дані його облікового запису викрадаються фішером.

Ці атаки найчастіше використовуються масово та з відносно низькими ставками, наприклад злом облікових записів споживачів потокового передавання або сайтів соціальних мереж. Це стає набагато більш серйозною загрозою, коли успішна фішингова атака відбувається на бізнес-пристрій або обліковий запис, який використовує електронну пошту чи пароль для бізнес-облікового запису користувача. Фішингові атаки покладаються на закон чисел, щоб досягти успіху та використовувати отриману інформацію для більш складних атак, таких як фішинг (докладніше нижче).

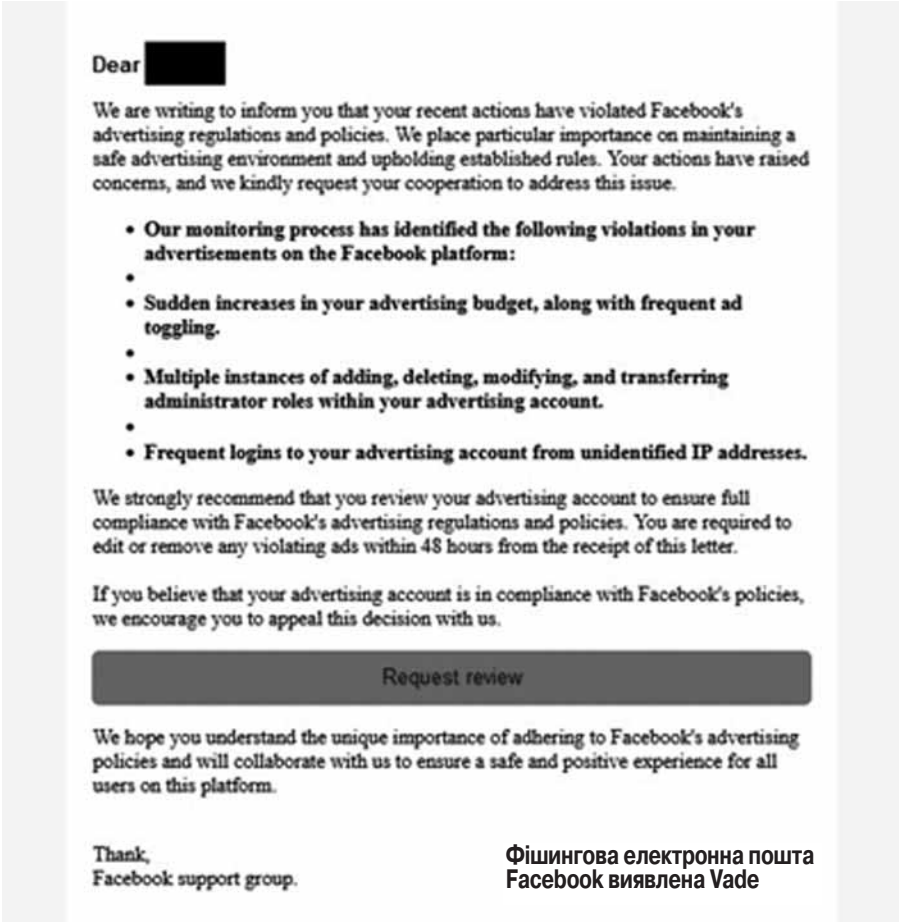
Електронна пошта QRishing

Spear фішинг

На відміну від фішингу, spear phishing , також відомого як компрометація бізнес-електронної пошти (BEC), атаки є суто особистими та цілеспрямованими атаками на електронну пошту, призначені для того, щоб обманом змусити користувачів виконати запит. Фішингові електронні листи, як правило, видають себе за людей, а не за бренди. Часто зловмисники видають себе за колег, ділових партнерів, продавців та інших знайомих.

Типовий фішинговий електронний лист короткий і по суті, містить лише текст. Найпоширеніші види фішингового шахрайства включають запити на подарункові картки, шахрайство з генеральним директором (дротове шахрайство) і податкове шахрайство.

Фішинг також зазвичай називають компрометацією бізнес-електронної пошти (BEC), оскільки отримання незаконного доступу до бізнес-акаунтів є одним із головних результатів таких атак. Під час атак BEC зловмисники часто видають себе за генерального директора організації, вимагаючи подарункових карток, банківських переказів або просто «відповісти якомога швидше». Вони також можуть змінити тенденцію, прикинувшись більш молодим працівником і попросивши перенаправити їхній прямий депозит до нового банку.


Dear [redacted]

We are writing to inform you that your recent actions have violated Facebook's advertising regulations and policies. We place particular importance on maintaining a safe advertising environment and upholding established rules. Your actions have raised concerns, and we kindly request your cooperation to address this issue.

- **Our monitoring process has identified the following violations in your advertisements on the Facebook platform:**
- **Sudden increases in your advertising budget, along with frequent ad toggling.**
- **Multiple instances of adding, deleting, modifying, and transferring administrator roles within your advertising account.**
- **Frequent logins to your advertising account from unidentified IP addresses.**

We strongly recommend that you review your advertising account to ensure full compliance with Facebook's advertising regulations and policies. You are required to edit or remove any violating ads within 48 hours from the receipt of this letter.

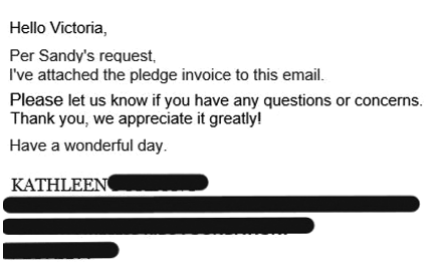
If you believe that your advertising account is in compliance with Facebook's policies, we encourage you to appeal this decision with us.

Request review

We hope you understand the unique importance of adhering to Facebook's advertising policies and will collaborate with us to ensure a safe and positive experience for all users on this platform.

Thank,
Facebook support group.

Фішингова електронна пошта Facebook виявлена Vade


Hello Victoria,

Per Sandy's request,
I've attached the pledge invoice to this email.

Please let us know if you have any questions or concerns.
Thank you, we appreciate it greatly!

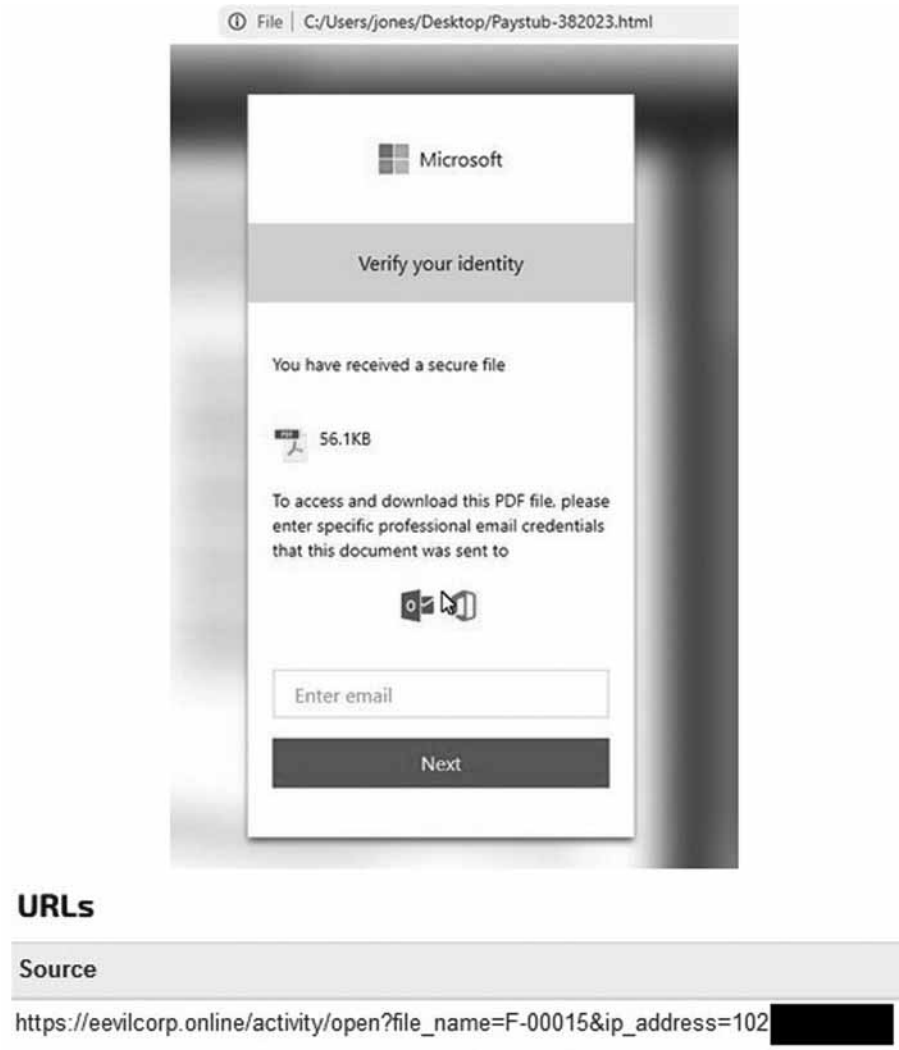
Have a wonderful day.

KATHLEEN [redacted]

Фішинговий електронний лист

Шкідливе програмне забезпечення

Зловмисне програмне забезпечення – це загальний термін для комп'ютерних вірусів, які часто поширюються через посилання та вкладення електронної пошти. Зловмисне програмне забезпечення існує в багатьох формах і з різним рівнем складності. Більшість шкідливих вірусів створено для завантаження на комп'ютер користувача без його відома



Фішингова сторінка, що підроблює Microsoft і підозрюється в розповсюдженні зловмисного програмного забезпечення

або без підозри. Це часто досягається шляхом маскування зловмисних вкладень такими назвами файлів, як «рахунок-фактура» або «оплата», або шляхом пересилання користувачів на веб-сайт, де шкідливий код завантажується у фоновому режимі.

Деякі зловмисні програми використовують різновид соціальної інженерії, відображаючи миготливе спливаюче вікно, закликаючи користувачів завантажити антивірусне програмне забезпечення або попереджаючи, що на їхній машині є вірус. Звичайно, коли користувач натискає спливаюче вікно, він встановлює справжній вірус.

Після того, як зловмисне програмне забезпечення було завантажено за посиланням або вкладенням, кіберзлочинці можуть шпигувати за користувачами, викрадати облікові дані та цифрові активи, копіювати себе або поширюватися на інші системи.

Як і у випадку з фішинговими атаками, початкові атаки зловмисного програмного забезпечення часто спрямовані на збір інформації чи облікових даних, а не на миттєве руйнування системи користувача. Одним із прикладів масового використання під час пандемії COVID-19 було встановлення програмного забезпечення для майнінгу криптовалют. Зловмисне програмне забезпечення встановлювало програмне забезпечення для майнінгу, яке працювало у фоновому режимі на машині користувача, вилучаючи ресурси без відома користувача. Для багатьох користувачів виявлення цього зловмисного програмного забезпечення відбулося лише після того, як їх жорсткий диск або відеокарти були непоправно пошкоджені.

Безпека електронної пошти – фішингова сторінка, що підмінює Microsoft і підозрюється в розповсюдженні зловмисного програмного забезпечення

Фішингова сторінка, що підроблює Microsoft і підозрюється в розповсюдженні зловмисного програмного забезпечення

Атаки «людина посередині» (MitM)

Атака MitM відбувається, коли хакери перехоплюють спілкування між двома сторонами та таємно передають або, можливо, змінюють повідомлення, якими обмінюються. Хакери можуть читати, змінювати або навіть вставляти шкідливий вміст в електронні листи, що потенційно може призвести до крадіжки даних, несанкціонованого доступу або поширення шкідливого програмного забезпечення.

Ці атаки можна запобігти шляхом автентифікації доступу через інший канал зв'язку. Це основна причина для багатофакторної автентифікації (MFA), яка гарантує, що хакери не зможуть перевірити себе без відома користувача.

Програми-вимагачі

Програми-вимагачі – це певний тип шкідливих програм, які шифрують комп'ютер користувача, забороняючи доступ до всіх програм і даних. У більшості атак програм-вимагачів вірус запускає повідомлення про програму-вимагач на екрані комп'ютера користувача, вимагаючи викуп в обмін на ключ дешифрування.

Коли пристрій, який було зашифровано та заблоковано, є рекреаційним планшетом, шкода здається мінімальною, але атаки програм-вимагачів завдали шкоди основним мережам охорони здоров'я, урядовим установам і великим підприємствам. У такому масштабі атака програм-вимагачів, ймовірно, організована кіберзлочинною організацією. Ранні успішні фішингові атаки, фішингові атаки або встановлення зловмисного програмного забезпечення часто є шляхами, які хакери використовують для ініціювання справді руйнівної атаки програм-вимагачів.

Як шкідливі електронні листи можуть вплинути на вашу організацію

Шкідливі електронні листи можуть мати серйозні наслідки для організацій, зокрема фінансові, юридичні, регулятивні та репутаційні. У фінансовому плані кібератаки можуть призвести до викрадення інтелектуальної власності, конфіденційних даних або коштів. Це також може призвести до простою або порушення безперервності бізнесу.

У той же час атаки на організації можуть поставити під загрозу довіру потенційних клієнтів і клієнтів, особливо у випадку гучних витоків даних. У разі викрадення даних клієнта або нападу на клієнта через кібератаку організації також можуть зіткнутися зі значною юридичною відповідальністю.

Положення про конфіденційність, такі як Загальний регламент захисту даних (GDPR) в ЄС і Закон про перенесення та підзвітність медичного страхування (HIPAA) у США, можуть накладати суворі покарання на організації, які не захищають конфіденційність даних споживачів. Наприклад, GDPR може оштрафувати організації на суму до 4% річного доходу або 20 мільйонів євро за серйозні порушення відповідності, залежно від того, що більше.

Загалом наслідки зловмисних електронних листів можуть бути далекосяжними, тому для організацій вкрай важливо впровадити надійні заходи безпеки електронної пошти для захисту від цих загроз.

Переваги безпеки електронної пошти

Впровадження заходів безпеки електронної пошти надає організаціям численні переваги, зокрема захист конфіденційної інформації та безперервність їхнього бізнесу.

1. Захист від найпоширеніших і дорогих кібератак: рішення для безпеки електронної пошти створені для захисту організацій від найбільших кіберзагроз. Сюди входить фішинг, який є найпоширенішою загрозою для облікових записів жертв, і фішинг, який є найдорожчою загрозоюза даними Центру скарг на злочини в Інтернеті (IC3). Загрози електронної пошти є основною причиною інцидентів безпеки та витоку даних. Згідно зі звітом IBM Cost of a Data Breach Report за 2023 рік , середня вартість витоку даних досягла рекордного рівня, особливо це стосується малих і середніх підприємств (SMB). У 2023 році середня вартість витоку даних для організацій із 500 або менше співробітників зросла на 13,4% порівняно з минулим роком і досягла 3,31 мільйона доларів США.

2. Покращене усунення інцидентів безпеки: кібербезпека не є досконалою наукою, коли йдеться про виявлення загроз. Інциденти безпеки неминучі, але лише за належної безпеки електронної пошти організації можуть виявити та усунути потенційні інциденти, перш ніж вони можуть завдати ще більшої шкоди. Очевидно, це залишається болючоюточкою для багатьох організацій. Згідно зі звітом IBM Cost of a Data Breach Report, організаціям потрібно в середньому 217 днів, щоб виявити витік даних, спричинений фішингом, і ще 76 днів, щоб його локалізувати. Загалом лише третина організацій, які зіткнулися з витоком даних у 2023 році, виявили це внутрішньо, що, ймовірно, погіршило репутаційні, фінансові та регуляторні наслідки атаки.

3. Підвищена довіра зацікавлених сторін: безпека електронної пошти захищає від загроз, які можуть завдати шкоди репутації організації в очах її клієнтів, потенційних клієнтів і партнерів. Це включає в себе обмеження ймовірності витоку даних, атаки на ланцюжок поставок або скомпрометованого облікового запису, який можна використовувати для націлювання на зовнішні сторони. У 2023 році компанії, які зіткнулися з витоком даних, зазнали збитків усередньому на 1,3 мільйона доларів через втрату доходу від обороту клієнтів, зниження продажів і порушення безперервності бізнесу. Ця цифра становить приблизно 30% від загальної вартості порушення.

4. Підвищення безперервності та продуктивності бізнесу: заходи безпеки електронної пошти допомагають підтримувати безперервність бізнесу, зменшуючи ризик закриття або простою, спричиненого атаками на основі електронної пошти. Вони також зберігають продуктивність від часу, витраченого на успішну кібератаку. Програмне забезпечення-вимагач, яке в основному поширюється через атаки на електронну пошту, призвело до середнього простою компаній на 25 днів у першому півріччі 2022 року . Ця цифра відповідає середньому світовому показнику.

Найкращі методи безпеки електронної пошти

Є низка передових методів безпеки електронної пошти, які можуть допомогти захистити вашу організацію від загроз електронної пошти. Хоча технології відіграють важливу роль у захисті, люди також надзвичайно важливі для безпеки електронної пошти та можуть бути останньою лінією захисту, коли бізнес зазнає атаки.

1. Розгорніть розширене рішення безпеки електронної пошти.

Впровадьте надійне рішення для захисту електронної пошти, яке використовує поєднання технологій штучного інтелекту та людської інформації для захисту від складних атак. Шукайте рішення, які пропонують комплексні та надійні функції для запобігання загрозам, їх виявлення та реагування. Рішення, які використовують машинне навчання або обробку природної мови, краще обладнані для моніторингу та виявлення фішингових атак.

2. Впровадити багатофакторну автентифікацію (MFA).

Зміцніть свою безпеку, вимагаючи від користувачів надання кількох форм підтвердження перед доступом до своїх облікових записів. Наприклад, це може включати пароль і унікальний код, надісланий на мобільний пристрій. Це зменшує ризик несанкціонованого доступу до облікових записів електронної пошти. Для найкращого захисту використовуйте багатофакторну автентифікацію, яка потребує перевірки через кілька каналів зв'язку (тобто код, згенерований на мобільному пристрої для надання доступу на робочому столі). Це допомагає запобігти атакам типу "людина посередині" та значно ускладнює крадіжку облікових даних.

3. Застосовуйте надійні паролі та часту заміну паролів.

Заохочуйте користувачів створювати надійні складні паролі, щоб мінімізувати ймовірність атак на основі паролів і несанкціонованого доступу до облікових записів електронної пошти.

4. Створіть програму навчання користувачів.

Розкажіть користувачам про найкращі методи безпеки електронної пошти, як-от виявлення спроб фішингу, уникнення підозрілих посилань і повідомлення про потенційні загрози. Навчальна програма з підвищення обізнаності про фішинг може підвищити їхню обізнаність і зменшити ймовірність того, що вони стануть жертвами атак електронною поштою.

5. Розгорніть програмне забезпечення для підвищення обізнаності користувачів.

Замість навчання в класі шукайте імітаційні навчальні рішення, які адмініструються автоматично та надають користувачам персоналізовані інструкції, адаптовані до їх ролі та контексту в організації. А ще краще запровадити тренінг для підвищення обізнаності користувачів, який пропонує контекстне навчання на основі дій користувача.

6. Наведіть курсор на посилання в електронних листах, щоб побачити кінцеву URL-адресу.

Заохочуйте користувачів наводити курсор миші на посилання в електронних листах, щоб переглянути фактичну цільову URL-адресу перед натисканням, що дасть їм змогу визначити та уникнути зловмисних посилань, які можуть призвести до фішингових вебсайтів або завантажень зловмисного програмного забезпечення. Якщо ви використовуєте рішення безпеки електронної пошти, яке переписує URL-адреси, щоб перевірити їх на безпеку, цей крок можна проігнорувати.

7. Не відкривайте вкладення від невідомих одержувачів.

Порадьте користувачам бути обережними, отримуючи вкладення електронної пошти від незнайомих відправників, оскільки вони можуть містити зловмисне програмне забезпечення або інший шкідливий вміст, який може скомпрометувати їхні системи. Якщо ви сумніваєтеся, доручіть своїм користувачам пересилати електронні листи команді з кібербезпеки. Якщо електронний лист здається важливим, створіть новий ланцюжок електронних листів, щоб зв'язатися з відправником і перевірити його автентичність. Ще краще, якщо ви вважаєте, що знаєте відправника, зателефонуйте йому напряму (змініть канал зв'язку), щоб перевірити електронну пошту. Пам'ятайте, що Spear Phishing часто полює на користувача, який хоче допомогти людині на іншому кінці, або що він не буде пильним.

Що таке політика безпеки електронної пошти?

Політика безпеки електронної пошти стосується набору правил і процедур для забезпечення безпечного та відповідального використання електронної пошти в організації. Це включає вимоги до того, як працівники мають обробляти конфіденційну інформацію, повідомляти про підозрілі електронні листи та дії та дотримуватись протоколів безпеки.

Як приклад, у політиці безпеки електронної пошти може бути вказано, як працівники мають повідомляти своєму

IT-адміністратору про спроби фішингу чи інші підозрілі електронні листи.

Політика безпеки електронної пошти має бути чітко написана легкою для розуміння мовою, бути легкою для виявлення працівниками компанії та регулярно оновлюватися відповідно до найкращих галузевих практик. Ціль політики має полягати в тому, щоб якомога легше для користувачів зрозуміти, як захищена електронна пошта в організації, і як вони можуть зробити свій внесок у безпеку електронної пошти як особи в цій організації.

Запровадивши політику безпеки електронної пошти, організації можуть створити культуру кіберпильності. Це може посилити їхню безпеку та мінімізувати ймовірність інциденту.

Як вибрати правильне рішення для потреб вашого бізнесу

Вибираючи рішення безпеки електронної пошти для вашої організації, слід враховувати кілька ключових факторів.

1. Інтеграція з пакетами продуктивності: вибирайте рішення безпеки електронної пошти, які інтегруються з вашим пакетом продуктивності, оскільки це додає ще один рівень кібербезпеки до вбудованих функцій безпеки. Інші рішення, такі як безпечні шлюзи електронної пошти (SEG), вимикають ці функції та їхні переваги.

2. Здатність і точність виявлення: шукайте рішення, які можуть виявляти як відомі, так і нові або нові загрози, зводячи до мінімуму кількість помилкових спрацьовувань і негативів. Розширені алгоритми штучного інтелекту, обробка природної мови та машинне навчання в поєднанні з аналізом даних у реальному часі з великої статистичної вибірки допомагають у цьому.

3. Фільтрація в режимі реального часу без карантину: щоб забезпечити своєчасний потік легітимних повідомлень, зосередьтеся на рішеннях, які не поміщають електронні листи в карантин для оцінки їхньої токсичності. Коли потрібна оцінка вручну, це може збільшити робоче навантаження IT-команди понаднормово. Замість цього вибирайте рішення, які можуть винести вердикт у режимі реального часу.

4. Відновлення після доставки: кібербезпека розвивається швидко, і щоміть з'являються нові розвідувальні дані. Віддавайте перевагу рішенням, які автоматично видаляють підозрілі електронні листи після доставки на основі нових знахідок. А ще краще шукайте рішення, які автоматично видаляють підозрілі електронні листи та надають докладні звіти щодо електронних листів щодо причини їх видалення. Ви можете виявити тенденції, які вимагають додаткового навчання користувачів, або попередити людей із групи ризику про збільшення кількості спроб фішингу.

5. Набір функцій для реагування на інциденти: багато рішень безпеки електронної пошти наголошують на виявленні за рахунок реагування на інциденти. Усі функції кібербезпеки важливі, включно з тими, які можуть допомогти захистити вас у найуразливіші моменти. Шукайте рішення, які дозволяють швидко отримувати доступ до повідомлень користувачів про підозрілі повідомлення та виправляти їх. Також визначте пріоритетність рішень, які дозволять вам безпечно досліджувати загрози. Це включає докладні журнали електронної пошти та інс-

трументи для перевірки вкладень без ризику для адміністраторів.

6. Інтерфейс користувача: вибирайте рішення, які надають вам єдине вікно для керування безпекою вашої електронної пошти від початку до кінця, включаючи виправлення звітів користувачів, дослідження судових доказів тощо. Можливість детально ознайомитись із деталями є важливою, але не менш важливим є і загальне бачення, яке ви можете взяти, щоб звітувати перед зацікавленими сторонами.

7. Розширений захист для шкідливих веб-сайтів: Електронна пошта є основним вектором, але збиток часто виникає через фішингові сторінки. Надайте пріоритет рішенням, які дозволяють захистити користувачів, які перенаправляються зі зловмисного електронного листа на невідомий веб-сайт.

8. Інтеграція з іншими рішеннями кібербезпеки. Замість того, щоб приймати комплексне рішення, найкраще зібрати колекцію найкращих рішень для свого стека кібербезпеки. Здатність цих рішень «розмовляти» одне з одним має першочергове значення для скоординованого інтелекту та ефективного реагування. Вибирайте рішення, які перехресно поєднують інтелектуальні дані в усьому стеку кібербезпеки, включаючи системи безпеки та керування подіями (SIEM), системи виявлення та реагування на кінцеві точки (EDR) або системи розширеного виявлення та реагування (XDR).

Враховуючи ці фактори, організації можуть вибрати рішення безпеки електронної пошти, яке відповідає їхнім конкретним бізнес-потребам і забезпечує ефективний захист від нових загроз електронної пошти.

Захистіть свою поштову скриньку за допомогою Vade

Захистіть свою поштову скриньку з Vade, глобальною компанією з кібербезпеки, яка поєднує штучний інтелект і людське виявлення та реагування для забезпечення безпечної взаємодії людей. Широкий асортимент продуктів і рішень Vade захищає окремих осіб, компанії та організації від широкого спектру кібератак на електронну пошту, включаючи шкідливі програми/вимагачі, фішингові/бізнес-електронну пошту та спроби фішингу.

Маючи багату історію, починаючи з 2009 року, Vade захищає понад 1,4 мільярда корпоративних і споживчих поштових скриньок, обслуговуючи ринки ISP, SMB і MSP. Наші відзначені нагородами продукти та рішення не лише покращують кібербезпеку, але й оптимізують ефективність IT, що робить Vade надійним вибором для захисту ваших електронних листів.

Поширені запитання

Яка різниця між безпекою електронної пошти Office 365 і безпекою електронної пошти Microsoft 365?

Хоча захист електронної пошти Office 365 і Microsoft 365 взаємозамінні, між ними є невеликі відмінності . Office 365 і Microsoft 365 — це два різні пакети передплати, які Microsoft пропонує компаніям. Обидва пакети продуктивності містять багато однакових бізнес-програм. Більшість їхніх планів також пропонують Exchange Online Protection (EOP), власне рішення безпеки електронної пошти Microsoft. Однак лише в плани Microsoft 365 включено опцію Microsoft Defender, розширенішого рішення безпеки електронної пошти Microsoft, ніж EOP.

Незважаючи на цю різницю, більшість інтегрованих сторонніх рішень безпеки електронної пошти працюють як з планами Microsoft 365, так і з Office 365.

Чи достатньо безпеки електронної пошти Office 365 чи Microsoft 365?

Пакет продуктів Office 365 містить вбудовані функції безпеки, які захищають від загроз електронної пошти, таких як деякі типи шкідливих програм. Незважаючи на те, що ці функції є корисними, вони не забезпечують належного захисту від багатьох сучасних сучасних кіберзагроз. Це пояснює, чому Gartner рекомендує організаціям розширити функції безпеки в Office 365 за допомогою інтегрованого стороннього рішення безпеки електронної пошти. Інтегроване рішення доповнює безпеку електронної пошти Office 365 і забезпечує додатковий захист від загроз, які Microsoft пропускає.

Як зробити свою електронну пошту Office 365 більш безпечною?

Використовуйте комбінацію заходів, щоб посилити захист електронної пошти Office 365. Почніть із прийняття інтегрованого рішення безпеки електронної пошти від надійного стороннього постачальника. Впровадити тренінги з підвищення обізнаності користувачів, щоб вони навчилися розпізнавати кібератаки та боротися з ними. Також заохочуйте своїх користувачів або колег бути пильними, повідомляючи про підозрілі електронні листи за допомогою функцій звітування Office 365.

Як я можу покращити безпеку електронної пошти?

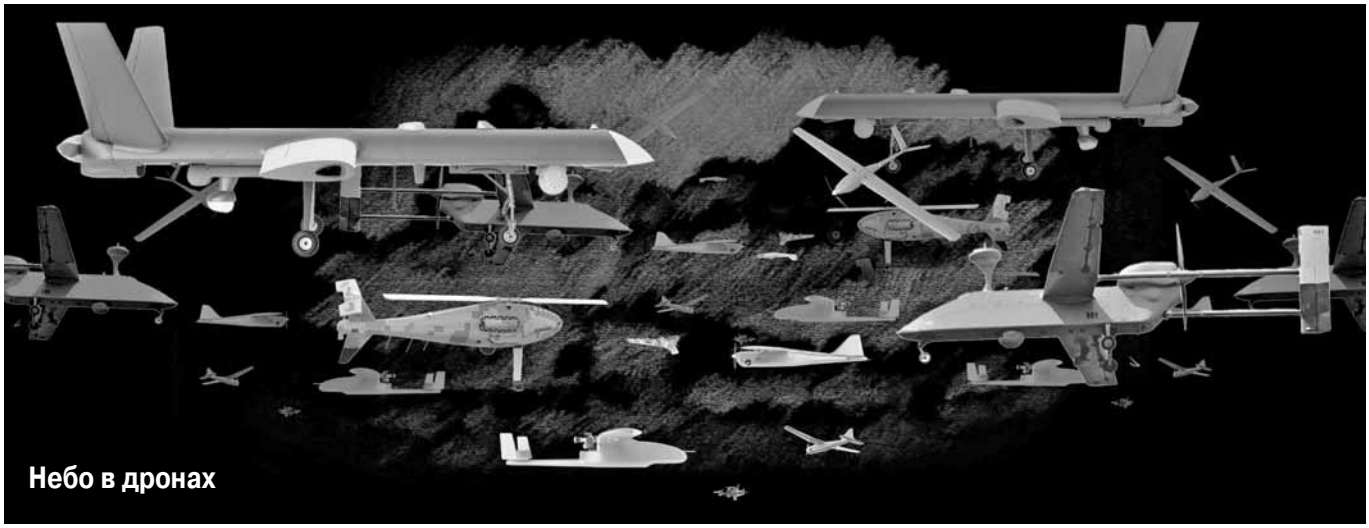
Використовуйте рішення безпеки електронної пошти, яке інтегрується з Microsoft 365, Google Workspace або іншим пакетом продуктів. Це забезпечує перевагу багаторівневого захисту власних функцій безпеки та може перехоплювати розширені загрози, зокрема відомі та невідомі. Також переконайтеся, що ви запровадили навчальну програму з фішингу та оберіть програму, яку можна проводити в електронному та автоматичному режимі.

Антон Шевченко
top-ai.com.ua

Антон Шевченко відомий своєю відданістю підвищенню рівня інформаційної грамотності в галузі штучного інтелекту. Він прагне створювати вміст, який б допомагав користувачам сайту Top-AI не лише зрозуміти технічні аспекти, але й розглядати етичні та соціальні виклики, пов'язані із штучним інтелектом.

Основні російські розвідувальні безпілотники

За свідченнями бійців, Росія переважає нас за кількістю безпілотників, як розвідувальних, так і ударних. І цю проблему потрібно вирішувати.



Небо в дронах

Дальні розвідувальні безпілотники дають ворогові змогу уражати нашу важливу зброю. Працює це так: безпілотник бачить і передає інформацію, а росіяни відразу запускають «Іскандер» або «Ураган-1М» по цілі.

Саме так окупанти вже знищили кілька українських вертольотів і пускову установку Patriot.

Розвідувальні безпілотники малого і середнього радіуса дії не менш небезпечні. Вони працюють безпосередньо на лінії фронту, допомагаючи російській артилерії вести точніший вогонь і завдавати максимальних втрат.

На жаль, Україна не може масово збивати розвідувальні безпілотники. Їх кількість надто велика, а можливості нашої ППО обмежені. Ще є радіоелектронна боротьба (РЕБ), але вона може лише завадити безпілотнику виконати завдання: зіткнувшись із перешкодами, він розвертається і летить назад.

Чому так важко збити російський безпілотник?

Непомітність. Багато моделей, особливо малі розвідувальні дрони, важко помітити чи почути під час роботи.

Відсутність теплового сліду. Безпілотники, що працюють на акумуляторах, не залишають теплового сліду. Це ускладнює їх виявлення інфрачервоними системами.

Обмежені можливості ППО. Не всі засоби ППО дістають до висоти польоту деяких розвідувальних безпілотників.

Дефіцит ракет. Україна відчуває постійний брак ракет для ППО.

Засоби РЕБ впливають не на всі літальні апарати. Ті, що летять у режимі повного радіомовчання, нічого не випромінюючи за інерцією, здійснюючи фотозйомку за заданим курсом, нечутливі до РЕБ.

На графіці червоним виділені «Орлан» і ZALA. Ці безпілотники найчастіше трапляються на полі бою, їх робоча висота 1800–2000 м. Про решту простий боєць може й не чути, вони не такі поширені. Проте фахівці, які вивчають російську зброю, документують їх використання.

Ефективним засобом проти БПЛА «Гранат» і квадрокоптерів є переносні зенітно-ракетні комплекси (ПЗРК), проте використовувати їх проти таких малорозмірних цілей не завжди доцільно.

«Елерон» і «Мерлін» піднімаються на висоту 5 км, але їх фіксують нечасто. Для боротьби з ними ефективно використовувати зенітно-ракетні комплекси «Оса» і «Тор».

«Оріон» і «Форпост» здатні підніматися на висоту до 7 км, що робить їх важкодоступними для більшості українських засобів ППО. Для боротьби з ними потрібні сучасні зенітно-ракетні комплекси, такі як «Куб», «Бук», IRIS-T.

Є випадки збиття «Орланів» FVP-дронами. Сподіваємося, це вдасться масштабувати.

За словами фахівця з РЕБ, найбільшу загрозу для нас становлять «Орлан», ZALA, Supercam (на графіці відсутній) та «Мерлін». ZALA, Supercam можуть використовуватися і як розвідники, і як коригувальники вогню, які ведуть пряму трансляцію з поля бою. ZALA також використовують для наведення дрона-камікадзе чи, точніше, баражуючого боєприпасу «Ланцет» (інші пролетіли, зафіксували ситуацію, і ворог отримує інформацію вже після повернення БПЛА).

Зазвичай вони піднімаються на висоту 2,5–3 км, адже з висоти 1,5 км їх уже можна уразити з кулемета. У хмарні дні можуть опускатися до 800 м.

«Орлан» — один із наймасовіших російських розвідувальних дронів, яким можна проводити як денну чи нічну, так і радіотехнічну розвідку. Він особливий тим, що його постійно модернізують, встановлюють на нього нове обладнання, зокрема новітні, просунуті камери.

«Орлан» також намагалися використовувати як ударний безпілотник, щоб скидати з нього боєприпаси, але від цієї ідеї відмовилися.

Надя Кельм,
Олег Гебура,
Олександр Шульман
Тексти.org.ua

Зграями дешевше. Як родина налагодила систему збирання FPV-дронів

Комунікаційниця Оля Гарбовська організувала безперервний процес збору коштів, закупівлі запчастин і складання FPV-дронів, який робить їх удвічі дешевшими. Ядро цієї команди — сестра Ольги, тато і татів колега. Десятки людей постійно жертвують кошти на запчастини. Вдалося зібрати вже п'ять зграй (83 дрони).

На прохання Texty.org.ua Оля поділилася своїм досвідом. Підтримати збір на чергову зграю її каканчиків, як вона називає свої вироби, можна за лінком наприкінці цієї статті. Далі пряма мова авторки.

Оля Гарбовська із сестрою Іриною Панчак, яка також у команді зі збирання дронів-камікадзе

Спалена «Весна»

Дешеві китайські гірлянди, ну й ще спалений магнітофон «Весна» в дитинстві. Саме вони тоді посіяли зерна віри в те, що я зможу зібрати дрон. Звичайно, у свої 10 чи 12 років я не думала про дрони-камікадзе, якими займатимуся через 25 років.

Просто хотілося, щоб обгортки від цукерок на ялинці (ключове «від», бо самі цукерки зникали, як шкарпетки в пральній машині) гарненько виблискували, відбиваючи дуже неякісні вогники, які щороку доводилося перепаювати.

Ну а з магнітофоном вийшло з димком, епічно. Досі не знаю, що пішло не так, але мене та ситуація навчила, що спершу потрібно розібратися, що й куди паяти, ну і якісно, щоб не коротнуло. От прочитає бабуся цей текст і нарешті дізнається, хто з чотирьох онуків спалив ту «Весну». Так, то була я.

Тато і я

Я допомагала війську ще з 2014 року, не масштабно, але трішки було. Після повномасштабного вторгнення впряглася вже суттєво. Якимось дивом, на адреналіні, жонглювала роботою менеджерки стратегічних комунікацій у міжнародній організації і волонтерською діяльністю. Було все: одяг, ліки, підгузки, намети, спальні мішки, тактичні аптечки, їжа, авто, генератори, евакуаційні ноші, медицина, човни, тепловізори, хімічні грілки, ну й різного типу дрони.

Знала, що на фронті є гостра потреба в дронах, і коли з'явилися перші відеоінструкції й онлайн-курси інженерів БПЛА, вкорінилася ідея-фікс спробувати спаяти хоча б один. Виношувала це бажання кілька місяців, почала проходити курс інженера БПЛА, а тоді якось із батьком вирішили спробувати зробити кілька дронів.

Я то озвучила, що спробуємо, глянемо, а там як Бог дасть, але вже тоді в голові стала прокручувати варіанти певної системної роботи, бо хотіла максимально використати наші з батьком навички і вміння. І ось як у нас це вийшло...

Каканчики

Свої дрони-камікадзе я називаю «каканчики». Чому каканчики? У перші роки повномасштабного вторгнення я жила в невеличкому містечку на Львівщині.

Майже кожний мій ранок розпочинався о п'ятій чи шостій. Спершу я займалася волонтерськими завданнями, а близько дев'ятої сідала виконувати свою основну роботу. І щоранку на сніданок до мене прилітали цілі зграї синичок. Якось я зробила фото, як їх годую майже з рук, і опублікувала на своїй сторінці у фейсбуці.

Фото з дронами-каканчиками допомагають Олі збирати в соцмережах кошти на нові зграї Фото з дронами-каканчиками допомагають Олі збирати в соцмережах кошти на нові зграї

І вже через деякий час до мене приїхав подарунок від друзів — годівничка й корм для какаду. Чому корм для какаду — загадка, але це нас дуже розсмішило, і ми жартували, що коли нагодувати українських синичок цим кормом, то вони трансформуються в такі собі каканчики. Мені це слово припало до душі, і я без вагань назвала ним дрони-камікадзе. Бо каканчики завдають ворогу непоправної каки.

Початок

Спершу ми визначилися з типом FPV-дронів, які хочемо робити. Для цього розпитали знайомих із 54-ї ОМБр (батальйон безпілотних систем «Небесна кара»), у яких саме дронах є потреба і які характеристики вони повинні мати.

Додатково перечитала поради проєкту Social Drone, поспілкувалася з кількома пілотами і склала перелік комплектуючих у найоптимальнішому варіанті. Оскільки вирішили робити дрони-камікадзе, було важливо підібрати не дуже дорогі, але якісні деталі, щоб дрон чітко працював і виконував своє завдання, а це, по суті, політ в один бік.

Маючи перелік, пішла я гуляти по Prom.ua та AliExpress. Підрахували і порівняли вартість (люблю ексельки). Зважили час доставок і вирішили все ж таки купувати деталі в Китаї.

Гроші. Де їх взяти? Зібрати! Запустила збір на перших дев'ять дронів, але мала трішки залишків ще з попередніх зборів, то досить швидко назбирали необхідну суму.

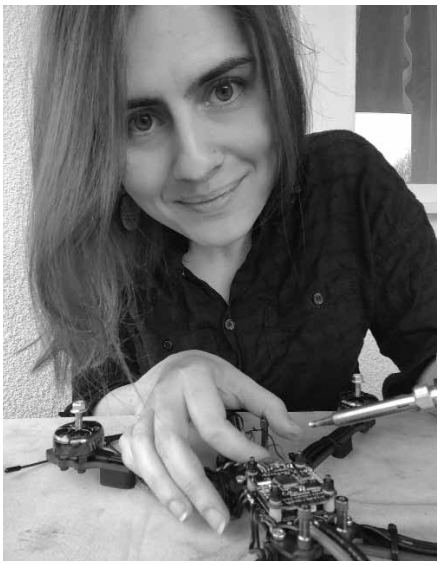
Далі замовили комплектуючі й чекали більш як три тижні. То було, напевно, чи не найдовше. Адже втрачала терпець, кортіло вже зібрати того дрона.

Перший дрон

Коли отримали всі деталі, тато спаяв перший, а за ним за паяльник взялась і я. Паяла п'ять годин, а батько перевіряв кожну пайку.

Батько Олі паяє дрон-камікадзе

Я не пручалася, бо добре пам'ятала епічну «Весну». Якість пайки важлива. І бажано не «мучити» ті плати, щоб випадково не пошкодити численними перепаюваннями, а раз запаяти і все. Я навіть попередньо взяла стару плату, щоб пригадати, як тримати паяльник у руках і робити хорошу пайку. Насправді це нескладно, і вже за годинку тренування впевненіше запаювала старі конденсатори.



Оля Гарбовська із власноруч спаяним дроном-камікадзе

Загалом можна сміливо керуватися ось цим відео, *(https://youtu.be/CsUqnlsswcg?si=MQby1IWss27a8ZcH)* якщо немає можливості працювати з людиною, яка вміє паяти. Пайка не такий вже й складний процес. А збірка дрона — конструктор.

Детально процес збірки іншого дрона з наочними ілюстраціями кожного етапу описаний тут. *(https://texty.org.ua/articles/113378/yak-ya-zrobyla-svij-pershyj-fpv/)*.

Зграями дешевше

А далі більшість процесів зі збору дронів тато взяв на себе, згодом підключився його колега, а я допомагала зі збором рам, бо левова частка мого часу йшла на прорахунок витрат, моніторинг замовлень деталей і фандрейзинг. Без грошей не було б що паяти. Але мені й досі кортить взяти паяльника в руки.

Поки закінчували збірку перших дронів, я зрозуміла, що потрібно братися відразу за наступний збір і робити замовлення, адже доставка займає дватри тижні.

Партія дронів готова до відправки

Є один лайфхак, простий, але він допомагає суттєво зменшити вартість дрона і, по суті, запустив певну системність у їх складанні. Шукаючи комплектуючі, ми помітили, що бувають мініоптові пропозиції на різні деталі. Наприклад, пропозиція з 10 антен коштує 40 доларів, а якщо купувати поштучно, то вийде 47 доларів. І так із багатьма комплектуючими. Відповідно ми почали полювати на вигідні пропозиції і намагалися максимально грамотно й вигідно робити закупівлі. Якось натрапили на дуже

велику кількість таких пропозицій, і одна зі зграй (так називаю партії каканчиків) обійшлася в 7415 грн за дрон (зазвичай вони обходяться у 8–9 тисяч).

Зауважу, що більшість дронів ми відправляємо батальйону без АКБ (акумуляторна батарея) – у них є своя майстерня, і вони мають можливість знаходити потрібні батареї за вигіднішими цінами, ніж купувала б їх я.

Оптимізація

Виловлюючи вигідні пропозиції, ми завжди маємо залишок деталей після кожної зграї, тому ведемо облік і постійно докуповуємо те, чого не вистачає на наступні партії. Але я завжди намагаюся чітко ставити реалістичну ціль, тобто кількість для кожної зграї. Такий підхід допомагає мені тримати фокус і планувати.

Найбільшу кількість дронів нам вдалося зібрати в третій зграї — 32 дрони. За місяць до свого дня народження запустила збір, плюс мали залишки деталей, і таким чином вдалося скласти таку кількість.

Ще один лайфхак. Дрон (без АКБ) складається з дев'яти деталей. Комплектуючі замовляємо в кілька етапів (залежно від наявності вигідних пропозицій та коштів), і спершу намагаємося замовити рами, польотні стеки (мозок дрона) та двигуни. Саме ці деталі є основою всього і потребують часу на збір і пайку. Маючи їх, починаємо працювати, доки доставляють решту: камери, приймачі, антени та інше.

Система, яку ми розробили, як на мене, досить проста і добре для нас працює з огляду на те, що всі залучені до цього процесу мають постійну роботу.

Якщо підсумувати, велике значення мають системність зборів, пошук вигідних пропозицій, першочергове придбання пріоритетних деталей, чіткі цілі щодо кількості та дедлайни.

Команда

Почнемо з того, що кількість людей, завдяки яким з'являються каканчики, порахувати важко. Насамперед це ті, хто підтримує фінансово, ті, хто допомагає зі зборами, ті, хто приймає доставки з Китаю, і ті, хто безпосередньо паяє.

Якщо говорити про ядро команди, то нас четверо. Починали ми з батьком удвох. Майже відразу підключилася сестра, теж допомагає зі зборами. Після першої зграї приєднався батьків колега.

Перші каканчики ми надіслали «Небесній карі» 7 квітня, на сьогодні вже передали 83 дрони і працюємо над шостою зграєю (23 дрони).

Труднощі

Найскладнішим для мене в цьому всьому процесі було визначення переліку всіх деталей. Я ніколи не мала з цим справи, відповідно голова трішки кипіла, поки зрозуміла, що VTX — це і є відеопередавач, а є ще приймач, а ще для рами Mark 4 та антени Rush Cherry 2 SMA краще брати не Foxeer Reeper Extreme, а Rush Max Solo.

Коли я сіла розбиратися з переліком на самому початку, спілкувалася з різними експертами, читала статті та інструкції, там фігурували різні терміни, виробники і назви. Переважно мені казали: або така, або така антена, ця рама ок і ця теж. Поки досліджувала все це діло, інтуїція підказувала, що може бути трішки халепа, бо не може бути все так стандартно і легко підганятися. Тому довелося посидіти кілька вихідних, подіставати питаннями знайомих, повторно переглянути різні тьюторіали. Чесно, голова в якийсь момент закипіла. Але все вдалося. Можливо, те, що мені було складно, для іншої людини таким не буде. Це суто мій досвід, бо я затятий гуманітарій. Мушу зазначити, що зараз можна без особливого головного болю отримати перелік усього і не перейматися так, як я це робила. Мені було важливо зробити саме ті дрони, які потребувала «Небесна кара». І оскільки технічно я не була в цих темах підкована, трішки заморочилася, але ні про що абсолютно не шкодую, бо, заглибившись, розширила свої знання і вміння. Певно, таким мав бути мій шлях. Високі гори мають глибокі доли.

Планування і комунікації

Я достатньо креативна панянка, і мені притаманний творчий хаос. Але досвід проєктної діяльності мене трансформував, і я, можна сказати, людина організованого творчого хаосу. Це додає мені достатньої гнучкості й допомагає не панікувати, коли щось іде не так, як я собі планувала. Можу швиденько адаптуватися, подумати і шукати нестандартні рішення. Досвід роботи з людьми допомагає вирішувати багато питань, і я майже завжди можу знайти потрібну мені людину, щоб подолати якусь перепону.

Ну й останнє, не менш важливе — мій досвід у комунікаціях, усі ті знання і навички. Масштабних інформаційних кампаній я не запускаю, але комунікації кожного збору пропрацьовую. Таким чином вдається знаходити ресурси для закупівлі деталей. Ось нещодавно сама зверстала швиденько невеличкий лендинг про каканчики, бо щоразу все розписувати не комільфо і мої дописи чи дописи друзів, які підключаються з дружніми банками, перетворюються на альманахи. А так даєш посилання на лендинг, і людина може собі детальніше все почитати: https://kakanchyky.in.ua.

З хлопцями із «Небесної кари», яким відправляємо дрони, ми постійно на зв'язку. Коли надіслали їм перші каканчики, я хвилювалася і чекала їхнього фідбеку. Від цього залежало, чи майструватимемо їх далі. Відгук був позитивний, і відтоді ми не зупиняємося. Доки буде можливість купувати комплектуючі й буде потреба в дронах, будемо їх робити.

Удвічі дешевше

Загалом складати дрони вигідніше, ніж купувати готові. Торік ті самі хлопці з 54-ї ОМБр просили купити їм кілька дронів. Комплектуючі були трішки інші, але за функціоналом приблизно те саме. Тоді за один дрон я віддавала від 16 до 20 тисяч гривень. Ну й, звісно, робила для цього збори. А наші каканчики дешевші, але не гірші, навпаки, комплектуючі якісніші й вартість суттєво нижча. Я приблизно порахувала, що 83 дрони нам обійшлися майже у 800 тисяч гривень, а не в 1,6 мільйона. А це означає, що можемо забезпечити військо більшою кількістю дронів за зібрані мною та друзями кошти.

Жодної копійки не йде на оргвитрати чи оплату праці. Дрібні витратні матеріали, такі як припій, флюс, купуємо власним коштом. Кілька разів доводилося розмитнювати деталі — також власним коштом. Я до того, що це не бізнес і я не маю жодного заробітку. У мене, як і в решти команди, інша мотивація.

По-перше, люди. Вберегти якнайбільшу кількість життів українців та українок.

По-друге, хочу жити у своїй країні. Мала і маю можливість переїхати за кордон, але не хочу. Хочу бути тут, хочу жити тут і продовжувати трансформувати й змінювати, розбудовувати те, чим я займалася до війни і під час паралельно з волонтерською діяльністю. Крейцер цінніший удома, ніж на чужині.

Ольга Гарбовська
Тексти.org.ua

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

Хто зупиниться, той програє. Як швидкість розвитку БПЛА впливає на війну

«Ми, українці, відкрили для себе можливості FPV-дронів від безвиході, а це вилилось у дуже ефективну зброю. І чим далі триває війна, тим більше ми розвиваємо цю сферу, але таким чином розвиваємо й ворога, який вчиться на нас і наших помилках. Якщо ми зупинимося в розвитку безпілотників, то ворог нас випередить».

Так про розвиток FPV-дронів каже Маркіян, результативний пілот одного з РУБАКів (підрозділ розвідувально-ударних безпілотних авіаційних комплексів). Це він знищив машину потужного російського комплексу радіоелектронної боротьби (РЕБ) Борисоглєбськ-2.

Маркіян, один із перших пілотів FPV-дронів, на його рахунку багато «жирних» цілей. Фото з особистого архіву

Це одна з найдорожчих цілей, знищених FPV-дронами за всю війну, загальною вартістю близько 200 мільйонів доларів. Росіяни заявляли, що він незнищенний, бо подавляє всі радіочастоти навколо. Але український дрон цей комплекс РЕБ подавити не зміг. Бо дрон мав топові на свій час характеристики і керував ним умілий пілот.

Але коли Маркіян тільки починав працювати з дронами, технології були далеко не найкращі.

Командування повірило

Яким був день, коли командування повірило, що дрони здатні відбивати штурми?

«Перший мій бойовий виліт був дуже короткий: дрон вибухнув у повітрі, бо ми тоді використовували неякісні плати ініціації, — пригадує Маркіян. — Це були такі дуже дешеві платки, які ми кріпили на сам боєприпас, а не припаювали до польотного контролера. Дрон вибухнув не від удару, а просто в повітрі під час польоту. Це було влітку 2023 року».

А вже на восьмому польоті наш співрозмовник влучив у ворожу БМП з піхотинцями, з яких кількох знищив, поранив і дезорієнтував інших. Це був штурм росіян, і на знищення тієї БМП уже було віддано наказ і танкістам, і джавелінщику, які стояли на тій ділянці.

Вони вже були готові використати танковий боєкомплект вартістю кілька тисяч доларів за один постріл чи ракету Javelin вартістю близько 100 тисяч доларів, щоб зупинити штурм. Але не знадобилося. Штурм зупинив талановитий дронщик маленьким FPV-дроном, зекономивши дорогі боєприпаси.

Штурм зупинив талановитий дронщик маленьким fpv-дроном.

Це була велика подія.

«І одразу «Мавіки» суміжних батальйонів прилетіли з гранатами й почали добивати піхоту, яка зіскочила з бехи. Це був насправді такий фурор. Тоді командування повірило, що дрони здатні відбивати штурми, а наша рота довела, що ми боєздатні».

Але процес пілотування був важкий: недосконале обладнання, яке складно використовувати. Маркіян описав деталі тієї події:

«Штурман мене коригував не по стрімах (онлайн-трансляція з поля бою. — Ред.), як зараз, а просто через рацію. Тобто хлопці сиділи в траншеї, отримували інформацію з КСП, кричали моєму штурману, штурман передавав мені, і все це було таким собі зіпсованим телефоном. А щоб підключитися до антени, я мусив стояти в посадці на повний зріст, хоча це було небезпечно».

Перегони технологій

Цікаво, що в період перших польотів Маркіяна та інших пілотів його підрозділу росіяни на їхньому відрізку фронту взагалі не використовували FPV. Але через якийсь час почали, ще й наситили ту ділянку РЕБами. Так пілот дрона став частиною чи не найважливішого процесу на війні — перегонів технологій, знань і вмінь.

Отже, каже Маркіян, через три місяці після нашого успішного штурму росіяни не тільки самі почали використовувати FPV-камікадзе, а й поставили РЕБ:

«РЕБ був у них на всіх ключових позиціях і техніці, БМП їхали всі з РЕБом і «мангалами», на опорних пунктах стояли окопні РЕБи або РЕБ-гармати. І нам літати стало нереально. Довелося у швидкому темпі вчитися протидіяти цьому — змінювати частоти (тобто довжину радіохвилі, на яких здійснюється керування дронами. — Ред.)».

Пілоти опанували зміну частот, потім стали повсюдно використовувати ретранслятори, тобто посилювачі радіосигналу, які дали змогу не втрачати радіосигнал між дроном і «базою» на нерівному ландшафті. Якийсь час літали в комфортних умовах.

Але ворог розвивався й активно розробляв потужніші та ефективніші засоби РЕБ. «Потім ми зіткнулися зі «шторою», коли глушать не сигнал управління, а частоти відео і на певній відстані картинку з дрона перебиває білий шум».

Протидією стало вміння пілотів використовувати властивості радіохвиль:

«Ми навчилися перемикати канали в повітрі й знаходити ту частоту, яку в конкретний момент не глушить ворожий РЕБ. Але якийсь період ефективних польотів втратили в той час».

Хоча б на крок попереду

Звісно, топові дрони, що технологічно більш просунуті, ніж ті, які має противник, здатні знищувати те, що ворог вважав незнищенним.

Згаданий раніше ворожий комплекс РЕБ Борисоглєбськ-2 Маркіян уразив саме тому, що дрон, яким він летів, технологічно перевершував ті, що були у використанні на той час. Як саме вдалось уразити РЕБ, детально не розповідатимемо. Але протягом наступного тижня окрім Борисоглєбська-2 тоді знищили ще Стрілу-10, БМП, «Град». Пошкодженої техніки було десятки одиниць — завдяки дронам із технологіями, які випереджали ворога на один крок.

Зараз Маркіян працює з дронами, створеними найкращими українськими розробниками. Їх посилюють потужні системи керування, передачі сигналу, що збільшує дальність польоту, забезпечує чітке зображення з відео дрона тощо.

«Довгі», «теплі» і «товсті»

Парк дронів у Маркіяна нині доволі різноманітний. І кожен безпілотник має свою спеціалізацію.

Нічні, або «теплі» (бо з тепловізійною камерою), дрони призначені для роботи вночі. Їх створенням зайнялися навесні 2023 року, бо «стан-

дартні» FPV тоді вже паралізували рух ворога вдень, усі переміщення вони стали робити в нічний час, і потрібне було рішення, як літати і вдень, і вночі.

Виробник дронів «Дикі шершні» наприкінці літа 2023-го написав у своєму телеграм-каналі: «Ми не стоїмо на місці, тепер можна буде завдавати ураження навіть вночі. Запускаємо масове виробництво FPV-дронів із нічними камерами». Інші компанії також працювали над нічними дронами, і під кінець 2023 року вони стали з'являтись у війську.

Маркіян розповідає:

«Якщо в грудні 2023-го це (дрони з нічною камерою. — Ред.) було такою дорогою новинкою, що нам видавався один дрон, тільки якщо треба знищити якусь важливу техніку, то тепер (восени 2024-го) це така буденність, що можна відправити нічний FPV, щоб знищити одну особу».

Є «довгі» дрони, які працюють на далекі дистанції. Їх створили, бо в якийсь момент (знову ж таки через насичення фронту дронами) близько до лінії бойового зіткнення вже перестала їздити ворожа техніка та пересуватись особовий склад великими групами і, щоб знайти ціль, потрібно летіти далі, у ближні тили ворога.

В українському війську є багато спеціалізованих під різні завдання FPV: «товсті» дрони, зенітні дрони, дрони-матки, FPV-крила та інші моделі.

Яскрава розробка — дрон-матка «Королева шершнів», яка доносить на собі малі FPV-камікадзе на велику дистанцію, скидає в повітрі для збільшення дальності їх польоту й одночасно працює ретранслятором сигналу для них. «Королеву» створив однин із найкращих українських розробників «Дикі шершні».

«Товсті» дрони піднімають відчутно більшу вагу боєприпасу, ніж «стандартні». «Королева шершнів» належить і до цієї категорії — це дрон-важковаговик. У червні 2024 року в телеграм-каналі її творців з'явилося відео, де вона піднімає танкову міну вагою 9,5 кг. «Час польоту — 7 хвилин, або 5 км в один бік. І це ще навіть не XL-версія. Далі більше», — написали «Дикі шершні» у своїй публікації. Ще вона може бути бомбером, камікадзе, переносити вантажі й здійснювати дистанційне мінування.

Перехоплювачі проти розвідників

Зенітні FPV-перехоплювачі — це протидія ворожим дронам-розвідникам. Влітку 2024-го ситуація з розвідниками була катастрофічною. Ворожі дрони не лише безперервно моніторили фронт, а й висіли над мирними містами, у глибокому тилу почувалися як удома.

Кричущим став випадок, коли 1 липня 2024 року розвідники навели ракети на військовий аеродром у Миргороді. Військовий авіапарк України зазнав втрат, хоча подробиці не розголошувалися.

Довгий час на це не було ради. І от наприкінці липня розвідників різко поменшало.

«Дикі шершні» написали28 серпня: «Ми модифікували свої дрони для знищення БПЛА-розвідників кацапів. Маємо більш як 100 збитих бортів». Інші виробники також працювали над створенням зенітних дронів-перехоплювачів.

Цей ланцюжок із дронами-розвідниками і дронами-перехоплювачами — ще один яскравий приклад боротьби технологій. Бо росіяни також уже шукають відповідь-протидію.

Західні медіа писали, що росіяни встановлюють відеокамери заднього виду й оснащують свої крила РЕБом. Сергій Флеш, блогер і спеціаліст із радіозв'язку, зазначає, що рішення вже з'явилося.

«Наш противник не стоїть на місці й шукає варіанти захисту від зенітних дронів, — пише він у телеграм-каналі. — Причому це рішення розійшлося в них по військах дуже швидко. Принцип роботи такий: пристрій ставиться на БПЛА і сканує в польоті відеоканали, знаходить відеосигнал від нашого зенітного дрона, розуміє за рівнем, коли наш дрон поруч, і на цій самій відеочастоті вмикає перешкоду, сильнішу за рівнем. Завада перебиває сигнал від нашого дрона, і український пілот втрачає картинку. Завада ставиться на 60 секунд і за потреби повторюється». Проте офіційного підтвердження використання такої технології поки що немає, і це позитивний показник.

РЕБ проти дронів, дрони з ШІ проти РЕБу

Боротьба технологій у ланцюжку дрони — РЕБ має такий вигляд: українці зробили цивільні FPV-дрони повноцінною зброєю і наситили ними фронт.

Росіянам довелося робити те саме й до того ж виставляти захист у вигляді різних РЕБ-систем: на всіх машинах, техніці, опорних пунктах і значущих точках по цілому букету антен, які глушать увесь (або більшу частину) діапазон. Наша відповідь на цю технологію — дрони з автозахопленням і автодоведенням, якими керує штучний інтелект (ШІ).

Принцип роботи дронів із ШІ такий: як тільки такий дрон підлітає на відстань, із якої камерою здатен побачити ціль, оператор фіксує її, і далі дрон долітає до неї сам, без участі оператора і не зважаючи на дію РЕБ.

ШІ в майбутньому також зможе керувати роєм дронів, щоб масовано й одночасно атакувати цілі. Адже люди в ручному режимі можуть синхронізувати політ до п'яти дронів. А для штучного інтелекту не буде проблемою одночасно пілотувати рій із сотні FPV.

Нині першочергове завдання — добре натренувати ШІ навігуватися, розуміти об'єкти, щоб дрон із ШІ розрізняв, де ворожий танк, а де тінь від дерева. Щоб вирішував, як наздогнати рухому, швидку ціль, яка маневрує.

Дмитро, побратим Маркіяна, інженер РУБАК, наводить приклад: «Якщо русня іде по полю і бачить дрон, вони починають бігати, увертатися, падати в кущі, в окопи. І штучний інтелект дрона, швидше за все, не зрозуміє, що йому треба залетіти в окоп, бо туди заховалася ціль. А пілот зрозуміє. З рухомою ціллю автодоведення в тому вигляді, у якому воно є зараз, не завжди справляється».

Безпілотники з ШІ досі існували у вигляді експозиційних, тестових моделей. Зараз українські розробники The Fourth Law, Vyriy Drone, Swarmer та інші, непублічні, швидко прогресують у створенні робочої моделі дронів із ШІ, адже, коли твоїх друзів убивають і твої домівки руйнують, темпи розробки пришвидшуються в рази.

Те, що допоможе просто зараз

Головна стратегія пошуку й втілення в життя технологічних рішень чи вдосконалення наявних у цій війні — обдумування того, що допомогло б на полі бою просто зараз.

Триває велика сучасна війна, інформація поширюється миттєво — у таких умовах не знайдеш рішення, яке було б дієвим сьогодні й через роки. Навіть кілька місяців — це вже дуже далека перспектива.

Розробники дронів відчайдушно намагаються намацати те, що якнайшвидше допоможе тим, хто воює, вирішувати проблеми, які виникають просто зараз.

Ідеї перевіряються одразу в бойових умовах, і поле бою підсвічує недоліки, які не могли розгледіти на етапі розробки в тилу. Велика кількість і швидкість ітерацій виробу дають змогу швидко створити робочу модель і відсіяти неробочі версії.

Хороший приклад відсіювання – інфрачервона підсвітка на світлочутливих камерах дронів. Тоді шукали рішення, як літати вночі. І хотіли, щоб було якомога дешевше. Запропонували підсвітку.

Інженер дронів Дмитро пояснює: «Вона не прижилася — треба було або летіти понад самою землею, але тоді пілот рано чи пізно починав губитися на ландшафті в темряві, або підніматися вгору, але навіть на невеликій висоті підсвітка вже нічого не підсвічувала, якщо не було повного місяця». А от дрони зі світлочутливими і тепловізійними камерами нині в широкому вжитку.

Утім, дрон із тепловізійною камерою ще має недоліки. Наприклад, поширена проблема минулої зими — при низьких температурах скло камери замерзало і керувати дроном ставало неможливо. Цього року український виробник FPV-дронів Odd Systems заявив, що вони створили тепловізійну камеру з повністю герметичним корпусом, який згадану проблему усуває. І це лише одна з її переваг. Але чи ця версія робоча, ми дізнаємося тільки взимку, коли будуть бойові вильоти при мінусових температурах.

Що далі

Як бачимо з низки конкретних прикладів, важко прогнозувати, які технології з'являться в майбутньому. Розробники не публікують у відкритих джерелах планів на майбутнє і не розповідають про те, над чим працюють, щоб не підказувати ворогові, у якому напрямку шукати протидію.

Але Маркіян перераховує свіжі новинки, які тільки-но з'явилися на бойових позиціях і про які вже відомо багатьом: «Є дрони на оптоволокні, які активно використовує ворог, є штучний інтелект, на який залучають максимальні сили всі, хто тільки може. З'являється все більше крил-камікадзе і крил-бомбардувальників, а також наземних дронів — як для мінування, так і турелі на гусеничній основі, які працюють на штурмі з піхотою».

Дарина Воропаєва
Тексти.org.ua

Як виявити шпигунське програмне забезпечення на смартфоні

В наш час важко уявити, як можна обійтися без мобільного гаджета зв'язку в роботі та спілкуванні. Однак, існує небезпека, що на вашому телефоні може бути шпигунське програмне забезпечення, яке може перехоплювати особисті дані та інформацію про дії на пристрої без вашого відома.

Його мета – стежити за всім, що ви робите, а потім повідомляти про це тому, хто вирішив шпигувати за найінтимнішими та особистими подробицями вашого життя.

У міру того, як смартфони все глибше «пускають коріння» в наше повсякденне життя, зростає і обсяг інформації, яку ми свідомо і несвідомо довіряємо цим пристроям. У багатьох відношеннях це стало благом, хоч і не тільки для тих, про кого ми думаємо.

«ПЗ для сталкінгу особливо небезпечне, тому що наші смартфони – це надзвичайно багате джерело інформації, – наводить видання Mashable слова директора з кібербезпеки правозахисної організації Electronic Frontier Foundation Єви Гальперін. – Це ПЗ може відстежувати ваше місцезнаходження, записувати ваші телефонні дзвінки та текстові повідомлення, красти паролі до облікових записів у соцмережах, у які ви заходите з телефону, відкривати доступ до ваших контактів, фотографій, електронних листів і навіть листування, захищеного методом наскрізного шифрування».

У 2023 році порівняно з 2022-м кількість кібератак на російських користувачів мобільних пристроїв під керуванням Android збільшилася в 1,5 рази. Про це свідчать наведені «Лабораторією Касперського» статистичні дані.

Види шкідливого мобільного програмного забезпечення:

37% - Трояни;
30% - Небажане рекламне ПЗ;
10% - Дропери;
9% - Завантажувачі;
5% - SMS-трояни.

Аналітики ESET, міжнародного розробника антивірусного програмного забезпечення зі штаб-квартирою в Словаччині відзначають, що активність шпигунських і сталкерських програм загалом у світі зросла більш ніж на 20% та зазначають, що сталкерське ПЗ може застосовуватися для прихованого спостереження та вторгнення в особисте життя людини.

«Області застосування шпигунського ПЗ досить великі: починаючи від бажання партнерів організувати тотальний контроль за своєю «другою половинкою», закінчуючи прагненням роботодавця контролювати своїх підлеглих. Такі програми реєструють натискання при наборі тексту та відправляють скріншоти екрану на сторонній сервер. Шпигунське ПЗ фіксує місце розташування та веде журнал активності в інтернеті і ще багато іншого. Отримана інформація може використовуватись для шантажу, вимагання грошей», – констатують аналітики.

Також використання шпигунських програм тісно пов'язане із сучасним домашнім насильством.

Під час роботи в Інтернеті ви можете випадково встановити шпигунське програмне забезпечення на телефон, навіть не підозрюючи про це. Відомо, що телефони Android більш сприйнятливі до шпигунських програм, ніж iPhone. Однак будь-якому власнику смартфона необхідно стежити за шпигунськими програмами, особливо якщо ваш телефон застарів або зламаний.

Що таке шпигунське програмне забезпечення?

Шпигунське ПЗ – це тип шкідливого ПЗ, яке відстежує активність на вашому пристрої без вашого відома. Він таємно встановлюється на телефон, планшет або комп'ютер і збирає вашу конфіденційну інформацію, таку як облікові дані, інформація про кредитну картку та історію переглядів. Зловмисники таємно встановлюють шпигунське програмне забезпечення, використовуючи вразливості в системі безпеки або обманом змушуючи вас встановити його.

Після встановлення на телефон шпигунське програмне забезпечення може збирати вашу інформацію, використовуючи камеру та мікрофон телефону для стеження за вами, записуючи натискання клавіш, відстежуючи ваше місцезнаходження та викрадаючи будь-які конфіденційні файли. Після того, як шпигунська програма зібрала вашу інформацію, вона відправляє її зловмиснику, який її встановив через інтернет-з'єднання вашого телефону. Зловмисники можуть продавати захоплену інформацію в даркнеті для власного збагачення.

Основні способи проникнення шпигунського програмного забезпечення на ваш мобільний апарат

Шпигунське програмне забезпечення може бути встановлене на мобільний телефон декількома способами:

Фішинг: Зловмисники можуть надіслати вам повідомлення або електронний лист з посиланням на шкідливий сайт. При переході за посиланням шпигунське програмне забезпечення автоматично завантажується на ваш пристрій.

Підроблені програми: Іноді шпигунське програмне забезпечення маскується під легітимні програми. Під час встановлення такої програми на телефон вона починає збирати ваші дані.

Шкідливі веб-сайти : Відвідування заражених веб-сайтів може призвести до автоматичного встановлення шпигунського програмного забезпечення на пристрій.

Фізичний доступж: Якщо хтось отримує фізичний доступ до вашого телефону, він може встановити шпигунське ПЗ вручну.

Експлойти і вразливості: Зловмисники можуть використовувати вразливості в операційній системі вашого телефону для установки шпигунського ПЗ без вашого відома.

Шпигунське ПЗ призначене для крадіжки персональних даних та їх передачі на сервери хакерів. За своїм типом подібні «шкідники» бувають тихими та активними. Перші всіляко приховують

свою присутність у телефоні. Другі, навпаки, захаращують гаджет різними спам-повідомленнями, зокрема рекламними. А також суттєво уповільнюють роботу смартфона та допомагають заробити зловмисникам. Наприклад, за кожен клік по рекламному банеру, що випливає, хакер отримує гроші.

Чим саме небезпечні «шпигуни» на смартфоні

Існує кілька причин, через які варто перевіряти телефон на шпигунські програми. Одна з головних – порушення конфіденційності особистих даних, а саме:

– тексти SMS та історію дзвінків;
– координати розташування;
– фото, відео та аудіо матеріали;
– логіни та паролі з браузера;
– дані банківських карток та доступ до них.

Список може продовжуватися нескінченно, а наслідки бувають найсумнішими. Погодьтеся, ніхто не хоче, щоб фото та відео з приватного архіву потрапляли до мережі. А говорити про фінансові дані та доступи до корпоративних сайтів зовсім не варто.

Як визначити наявність шпигунської програми на телефоні

Якщо ви не використовуєте антивірусне програмне забезпечення на смартфоні, то визначити наявність «шпигуна» в гаджеті досить складно. Але є кілька основних ознак, які вказують на високу ймовірність зараження подібним вірусом. Ось деякі з них:

– Великі витрати заряду акумулятора. Коли батарея на телефоні почала різко і швидко розряджатися, значить з'явилася програма, яка активно витрачає заряд. Якщо смартфон швидко сідає навіть у режимі очікування, це цілком можливо зараження шпигунським ПЗ, яке регулярно записує розмови. Насамперед необхідно провести аналіз акумулятора. Для цього потрібно перейти в «Налаштування», вибрати пункт «Обслуговування пристрою» та натиснути на розділ «Батарея». Смартфон проведе аналіз програм, які активно витрачають заряд батареї.

– Надшвидка витрата мобільного інтернету. Якщо при підключенні до Wi-Fi ми не звертаємо увагу на кількість трафіку, з обмеженими мегабайтами від провайдера все інакше. У випадку, якщо на телефоні дуже швидко витрачається мобільний інтернет без вашої участі, швидше за все, у вас встановлена шпигунська програма. Все тому, що вона регулярно передає записані дані на сервер зловмисника.

Ще може бути така ситуація. Ваш телефон відключений від мобільного інтернету, і раптом вам надходить повідомлення, що вам нараховано пакет n - МБ за М- гривень до кінця доби. Тут може бути два варіанти: помилка оператора мобільного зв'язку в тарифікації, або ж у вашому смартфоні шпигунське ПЗ передає інформацію. У цьому випадку необхідно перевірити обсяг переданих даних, якщо це будуть одиниці байт, зверніться до оператора мобільного зв'язку. Наразі українські оператори полюбляють нав'язувати послуги, які ви не замовили. В іншому випадку це може бути шпигунське ПЗ. Помічено, що деякі ігри також можуть витрачати інтернет навіть коли не запущені.

– Камера телефону та мікрофон включаються випадковим чином.

Вам потрібно бути обережним, якщо ви помітили, що камера та мікрофон вашого телефону включаються випадково. Якщо камера та мікрофон вашого телефону включаються без вашої участі, то, швидше за все, ваш телефон заражений шпигунським програмним забезпеченням. Шпигунське програмне забезпечення буде використовувати камеру та мікрофон вашого телефону для прослуховування розмов та збору конфіденційної інформації.

– Ви чуєте шум під час телефонних дзвінків.

Під час телефонної розмови можна помітити звуковий сигнал, віддалені голоси та перешкоди. Іноді ці проблеми можна пояснити поганим сигналом, але вони можуть бути ознакою шпигунського ПЗ. Шпигунське програмне забезпечення спробує прослухати ваші телефонні дзвінки, прослухати ваші розмови та записати їх.

– Ваш телефон має проблеми з продуктивністю.

Якщо ви помітили різке зниження продуктивності свого телефону, то швидше за все він заражений шпигунським ПЗ. Шпигунські програми працюють у фоновому режимі, роблячи ваш телефон повільним та непридатним для використання. Це може призвести до зависання, тривалого завантаження, системних помилок, швидкого розряду батареї, проблем з вимкненням або перезавантаженням.

– З'явилися невідомі програми на робочому столі, піктограми або інші зміни на вашому пристрої. Явною ознакою наявності шпигунського ПЗ на вашому телефоні є поява нових програм або файлів, які ви не можете пізнати або не пам'ятаєте, як завантажували. Ці програми самі собою є шпигунськими програмами чи іншими видами шкідливого ПЗ, замаскованими під нешкідливі програми.

У більшості випадків подібні неприємності відбуваються після встановлення програм з невідомих сайтів. Для швидкого вирішення цієї проблеми, у тому числі очищення шпигунського ПЗ, досить просто видаліть нещодавно завантажені програми через «Налаштування» телефону. Також рекомендується очистити cookie у браузері та запустити телефон у безпечному режимі для перевірки.

– Ви отримуєте незвичайні повідомлення.

Якщо ви отримуєте незвичайні повідомлення, такі як часті повідомлення про помилки, рекламу або фішингові повідомлення, що спливають, то, швидше за все, ваш телефон заражений шпигунським ПЗ. Ці повідомлення можуть бути викликані рекламним програмним забезпеченням, встановленим разом зі шпигунськими програмами на вашому телефоні. Рекламне програмне забезпечення буде надсилати вам повідомлення, намагаючись обманом змусити вас розкрити вашу особисту інформацію.

– Ваш телефон постійно перегрівається.

Деякі телефони перегріваються через те, що апаратна частина з часом виходить з ладу. Однак якщо перегрів телефону відбувається раптово, то швидше за все телефон заражений шпигунським ПЗ. Шпигунське програмне забезпечення буде працювати у фоновому режимі та використовувати ресурси та дані вашого телефону для крадіжки та передачі даних.

Як видалити шпигунське програмне забезпечення з телефону?

Якщо ви помітили будь-які з цих ознак на телефоні, швидше за все, у вас є шпигунське програмне забезпечення. Щоб зловмисники не змогли вкрасти вашу інформацію, необхідно негайно видалити шпигунське програмне забезпечення з телефону. Щоб видалити шпигунське програмне забезпечення з телефону, потрібно зробити таке.

– Перезавантажте телефон у безпечному режимі. Перше, що вам потрібно зробити, якщо на вашому телефоні встановлено шпигунське програмне забезпечення, – це відключитися від Інтернету і перезавантажити його в безпечному режимі, в якому використовуються лише основні та необхідні програми, необхідні для включення вашого телефону. Перезавантаження телефону в безпечному режимі перериває будь-який зв'язок між шпигунським програмним забезпеченням та зловмисниками. Безпечний режим також дозволяє перезавантажити телефон без втручання шпигунського програмного забезпечення.

– Видаліть незнайомі програми та файли. Після перезавантаження телефону в безпечному режимі вам необхідно перевірити програми та файли на вашому телефоні. Знайдіть програми та файли, які ви не пам'ятаєте, чи завантажували або які виглядають підозріло. Після того, як ви знайшли шкідливі програми та файли, видаліть їх зі свого телефону. Ви також повинні очистити кеш браузера, щоб видалити всі шкідливі веб-сайти.

– Запустіть антивірусне програмне забезпечення. Деякі шпигунські програми будуть виглядати як законні програми та файли, які важко знайти самостійно. Щоб виявити приховане шпигунське програмне забезпечення, вам необхідно встановити на телефон антивірусне програмне забезпечення. Антивірусне програмне забезпечення сканує ваш телефон на предмет прихованих шпигунських програм та видаляє їх з вашого телефону. На вашому телефоні завжди має бути встановлене антивірусне програмне забезпечення, яке допоможе видалити всі існуючі шпигунські програми та запобігти їх появі.

– Перезавантажте телефон у звичайному режимі. Після виконання попередніх кроків ви можете вивести телефон із безпечного режиму та перезавантажити його у звичайному режимі. Після завантаження телефону вам необхідно запобігти встановленню на нього майбутніх шпигунських програм, оновивши програмне забезпечення та дотримуючись рекомендацій щодо кібербезпеки.

Якщо всі перераховані вище способи не принесли жодного результату, саме час переходити до радикальних заходів. Одним із найдієвіших способів видалення шпигунської програми з телефону є скидання смартфона до заводських налаштувань.

У 99% випадків цієї маніпуляції буде достатньо. Але є особливо «хитрі» програми шпигуни, залишкові файли яких виживають навіть після таких суворих заходів. Все тому, що вони заражають системні файли, які неможливо очистити.

Тому навіть після повного скидання телефону рекомендується перевірити наявність вірусів через програму-антивірус.

Для платформи Android їх чимало, є платні і безкоштовні. Найбільш ефективними, як показують тести, проти сучасного spyware виявляються:

– Malwarebytes Security;

– Incognito - Spyware Detector and Phone Security;

– Kaspersky Mobile Antivirus;

– Avast Mobile Security;

– Bitdefender.

Саме це ПЗ дозволяє виявити шкідника без вживання радикальних заходів.

Наприклад, Bitdefender знаходить різного роду віруси, трояни та шпигунське програмне забезпечення. Він здатний сканувати не тільки внутрішню пам'ять гаджета, а й знімні носії, наприклад, карту пам'яті. Антивірус аналізує програми навіть під час їх встановлення, що запобігає зараженню телефону. Ще одна перевага – робота через хмару. Це дозволяє системі завжди перебувати в активному стані та моніторити можливі загрози ззовні.

Крім звичайного скана, Bitdefender має функцію аудиту, яка перевіряє дозволи всіх встановлених програм. Більш того, антивірус моніторить усі вхідні повідомлення на предмет небезпечних файлів та запобігає доступу до сумнівних посилань.

Як захистити себе від шпигунського програмного забезпечення?

Шпигунське програмне забезпечення може вкрасти інформацію без вашого відома. Ви повинні захистити свою інформацію від крадіжки, запобігши встановленню шпигунського ПЗ на ваш телефон. Ви можете захиститися від шпигунського програмного забезпечення, дотримуючись наступних правил.

– Не завантажуйте програми з ненадійних веб-сайтів

Зловмисники намагатимуться обманом змусити вас завантажити програмне забезпечення, яке насправді є шпигунським програмним забезпеченням. Це шкідливе програмне забезпечення відоме як троян. Це метод доставки шкідливого програмного забезпечення, який маскує зловмисне програмне забезпечення, таке як шпигунське програмне забезпечення, під реальне програмне забезпечення. Ніколи не завантажуйте програми з ненадійних веб-сайтів або рекламних оголошень, щоб уникнути випадкового встановлення шпигунського програмного забезпечення. Завантажувати програми слід лише з надійних джерел, таких як App Store та Google Play.

– Не натискайте на небажані повідомлення.

Шпигунське ПЗ часто може поширюватися через фішингові електронні листи, які намагаються змусити вас завантажити вкладення зі схованим шкідливим програмним забезпеченням або клацнути зловмисне посилання. Вам слід уникати взаємодії з будь-якими небажаними повідомленнями, які містять підозрілі вкладення або посилання. Якщо ви стурбовані тим, що повідомлення небезпечне, ви можете відсканувати вкладення і оминути приховане в ньому шкідливе програмне забезпечення. Ви також можете перевірити безпеку посилання, перевіривши будь-які невідповідності в URL-адресі або скориставшись засобом перевірки URL-адрес.

– Переглядайте лише безпечні веб-сайти.

Зловмисники можуть встановити шпигунське програмне забезпечення на ваш телефон, використовуючи автоматичні завантаження. Завдяки попутним завантаженням вони можуть заразити ваш телефон шкідливим програмним забезпеченням, коли ви зайдете на заражений веб-сайт. Щоб уникнути попутних завантажень через встановлення шпигунського ПЗ на телефон, переглядайте тільки безпечні веб-сайти, яким ви довіряєте. Введіть URL-адресу вебсайту, яку ви намагаєтеся відвідати, і не натискайте на підозрілі посилання та не шукайте її в пошукових системах.

– Оновлення програмного забезпечення телефону.

Зловмисники часто використовують уразливості в системі безпеки, виявлені у програмному забезпеченні або програмах вашого телефону, щоб заразити його шпигунським програмним забезпеченням. Вам необхідно регулярно оновлювати програмне забезпечення вашого телефону, щоб усувати будь-які недоліки безпеки та додавати функції безпеки, які забезпечують найкращий захист вашого телефону. Оновлюючи програмне забезпечення, ви запобігаєте інсталяції шпигунського програмного

забезпечення на ваш телефон зловмисниками.

– Використовуйте менеджер паролів.

Зловмисники спробують вкрасти ваші облікові дані для входу в систему, використовуючи шпигунське програмне забезпечення, відоме як кейлоггер, для запису ваших натискань клавіш. Ви можете захистити свою особисту інформацію від шпигунського програмного забезпечення, зберігши її в менеджері паролів.

Менеджер паролів – це інструмент, який надійно зберігає вашу особисту інформацію, таку як облікові дані для входу в систему та номери кредитних карток, і керує ним у зашифрованому сховищі. Ваше цифрове сховище захищає вашу особисту інформацію за допомогою кількох рівнів шифрування, і доступ до нього можливий лише за допомогою надійного майстер-паролю. Деякі менеджери паролів пропонують функцію автозаповнення, яка заповнює ваші облікові дані при спробі увійти до своїх облікових записів і не дозволяє шпигунським програмам відстежувати ваші натискання клавіш.

– Встановіть антивірусне програмне забезпечення.

Антивірусне програмне забезпечення – це програма, яка запобігає, виявляє та видаляє шкідливе програмне забезпечення з вашого пристрою. Вам необхідно знайти надійне мобільне антивірусне програмне забезпечення, яке допоможе вам виявити будь-яке приховане шпигунське програмне забезпечення, вже встановлене на вашому телефоні, і видалити його. Антивірусне програмне забезпечення також допомагає запобігти зараженню вашого телефону будь-яким вхідним шкідливим програмним забезпеченням. Якщо ви зазнаєте потенційної загрози, антивірусне програмне забезпечення повідомить вам про необхідність залишити шкідливий веб-сайт або скасувати шкідливе завантаження.

– Перевірте список інстальованих програм.

На додаток до використання антивірусного програмного забезпечення, можна перевірити список встановлених програм. Якщо ви помітите якусь програму, яку не встановлювали або не пам'ятаєте, це може бути ознакою того, що на ваш телефон було встановлено шпигунське програмне забезпечення. У цьому випадку видаліть цю програму та перевірте, як це вплине на роботу пристрою.

– Перевірте активність програм.

Ще один спосіб – перевірка активності програм на телефоні. Зверніть увагу на програми, які постійно запущені та використовують велику кількість ресурсів. Ви можете спробувати закрити ці програми та перевірити, як це вплине на подальшу роботу. Якщо телефон почав працювати швидше, варто додатково перевірити ці програми і можливо видалити повністю.

– Перевірте доступ до мікрофона та камери.

Якщо на вашому телефоні встановлено шпигунське програмне забезпечення, воно може отримати доступ до мікрофона та камери пристрою. Перевірте доступ до мікрофона та камери: перейдіть до налаштувань телефону та перегляньте дозволи для програм. Якщо ви помітите, що будь-яка програма має дозвіл на доступ до мікрофона або камери, яку ви не давали, призупиніть доступ і проскануйте телефон.

Ми розглянули кілька способів перевірки наявності шпигунського програмного забезпечення на вашому телефоні. Якщо ви виявили будь-які ознаки того, що на вашому пристрої встановлено шкідливе ПЗ, слід негайно видалити його і вжити заходів для захисту вашого пристрою від майбутніх атак.

Шпигунське ПЗ

За даними опитування про законність телефонного стеження, що була проведена нещодавно, узагальнено інформацію та пропонуємо для ознайомлення читачам журналу «Бізнес та безпека».

У ході опитування понад 2,000 людей зі США та Великобританії людей запитали, що вони думають про стеження за мобільними телефонами дітей, співробітників та близьких, підключених до кіберпростору. Опитування отримало тривожні відповіді.

Понад п'ять відсотків респондентів вважають, що стеження за іншим мобільним телефоном є незаконним.

Чверть людей, які взяли участь в опитуванні, не знали про законність стеження мобільних телефонів.

Понад 18% учасників заявили, що стеження за чиїмось телефоном є законним.

29% людей кажуть, що не знають про це.

Майже 50% людей кажуть, що шпигувати за мобільним телефоном без згоди незаконно.

Як правило, шпигувати за додатком на чиємусь мобільному телефоні без згоди незаконно. Однак у багатьох випадках стеження за мобільним телефоном без їхнього відома може стати законним, наприклад шпигувати за телефоном вашого підлітка з метою його безпеки законно.

Список 10 кращих шпигунських програм для телефону

У разі підозри на те, що на вашому мобільному апараті встановлено шпигунську програму, ви повинні знати її основні функції. В інформації викладеній нижче наведено основні функції найбільш популярних шпигунських програм, що доступні в мережв Інтернет.

1. TheOneSpy – перша шпигунська програма без рута, прихована і складна щодо виявлення користувачем для мобільних телефонів.

TheOneSpy – найкращий додаток для потайного моніторингу. Його розширені функції допомагають користувачам

контролювати, відстежувати та записувати дії дітей та працівників з будь-якого місця та у будь-який час. Він має низку функцій, які дозволяють ефективно відстежувати пристрій. Користувачі можуть використовувати його без складних кроків на пристрої Android, iPhone, Windows або MAC.

Записуйте, слухайте та зберігайте

Дозволяє записувати телефонні дзвінки, VoIP-дзвінки, об'ємні звуки для прослуховування у прямому ефірі та зберігати їх на захищеному носії.

Соціальний моніторинг ЗМІ

Слідкуйте за обліковими записами в соціальних мережах, таких як FB, Instagram, Whatsapp, Tinder, Wire тощо. Відстежуйте повідомлення, голосові нотатки та дзвінки.

Розташування Tracker

Дозволяє здійснювати GPS-відстеження та моніторинг карт маршрутів, а також створює обгороджену територію для цільового пристрою.

Прив'язуй та дивись

Записуйте екрани пристрою в реальному часі та отримуйте повне уявлення про діяльність пристрою.

Заходи за дверима

Функція live spy360 дозволяє керувати передньою та задньою камерою, а також мікрофоном, щоб прослуховувати розмови та ділитися екранами.

Запис VoIP-дзвінка

Це перша нерутирована програма для запису VoIP-дзвінків, яка приховано і віддалено записує WhatsApp, FB, Wire, Line, IMO і голосові виклики.

Точність та досконалість: втілення якісних характеристик

Крім того, з TheOneSpy у вас є багато ексклюзивних функцій, які дозволяють віддалено перевіряти дії цільового пристрою. Він надає вам повний доступ та контроль над цільовим пристроєм. Найкраще те, що він працює у повністю прихованому режимі. Нижче наведені деякі потужні функції.

Запис дзвінків та журнали

Прослуховуйте та записуйте телефонні дзвінки, а також перевіряйте повну інформацію про дзвінок, включаючи номер, ім'я та часову мітку.

Прослуховування мікрофона та камери

Найвибагливіша функція «Прослуховування мікрофона та камери» для віддаленого та непомітного прослуховування та перегляду записів з цільового пристрою.

Реєстрація натискань клавіш

Реєстрація натискання клавіш фіксує кожне натискання клавіші на цільовому цифровому пристрої. Він може запису-

вати ключові журнали текстових повідомлень, миттєвих повідомлень, чатів, паролів та електронних листів.

Моніторинг соціальних мереж

Відстежуйте всі дії в обліковому записі соціальних мереж, включаючи повідомлення чату, VoIP-дзвінки та голосові нотатки.

Відстеження розташування GPS

Ви можете швидко відслідковувати розташування мобільного телефону, використовуючи карти маршрутів, точне розташування та історію GPS за допомогою TheOneSpy.

Screen Recorder

Пристрій запису екрана OneSpy віддалено записує екрани цільових мобільних телефонів та настільних комп'ютерів та зберігає записані файли, які доступні на захищеній панелі керування.

Пряма трансляція 360°

Слідкуйте за оточенням цільового пристрою та слухайте, що він говорить з іншою людиною в режимі реального часу за допомогою Spy360 у реальному часі.

Галерея фотографій монітора

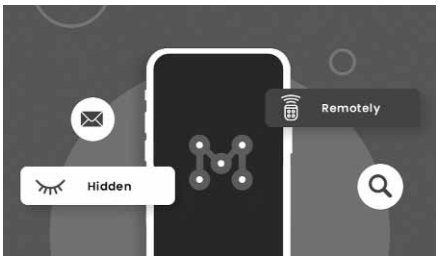
Отримайте уявлення про збережені ними мультимедійні файли та легко отримайте доступ до їхніх фотографій, знімків екрана та музичних файлів.

Пароль Chaser

Шукайте паролі на будь-якому мобільному телефоні, такі як цифрові коди доступу, шаблони та паролі облікових записів соціальних мереж.

TheOneSpy – не єдиний шпигунський додаток для мобільних телефонів. Це бренд, який представляє кілька шпигунських продуктів для мобільних телефонів та комп'ютерних пристроїв. Шпигунське програмне забезпечення має унікальні характеристики порівняно з будь-яким іншим шпигунським додатком.

2. OgyMogy – додаток для прихованого та віддаленого шпигунства за мобільним телефоном.



OgyMogy – одна з найкращих програм для стеження за телефоном, що пропонує шпигунські інструменти для Android із прихованими та віддаленими можливостями. Ця програма з унікальними характеристиками, завдяки яким вона займає друге місце в нашому списку найкращих шпигунських програм для телефонів.

Моніторинг співробітників

Програмне забезпечення OgyMogy для моніторингу співробітників дозволяє роботодавцям відстежувати та записувати активність співробітників, наприклад, використання ними комп'ютера, відвідування веб-сайтів та час, що витрачається на виконання завдань. Цю інформацію можна використовувати для підвищення продуктивності співробітників, визначення областей для покращення та забезпечення дотримання співробітниками політики компанії.

Додаток для батьківського контролю

Створіть безпечне цифрове середовище для дітей за допомогою програмного забезпечення для батьківського контролю OgyMogy. Він може відстежувати дії ваших дітей в Інтернеті, щоб захистити їх від кіберзалякування, сексуальних домагань та відвертого контенту. Це допомагає вам контролювати час використання пристроїв, відстежувати та обмежувати їх переміщення за допомогою геозони, а також блокувати небажані веб-сайти.

Індивідуальний моніторинг

Захистіть дані особистого пристрою за допомогою програми моніторингу OgyMogy, якщо ви їх втратили або вкрали. Таким чином, ви можете дізнатися його місцезнаходження GPS в реальному часі. Крім того, ви можете ідентифікувати пристрій по навколишніх голосах. Крім того, відновіть дані пристрою у разі видалення даних. Збережіть особисті дані мобільного телефону та комп'ютера за допомогою веб-панелі OgyMogy.

OgyMogy працює на пристроях Android, Mac або Windows.

Основні функції:

– Приховане шпигунське рішення для запису дзвінків мобільного телефону, читання повідомлень та захоплення натискань клавіш;

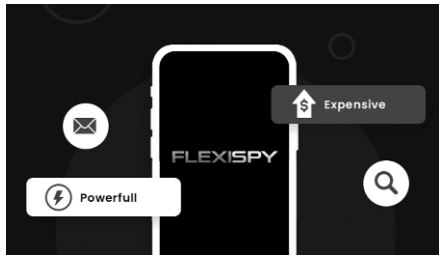
– Віддалений моніторинг текстових повідомлень, телефонних дзвінків та реєстрації ключів;

– GPS відстеження розташування та журналів соціальних мереж;

– Віддалена синхронізація даних через онлайн-панель керування;

– Програма дозволяє прослуховування та перегляд оточення мобільного апарату.

3. FlexiSpy – найдорожче та потужне шпигунське програмне забезпечення для телефонів.



Flexispy – одна з перших програм для телефонного шпигунства. Хоча додаток має безліч різних характеристик, на сьогоднішній день це найдорожчий додаток для телефонного шпигунства в галузі стеження за телефонами. Отже, рішення для відстеження телефонів Flexispy включає функції, які спрощують процес моніторингу. Ви можете використовувати його для спостереження за безпекою своїх працівників та дітей.

Основні особливості Flexispy, про які вам потрібно знати:

Моніторинг встановлених програм

Перегляд встановлених програм, історії установки, версій та моніторингу частоти використання;

Запис телефонних розмов

Прослуховування у прямому ефірі та запис реальних телефонних дзвінків, а також дзвінків по VOIP, таких як skype, LINE та багатьох інших;

Моніторинг соціальних мереж та служб миттєвих повідомлень

Читає повідомлення та стікери, що надсилаються та одержуються в чатах, таких як Facebook Messenger, LINE, та багато іншого;

Слідкування за місцем розташування пристрою

Веде журнал позиціонування пристрою. Виконує експорт координат у ваш улюблений додаток для GPS-навігації для перегляду з висоти пташиного польоту;

Слідкування за цифровими комунікаціями

Читає вміст вихідних та вхідних повідомлень електронної пошти та SMS;

Перегляд медіа-файлів

Отримує доступ та завантажує фотографії та відео, зняті камерою телефону;

Керує використання Інтернету

Контролює відвідувані сайти, пропускну здатність, паролі;

Прослуховує навколишній простір

Керує мікрофоном пристрою та прослуховує навколишній простір;

Оповіщення, звіти, безпека

Вхід з використанням 2FA безпеки для доступу та завантаження даних, можливість оповіщення по ключових словах та місцезнаходження, завантаження звітів та оновлення програмного забезпечення;

Безкоштовний мобільний переглядач

Безкоштовний мобільний додаток для iPhone або Android, який дозволяє отримувати доступ до відстежуваних даних на ходу.

4. Mspy – рутований телефонний шпигун.

Mspy – відомий бренд для стеження за телефонами. Це шпигунська програма для мобільних телефонів, яка, швидше за все, працюватиме на стільникових телефонах з root-доступом. Крім того, виявлення або невиявлення MSPY залежить від цільових операційних систем мобільних телефонів та версій ОС. Таким чином, додаток-шпигун на телефоні здається заплутаним та невизначеним. Він надає вам повний доступ до дій цільової людини на його iPhone.

Основні характеристики програмного забезпечення для відстеження телефонів MSPY:

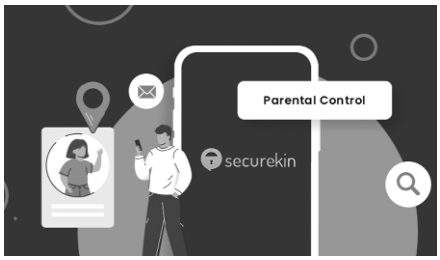
– Рут необхідний, коли справа доходить до стеження журналів месенджерів;

– Виявлення чи невиявлення залежить від використовуваної операційної системи та моделі мобільного телефону;

– Пропонуються базові та преміальні плани для стеження за мобільним телефоном із рутуванням або без нього;

– Має кілька функцій моніторингу соціальних мереж, які можуть працювати без рута.

5. SecureKin – надійне та безкоштовне програмне забезпечення для апаратів Android та iPhone, що використовується для батьківського контролю.



SecureKin – новий продукт на ринку, але він мало чим відрізняється від інших шпигунських програм і так званих шпигунських програм для батьківського телефону. Securekin надає послуги установки батьківського контролю на пристроях Android і iPhone. Це одна з небагатьох безкоштовних програм для батьківського контролю, які дозволяють визначати місце розташування в режимі реального часу, історію переглядів, час використання екрану, журнали активності, блокування програм, історію розташування і кейлоггер.

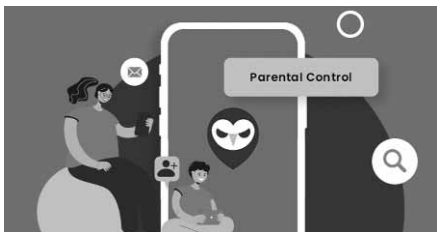
Основні можливості програми Securekin

– Це безкоштовне програмне забезпечення для батьківського контролю для мобільних телефонів;

– Працює на Android та iPhone безкоштовно;

– У ньому є всі функції, які має володіти кращий шпигунський додаток.

6. Hoverwatch – найкращий додаток для батьківського шпигунства для мобільних телефонів.



Компанія Hoverwatch відома своїми рішеннями для шпигунства за мобільними телефонами. ПЗ має найкращі інструменти для батьків, але його часто позиціонують як безкоштовний додаток для стеження за телефоном, що дозволяє встановити батьківський контроль на телефонах дітей. Використовуючи це, ви можете отримати доступ до журналів викликів цільової особи та прочитати її повідомлення.

Hoverwatch пропонує низку функцій, включаючи:

Відстеження розташування: Програма дозволяє відстежувати розташування пристрою в режимі реального часу.

Запис дзвінків та повідомлень: Hoverwatch записує вхідні та вихідні дзвінки, а також зберігає текстові повідомлення.

Спостереження за соціальними мережами: Програма моніторить активність користувача в таких програмах, як WhatsApp, Facebook та Viber.

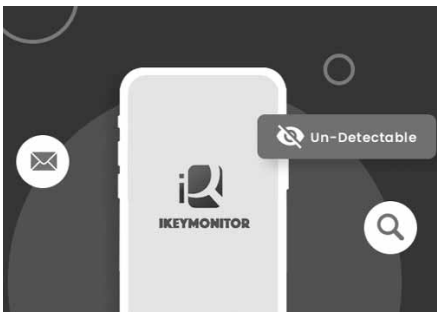
Скріншоти екрана: Hoverwatch періодично робить скріншоти екрану пристрою.

Відстеження веб-активності: Програма зберігає історію відвідуваних вебсайтів.

Підтримка різних платформ: Hoverwatch сумісний з Android, Windows та MacOS, що розширює його можливості застосування.

Прихованість програми: Hoverwatch працює у фоновому режимі, не повідомляючи користувача пристрою про свою присутність.

7. iKeyMonitor – шпигунське ПЗ для мобільних телефонів.



Компанія Awosoft Technology пропонує шпигунську програму iKeyMonitor, призначену для пристроїв з iOS та Android.

Багато програм для відстеження телефонів в Інтернеті відкрито заявляють, що їх неможливо виявити, і iKeyMonitor – одна з них. Це шпигунське програмне забезпечення з обмеженими можливостями, але робить величезні заяви про стеження за мобільними телефонами. Це допомагає вам контролювати дії дітей, щоб захистити їх від участі в ризикованих діях.

iKeyMonitor – це професійна програма для шпигуна, яка не тільки дозволяє вам відстежувати повідомлення та голосові повідомлення, надіслані та отримані, але також записувати натискання клавіш, захоплювати скріншоти та відстежувати текстові повідомлення SMS та журнали викликів, відвідувані вебсайти, GPS розташування, серфінг в мережі Інтернет, вхідні та вихідні чати на WhatsApp, Facebook, WeChat, Skype, Hike та багато іншого.

Крім того, iKeyMonitor доставляє всі ці журнали на попередньо налаштовану адресу електронної пошти, FTP (iOS) або хмарний онлайн-сервер для віддаленої перевірки. До речі, якщо ви хочете дізнатися, як відновити історію чату iKeyMonitor стане гарним вибором.

8. Mobistealth – зручний додаток для телефонного шпигунства

«Дбайте про своїх близьких, не відштовхуючи їх», – йдеться на сайті шпигунської програми Mobistealth. Розробники позиціонують її як продукт для батьківського контролю за смартфонами та комп'ютерами дітей.

Основні функції програми

Запис розмов: Ви можете записувати вхідні та вихідні телефонні дзвінки на Android;

Запис оточуючого звуку: може записувати навколишнє звучання мобільного телефону, використовуючи його мікрофон, та слухати чати та голосові розмови;

Шпигун у соціальних мережах: може стежити за діями месенджера, такими як чат, медіа, повідомлення та інші;

Текстові повідомлення: може читати надіслані та отримані повідомлення на цільовому мобільному телефоні;

Електронний шпигун: можете читати та відстежувати надіслані та отримані електронні листи за допомогою програмного забезпечення для відстеження електронної пошти;

Мультимедіа: може відстежувати загальні фотографії, відео та зображення на мобільному телефоні;

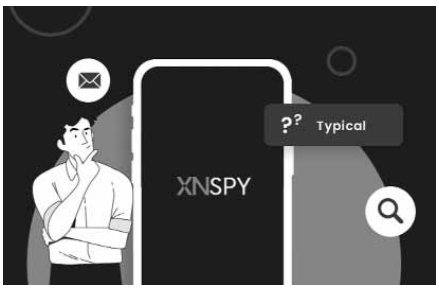
Історія дзвінків: може отримати журнали вхідних, вихідних та пропущених дзвінків на Android;

Історія браузера: стежеить за історією Інтернету з огляду на відвідувані вебсайти та закладки.

Встановлені програми: дозволяє переглянути всі встановлені програми на цільовому пристрої у вигляді списку.

Геолокація.

9. XNSPY – дуже типова програма для телефонного шпигунства.



Програма Xnspy для мобільних пристроїв вкрала особисті дані десятків тисяч власників мобільних пристроїв на iOS та Android. Найчастіше користувачі навіть не підозрювали про те, що їхня інформація потрапила до третіх рук.

Xnspy можна назвати класичним сталкерським софтом (stalkerware), який подається як програма для відстеження активності дітей, а насправді просто

шпигує за власником мобільного пристрою без його відома.

Основні функції

– доступ до книги контактів;
– доступ до журналу вхідних та вихідних дзвінків;
– читання текстових повідомлень або SMS;
– доступ до електронних листів;
– доступ до месенджерів WhatsApp, Viber, Facebook Messenger, KIK, Skype, Line та інших (читання, прослуховування тощо);
– перегляд надісланих та отриманих мультимедійних файлів;
– місцезнаходження у реальному часі через GPS;
– створення списку спостереження з миттєвими повідомленнями для кожного введеного вами розташування, контакту або ключового слова;
– запис середовища оточення.

10. Spyine –шпигунський додаток для мобільних телефонів.

За допомогою Spyine ви можете без проблем стежити за мобільним телефоном вашої дитини.

Основні функції:

– ***GPS -координати***. Дозволяє слідкувати за дітьми чи співробітниками в режимі реального часу;
– ***Доступ до SMS***. Дозволяє читати повідомлення ваших дітей або співробітників;
– ***Слідкування за дзвінками***. Додаток-шпигун для IPhone збирає дані про всі вхідні або вихідні дзвінки;
– ***Геосерфінг***. Вказує, куди не слід ходити. Надсилає сповіщення при перетині цього кордону;
– ***Кейлоггер***. Реєструє все, що було набрано на клавіатурі телефону з Android – без злому прошивки;
– Фото/відео. Дає доступ до всіх фото та відео, що зняті або отримані вашою дитиною;
– ***Snapchat***. Дає змогу читати повідомлення у Snapchat та інших месенджерах, що пише ваша дитина у соцмережах;
– ***Історія браузера***. Відслідковує історію браузера на пристрої вашої дитини онлайн для забезпечення її безпеки;
– ***Шпигун-невидимка***. Абсолютно прихований та анонімний моніторинг.

Отже, підбивши підсумки, з'ясуємо чим же небезпечне spyware ПЗ.

Шпигунські програми для мобільних пристроїв небезпечні тим, що ретельно стежать за власниками пристроїв. За допомогою spyware нечисті на руку програмісти крадуть:

– тексти повідомлень,
– історію викликів,
– координати GPS,
– авторизаційні дані з браузера,
– фотографії,
– відеозаписи,
– аудіозаписи телефонних розмов.

Вам може здаватися, що нічого особливого у вашому телефоні не зберігається. Наприклад, SMS, ви можете скористуватися ними рідко, але не забувайте про мобільний банкінг. Додатку досить витягти з SMS разовий пароль на авторизацію в онлайн-банку, і ваш банківський рахунок стане доступним третім особам. Так само через пароль надісланий у повідомленні викрадають сторінки в соціальних мережах, електронні гаманці, доступи до корпоративних сайтів тощо.

Отримана обманним шляхом історія викликів, як правило, додається до платних баз для розсилки комерційних повідомлень. Тому, якщо вас почали активно спамити, можливо, когось зі списку контактів зламали через spyware.

З мультимедіа і так зрозуміло: ніхто не любить, коли знімки та записи з приватного архіву опиняються у мережі. Особливо, коли йдеться про інтимні знімки. За особливо яскраву «полуничку» шахраї можуть навіть вимагати гроші, тільки не факт, що коли ви заплатите шантажисту, він справді позбудеться краденого вмісту галереї з чужого телефону.

Тому варто дотримуватись рекомендацій щодо захисту вашого гаджета від шпигунського ПЗ.

PS.

Чи знаєте ви, яку інформацію можна отримати, маючи тільки номер телефону?

Наприклад, місце проживання, роботи, сімейний та матеріальний стан і, можливо, навіть кодове слово у банку. А під час війни такий деанон може бути питанням життя та смерті.

Пошук у месенджерах

Отримавши номер телефону, злодій насамперед збереже його в контакти та створить бесіду в месенджері – Telegram, WhatsApp або Viber. Часто користувачі вказують у профілі справжнє ім'я та прізвище, а також прикріплюють реальне фото.

Знаючи ім'я, прізвище та місто, легко знайти людину у Facebook або Linkedin, а з них вже перейти до Instagramy – якщо користувач сам залишив на нього посилання.

Пошук по фото

Якщо в соцмережах стоїть таке саме фото, як у месенджері, достатньо завантажити його в Google-пошук по картинці, і пошуковик сам здасть ваш профіль.

Що можна дізнатися із соцмереж

Власне, все, що вказали там ви та ваші друзі. А саме: місце проживання, навчання, роботи (отже і фінансові справи), сімейний стан, інформацію про членів сім'ї та навіть домашніх тварин. Нерідко клієнти банків вказують дівоче прізвище матері або прізвисько улюбленця як кодове слово.

Номер машини на фото у соцмережах

Якщо користувач викладає фото своєї машини, забуваючи замалювати номер – це дозволить дізнатися таке:

– дані про ДПТ (можуть використовуватися для шантажу);
– кількість власників;
– на кого зареєстровано;
– географію експлуатації тощо.

Існує низка легальних сайтів та мобільних додатків для пошуку власника за номерами машини.

Д.Мусієнко

За матеріалами сайтів:

https://kl.informator.ua/2022/05/12/telefon-shpion-shho-rozpovist-sam-tilky-nomer-mobilnogo/
https://bitdefender.ua/ru/blog/ru-kak-proverit-telefon-na-shpionskie-programmy-i-udalit-ikh/
https://allsoft.ru/news-soft/kak-proverit-chto-na-telefone-net-shpionskogo-po/
https://www.keepersecurity.com/blog/ru/2024/02/09/how-to-tell-if-spyware-is-on-your-phone-and-how-to-remove-it/
https://www.theonespy.com/ru/
https://ogymogy.com/ru/features
https://www.flexispy.com/ru/
https://www.securitylab.ru/blog/personal/SimlpeHacker/353060.php
https://www.theonespy.com/ru/theonespy-vs-mobistealth/
https://www.showmetech.com.br/ru/
https://spyine.com/ru/android-spy-app.html
https://www.theonespy.com/ru/top-10-phone-spy-apps-unique-traits/
https://softdroid.net/luchshie-prilozheniya-dlya-udaleniya-spyware-s-telefona

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

Сучасний світ ставить перед нами нові виклики, і питання безпеки населення набуває особливого значення. Компанія «ALD engineering company», усвідомлюючи відповідальність перед суспільством, ставить людей на перше місце. Ми віримо, що люди важливіші за процеси, і саме тому зосередили свої зусилля на розробці захисних укриттів, які забезпечать безпеку в критичних ситуаціях.

Наші спеціалісти розробили плити із залізобетону зі спеціальними замками, що дозволяють зводити споруди будь-якої складності та розміру. Зовнішній вигляд цих плит, оптимальний склад бетону та металу, тип армування - все це розрахували та розробити спеціалісти проєктного інституту ALD engineering company.

Зокрема, ці залізобетонні конструкції використовуються для будівництва модульних укриттів наземного та підземного типу.

ALD engineering company виготовляє плити для різних конструкцій у себе в цеху. Їх легко транспортувати, а конструкція замків дозволяє дуже швидко зводити споруди з цих плит в будь-якому місці, на будь-якому майданчику — там, де це потрібно замовнику.

Для швидкої збірки використовується зварювання та додаткові болтові з'єднання - це теж прискорює монтаж споруди.

Надійність захисних споруд підтверджується міжнародними сертифікатами якості ISO 9001:2015 та ДСТУ ISO 9001:2015.

Захисні споруди, створені ALD engineering company із залізобетону, надійно захищають від вибухової хвилі, уламків, гранат та стрілецької зброї.

Особливу увагу приділяємо безпеці споруд. Захисні конструкції ALD engineering company успішно пройшли подвійне тестування: перше — у науково-дослідному інституті будівельних конструкцій, а друге — на полігоні, де наші плити витримують вибухові навантаження і стрілецьку зброю. Це забезпечує надійність укриттів у бойових умовах та гарантує безпеку людей всередині.

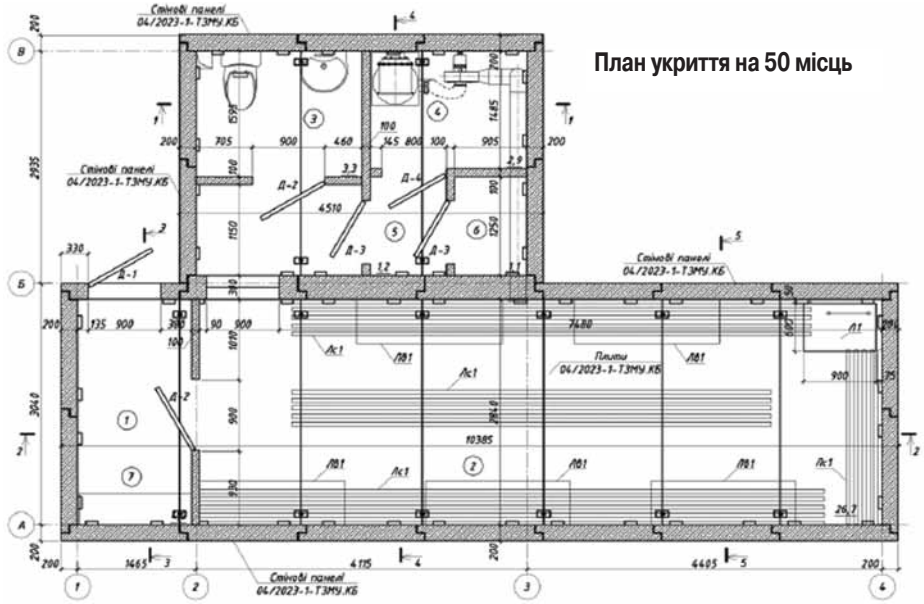
Конструкції із залізобетону дозволяють створювати укриття будь-якої конфігурації та площі. Це може бути захисна споруда як на 3-5 людей, так і на 500-600. Наразі спеціалісти додатково пропрацювали варіант з більш відкритим внутрішнім простором: крім плит туди додаються ще балки та колони, і це дозволяє побудувати підземне укриття ще для більшої кількості людей.

В залежності від побажань замовника, може бути "зібрати" як найпростіше укриття, так і повноцінну захисну споруду, розроблену згідно з вимогами ДСТУ — з системою вентиляцією, кількома приміщеннями, санвузлом, електрикою тощо.

У містах нашої країни активно встановлюються малі архітектурні форми для комерційних цілей. Один з напрямків роботи компанії ALD engineering company — виготовлення міських захисних конструкцій, які поєднують торгову точку з укриттям. Завдяки цій унікальній стратегії бізнес може інвестувати у захист населення, зменшуючи навантаження на державний бюджет і дозволяючи направити кошти на вирішення інших нагальних потреб.

Ці модульні укриття обладнані двома входами та двома виходами, вони захищають людей від уламків і оснащені сигналізацією, пов'язаною із системою МАСЦО, що забезпечує автоматичне відкриття укриття під час повітряної тривоги.

Компанія ALD engineering company утримує провідні позиції на ринку завдяки постійним інноваціям та вдосконаленням, залишаючись відкритою до нових цікавих проектів



План укриття на 50 місць

Для отримання додаткової інформації відвідайте сайт **https://aldholding.com/**

ТОВ «АЛД ІНЖИНІРИНГ І 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

Апаратне забезпечення інформаційної безпеки держави

(Коротка історія створення спеціальної апаратури магнитного запису в Україні)

В березні 1967р. в НДІ ЕМП на базі лабораторії №44 [1] був створений відділ №10 з цільовим призначенням – розробка засобів магнітного запису широкосмугових сигналів, що отримуються засобами радіорозвідки в складі двох лабораторій (№101 – розробка широкосмугових пристроїв магнітного запису оперативної пам'яті та транспоніаторів спектру на жорстких носіях; №102 – розробка широкосмугових пристроїв магнітного запису довготривалої пам'яті та транспоніаторів спектру на стрічкових носіях). Першим начальником його було призначено досвідченого розробника АТМЗ Мачинського В.К.

Зволинський В.М.

Протягом існування відділу було виконано низку робіт, а на початку до його тематики увійшли НДДКР «Поле-2», «Запас», «Каравелла» та «Широта». [1, 2, 4] Так сталося, що начальник лабораторії №102 Зволинський В.М., пізніше, після уходу на іншу роботу Мачинського В.К., маючи вже вдалий досвід робіт в якості Головного конструктора АТМЗ на стрічковому носії «Поле-2» (про це в наступній статті) очолив відділ №10 і став Головним конструктором АТМЗ на жорстких носіях – магнітних дисках.

Життєвий і творчий період Зволинського Вадима Михайловича був стрімкий і короткий. Головною якістю цього одержимого трудівника, дослідника й теоретика була ні із чим не порівнянна оригінальність. Він пройшов шлях від техніка до заступника директора інституту по науці (вища наукова посада). Його ім'я нерозривно пов'язане зі створенням АТМЗ. Причому, створена апаратура практично повністю оригінальна. Це був час молодих інженерів – час винаходів, відкриттів, досягнень.

Блискучий організатор ураховував велику відповідальність за покладений на нього напрямок техніки й залучав до роботи провідних спеціалістів з різних галузей науки і техніки, що дозволило створювати апаратуру на високому науково-технічному рівні.

Поряд з такими корифеями НДІ ЕМП як Бабич О.І., Мачинський В.К., Жила М.І., Калюжний О.Д. [9, 10] та ін. він став одним з основоположників становлення й успішного розвитку інституту.

У ході виконання завдань по закріпленому напрямку техніки під керівництвом В.М. Зволинського вперше в країні створена й впроваджена у виробництво АТМЗ «МУЗ-10» на магнітних дисках для реєстрації й оперативного аналізу радіосигналів у смузі частот до 5 Мгц в інтересах ВМФ (ДКР «Сульфат-Д», замовник в/ч 30882).

Згадана апаратура відноситься до особливо складної й характеризується застосуванням також прецизійної механіки. Для проектування й виготовлення нових високоточних засобів магнітного запису потіребно було створення необхідної функціонально-вузлової бази, у тому числі спеціальних магнітних головок, електродвигунів власного виготовлення, пристроїв функціональної електроніки. Для виготовлення зазначеної АТМЗ були розроблені зразки високопродуктивного прецизійного устаткування для обробки матеріалів, впроваджені в практику прогресивні технологічні процеси й інструменти.

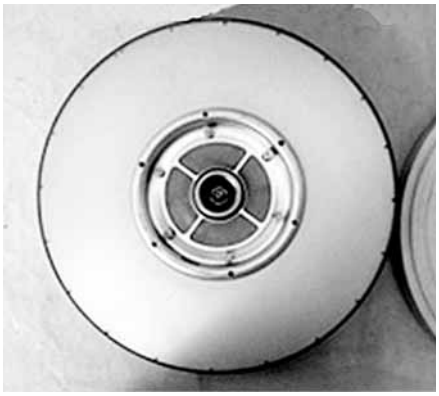
Розглянемо деякі із створених у ті часи виробів апаратури точного магнітного запису та відтворення аналогових сигналів на жорстких носіях Головного конструктора Зволинського В.М.

Виріб «Каравелла-РД»

Виріб «Каравелла-РД» стаціонарна морська апаратура точного магнітного запису та відтворення широкосмугових недетектованих сигналів в складі комплексу радіорозвідки «Каравелла» [1].

Апаратура дозволяла проводити оперативний запис та циклічне відтворення радіосигналів з можливістю аналізу окремої ділянки інформації. Апаратура призначалась для використання в складі корабельного та наземного комплексів радіорозвідки.

Комплект складається з функціональної стійки, блока магнітних дисків [2], а також пульта дистанційного керування. Запис відбувається на пакеті магнітних дисків типу ЕС-5053 (на фото нижче, тоді використовувався достатньо широко в обчислювальних машинах серії ЕС ЕОМ).



Пакет магнітних дисків ЄС-5053 складається із шести алюмінієвих дисків, зовнішній діаметр яких дорівнює 336,4 мм. Поверхні дисків покриті ферролаком товщиною 4-5 мкм або кобальто-вольфрамовим сплавом товщиною 0,25-0,30 мкм. В останньому випадку магнітний шар наноситься гальванічним способом на мідну підкладку. До дисків пред'являються високі вимоги щодо однорідності магнітних властивостей і таких геометричних характеристик, як площинність, товщина, шорсткість поверхні тощо. Для запису інформації використовуються десять внутрішніх поверхонь дисків, зовнішні поверхні верхнього і нижнього дисків не використовуються.

Інформація записується на робочих поверхнях дисків по концентричним колам - доріжкам. Якщо в процесі експлуатації пакета з'являється дефект у покритті на будь-якій з робочих доріжок, то вся ця доріжка не використовується, а замість неї використовується одна із запасних доріжок.

Основні технічні характеристики диска:
- ємність 7,25 Мбайт;
- щільність запису 30-45 біт/мм;
- щільність доріжок 4 мм;
- швидкість 2400 об/хв.;

Основне призначення: для ЕОМ ЕС-5052.

У робочому стані пакет дисків постійно обертається у накопичувачі зі швидкістю 2400 об/хв. Для запису та зчитування інформації накопичувач має десять магнітних головок: по одній головці на кожну робочу поверхню. Магнітна головка складається з універсальної головки (для запису та відтворення інформації) та головки стирання, розміщених в одному корпусі. Магнітні головки розташовуються одна під одною і укріплені на каретці, яка може переміщувати їх у радіальному напрямку щодо дисків.

На відміну від накопичувача на магнітних стрічках у накопичувачах прямого доступу використовується безконтактний метод запису та зчитування інформації. Це пов'язано з тим, що диски нееластичні і контакт з головками може призвести до механічного пошкодження магнітного шару дисків. З іншого бо-

Виріб «Каравелла-РД»

ку, небажано жорстко фіксувати головки в просторі над поверхнями дисків, оскільки практично неможливо виготовити диски абсолютно плоскими, а отже, через нерівність їх поверхонь при обертанні дисків відстань між головками і магнітним шаром постійно змінювалася б. Це, по-перше, не дозволяє забезпечити високу щільність запису і, по-друге, відбивається на амплітуді сигналів, що зчитуються. Компенсувати деякі дефекти можна, використовуючи в накопичувачах прямого доступу так звані магнітні головки, що «плавають».

Умови експлуатації Виробу «Каравелла-РД»: 24 група нормалі НО 005.026/с.

Рік виконання НДДКР-1971-1977, серійне виробництво з 1980р.

Основні технічні характеристики виробу «Каравелла-РД»:

- кількість каналів - 5;
- частотний діапазон 0,3 - 300 кГц;
- швидкість запису/відтворення - 24 см/с;
- час запису – 8 с;
- вид запису аналогових сигналів - ЧМ;
- коефіцієнт детонації - 0,01 %;
- керування апаратом дистанційне; електроживлення - 220В 400 Гц від трифазної мережі 380В;
- споживана потужність 1,0 кВА;
- маса - 250кг, 600 х 641 х 1468 мм;
- потреба - 32 шт на рік.

В розробці брали участь заступники Головного конструктора (ГК): з радіотехнічної частини - Савчук В.П., з дискових систем - Любашенко Л.Т.; з технологічної частини - Корольов В.М, з конструкторської частини - Муравйов Г.Г.; науковці: с.н.с. Корнієнко В.А., м.н.с. Ухов С., с.н.с Спіцин А.М.; інженерно-технічні робітники: Зайцев А.П., Межерицький В.А., Скрипнюк В.В., Спільник А.А., Ковалевський Б.М., Барановський Б.В., Зарубіна Р.Ф., Собчук Г.М. та інші.

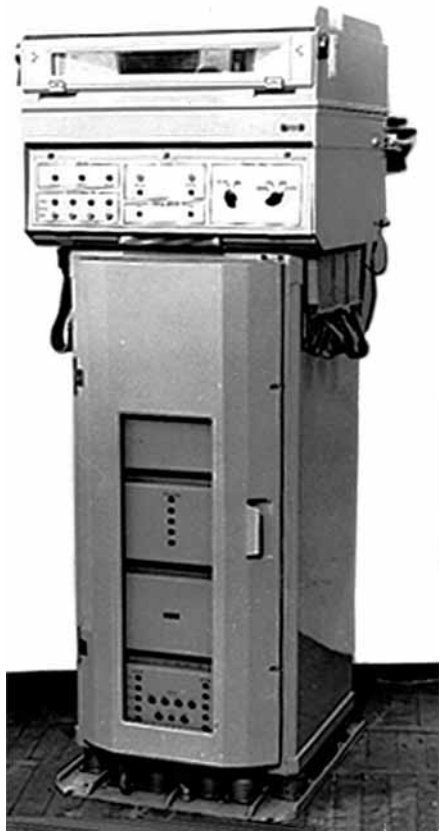
Дослідне виробництво НДІ ЕМП виготовляло зразки виробу під замовлення та постачало Замовнику.

Виріб «Каравелла-РЗ»

Виріб «Каравелла-РЗ» – апаратура безперервної часової затримки радіосигналів.

Апаратура призначалась для використання в складі корабельного та наземного комплексів радіорозвідки «Каравелла» [1].

Конструктивно апаратура «Каравелла-РЗ» подібна апаратурі «Каравелла-РД» і відрізняється від неї робочим діапазоном частот, що записуються та відтворюються та часом запису-відтворення.



Виріб «Каравелла-РЗ»

Рік виконання НДДКР-1971-1977, серійне виробництво з 1980р.

Основні технічні характеристики виробу «Каравелла-РЗ»:

- кількість каналів - 5;
- частотний діапазон 0,003 - 0,2 МГц; час запису - 1,4 с;
- вид запису аналогових сигналів - ЧМ;
- коефіцієнт детонації - 0,01 %;
- керування апаратом дистанційне; електроживлення - 220 В 400 Гц від трифазної мережі 380 В;
- споживана потужність 1,0 кВА;
- маса - 250 кг, 600 х 641 х 1468 мм;
- потреба - 32 шт на рік.

В розробці брали участь заступники Головного конструктора: Савчук В.П., з дискових систем - Любашенко Л.Т., з технологічної частини - Трухан О.І., з конструкторської частини - Муравйов Г.Г.; науковці: к.т.н. Слєпишев І.В., с.н.с. Корнієнко В.А., с.н.с Спіцин А.М.; інженерно-технічні робітники: Зайцев А.П., Межерицький В.А., Скрипнюк В.В., Семенюк В.М., Спільник А.А., Ковалевський Б.М., Зарубіна Р.Ф. та інші.

Малосерійні зразки виробів виготовляло дослідне виробництво НДІ ЕМП і постачало Замовнику, на одному з об'єктів якого, у м. Зеленоградську Калінінградської обл., одночасно використовувалось до 12 шт виробів «Каравелла» - фахівці інституту виконували пуско-налагоджувальні роботи та технічне обслуговування.

Вироби «Широта-1», «Широта-1М»

Вироби «Широта-1», «Широта-1М» – апаратура оперативного запису радіосигналів з затримкою відтворення та довготривалого запису сигналограм з наступним циклічним відтворенням [1].

Апаратура призначалась для використання в складі комплексів радіорозвідки «Лавина-У», «Защита».

Запис відбувається на пакеті магнітних дисків типу ЕС-5053 (аналогічно виробу «Каравелла»).

Конструктивно виріб «Широта» виконано з двох радіоелектронних стійок, між якими встановлено блок магнітних дисків та пульт керування.

Конструктивне виконання виробу «Широта-1М» складається з двох функціональних стійок, блока магнітних дисків, а також пульта дистанційного керування. Запис відбувається на пакеті магнітних дисків типу ЕС-5053.

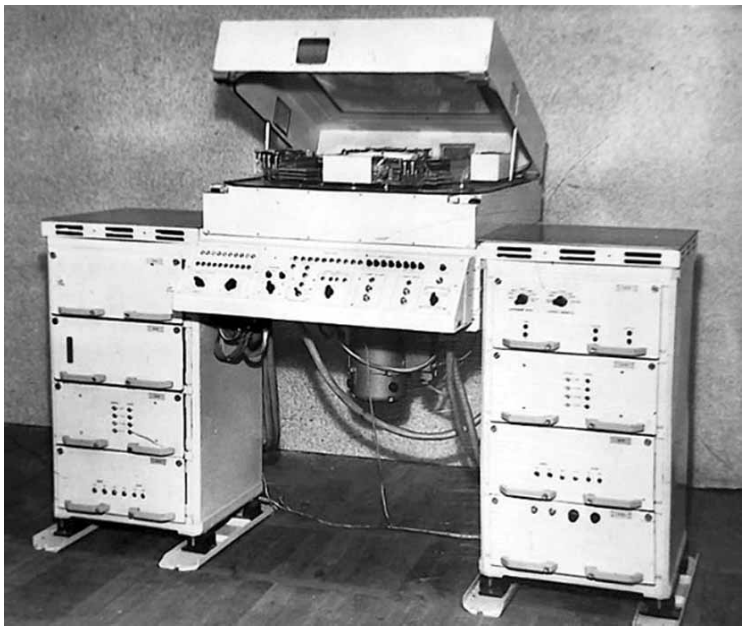
Умови експлуатації: 2 група нормалі НО 005.026/с.

Рік виконання НДДКР-1972-1976, держвипробування: 1979 - 1980р.

Основні технічні характеристики виробу «Широта-1М»:

- кількість каналів - 1;
- частотний діапазон 50 - 1000 кГц;
- швидкість запису/відтворення - 30-40 см/с;
- час запису – 20 с;
- вид запису аналогових сигналів - ЧМ;
- коефіцієнт нелінійних спотворень - 3 %;
- коефіцієнт детонації – 0,03 %;
- керування апаратом дистанційне та місцеве;
- електроживлення – 220 В 50 Гц;
- споживана потужність 1,2 кВА;
- маса – 340 кг;
- габарити 498 х 1400 х 1700 мм;
- потреба – 3 компл. на рік.

В розробці брали участь заступники Головного конструктора: Савчук В.П., з електроніки наскрізного тракту запису-відтворення - с.н.с Спіцин А.М.; по дисковому апарату - Любашенко Л.Т., з технологічної частини - Трухан О.І., з конструкторської частини Муравйов Г.Г.; науковці: к.т.н. Слєпишев І.В., с.н.с. Корнієнко В.А., м.н.с. Ухов С.М., інженерно-технічні робітники: Любченко О.М., Зайцев А.П., Скрипнюк В.В., Баранов-



Виріб «Широта-1»

«Широта-1М»

ський Б.В., Лазарєв В.Д., Іваненко Б.М., Гловацький Є.К., Калюжний О.Д., Межерицький В.А. та інші.

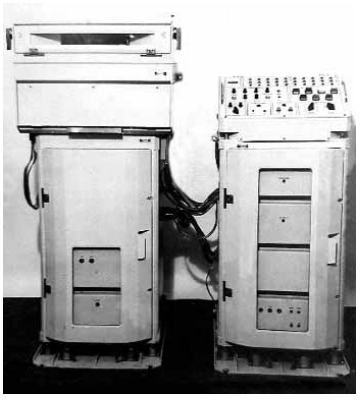
Дослідне виробництво НДІ ЕМП виготовляло зразки виробу під замовлення та постачало Замовнику.

Виріб «МУЗ-6»

Виріб «МУЗ-6» – комплект апаратури широкосмугового запису сигналів з наступним циклічним відтворенням та довготривалим записом сигналограм з наступним циклічним відтворенням для забезпечення аналізу структури короткочасних сигналів радіо та радіотехнічних засобів [1].

Виріб складався з комплекту апаратури, до складу якої входили згідно з рис.1 два вироби: «МУЗ-6Л» на стрічковому магнітному носії інформації шириною 50,8 мм та «МУЗ-6Д» на жорстких магнітних дисках у пакеті типу ЄС-5053(див. вище). Задані до початку створення технічні характеристики обох виробів відображено у таблиці на рис. 1.

Конструктивно виріб «МУЗ-6Л» виконано з трьох суміжних радіоелектронних стійок, на які встановлено вертикальний стрічкопротяжний механізм та пульта дистанційного керування. Конструктивне виконання виробу «МУЗ-6Д» подібне конструктивному виконанню виробу «Широта-1М».



Виріб МУЗ-6 (Л) Виріб МУЗ-6Д

Основні технічні характеристики виробу «МУЗ-6Л»:

- кількість каналів - 3;
- частотний діапазон 0,1 - 6000 кГц;
- швидкість запису/відтворення - 50,8 см/с;
- швидкість перемотування - 7 м/с;
- час запису - 30 хв.;
- вид запису аналогових сигналів - ЧМ/АМ (анал. сигнал/мова);
- коефіцієнт нелінійних спотворень - 5 %;
- коефіцієнт детонації - 0,01 %;
- керування апаратом дистанційне; електроживлення - 220 В 400 Гц;
- споживана потужність 1,5 кВА;
- маса - 850 кг; габарити 2 м³;
- потреба - 14 шт на рік.

В роботі брали участь (до призначення Зволинського В.М. Головними конструкторами були спочатку Мачинський В.К, потім Петровський Б.В.) заступники ГК: Завацький А.Ф., з радіоелектронної частини - Зайцев А.П., по системам забезпечення руху - Векліч В.П., з конструкторської частини - к.т.н. Травніков Є.М., з технологічної частини - Барановський Б.В., потім Трухан А.І.; науковці; с.н.с. Спіцин А.М., м.н.с. Проценко І.Д., інженерно-технічні робітники: Левицький Л.Д., Петровський Б.В., Михалець П.М., Бондаренко В.И., Коліщук В.Т., Томін В.Є., Спичка В.С., Соколовский Ю., Смірнов В., Войтович В.В., Золотар І.Н., Орлова Л., Трипольський Ю.С., Турчин Я.В., Шпаченко В.П., Школяренко В.М., Подоляк Г.Є., Верлинський П.Х., Зволинская Л.М., виробничники Шпента Ю.В., Петренко П.С., Шандрук К.І. та інші.

Основні технічні характеристики виробу «МУЗ-6Д»:

- кількість каналів - 1;
- частотний діапазон 0,1 - 1000 кГц;
- швидкість запису/відтворення - 40 см/с;
- час запису - 20 с.;

Рис.1 Функціональний склад виробу «МУЗ-6»

- вид запису аналогових сигналів - ЧМ;
- коефіцієнт нелінійних спотворень - 5 %;
- коефіцієнт детонації - 0,03 %;
- керування апаратом дистанційне; електроживлення - 220 В 50 Гц;
- споживана потужність 1,2 кВА;
- маса - 340 кг;
- габарити 498 х 1400 х 1700 мм;
- потреба - 14 шт на рік.

В роботі брали участь заступники ГК: Савчук В.П., з електроніки тракту запису-відтворення с.н.с. Спіцин А.М., з радіоелектронної частини - Зайцев А.П; з конструкторської частини - Муравйов Г.Г., з технологічної частини - Барановський Б.В. та Трухан О.І.; науковці: с.н.с. Кульпанович С.П., с.н.с. Фуфаєв П., к.т.н. Травніков Є.М., м.н.с. Проценко І.Д.; інженерно-технічні робітники: Іванов А., Бондаренко В.І., Кощук Г.В., Шпаченко В.П., Золотар І.Н. та інші.

Умови експлуатації: 24 група нормалі НО 005.026/с.

Рік виконання НДДКР-1970-1977, держвипробування: 1978-1979 рр.

Зразки виробу «МУЗ-6» виготовляло дослідне виробництво НДІ ЕМП і постачало Замовнику.

В ході виконання робіт по створенню виробів «Каравелла», «Широта», «МУЗ-6» нач. сектора с.н.с. Спіциним А.М. було підготовлено дисертацію на здобуття наукового ступеня к.т.н. на тему «Дослідження граничних можливостей АМЗ радіосигналів».

Виріб МУЗ-6 встановлювався, зокрема, у м. Севастополь, на кораблі радіоелектронної розвідки (РЕР) «Кильдин» Чорноморського флоту СРСР, закамуфльованому під рибальський сейнер. В пуско-налагоджувальних роботах виробу брали активну участь провідні фахівці НДІ ЕМП – учасники створення виробу, у співробітництві по його технічному обслуговуванню з головним інженером РЕР ЧФ Чеховським А.Г. та іншими фахівцями РЕР.

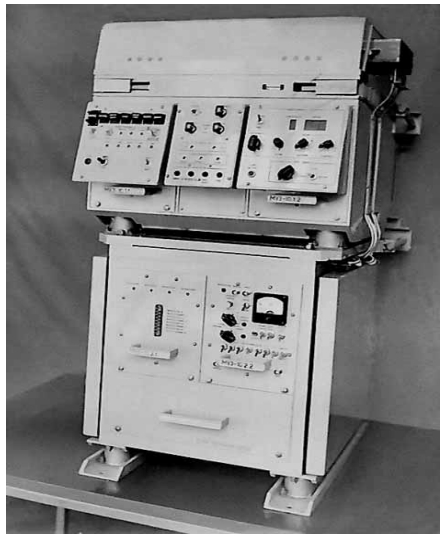
Виріб «МУЗ-10»

Виріб «МУЗ-10» – апаратура для реєстрації аналогових сигналів з метою багатократного циклічного відтворення [1, 6].

Апаратура призначалась для використання на надводних кораблях та підводних човнах, а також опалюваємих кузовах автомобілів (не на ходу) та в стаціонарних приміщеннях в складі комплексів радіорозвідки для досліджень короткочасних процесів, що рідко повторюються, час появи яких невідомий.

Запис сигналів забезпечується чотирма плаваючими головками на 4 поверхнях двох магнітних дисків по спіралеподібним доріжкам двома способами: з високочастотним підмагнічуванням та з частотною модуляцією. Виріб забезпечує наступні режими роботи: «Запис», «Відтворення», «Відтворення циклічне», « Відтворення 1/120», «Відтворення стопове», «Реверс», «Пошук», «Пам'ять». Виріб складається з блока дискового механізму, блока електроніки та блока пульта дистанційного керування, всі блоки розміщені в алюмінієвих корпусах [5].

Дисковий механізм (Рис. 2) обертає дводисковий пакет магнітних дисків з постійною швидкістю і переміщує магнітні головки вздовж радіуса дисків таким чином, щоби доріжка запису уявляла собою спіраль Архімеда з кроком 0,3 мм. Безперервність запису-відтворення забезпечується зворотно-поступальним переміщенням магнітних голівок понад поверхнею магнітних дисків вздовж радіуса. При цьому коли одна каретка з магнітними головками здійснює прямий хід, друга - повертається у вихідне становище, здійснюючи зворотній хід. Магнітні диски обертаються зі швидкістю 3000 об/хв. і при русі магнітних головок вздовж радіуса дисків на їх робочій поверхні утворюється спіралеподібна доріжка запису протягом 2,5 с. Послідовним переключенням запису-відтворення з поверхні на поверхню забезпечується тривалість безперервної сигналограми, яка дорівнює 10 с. Запис відбувається на пакеті ферролакових магнітних дисків (з 2шт.) типу ЕС-5266.



Виріб МУЗ-10

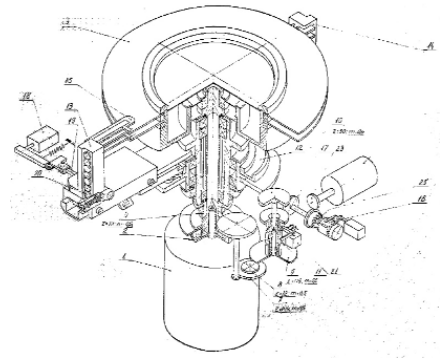


Рис. 2. Кінематична схема дискового механізма

На кінематичній схемі:
1 – електродвигун ДСП-120;
2 - муфта;
3 – пакет дисків з 2-х шт.;
12 – плаский кулачок;
13, 14 - каретки;
15 – блоки магнітних головок;
18 – електромагніт;
22- електродвигун ДСП-10а;

Табл. 2 . Основні технічні характеристики виробів

Технічні характеристики	«Пион-2М»	«Каравелла-РД»	«Каравелла-РЗ»	«Широта-1» «Широта-1М»	«МУЗ-6Л»	«МУЗ-6Д»	«МУЗ-10»
Діапазон записуваних частот, МГц	0,142…0,272	0,03…0,3	0,003…0,2	0,05…0,65	0,1…6	0,1…1	0,001…10
Співвідношення сигнал/шум, дБ	40	40	40	26	24	26	26
Нестабільність частоти відтвореного сигналу					$5x10^{-4}$	$2x10^{-3}$	-
Кількість каналів	2	5	5	1	3	1	1
Час запису/відтворення, с.	10	8	1,4	20	80 хв.	0,33 хв.	10
Габарити, см/дм^3	125x62x134	147x60x64	147x60x64	128x66x77 107x45x77	1,9м^3	1,03 м^3	295 дм^3
Маса, кг	350	250	250	340	850	340	-

Муравйов Г.Г.

Межерицький В.А.

При виробництві було передбачено можливість використання як вітчизняних, так і імпортних магнітних дисків.

Виріб за елементною базою і технічними рішеннями відноситься до IV покоління апаратури магнітного запису. Виріб було створено на заміну описаного вище виробу «МУЗ-6Д».

Основні технічні характеристики виробу відповідали основним характеристикам зарубіжного аналогу MD-600 фірми «Ampex».

Основні технічні характеристики виробу «МУЗ-10»:

- частотний діапазон 0,5 - 5000 кГц (прямий запис);
- нерівномірність АЧХ при прямому запису не більше ± 3 дБ;
- коефіцієнт гармонік при прямому запису не більше 5 %;
- відношення сигнал/завада при прямому запису та ЧМ - запису не менше 26 дБ;
- частотний діапазон 0,1 - 1000 кГц (при ЧМ-запису);
- нерівномірність АЧХ при ЧМ-запису не більше ± 2 дБ;
- коефіцієнт гармонік при ЧМ-запису не більше 3 %;
- коефіцієнт передачі при прямому та ЧМ-запису - 1;
- час запису/відтворення - 10 с;
- коефіцієнт коливання швидкості запису/відтворення - 3 х 10^{-6};
- керування апаратом дистанційне; електроживлення - 220 В 50 Гц;
- споживана потужність 0,4 кВА;
- середній наробіток на відмову не менше 500 год.;
- габарити 295 $дм^3$;
- виріб стійкий при впливі певних синусоїдальних вібрацій (зокрема при синусоїдальній вібрації 25 Гц при прискоренні 19,6 см/с)
- вартість в цінах 1992р. - 810 тис. руб.;
- орієнтовна потреба 2 шт./рік [6, 7].

В роботі брали участь заступники ГК: з комплексних питань - Савчук В.П., з електроніки наскрізного тракту запису-відтворення - Спіцин А.М., по системам авторегулювання і керування виробом - Межерицький В.А., з конструкторської частини - Муравйов Г.Г., з технологічної частини - Корольов В.М.; науковці: с.н.с. Корнієнко В.А., м.н.с. Проценко І.Д.; інженерно-технічні робітники: Михалець П.М., Гловацький Є.К., Векліч В.П., Гоменюк А.К., Зубов О.М., Староватов А.О., Дорошенко Р.Т. та інші.

Умови експлуатації: група 1.7, та 2.1.1 за ГОСТ В 20.39.305-76. Виріб захищений від витоку інформації каналами ПЕМВН пасивними (екранування та фільтрація) та активними засобами (система активного захисту - блок 101А.5) по третій категорії норм ДТК СРСР, роботи забезпечувала Головна науково-дослідна лабораторія з ПД ІТР підприємства (нач. Железняк В.К., Худяков В.О., Гаврильченко В.В.) [8].

Рік виконання НДДКР-1983-1987. Замовник виробу в/ч 30882. За результатами Держвипробувань апаратуру МУЗ-10 було рекомендовано для прийняття на озброєння частин Радянської армії та Військово-Морського флоту. Міжвідомча комісія відбулась у 1987р., виробу присвоєно літеру $О_1$ і його було рекомендовано до серійного виробництва.

Зразки пристрою виготовляло дослідне виробництво НДІ ЕМП і постачало Замовнику.

Варто відмітити, що у всіх вище зазначених виробах використовувались блоки живлення, які розроблялись у підрозділі джерел електроживлення під керівництвом спочатку Моісеєва В.М., а потім Аймбіндера О.М. інженерно-технічними робітниками такими як: Цуренко А., Терещенко В.А., Терещенко М., Тимофеєв С.С., Щур Ю.В., Ковтун С.Л., Безпала І., Полянська О.В., конструкція їх розроблялась конструкторами під керівництвом нач. сектора Воробйова В.М.

Конструкторську документацію на всі вище зазначені вироби оформляла група документації в складі Мухіної Т., Голуб Н., Данілової Л., Жигаленко А., Харченко А.А. під керівництвом Чередніченко А.П.

Насамкінець варто зазначити, що поява АТМЗ на жорстких дисках була зумовлена декілька основними негативними факторами АТМЗ на стрічковому носії. Дискові апарати призначені для використання в якості оперативної пам'яті в системах консервації і збереження інформації; АТМЗ на магнітній стрічці використовуються як засіб тривалого зберігання великих обсягів інформації, при цьому пошук необхідної інформації сильно ускладнений на відміну від дискових апаратів тому, що довжина доріжки запису - відтворення їх набагато менше, ніж у стрічкових апаратів при інших рівних умовах.

При цьому проводити пошук потрібного місця запису на диску можна практично миттєво, а при аналізі інформації доступне ще й циклічне відтворення інформації у реальному масштабі часу. Тому для запису-відтворення короткочасних процесів (у тому числі спортивних) і сигналів переважно використовуються дискові апарати, зокрема для завдань радіорозвідки.

Крім того, конструктивне виконання зазначених виробів ілюструється фото виробів «МУЗ-6Л» та «МУЗ-6Д» та іх масогабаритним характеристиками на користь дискового апарату «МУЗ-6Д», які є значно меншими (табл. 2). Виріб «МУЗ-6» це приклад поєднання складових частин з кінцевою метою оперативного аналізу інформації, яка перехоплювалась засобами радіорозвідки і накопичувалась у виробі «МУЗ-6Л».

(Далі буде)

Олександр Провозін
Заст. Голови правління АТ «НДІ ЕМП»

Література.

1. Річні звіти діяльності та накази по НДІ ЕМП за 1967 – 1987 рр.

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

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

4. Перечень специальной аппаратуры магнитной записи, разработанной (разрабатываемой) и выпускаемой малыми сериями (планируемой к освоению производства) на предприятиях организации п/я Г4965, а также планируемой к освоению производства на предприятиях других министерств. Инв. №10, Киев, 1975г.

5. ОКР «Сульфат-Д». Эскизно-технический проект. Пояснительная записка ЛЩ1 750.059 ПЗ, 1984.

6. МУЗ-10. Технические условия. ЛЩ1 750.059 ТУ, 1986.

7. МУЗ-10. Технико-экономическая характеристика. ЛЩ1 750.059 Д9, 1986.

8. МУЗ-10. Техническое описание. Часть 7. Прибор 101А.5. ЛЩ1.750.059 ТО6, 1986.

9. Бізнес і Безпека, №5, 2024р., стор. 47-53.

10. Бізнес і Безпека, №1, 2020р., стор. 48-54.

КОМПЛЕКТ ЗАСОБІВ ДЛЯ РОЗМІНУВАННЯ ТА ДИСТАНЦІЙНОГО ДЕАКТИВУВАННЯ ПРОТИТАНКОВИХ МІН «КЛЮЧ»

Комплект засобів призначений для розмінування, дистанційного знешкодження (деактивування) та викручування підривників протитанкових мін типу (далі ПТМ) «ТМ-62» та аналогів.

Комплект служить для технічного забезпечення саперів інженерно-саперних підрозділів під час виконання ними робіт по розмінуванню ПТМ «ТМ-62» та аналогів. За допомогою пристроїв та комплектуючих даного комплекту можна виконувати роботи по дистанційному вилученню та перевертанню ПТМ, по переводу підривників з робочого в неробоче положення, викручувати та вкручувати в ПТМ підривники типу «МВЧ» та «МВП», вилучати вкопані ПТМ за допомогою допоміжного важілю дистанційної деактивації мін, дистанційно викручувати підривники типу «МВЧ» та «МВП» з мін, які заходяться в грунті, при цьому виявляючи вибухонебезпечні пастки, які можуть бути встановлені під ПТМ. Паракорд, загальною довжиною 100 м та товщиною 6 мм забезпечує достатню відстань та зусилля, для безпечної роботи саперів. Набір розташований в наплічному рюкзаку, що робить його ефективним при використанні та застосуванні.

Набір розміщений в сумці у вигляді ранцю, має невеликі розміри та мінімальну вагу, що робить його зручним у використанні спеціалістами під час проведення пошукових робіт.

ТЕХНІЧНІ ХАРАКТЕРИСТИКИ

1. Габаритні розміри сумки, мм, не більше . .. . - 550 x 330 x 130
2. Загальна вага, кг, не більше. . . . . .- 6,5

Комплектація:


Дистанційний універсальний викручувач для підривачів типу «МВЧ» та «МВП» з ПТМ . . . . . - 1 шт.


Універсальний спеціальний ключ для підривачів типу «МВЧ» та «МВП» - 1 шт.


Екстрактор - гак для вилучення ПТМ «ТМ-62» зі спорядженням. . . . . - 1 шт.


Гак для вилучення ПТМ «ТМ-62» з грунту. . . . . - 1 шт.


Зачіп-хомут для вилучення ПТМ з підривниками типу «МВП» з грунту - 1 шт.


Зачіп для вилучення ПТМ з підривниками типу «МВЧ» з грунт . . . . . .- 1 шт.


Захват мотузковий . . . . . .- 1 шт.


Універсальний ключ для переводу підривників ПТМ . . . . . .- 1 шт.


Паракорд 6 мм довжиною 50 м з карабіном . . . . . .- 2 шт.


Ласо з паракорду довжиною 1,5 м з карабіном . . . . . .- 5 шт.


Допоміжний важіль для дистанційної деактиваці ПТМ . . . . . .- 1 шт.


Рюкзак спеціальний . . . . . .- 1 шт.

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

Секрет міцності давньоримського бетону

Стародавні римляни були неперевершеними майстрами багато в чому, зокрема — будівництві та інженерії. Найбільш відомими їх витворами можна назвати акведуки — древні водоводи.

Найвищий давньоримський акведук Пондю-Гар, що зберігся.

Ці споруди засновані на унікальному будівельному матеріалі: неймовірно міцному пуцолановому цементі, який надавав спорудам довговічність.

Одна з великих споруд римлян – Пантеон, або «Храм усіх богів», побудований між 118 і 128 роками нашої ери, – збереглася до наших днів і, крім цього, є рекордсменом за величиною купола з неармованого (тобто не укріпленого каркасом) бетону усьому світі.

Купол Пантеону

Незвичайні властивості «римського бетону» зазвичай приписуються його інгредієнтам. По-перше, зазвичай це пуццолан – суміш вулканічного попелу, пемзи та туфу, названа на честь італійського міста Поццуолі, де можна знайти її багате родовище. Другий інгредієнт – вапно. При змішуванні з водою ці два матеріали можуть утворити міцний цемент.

Але це, як виявилось, не вся розгадка. Міжнародна група дослідників на чолі з Массачусетським технологічним інститутом (MIT) виявила, що не тільки матеріали, які використовували римляни, мали унікальні властивості, а й методи їх змішування помітно відрізнялися від сучасних способів створення цементу. Вчені загострили увагу на вкрапленнях вапна, які виявлялися в, начебто, добре перемішаному матеріалі.

«Мене завжди непокоїла думка про те, що присутність цих уламків вапна просто пов'язана з низьким контролем якості. Якщо римляни доклали стільки зусиль для створення видатного будівельного матеріалу, дотримуючись усіх докладних рецептів, які вдосконалювалися протягом багатьох століть, чому вони не подбали про те, щоб перемішати цемент? У цій історії має бути щось більше», – розповів Адмір Масік, провідний автор дослідження з MIT.

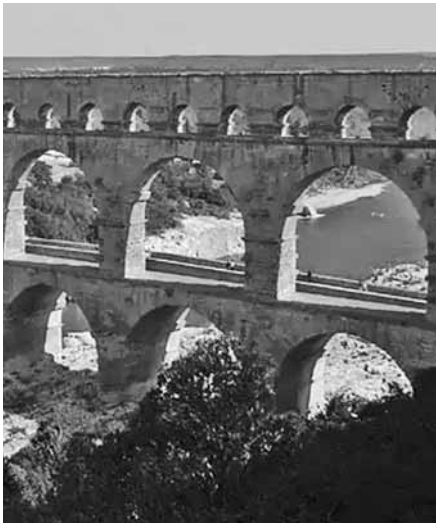
Масик та його команда ретельно вивчили 2000-річні зразки римського бетону з археологічних розкопок Привернум в Італії. Ці зразки були піддані таким тестам як скануюча електронна мікроскопія великої площі, енергодисперсійна рентгенівська спектроскопія, рентгенівська порошкова дифракція та конфокальна раманівська візуалізація.

Гашене вапно вважалося одним з головних інгредієнтів пуцоланового цементу. Вважалося, що вапняк нагрівають при високих температурах для отримання високої концентрації їдкого порошку, званого негашеним вапном, або оксидом кальцію. При змішуванні негашеного вапна з водою виходить гашене вапно, або гідроксид кальцію: трохи менш реактивна і менш їдка паста. Згідно з теорією дослідників, саме це гашене вапно древні римляни змішували з пуццоланом.

Але, згідно з новими висновками, уламки вапна у зразках не відповідають цьому методу. Швидше за все, «римський бетон» виготовляли шляхом змішування негашеного вапна безпосередньо з пуццоланом і водою при надзвичайно високих температурах, окремо або на додаток до гашеного вапна. Цей процес дослідники назвали «гарячим змішуванням», у результаті якого й утворюються уламки вапна.

Як виявилося, такий спосіб має чимало переваг. Наприклад, уламки вапна надають цементу чудової здатності до самовідновлення.

Коли в бетоні утворюються тріщини, вони переміщаються до уламків вапна, які мають більшу площу поверхні, ніж інші частинки в матриці. Коли вода потрапляє в тріщину, вона вступає в реакцію саме з вапном, утворюючи розчин, багатий на кальцій, який висихає і твердне у вигляді карбонату кальцію, склеюючи тріщину і запобігаючи її подальшому поширенню.



Аналогічний процес було помічено біля бетону з гробниці Цецилії Метелли, де тріщини були заповнені кальцитом. Це також може пояснити, чому римський бетон із морських гребель, побудованих 2000 років тому, зберігався цілим протягом тисячоліть, незважаючи на постійний вплив океану.

Вчені підтвердили свої висновки, виготовивши пуцолановий цемент за старовинними та сучасними рецептами з використанням негашеного вапна. Вони також зробили контрольний зразок без негашеного вапна та провели випробування на тріщиноутворення. Справді, бетон, що тріснув, з негашеного вапна повністю «зажив» протягом двох тижнів, але контрольний бетон залишився поцяткований тріщинами.

Наразі команда працює над комерціалізацією свого методу як екологічно чистішої альтернативи існуючим будівельним матеріалам.

mors.in.ua

Німецькі автобани: секрети найкращих доріг світу

Німецькі автобани вважаються одними з найкращих у світі. Їхня якість та довговічність викликає захоплення, особливо у пострадянському просторі. Але які ж технології застосовують німці для їхнього будівництва?

Насправді німецькі автобани роблять із таких же матеріалів, як і в усьому світі: бетону та асфальту. Головною їх особливістю є підкладка, яку розміщують під дорожнім покриттям. Вона може досягати товщини до 2 метрів і складається з кількох шарів будівельних матеріалів.

Перш ніж збудувати дорогу, землерийна техніка видаляє від 1 до 2 метрів ґрунту на її місці. Потім у отриману траншею пошарово укладають «подушку» з гравію, піску та глини (іноді в георешітку), ретельно утрамбовуючи кожен шар. Утворений «шарований пиріг» поливають вапняним розчином або розчином хлориду кальцію, ретельно перемішують, а потім знову утрамбовують.

Завдяки таким маніпуляціям, підкладка здатна постійно утримувати необхідний рівень вологи, що забезпечує дорожнє покриття здатністю не просідати і не «спухати». Лише після цього на створену подушку укладають бетонне або асфальтне покриття. Бетонні дороги додатково покривають спеціальною захисною плівкою, яка запобігає розтріскуванню від сонця та вологи.

Якщо під час укладання асфальту йде дощ, німецькі робітники, на відміну від наших, обов'язково зупиняють роботи та відновлюють їх лише після повного висихання ділянки.

Німецькі дороги будують таким чином, щоб вони не заважали людям, які живуть поруч. Для цього їх покривають спеціальним звукопоглинаючим матеріалом, товщина якого може досягати 10 см.

mors.in.ua

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

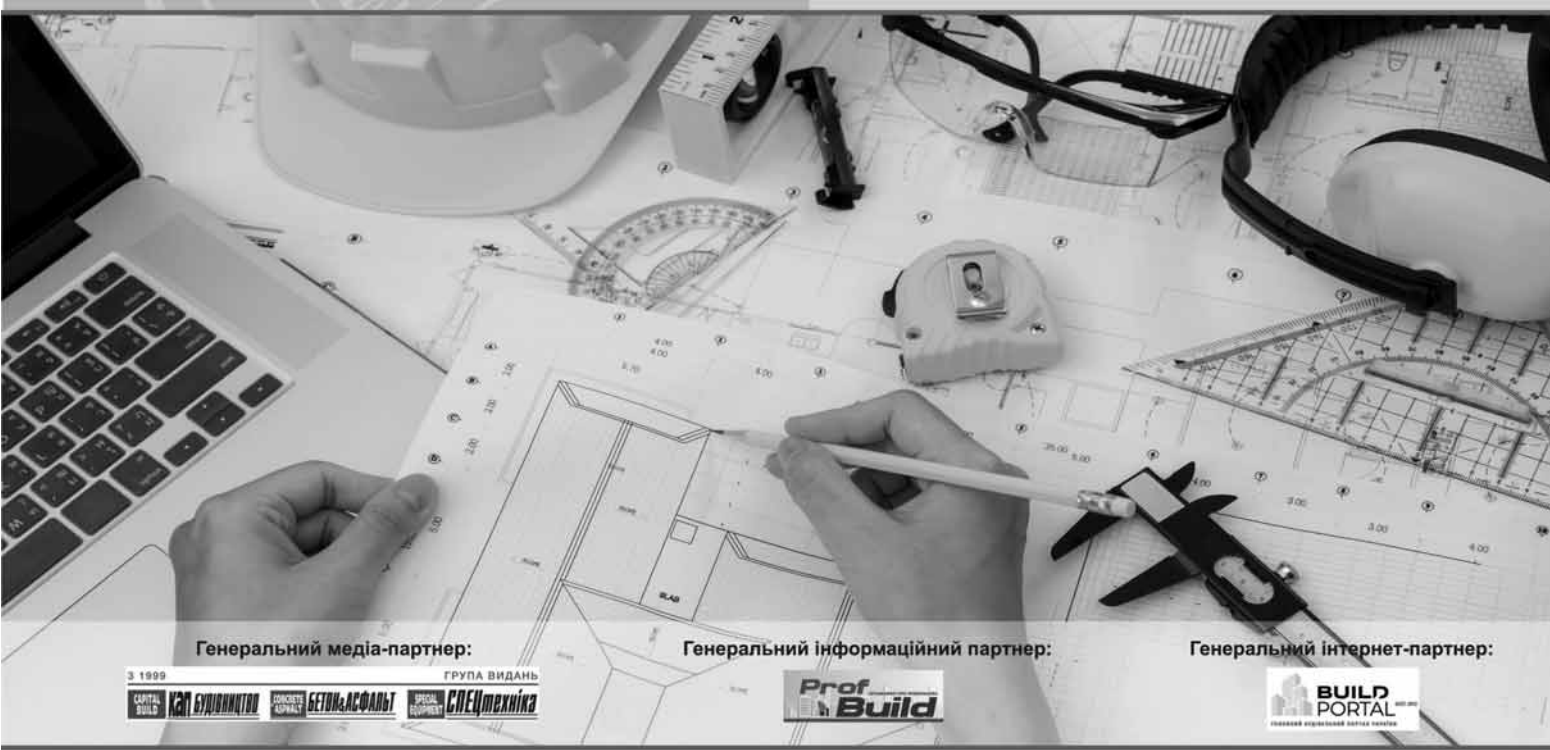
Асоціації малих міст України

Всеукраїнської Асоціації об'єднаних територіальних громад

Національного Експертно-Будівельного Альянсу України

Федерації роботодавців України

14–16 жовтня



Генеральний медіа-партнер:

З 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

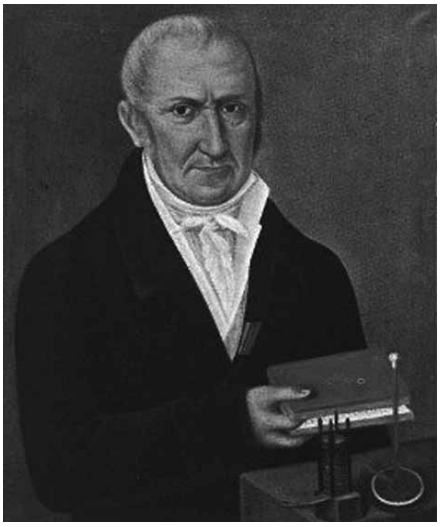
a.nenko@iec-expo.com.ua

www.iec-expo.com.ua

Типи акумуляторних батарей

Акумуляторна батарея – це джерело постійного струму, яке призначене для накопичення та зберігання енергії. Переважна кількість типів акумуляторних батарей заснована на циклічному перетворенні хімічної енергії на електричну, це дозволяє багаторазово заряджати і розряджати батарею. . В основі дії більшості моделей - циклічне перетворення хімічної енергії на електричну, Це забезпечує багаторазовість використання пристрою (цикли заряду-розряду). Для різних умов експлуатації призначено певні види акумуляторів.

Ще в 1800 році Алессандро Вольта зробив разюче відкриття, коли опустив у банку, наповнену кислотою, дві металеві пластини - мідну і цинкову, після чого довів, що по дроту, що з'єднує їх, протікає електричний струм. Більш ніж через 200 років, сучасні акумуляторні батареї продовжують виробляти на основі відкриття Вольта.

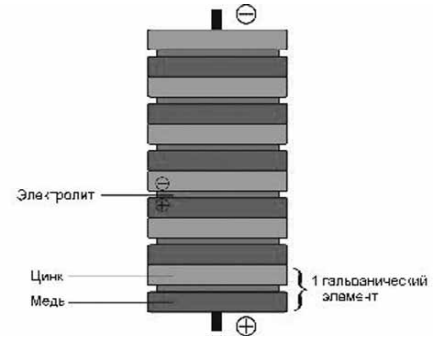


Алессандро Джузеппе Антоніо Анастасіо Вольта

Види акумуляторних батарей

З часу винаходу першого акумулятора минуло не більше 140 років і зараз важко уявити сучасний світ без резервних джерел живлення на основі батарей. Акумулятори застосовуються всюди, починаючи з найнешкідливіших побутових пристроїв: пульти керування, переносні радіоприймачі, ліхтарі, ноутбуки, телефони, і закінчуючи системами безпеки фінансових установ, резервними джерелами живлення для центрів зберігання та передачі даних, космічною галуззю, атомною енергетикою, зв'язком тощо. буд.

Світ, що розвивається, потребує електричної енергії настільки сильно, скільки людині потрібен кисень для життя. Тому конструктори та інженери щодня ведуть роботу з оптимізації наявних типів акумуляторів та періодично розробляють нові види та підвиди.



Стовп Вольта із шести елементів

Таблиця №1. Класифікація акумуляторних батарей.

Тип	Застосування	Позначення	Робоча температура, °С	Напруга елемента,	Питома енергія, Вт ч/кг
Літій-іонний (Літій-полімерний, літій-марганцевий, літій-залізно-сульфідний, літій-залізно-фосфатний, літій-залізо-іттрій-фосфатний, літій-титанатний, літій-хлорний, літій-сірчаний)	Транспорт, телекомунікації, системи сонячної енергії, автономне та резервне електропостачання, Hi-Tech, мобільні джерела живлення, електроінструмент, електромобілі і т.д.	Li-Ion (Li-Co, Li-pol, Li-Mn, LiFeP, LFP, Li-Ti, Li-Cl, Li-S)	-20 … +40	3,2-4,2	280
нікель-сольовий	Автомобільний транспорт, Ж\Д транспорт, Телекомунікації, Енергетика, в тому числі альтернативна, Системи накопичення енергії	Na/NiCl	-50 … +70	2,58	140
нікель-кадмієвий	Електрокари, річкові та морські судна, авіація	Ni-Cd	-50 … +40	1,2-1,35	40 - 80
залізо-нікелевий	Резервне електроживлення, тягові для електротранспорту, ланцюги керування	Ni-Fe	-40 … +46	1,2	100
нікель-водневий	Космос	Ni-H2		1,5	75
нікель-метал-гідридний	електромобілі, дефібрилятори, ракетно-космічна техніка, системи автономного енергопостачання, радіоапаратура, освітлювальна техніка.	Ni-MH	-60 … +55	1,2-1,25	60 – 72
нікель-цинковий	Фотоапарати	Ni-Zn	-30 … +40	1,65	60
свинцево-кислотний	Системи резервного харчування, побутова техніка, ДБЖ, альтернативні джерела живлення, транспорт, промисловість та ін.	Pb	-40 … +40	2, 11-2,17	30 - 60
срібно-цинковий	Військова сфера	Ag-Zn	-40 … +50	1,85	<150
срібно-кадмієвий	Космос, зв'язок, військові технології	Ag-Cd	-30 … +50	1,6	45 – 90
цинк-бромний		Zn-Br		1,82	70 - 145
цинк-хлорний		Zn-Cl	-20 … +30	1,98-2,2	160 – 250

Виходячи з наведених даних у таблиці №1, можна дійти висновку, що існує досить багато видів акумуляторів, відмінних за своїми характеристиками, які оптимізовані для застосування у різноманітних умовах та з різною інтенсивністю. Застосовуючи для виробництва нові технології та компоненти, вченим вдається досягати необхідних показників для конкретної галузі застосування, наприклад, для космічних супутників, космічних станцій та іншого космічного обладнання розробили нікель-водневі акумулятори. Звичайно, в таблиці наведено далеко не всі типи, а лише основні, які набули поширення.

АКБ відрізняються характеристиками, адаптованими для використання з необхідною інтенсивністю і в різних умовах. Найбільш поширені пристрої:

Свинцево-кислотні. Завдяки простій технології виготовлення відрізняються доступною ціною. Переваги: надійність, просте обслуговування, мінімальна саморозрядність. Бувають чотири типи: стаціонарні – для енергетичного обладнання, портативні – для електроінструментів, тягові – для електромобілів, Стартерні – для авто.

Літій-іонні. Відмінні риси: малі габарити, високий ресурс та можливість добре працювати при низькій температурі. Підходять для інтенсивної експлуатації, виносять часті цикли розряджання-заряджання. Літій-іонний акумулятор – оптимальний вибір для техніки, яка використовується регулярно та часто, наприклад, смартфонів, ноутбуків будівельних інструментів.

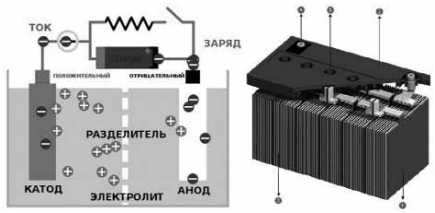
Нікель-кадмієві. Здатні функціонувати у широкому діапазоні температур, витримують велику кількість циклів заряду та розряду, підтримують швидку зарядку. Найбільш ефективні за періодичного використання. Встановлюються в електрокари, морські та річкові судна, трамваї, тролейбуси тощо.

Нікель-залізні.

Сучасні системи резервного та автономного електроживлення для промислового та побутового сегмента засновані на різновидах свинцево-кислотних, нікель-кадмієвих (рідше застосовуються залізо-нікелевий тип) та літій-іонних акумуляторах, оскільки ці хімічні джерела живлення безпечні та мають прийнятні технічні характеристики та вартість.

Свинцево-кислотні акумуляторні батареї

Цей тип є найбільш затребуваним у сучасному світі через універсальні особливості та невисоку вартість. Завдяки наявності великої кількості різновидів, свинцево-кислотні акумулятори застосовується в областях систем резервного живлення, системах автономного електропостачання, сонячних електростанцій, ДБЖ, різних видах транспорту, зв'язку, системах безпеки, різних видах портативних пристроїв, іграшках і т.д.



Електрохімічна схема свинцево-кислотного акумулятора (VRLA)

Принцип дії свинцево-кислотних батарей

Основа роботи хімічних джерел живлення заснована на взаємодії металів та рідини – оборотної реакції, що виникає при замиканні контактів позитивних та негативних пластин. Свинцево-кислотні акумулятори, як відомо з назви, складаються із свинцю та кислоти, де позитивно зарядженими пластинами є свинець, а негативно зарядженими – оксид свинцю. Якщо підключити до двох пластин лампочку, ланцюг замкнеться і виникне електричний струм (рух електронів), а всередині елемента виникне хімічна реакція. Зокрема відбувається корозія пластин батареї, свинець покривається сульфатом свинцю. Таким чином, у процесі розряду акумулятора на всіх пластинах утворюватиметься наліт із сульфату свинцю. Коли акумулятор повністю розряджений, його пластини покриті однаковим металом - сульфатом свинцю і мають практично однаковий заряд щодо рідини, відповідно, напруга батареї буде дуже низька.

Якщо до батареї підключити зарядний пристрій до відповідних клем і включити його, струм протікатиме в кислоті у зворотному напрямку. Струм викликатиме хімічну реакцію, молекули кислоти – розщеплюватись і за рахунок цієї реакції відбуватиметься видалення сульфату свинцю з позитивних та негативних пластилін батареї. У фінальній стадії зарядного процесу пластини матимуть первозданний вигляд: свинець та оксид свинцю, що дозволить їм знову отримати різний заряд, тобто батарея буде повністю заряджена.

Однак на практиці все виглядає трохи інакше і пластини електродів очищаються не повністю, тому акумулятори мають певний ресурс, по досягненні якого знижується ємність до 80-70% від початкової.

Типи свинцево-кислотних батарей

Lead-Acid, що обслуговуються - 6, 12В батареї. Класичні стартерні акумулятори для двигунів внутрішнього згоряння та не тільки. Потребують регулярного обслуговування та вентиляції. Схильні до високого саморозряду.

Valve Regulated Lead-Acid (VRLA), що не обслуговуються - 2, 4, 6 і 12В батареї. Недорогі акумулятори в герметизованому корпусі, які можна використовувати у житлових приміщеннях, не потребують додаткової вентиляції та обслуговування. Рекомендовані для використання у буферному режимі.

Absorbent Glass Mat Valve Regulated Lead-Acid (AGM VRLA), які не обслуговуються - 4, 6 і 12В батареї. Сучасні акумулятори свинцево-кислотного типу з абсорбованим електролітом (не рідкий) та скловолоконними роздільними сепараторами, які значно краще зберігають свинцеві пластини, не даючи їм руйнуватися. Таке рішення дозволило значно знизити час заряду батарей AGM, оскільки зарядний струм може досягати 20-25, рідше 30% від номінальної ємності.

Акумулятори AGM VRLA мають безліч модифікацій з оптимізованими характеристиками для циклічного та буферного режимів роботи: Deep – для частих глибоких розрядів, фронт-термінальні – для зручного розташування в телекомунікаційних стійках, Standard – загального призначення, High Rate – забезпечують кращу розрядну характеристику до 30% підходять для потужних джерел безперебійного живлення, Modular – дозволяють створювати потужні батарейні кабінети тощо.

Малюнок №4. AGM VRLA акумулятори EverExceed.

GEL Valve Regulated Lead-Acid (GEL VRLA), що не обслуговуються - 2, 4, 6 і 12В батареї. Одна із останніх модифікацій свинцево-кислотного типу акумуляторів. Технологія заснована на застосування гелеподібного електроліту, який забезпечує максимальний контакт з негативними та позитивними пластинами елементів та зберігає одноманітну консистенцію по всьому об'єму. Даний тип акумуляторів вимагає «правильного» зарядного пристрою, який забезпечить необхідний рівень струму та напруги, лише в цьому випадку можна отримати всі переваги порівняно з типом AGM VRLA.

Хімічні джерела живлення GEL VRLA, як і AGM, мають безліч підвидів, які найкраще підходять для певних режимів роботи. Найпоширенішими є серії Solar – використовуються для систем

Малюнок №5. GEL VRLA акумулятор EverExceed.

сонячної енергії, Marine – для морського та річкового транспорту, Deep Cycle – для частих глибоких розрядів, фронтермінальні – зібрані у спеціальних корпусах для телекомунікаційних систем, GOLF – для гольф-карів, а також для підлогомийних машин, Micro - невеликі акумулятори для частого використання в мобільних додатках, Modular - спеціальне рішення щодо створення потужних акумуляторних банків для накопичення енергії і т.д.

GEL-батареї різняться за призначенням. Наприклад:

- Solar — для сонячних панелей;
- Golf — для гольф-карів та підлогомийного обладнання;
- Micro — для мобільних систем;
- Marine — для річкових та морських транспортних засобів.

Також вони широко застосовуються у телекомунікаціях, системах вуличного освітлення та автономного електропостачання, у промисловості, що займається виробництвом обладнання.

OPzV, що не обслуговуються - 2В батареї. Спеціальні свинцево-кислотні елементи типу OPZV виготовлені із застосуванням трубчастих пластин анода та сірчанокислотним гелеподібним електролітом. Анод та катод елементів містять додатковий метал – кальцій, завдяки якому підвищується стійкість електродів до корозії та збільшується термін служби. Негативні пластини – намазні, ця технологія забезпечує найкращий контакт із електролітом.

Акумулятори OPzV стійкі до глибоких розрядів і мають тривалий термін служби до 22 років. Як правило, для виготовлення подібних елементів живлення застосовують лише кращі матеріали, щоб забезпечити високу ефективність роботи в циклічному режимі.

Застосування OPzV акумуляторів затребуване в телекомунікаційних установках, системах аварійного освітлення, джерелах безперебійного живлення, системах навігації, побутових та промислових системах накопичення енергії та сонячниої електрогенерації.

OPzS, малообслуговуються - 2, 6, 12В батареї. Стаціонарні заливні свинцево-кислотні акумулятори OPzS виготовляються із трубчастими пластинами анода з додаванням сурми. Катод також містить невелику кількість сурми і являє собою намазний ґратчастий тип. Анод і катод розділені мікропористими сепараторами, які запобігають короткому замиканню. Корпус акумуляторів виконаний із спеціального ударостійкого, стійкого до хімічного впливу та вогню прозорого пластику, а вентильовані клапани відносяться до пожежобезпечного типу та забезпечують захист від можливого попадання полум'я та іскор.

Прозорі стінки дозволяють зручно контролювати рівень електроліту за допомогою позначок мінімального та максимального значення. Спеціальна структура клапанів дає можливість без їх зняття доливати дистильовану воду та вимірювати щільність електроліту. Залежно від навантаження, доливання води здійснюється раз на один – два роки.

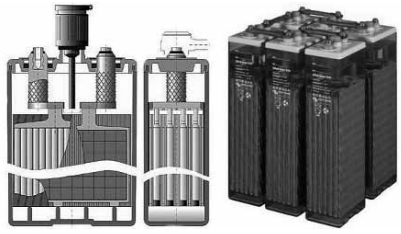
Акумуляторні батареї типу OPzS мають найвищі характеристики серед усіх інших видів свинцево-кислотних батарей. Термін служби може досягати 20 – 25 років та забезпечувати ресурс до 1800 циклів глибокого 80% розряду.

Застосування таких батарей необхідно в системах з вимогами середнього та глибокого розряду, в т.ч. де спостерігаються пускові струми середньої величини.

Такі моделі купують для живлення:

- сигналізацій;
- комп'ютерного обладнання;
- аварійного освітлення;
- телекомунікаційного обладнання;
- систем моніторингу та контролю на розподільчих та електростанціях, в аеропортах тощо.

Малюнок №6. Будова OPzV акумулятора EverExceed.



Малюнок №7. OPzS акумулятор Victron Energy.

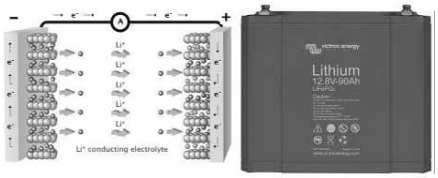
Характеристики свинцево-кислотних акумуляторів

Аналізуючи наведені в таблиці №2 дані, можна дійти висновку, що свинцево-кислотні акумулятори мають широкий вибір моделей, які підходять для різних режимів роботи та умов експлуатації.

Для аналізу використовувалися середні дані більш ніж 10 виробників батарей, продукція яких представлена на ринку України протягом тривалого часу і успішно застосовується в багатьох областях (EverExceed, BB Battery, CSB, Leoch, Ventura, Challenger, C&D Techologies, Victron Energy, SunLight, Troian та інші).

Літій-іонні (літієві) акумуляторні батареї

Історія виникнення цього типу акумуляторів йде з 1912 р, коли Гілберт Ньютон Льюїс працював над обчисленням активностей іонів сильних електролітів і проводив дослідження електродних потенціалів цілого ряду елементів, включаючи літій. З 1973 року роботи було відновлено і в результаті з'явилися перші елементи живлення на основі літію, які забезпечували лише один цикл розряду.



Малюнок №8. Електрохімічна схема літій-іонного акумулятора.

Таблиця №2. Порівняльні характеристики за видами свинцево-кислотних батарей

Тип	LA	VRLA	AGM VRLA	GEL VRLA	OPzV	OPzS
Місткість, Ампер/година	10 – 300	1 – 300	1 – 3000	1 – 3000	50 – 3500	50 – 3500
Напруга, Вольт	6, 12	4, 6, 12	2, 4, 6, 12	2, 6, 12	2	2
Оптимальна глибина розряду, %		30	<40	<50	<60	<60
Допустима глибина розряду, %		<75	<80	<90	<90	<100
Циклічний ресурс, DOD = 50%		<250-300	<1000	<1400	<3200	<3300
Оптимальна температура, °С	0 … +45	+15 … +25	+10 … +25	+10 … +25	0 … +30	0 … +30
Діапазон робочих температур, °С	-50 … +70	-35 … +60	-40 … +70	-40 … +70	-40 … +70	-40 … +70
Термін служби, років при +20 ° С	<7	<7	5 – 15	8 – 15	15 – 20	17 – 25
Саморозряд, %	3 – 5	2 – 3	1 – 2	1 – 2	1 – 2	1 – 2
Макс. струм заряду, % від ємності	10 – 20	20 - 25	20 – 30	15 – 20	15 – 20	10 - 15
Мінімальний час заряду, год	8 – 12	6 – 10	6 – 10	8 – 12	10 - 14	10 - 15
Вимоги до обслуговування	3 - 6 міс.	ні	ні	ні	ні	1 – 2 роки
Середня вартість, $, 12В/100Ач.	70 - 150	200 – 250	250 – 380	350 – 500	1000 – 1400	1500 – 3500

Спроби створити літієвий акумулятор ускладнювалися надактивними властивостями літію, які при неправильних режимах розряду або заряду викликали бурхливу реакцію з виділенням високої температури і навіть загорянням. Компанія Sony випустила перші мобільні телефони з подібними акумуляторами, але змушена була відкликати продукцію назад після кількох неприємних інцидентів. Розробки не припинялися і в 1992 з'явилися перші «безпечні» акумулятори на основі іонів літію.

Акумулятори літій-іонного типу мають високу щільність енергії і завдяки цьому при компактному розмірі та легкій вазі забезпечують у 2-4 рази більшу ємність порівняно зі свинцево-кислотними акумуляторами. Безперечно, великою перевагою літій-іонних батарей є висока швидкість повної 100% перезаряджання протягом 1-2 годин.

Li-ion батареї набули широкого застосування в сучасній електронній техніці, автомобілебудуванні, системах накопичення енергії, сонячної генерації електроенергії. Вкрай потрібні у високотехнологічних пристроях мультимедіа та зв'язку: телефонах, планшетних комп'ютерах, ноутбуках, радіостанціях і т. д. Сучасний світ складно уявити без джерел живлення літій-іонного типу.

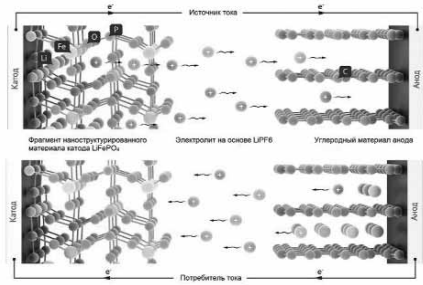
Принцип дії літієвих (літій-іонних) батарей

Принцип роботи полягає у використанні іонів літію, пов'язаних молекулами додаткових металів. Зазвичай, на додаток до літію застосовуються літійкобальтоксид та графіт. При розряді літій-іонного акумулятора відбувається перехід іонів від негативного електрода (катода) до позитивного (аноду) і при заряді. Схема акумулятора передбачає наявність роздільного сепаратора між двома частинами елемента, це необхідно для запобігання мимовільному переміщенню іонів літію. Коли ланцюг акумулятора замкнутий і відбувається процес заряду або розряду, іони долають розділовий сепаратор, прагнучи протилежно зарядженого електрода.

Завдяки своїй високій ефективності, літій-іонні акумулятори отримали бурхливий розвиток та безліч підвидів, наприклад, літій-залізо-фосфатні акумулятори (LiFePO4). Нижче наведено графічну схему роботи цього підтипу.

Літієві джерела живлення чутливі до перезаряду. Надмірний заряд призводить до нагромадження металевого літію на поверхні анода. Цей осад може розпочинати реакцію з електролітом. При цьому на катоді починає активно виділятися кисень, про що свідчить інтенсивне нагрівання, підвищення тиску та розгерметизація АКБ.

Заряджання приладів проходить у два етапи. Перший - здійснюється при стабільному струмі 0,2С-1С до напруги 4,2, займає приблизно 40 хвилин. Другий - виконується при незмінному напрузі. Заряджання завершується, коли зарядний струм знижується до значення, що становить 3% від номінального. Щоб літієва батарея прослужила довго, необхідно заряджати струмом, що становить 50% від ємності (0,5С).



Малюнок №9. Електрохімічна схема процесу розряду та розряду LiFePO4 батареї.

Згодом АКБ Li-ion «старіють», усередині накопичуються продукти окислення, втрачається частина ємності. Життєвий цикл акумулятора завершується, коли він втрачає 30% вихідної ємності. Ресурс моделей у середньому становить 1000 зарядів та розрядів. Щоб продовжити термін експлуатації, рекомендується не перевищувати оптимальний струм заряду (50% номінальної ємності пристрою). Наприклад, ідеальний струм заряду для батареї на 20 мАг - 10С. Також важливо уникати глибокого розряду та перезаряду АКБ, виключити переохолодження та перегрів, не зберігати розрядженим протягом тривалого часу.

Типи літій-іонних акумуляторів

Сучасні літій-іонні акумулятори мають багато підтипів, основна різниця яких полягає у складі катода (негативно зарядженого електрода). Також може змінюватися склад анода для заміни графіту або використання графіту з додаванням інших матеріалів.

Різні види літій-іонних акумуляторів позначаються за їх хімічним розкладанням. Для рядового користувача це може бути складно, тому кожен тип буде описаний максимально докладно, включаючи його повну назву, хімічне визначення, абревіатуру і коротке позначення. Для зручності опису використовуватиметься скорочена назва.

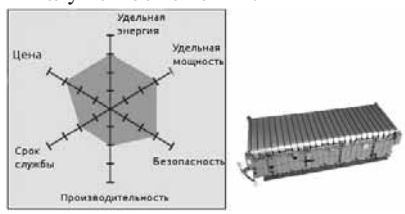
Літій кобальт оксид (LiCoO2) – Має високу питому енергію, що робить літій-кобальтовий акумулятор затребуваним у компактних високотехнологічних пристроях. Катод батареї складається з оксиду кобальту, а анод – з графіту. Катод має шарувату структуру і під час розряду іони літію переміщуються від анода до катода. Недоліком цього є відносно короткий термін служби, невисока термічна стабільність і лімітована потужність елемента.

Малюнок №10. Діаграма основних властивостей акумуляторів $LiCoO_2$.

Літій-кобальтові батареї не можуть розряджатися і заряджатися струмом, що перевищує номінальну ємність, тому акумулятор із ємністю 2,4Ач може працювати зі струмом 2,4А. Якщо для заряду застосовуватиметься велика сила струму, це викличе перегрів. Оптимальний зарядний струм становить 0,8 ˚ С, у цьому випадку 1,92 А. Кожен літій-кобальтовий акумулятор комплектується схемою захисту, яка обмежує заряд та швидкість розряду та лімітує струм на рівні 1С.

На графіці (Рис. 10) відображені основні властивості літій-кобальтових акумуляторів з точки зору питомої енергії або потужності, питома потужність або здатність забезпечувати високий струм, безпеки або шанси займання при високому навантаженні, робоча температура довкілля, термін служби та циклічний ресурс, вартість .

Літій Оксид Марганця ($LiMn_2O_4$, LMO) – перша інформація про використання літію з марганцевими шпинелями була опублікована у наукових доповідях 1983 року. Компанія Moli Energy у 1996 році випустила перші партії акумуляторів на основі літій-оксид-марганцю як матеріал катода. Така архітектура формує тривимірні структури шпинелі, що покращує потік іонів до електрода, тим самим знижуючи внутрішній опір та підвищуючи можливі струми заряду. Також перевага шпинелі у термічній стабільності та підвищеній безпеці, проте циклічний ресурс та термін служби обмежений.



Малюнок №11. Діаграма основних властивостей акумуляторів $LiMn_2O_4$.

Низький опір забезпечує можливість швидкого заряду та розряду літій-марганцевого акумулятора з високим струмом до 30А та короткочасно до 50А. Застосовується для потужних електроінструментів, медичного обладнання, а також гібридних та електричних транспортних засобів.

Потенціал літій-марганцевих акумуляторів приблизно на 30% нижче порівняно з літій-кобальтовими батареями, проте ця технологія має приблизно на 50% кращі властивості, ніж акумулятори на основі нікелевих хімічних компонентів.

Гнучкість конструкції дозволяє інженерам оптимізувати властивості батареї та досягти тривалого терміну служби, високої ємності (питома енергія), можливості забезпечувати максимальний струм (питома потужність). Наприклад,

з тривалим терміном експлуатації типорозмір елемента 18650 має ємність 1,1Ач, тоді як елементи, оптимізовані на підвищену ємність - 1,5Ач, але при цьому вони мають менший термін служби.

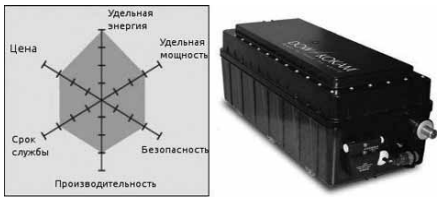
На графіці (Рис. 12) відображені не найвражаючі характеристики літій-марганцевих акумуляторів, проте сучасні розробки дозволили суттєво підвищити експлуатаційні характеристики та зробити цей тип конкурентним та широко застосовуваним.

Сучасні акумулятори літій-марганцевого типу можуть вироблятися з додаваннями інших елементів – літій-нікель-марганець-кобальт оксид (NMC), подібна технологія суттєво продовжує термін служби та підвищує показники питомої енергії. Цей склад привносить кращі властивості кожної системи, так звані LMO (NMC) застосовуються для більшості електромобілів, таких як Nissan, Chevrolet, BMW і т.д.

Літій-Нікель-Марганець-Кобальт оксид (LiNiMnCoO2 або NMC) – провідні виробники літій-іонних батарей зосередилися на поєднанні нікелю-марганцю-кобальту як матеріали катоду (NMC). Подібний до літій-марганцевого типу, ці акумулятори можуть бути адаптовані для досягнення показників високої питомої енергії або високої питомої потужності, однак, не одночасно. Наприклад, елемент NMC типу 18650 може помірної навантаження має ємність 2,8Ач і може забезпечити максимальний струм 4-5А; NMC елемент, оптимізований до параметрів підвищеної потужності, має лише 2Втч, але може забезпечити безперервний струм розряду до 20А. Особливість NMC полягає в поєднанні нікелю та марганцю, як приклад можна навести кухонну сіль, в якій основні інгредієнти натрій та хлорид, які окремо є токсичними речовинами.

Нікель відомий своєю високою питомою енергією, але низькою стабільністю. Марганець має перевагу формування структури шпинелі і забезпечує низький внутрішній опір, але при цьому має низьку питому енергію. Комбінуючи ці два метали, можна отримувати оптимальні характеристики NMC акумулятора для різних режимів експлуатації.

NMC акумулятори чудово підходять для електроінструменту, електровелосипедів та інших силових агрегатів. Поєднання матеріалів катода: третина нікелю, марганцю та кобальту забезпечують унікальні властивості, а також знижують вартість продукту у зв'язку із зменшенням вмісту кобальту. Інші підтипи, як NCM, CMN, CNM, MNC та MCN



Малюнок №12. Діаграма основних властивостей акумуляторів $LiNiMnCoO_2$.

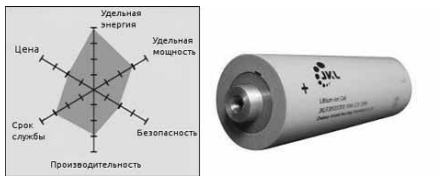
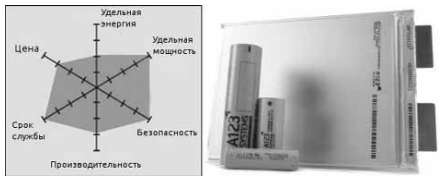


Рисунок №14. Діаграма основних властивостей акумуляторів LiNiCoAlO2.

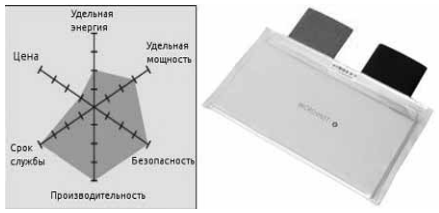
мають відмінне співвідношення трійки металів від 1/3-1/3-1/3. Зазвичай, точне співвідношення тримається виробником у секреті.

Літій-Залізо-Фосфатні (LiFePO4) – у 1996 році в університеті штату Техас (та іншими учасниками) був застосований фосфат як катодний матеріал для літієвих акумуляторів. Літій-фосфат пропонує хороші електрохімічні характеристики із низьким опором. Це стало можливим із нано-фосфатом матеріалу катода. Основними перевагами є високий струм, що протікає, і тривалий термін служби до того ж, хороша термічна стабільність і підвищена безпека.

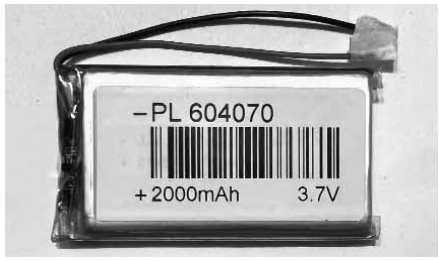


Малюнок №13. Діаграма основних властивостей акумуляторів LiFePO4.

Літій-залізо-фосфатні акумулятори терпимо до повного розряду і менш схильні до «старіння», ніж інші літій-іонні системи. Також LFP більш стійкі до перезаряду, але, як і в інших акумуляторах літій-іонного типу, перезаряд може спричинити пошкодження. LiFePO4 забезпечує дуже стабільну напругу розряду – 3,2В, це дозволяє використовувати всього 4 елементи для створення батареї стандарту 12В, що в свою чергу дозволяє ефективно замінювати свинцево-кислотні батареї. Літій-залізо-фосфатні акумулятори не містять кобальту, це суттєво знижує вартість продукту і робить його більш екологічно чистим. У процесі розряду забезпечує високий струм, а також може бути заряджений номінальним струмом за одну годину до повної ємності. Експлуатація при низьких температурах навколишнього середовища знижує продуктивність, а температура понад 35 °С – дещо скорочує термін служби, але показники набагато кращі, ніж у свинцево-кислотних, нікель-кадмієвих або ні-



Малюнок №15. Діаграма основних властивостей акумуляторів Li4Ti5O12.



Малюнок №16. Зовнішній вигляд Li-Polymer акумулятора.

кель-металогідридних акумуляторів. Літій-фосфат має більший саморозряд, ніж інші літій-іонні акумулятори, що спричиняє потребу балансування батарейних блоків.

Літій-Нікель-Кобальт-Оксид Алюмінію ($LiNiCoAlO_2$) – літій-нікель-кобальто-оксид алюмінієві батареї (NCA) з'явилися в 1999 році. Цей тип забезпечує високу питому енергію та достатню питому потужність, а також тривалий термін служби. Однак існують ризики займання, внаслідок чого було додано алюміній, який забезпечує більш високу стабільність електрохімічних процесів, що протікають в акумуляторі при високих струмах розряду та заряду.

Літій-титанат (Li4Ti5O12) – акумулятори з анодами з літій-титанату були відомі з 1980-х років. Катод складається з графіту і має подібність до архітектури типової літій-металевої батареї. Літій-титанат має напругу елемента 2,4В, може бути швидко заряджений і забезпечує високий розрядний струм 10С, який у 10 разів перевищує номінальну ємність батареї.

Літій-титанатні акумулятори відрізняються підвищеним циклічним ресурсом у порівнянні з іншими Li-ion видами батарей. Мають високу безпеку, а також здатні працювати за низьких температур (до - 30 °С) без відчутного зниження робочих характеристик.

Недолік полягає у досить високій вартості, а також у невеликому показнику питомої енергії, близько 60-80Втч/кг, що цілком можна порівняти з нікель-кадмієвими акумуляторами. Області застосування: електричні силові агрегати та джерела безперебійного живлення.

Літій-полімерні акумулятори (Li-pol, Li-polymer, LiPo, LIP, Li-poly) – літій-полімерні акумулятори відрізняються від літій-іонних тим, що в них використовується спеціальний полімерний електроліт. Ажиотаж, що виник до цього виду батарей з 2000-х років, триває до сьогодні. Заснований не безпідставно, т.е. до. за допомогою спеціальних полімерів вдалося створити батарею без рідкого або гелеподібного електроліту, це дає можливість створювати батареї практично будь-якої форми. Але основна проблема полягає в тому, що полімерний твердий електроліт забезпечує погану провідність при кімнатній температурі, а кращі властивості демонтує в розігрітому стані до 60°С. Усі спроби

Таблиця №3. Характеристики літій-іонних акумуляторів

Параметр \ Тип	LiCoO2	LiMn2O4	LiNiMnCoO2	LiFePO4	LiNiCoAlO2	Li4Ti5O12
Напруга елемента, Вольт;	3.6	3.7	3.6-3.7	3.2	3.6	2.4
Оптимальна глибина розряду, %;	85-90	85-90	85-90	85-90	85-90	85-90
Допустима глибина розряду, %;	100	100	100	100	100	100
Циклічний ресурс, DOD = 80%;	700 – 1000	1000 – 2000	1000 – 2000	1000 – 2000	1000 – 2000	5000 – 8000
Оптимальна температура, °З;	+20...+30	+20...+30	+20...+30	+20...+30	+20...+30	+20...+30
Діапазон робочих температур, ° С;	-10 ... +60	-10 ... +45	-10 ... +55	-10 ... +60	-10 ... +55	-10 ... +45
Термін служби, років при +20 ° С;	5 – 7	10	10	20 - 25	20 - 25	18 - 25
Саморозряд у міс., %	1 – 2	1 – 2	1 – 2	1 – 2	1 – 2	1 – 2
Макс. струм розряду	1С	10С/30С 5с	2С	25 - 30С	1С	10С/30С 5с
Макс. струм заряду	0,7-1С	0,7-1С	0,7-1С	1С	0,7С	1С
Мінімальний час заряду, год	2 - 3	2 - 2.5	2 - 3	2 - 3	2 - 3	2 - 3
Вимоги до обслуговування	ні	ні	ні	ні	ні	ні
Рівень вартості	високий	середній	середній	низький	середній	високий

вчених виявити вирішення цього завдання марні.

У сучасних літій-полімерних батареях застосовується невелика кількість гелевого електроліту для кращої провідності за нормальної температури. А принцип роботи побудовано одному з описаних вище типів. Найпоширенішим є літій-кобальтовий тип із полімерним гелеподібним електролітом, який застосовується в більшості випадків.

Основна різниця між літій-іонними акумуляторами та літій-полімерними полягає в тому, що мікропористий полімерний електроліт замінюється на традиційний розділовий сепаратор. Літій-полімер має трохи більший показник питомої енергії і дає можливість створювати тонкі елементи, але ціна на 10-30% вища, ніж літій-іонна. Істотна різниця є і у структурі корпусу. Якщо для літій-полімерних застосовується тонка фольга, яка дає можливість створювати настільки тонкі елементи живлення, що вони схожі на кредитні картки, то літій-іонні збираються в жорсткому металевому корпусі для фіксації електродів.

Характеристики літій-іонних акумуляторів

У таблиці відсутня максимальна ємність елементів. до. технологія літій-іонних акумуляторів не дозволяє виробляти потужні окремі елементи. Коли необхідна висока ємність або постійний струм, батареї з'єднаються паралельно та послідовно за допомогою перемичок. Стан обов'язково має контролювати система батарейного моніторингу. Сучасні батареї для ДБЖ і сонячних електростанцій на основі літієвих елементів можуть досягати напруги 500-700В постійного струму з ємністю близько 400А/год, а також ємності 2000 - 3000Ач з напругою 48 або 96В.

Нікель-кадмієві акумуляторні батареї

Винахідником є шведський вчений Вальдемар Юнгнер, який запатентував технологію виробництва нікель кадмієвого типу у 1899 році. D 1990 виникла патентна суперечка з Едісоном, який Юнгнер програв через те, що не володів такими засобами, як його опонент. Компанія «Ackumulator Aktiebolaget Jungner», заснована Вальдемаром, опинилася на межі банкрутства, проте, змінивши назву на «Svenska Ackumulator Aktiebolaget Jungner», підприємство все ж таки продовжило свій розвиток. В даний час підприємство, засноване розробником, носить назву SAFT AB і виробляє одні з найнадійніших нікель-кадмієвих акумуляторів у світі.

Малюнок №17. Будова Ni-Cd акумулятора.

Нікель-кадмієві акумулятори відносяться до дуже довговічного та надійного типу. Існують моделі, що обслуговуються і не обслуговуються, з ємністю від 5 до 1500Ач. Зазвичай поставляються у вигляді сухо-заряджених банок без електроліту з номінальною напругою 1,2В. Незважаючи на схожість конструкції зі свинцево-кислотними, нікель-кадмієві батареї мають низку істотних переваг у вигляді стабільної роботи при температурі від – 40°С, можливості витримувати високі пускові струми, а також оптимізовані моделями для швидкого розряду. Ni-Cd батареї стійкі до глибокого розряду, перезаряду та не вимагають моментального заряду як свинцево-кислотний тип. Конструктивно виробляються в ударостійкому пластику і добре переносять механічні ушкодження, не бояться вібрації тощо. Часто використовуються у переносних радіостанціях, авіації, на об'єктах енергетичної інфраструктури та нафтогазової промисловості, а також для різних транспортних засобів: тролейбусів, електрокарів тощо.

Принцип дії нікель-кадмієвих батарей

Лужні акумулятори, електроди яких складаються з гідрату окису нікелю з додаванням графіту, окису барію та порошкового кадмію. Як електроліт, як правило, виступає розчин з 20%-ним вмістом калію і додаванням моногідрату літію. Пластини розділені ізолюючими сепараторами, щоб уникнути замикання, одна негативно заряджена пластина розташована між двома позитивно зарядженими.

Вона не є вибухонебезпечна, стійка до дії вогню, не має запаху. Корпус герметичний, тому електроліт не витрачається у процесі роботи. На верхній частині корпусу розміщені струмознімальні контакти, необхідні для з'єднання елементів усередині конструкції. У кришці передбачений отвір для виходу надлишкових газів.

У процесі розряду нікель-кадмієвої батареї відбувається взаємодія між анодом з гідратом оксиду нікелю та іонами електроліту, утворюючи гідрат закису нікелю. В цей же час катод з кадмію утворює гідрат окису кадмію, тим самим створюючи різницю потенціалів до 1,45В забезпечуючи напругу всередині акумулятора та зовнішнього замкненого ланцюга.

Процес заряду нікель-кадмієвих акумуляторів супроводжується окисленням активної маси анодів та переходом гідрату закису нікелю в гідрат окису нікелю. Одночасно катод відновлюється із заснуванням кадмію.

Перевагою принципу дії нікель-кадмієвої батареї є те, що всі складові, які утворюються в процесі циклів розряду та заряду, майже не розчиняються в електроліті, а також не вступають у будь-які побічні реакції.

Типи нікель-кадмієвих акумуляторів

В даний час батареї Ni-Cd використовують найчастіше в промисловості, де потрібно забезпечувати живленням різноманітні пристрої.

Нікель-кадмієві пристрої бувають обслуговуються та необслуговуються.

Залежно від особливостей виконання вони поділяються на два типи:

- **Циліндричні**. Електроди мають вигляд стрічки, яка згортається у рулони. Між анодом та катодом розміщується сепаратор.

- **Призматичні**. Електроди виготовлені у вигляді пластин. Вони розташовані один на одному через сепаратор.

Виробники випускають різні види акумуляторів Ni-Cd, що відрізняються часом розряду та іншими характеристиками. Дізнатися про технічні параметри конкретної моделі допомагає маркування. Перші цифри у ній позначають, скільки окремих елементів з'єднані в АКБ. Літери "НК" або "К" вказують на те, що це нікель-кадмієвий пристрій. Наступні літери говорять про режим розряду: L – тривалий, H – короткочасний. Цифра за ними – ємність акумулятора. Літера «Р» у маркуванні свідчить про те, що корпус виготовлений із пластику.

Характеристики нікелево-залізних акумуляторів

Основні параметри батарей Ni-Cd:

- Ємність - від 1 до 1500 Ач.
- Мінімальна розрядна напруга - 0,9 В.
- Можлива глибина розряду – 100%.
- Робоча температура - 50 до + 40°С.
- Саморозряд на місяць – 4%.
- Питома енергоємність до 65 Втч/кг.
- Кількість робочих циклів - 2300.
- Термін експлуатації - 20-25 років.

Високі технічні характеристики роблять цей тип акумуляторних батарей дуже привабливим для вирішення виробничих завдань, коли потрібне високонадійне джерело резервного живлення з тривалим терміном служби.

Вперше були створені Вальдемаром Юнгнером в 1899 році, коли він намагався знайти більш дешевий аналог кадмію в складі нікель-кадмієвих батарей – розробив нікель-залізний акумулятор, який живив електромобілі «Baker Electric» та «Detroit Electric».

Дешевизна виробництва дозволила нікель-залізним акумуляторам стати затребуваними в електротранспорті як тягові батареї, що також застосовуються для електрифікації пасажирських вагонів, живлення ланцюгів керування. В останні роки про нікель-залізні акумулятори заговорили з новою силою, тому що вони не містять токсичних елементів на кшталт свинцю, кадмію, кобальту і т. д. В даний час деякі виробники застосовують їх для систем відновлюваної енергетики.

Принцип дії нікелево-залізних батарей

Стандартна Ni-Fe батарея виконана у вигляді блоку плоских електродів, які поміщені у сталевий корпус. У верхній частині приладу розташовані струмознімач та пробка, яка відкручується для заливки електроліту. Характеристики акумуляторів залежать від конструкції та технології виробництва електродів, що відрізняються типами струмопровідних каркасів. У ламельній конструкції активна маса розміщується в перфорованій сталевій оболонці. У безламельних рішеннях вона напресовується на сітку із сталі.

Акумуляція електроенергії відбувається за допомогою нікель оксиду-гідроксиду, що застосовується як позитивні пластини, заліза – як негативні пластини і рідкий електроліт у вигляді їдкого калію. Нікелеві стабільні трубки або «кишені» містять активну речовину.

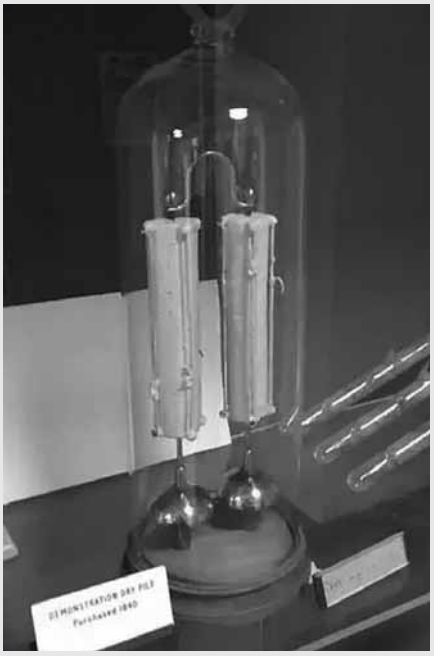
Нікелево-залізний тип дуже надійний, витримує глибокі розряди, часті перезаряди, а також може перебувати в недозарядженому стані, що дуже згубно для свинцево-кислотних батарей.

Характеристики нікелево-залізних акумуляторів

- Ємність - від 10 до 1000 Ач.
- Номінальна напруга - 1,2 Ст.
- Робоча температура - 40 до +46 °С.
- Саморозряд на місяць - 15 - 40.
- Циклічний ресурс - 1800-2300.
- Допустима глибина розряду — 100%.
- Мінімальний час заряду - 12-16 годин.
- Термін експлуатації – 20 років і більше.

energy-gmbh.com.ua
best-energy.com.ua

Найдовший експеримент у світі - найстаріша акумуляторна батарея працює вже понад 180 років

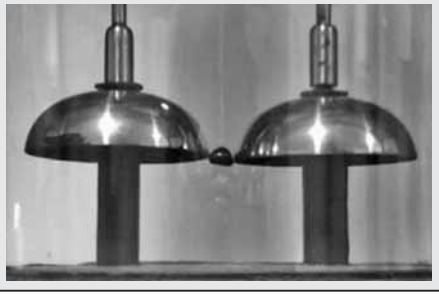


У самому серці Оксфордського університету триває один з найдовших наукових експериментів у світі. Це Oxford Electric Bell, або дзвін Кларендона, який працює безперервно з 1840 року. Незважаючи на те, що його дзвін ледве чути, він вражає своєю довговічністю.

Цей дивовижний пристрій був придбаний професором фізики преподобним Робертом Уокером у 1840 році. Сьогодні його можна побачити в лабораторії Кларендона, де він захищений двома шарами скла. Цей дзвін також відомий як Clarendon Dry Pile – тип батареї, яка складається зі стопок металевих дисків і здатна працювати дуже довго. Однією з причин такої довговічності є надзвичайно низьке енергоспоживання. Маленький свинцевий дзвіночок безперервно коливається між двома дзвонами, заряджаючись і розряджаючись.

Доктор Роберт Тейлор з BBC пояснив, що мінімальна кількість заряду просочується між двома кінцями, а єдина втрата енергії відбувається через опір повітря. Це дозволяє зберігати енергію і забезпечує безперебійну роботу дзвону.

Склад і будова батареї, яка живить дзвін, залишається загадкою. Вчені припускають, що вони схожі на батареї, створені італійським священиком і фізиком Джузеппе Замбоні. Батарея Замбоні складалася з приблизно 2000 пар дисків олов'яної фольги, приклеєних до паперу, просоченого сульфатом цинку та покритого діоксидом марганцю.



Батареї Oxford Electric Bell запечатані зовнішнім покриттям, яке містить сірку, що робить їх схожими на свічки. Однак, якщо їх відкрити, експеримент буде зіпсовано, тому точний склад батарей залишається невідомим. Дзвін може працювати ще п'ять або десять років, хоча за останні 40 років його швидкість помітно зменшилась. Доктор Тейлор зазначив, що причиною зупинки буде розрядка батарей.

У чому полягала первісна суть досліду з цим електричним дзвінком, і чи був це взагалі експеримент чи просто демонстрація, вже точно не відомо. Однак на даний момент, фізики були б раді дізнатися, як влаштоване джерело живлення в цьому дзвінку, але, на жаль, циліндри запечатані, а технічна документація давно втрачена. Однак, є кілька міркувань з цього приводу. Справа в тому, що інші сухі батареї, створені в той час, складаються з багатьох металевих дисків поставлених один на одного і залитих сіркою. З одного боку, диски покриті сульфатом цинку, з іншого - діоксидом марганцю.

У минулому якось вдалося зробити так, щоб батареї служили неймовірно довго. Вчені не поспішають розкривати дзвінок. Спочатку вони хочуть дізнатися, як довго він прослужить, але як тільки він перестане працювати, фізики швиденько проведуть його дослідження.

/mors.in.ua/

Акумулятор: регулювання щільності, приготування електроліту, усунення сульфатації

Сульфатація акумулятора визначається порівнянням ЕРС, підрахованою по щільності, з напругою, виміряним вольтметром без навантаження за формулою:

ЕРС = 0,84 + Р

де **Р** - щільність, приведена до 15°С, г/см^3.

Поправка до щільності - 0,0007 на кожен градус (приблизно 0,01 на кожні 15°С) від вихідної температури (вихідна: 15°С), тобто, якщо температура АКБ вище 15°С, то ця поправка додається до показань ареометра, якщо нижче - віднімається.

Приготування електроліту з сірчаної кислоти щільністю 1,83 г/см^3	
Густина електроліту, приведена до 15°С, г/см^3	На 1 літр дистильованої води додати сірчаної кислоти, л
1,210	0,245
1,230	0,280
1,250	0,310
1,265	0,335
1,270	0,345
1,290	0,385
1,400	0,650

Якщо заміряна напруга буде більше ЕРС, це значить, що електроди сульфатовані. Для усунення сульфатації проводиться кілька циклів розрядів-зарядів при малій щільності електроліту (1,11-1,2 г/см^3). Заряд проводиться силою струму не більше 5% від номінальної ємності АКБ.

Після цього слід довести щільність до потрібного значення, потім провести контрольний розряд силою струму 10% від ємності.

Розряд закінчують, коли напруга знизиться до 10,2 В.

АКБ вважається справною, якщо час розряду не менше 7,5 годин для батареї із щільністю 1,29 г/см^3; 6,5 годин - для 1,27; 5,5 - для 1,25.

Перевірка навантажувальною вилкою

Витримати АКБ під навантаженням протягом 5 сек., перевірити напругу - у повністю зарядженої батареї. Вона має бути не менше 10,8 Ст.

Приготування електроліту з концентрату щільністю 1,40 г/см^3		
Необхідна щільність при 15°С, г/см^3	Об'єм води, л	Об'єм електроліту щільністю 1,40 г/см^3
1,23	0,467	0,542
1,25	0,418	0,596
1,27	0,364	0,647
1,29	0,313	0,698
1,31	0,256	0,758

За стандартом SAE струм холодної прокрутки визначається на 30-й секунді розряду при температурі 18°С і напрузі на виводах не менше 7,2 Ст.

Струм стартерного розряду за стандартом DIN визначають при тих же умовах, але кінцева напруга на висновках АКБ повинно бути не менше 9В.

Перевірка якості дистильованої води

Налити дистильовану воду в банку з поліетиленовою кришкою, через яку пропустити два дротових електрода.

Занурити електроди на глибину близько 10 мм з відстанню між ними 15-30 мм. Виміряти опір на електродах. Має бути не менше 30 кОм.

energy-gmbh.com.ua

Підвищення щільності електроліту в АКБ
Після видалення необхідної кількості електроліту з АКБ (відповідно до табл.), додати таку ж кількість електроліту щільністю 1,40 г/см^3

Необхідна щільність, г/см^3	Реальна щільність електроліту, г/см^3														
1,15	**1,16**	**1,17**	**1,18**	**1,19**	**1,20**	**1,21**	**1,22**	**1,23**	**1,24**	**1,25**	**1,26**	**1,27**	**1,28**	**1,29**	
1,24	254	220	201	181	158	133	105	74	40						
1,26	290	275	259	241	222	200	176	149	119	84	45				
1,28	342	330	316	301	285	266	246	223	198	169	136	97	53		
1,30	396	385	374	362	348	333	316	242	277	253	226	194	158	115	63
	Об'єм повітря, що видаляється з АКБ електроліту, см^3														

Зниження щільності електроліту в АКБ
Після видалення необхідної кількості електроліту з АКБ (відповідно до табл.), додати таку саму кількість дистильованої води

Необхідна щільність, г/см^3	Реальна щільність електроліту, г/см^3									
1,25	**1,26**	**1,27**	**1,28**	**1,29**	**1,30**	**1,31**	**1,32**	**1,33**	**1,34**	
1,24	24	47	68	87	105	112	138	153	167	181
1,26			23	44	63	82	99	115	130	145
1,28					21	41	59	77	93	108
1,30							20	38	56	72
	Об'єм повітря, що видаляється з АКБ електроліту, см^3									

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

Захист дітей у воєнних конфліктах: роль дитячих протигазів

Збройна агресія проти Україні призвела до серйозних викликів і загроз, особливо для дітей. Застосування хімічної зброї, військові дії та техногенні аварії внаслідок атак по цивільним об'єктам, створюють великі загрози для життя та здоров'я дітей. Одним із важливих засобів захисту дітей в таких умовах є дитячі протигази.

Протигаз дитячий MD-1 — це засіб індивідуального захисту, який набуває особливого значення в умовах війни, що триває в Україні. Війна принесла з собою численні загрози для цивільного населення, особливо для дітей. Вибухи, обстріли, хімічні атаки та радіаційні загрози стали реальністю, з якою щодня стикаються мільйони українців. У таких умовах, коли небезпеки можуть виникнути несподівано, забезпечення захисту дітей стає першочерговим завданням для кожного батька.

Протигаз MD-1 розроблений спеціально для дітей віком від 3 до 12 років, щоб забезпечити їм надійний захист від основних видів загроз, які можуть виникнути під час бойових дій. Це не просто засіб захисту — це надійний бар'єр між вашою дитиною та потенційно смертельними небезпеками, що можуть бути спричинені війною.

Переваги протигазу MD-1:

Захист від хімічних речовин: У випадку хімічних атак фільтри MD-1 ефективно нейтралізують отруйні гази, захищаючи дихальні шляхи дитини.

Радіаційний захист: Протигаз забезпечує надійний захист від вдихання радіоактивного пилу, що особливо важливо в разі ядерних атак або аварій на атомних електростанціях.

Біологічний захист: Фільтри MD-1 затримують небезпечні мікроорганізми, захищаючи від біологічних загроз.

Захист від чадного газу: У випадку пожеж, які часто супроводжують обстріли, протигаз ефективно захищає дитину від отруєння чадним газом.

В умовах війни, коли кожен день приносить нові виклики, **протигаз MD-1** стає важливим інструментом для захисту життя і здоров'я дітей. Це ваш спокій і впевненість у безпеці найціннішого.

Дитячі протигази: що це таке?

Дитячі протигази - це спеціальні протигазні маски та фільтри, розроблені для захисту дітей від шкідливих газів та аерозолів, які можуть використовуватися під час воєнних дій та бути наслідком техногенних катастроф. Протигази забезпечують надійний захист дихальних шляхів та очей не тільки від радіоактивного пилу а і від шкідливих речовин, таких як: циклогексан,діоксид сірки хлор, аміак, фосген та інші.

Чому вони необхідні зараз?

З початком повномасштабної агресії в Україні ситуація стала критичною, а застосування хімічної зброї на полі бою та проти цивільного населення стало реальною загрозою. Діти, як найвразливіша частина населення, потребують особливого захисту. Дитячі протигази надають їм шанс на виживання і мінімізацію ризиків для їхнього здоров'я.

Переваги дитячих протигазів:

1. Захист дихальних шляхів: Протигази ефективно фільтрують повітря, дозволяючи дітям дихати безпечним повітрям в умовах хімічного та радіоактивного забруднення атмосфери.

2. Захист очей: Дитячі протигази також включають захист для очей, що особливо важливо під час військових дій.

3. Зручність та легкість використання: Сучасні дитячі протигази легкі для носіння і мають кілька розмірів шо зумовлює використання дітьми навіть раннього віку (від 3-х років).

Психологічний захист:

Діти особливо вразливі перед стресом і травматичними подіями, такими як хімічні атаки. Наявність дитячих протигазів може зменшити страх та тривожність у дітей, знаючи, що вони обладнані для захисту.

Захист від наслідків хімічних атак:

Хімічні атаки та техногенні аварії можуть мати довгострокові наслідки для здоров'я. Дитячі протигази допомагають запобігти вдиханню отруйних речовин, які можуть призвести до хронічних захворювань.

Навчання та підготовка:

Важливим аспектом забезпечення ефективного захисту дітей є навчання та підготовка. Дітям і їхнім батькам або опікунам слід отримувати інформацію про те, як правильно використовувати протигази, як надягати їх і перевіряти на герметичність. Це також включає навчання дітей важливим навичкам, таким як виявлення небезпечних ознак і дії в разі хімічної атаки.

Військовий час завжди становить загрозу для дітей, і забезпечення їхнього захисту повинно бути на першому плані. Дитячі протигази - це необхідний інструмент для мінімізації ризиків, пов'язаних з військовими діями та їх наслідками. Важливо забезпечити дітей знаннями та навчанням з його використання, а також забезпечити державну та міжнародну підтримку для поставки таких засобів в Україну. Тільки так можна забезпечити безпеку для дітей в країні, де військові дії є реальністю та можливим майбутнім.

ІНДИВІДУАЛЬНИЙ ЗАХИСТ ОРГАНІВ ДИХАННЯ

ІЗОД

www.izod.com.ua

ПРИВАТНЕ ПІДПРИЄМСТВО «СЕЛЛ`КОМ» працює на українському ринку засобів індивідуального захисту більше 10 років і займає лідируючі позиції серед компаній, що займаються виробництвом та постачанням засобів індивідуального захисту органів дихання. Наша компанія є ексклюзивним дистриб'ютором компанії **«TRAYAL CORPORATION»** та **«SIGMA s.r.o.»** які є провідними виробниками протигазів, фільтрів і масок.

ПРИВАТНЕ ПІДПРИЄМСТВО «СЕЛЛ`КОМ» має реєстрацію та дозвіл на імпорт в Україну продукції військового та подвійного призначення. Наша компанія виготовляє, комплектує та постачає засоби індивідуального захисту (протигази різних типів) для найбільших підприємств України, Збройним Силам України та ДСНС України.

TRAYAL KORPORACIJA

SIGMA

ПРИВАТНЕ ПІДПРИЄМСТВО «СЕЛЛ`КОМ» +38 067 640 80 10, +38 066 400 66 85, www.izod.com.ua

Пожежна небезпека РІДКОГО ПАЛИВА, МАСЕЛ та ІНШИХ НАФТОПРОДУКТІВ

При одному з бомбових ударів ворожої авіації була пошкоджена нафтобаза, яка була розташована на більш високій відмітці по відношенню до населеного пункту. Вибухами були пошкоджені резервуари з пальним та виникла пожежа. Пальне палаючою лавиною полилося по несеному пункту, підпалюючи на своєму шляху жилі будинки та інші господарські споруди. Цього могло б не статись, якби своєчасно на стадії проектування та будівництва були виконані діючі нормативні вимоги та нафтобаза була розміщена на більш низькій відмітці по відношенню до населеного пункту. В зв'язку з цим починаємо публікування нормативних вимог, що торкаються проектування та будівництва складів нафти та нафтопродуктів.

СКЛАДИ РІДКОГО ПАЛИВА, МАСЕЛ та ІНШИХ НАФТОПРОДУКТІВ

Загальні вимоги

Проектування складів рідинного палива, мастил та інших нафтопродуктів на підприємствах паливно-енергетичного комплексу повинно виконуватись відповідно до ВБН В.2.2-58.1-94 та ВБН В.2.2-58.2-94.

Склади з резервуарами мазуту, дизельного палива, мастил та інших видів нафтопродуктів, які розташовані на підприємствах паливно-енергетичного комплексу відносяться до другої групи.

На складах нафтопродуктів, які входять до складу енергетичних підприємств, допускається зберігати при наземному виді зберігання 2000 м^3 ЛЗР або 10000 м^3 ГР, при підземному зберіганні - 4000 м^3 ЛЗР 20000 м^3 ГР.

При наземному і підземному зберіганні одночасно ЛЗР і ГР загальна приведена місткість такого складу не повинна перевищувати місткості, наведеної вище, при цьому приведена місткість визначається з врахуванням: 1 м^3 ЛЗР прирівнюються до 5 м^3 ГР при наземному зберіганні. Проектування складів місткістю більше вказаних вище повинно здійснюватись за нормами проектування складів першої групи (п.3.1.3 НАПБ 05.033-2002).

Територія складу нафтопродуктів повинна бути огороджена провітрюваною огорожею з негорючих матеріалів висотою не нижче 2 м, якщо склад знаходиться поза територією підприємства.

При розміщенні складу на території підприємства, що має огорожу, улаштування спеціальної огорожі не потрібно. Необхідність улаштування спеціальної огорожі встановлюється замовником в завданні на проектування (п.3.1.4 НАПБ 05.033-2002).

При проектуванні складів нафти і нафтопродуктів слід передбачати захист від проявів статичної електрики відповідно до РД 39-22-113-78 та блискавки відповідно до ДСТУ Б В.2.5-38:2008.

По межах резервуарного парку і для під'їзду до площадок зливно-наливних пристроїв слід проектувати проїзди для пожежних машин, як правило, з проїзною частиною шириною 3,5 м і покриттям перехідного типу.

Для зливно-наливних залізничних естакад, обладнаних зливно-наливними пристроями з двох сторін, проїзд для пожежних машин повинен бути кільцевим (п.3.1.6 НАПБ 05.033-2002).

Проїзні дороги на резервуарних складах повинні мати освітлення, з'єднуватися з дорогами загального користування, знаходитись в справному стані, зимою очищатися від снігу.

На територіях складів необхідно періодично скошувати траву і вивозити її за межі складів.

У виробничих приміщеннях і на території складів повинні бути встановлені знаки безпеки згідно стандарту.

Тунелі, камери засувок і канали трубопроводів слід підтримувати в чистоті, регулярно очищати від розлитих нафтопродуктів, води і інших матеріалів.

Блискавкозахист, електричне освітлення складів нафтопродуктів, а також охоронне освітлення по периметру повинні знаходитися в справному стані.

На території складів з нафтопродуктами забороняється:

- встановлювати тимчасові інвентарні будівлі і побутові вагончики, а також зберігати різні матеріали і обладнання, які не відносяться до технології переробки та зберігання нафтопродуктів;
- використовувати відкритий вогонь при оглядах та підігріванні труб, а також палити поруч з резервуарами, в насосних, в камерах засувок і допоміжних приміщеннях (п.3.1.12 НАПБ 05.033-2002).

Резервуарні парки

Резервуарні парки складів нафтопродуктів, як правило, повинні розміщуватись на більш низьких відмітках землі по відношенню до відміток території сусідніх населених пунктів, підприємств, залізниць та автомобільних шляхів загальної мережі.

При розташуванні території резервуарних парків на більш високих відмітках в порівнянні з цими об'єктами, а також при розміщенні резервуарних парків в прибережній смузі водних об'єктів повинні передбачатись заходи по запобіганню розливу рідини при аварії наземних резервуарів:

- влаштування додаткового обвалування або огороджуючої стіни;
- влаштування відкритого земляного амбару;
- влаштування відвідних канав (траншей).

Технологічні трубопроводи повинні забезпечувати можливість перекачки у випадку аварії з резервуарів однієї групи в резервуари іншої групи, а при наявності в резервуарному парку однієї групи - з резервуару в резервуар (п.3.2.1 НАПБ 05.033-2002).

Для кожної групи наземних резервуарів по периметру повинно передбачатись замкнуте обвалування шириною по верху не менше:

- 0,5 м - при висоті обвалування менше 2,5 м;
- 1,0 м - при висоті обвалування 2,5 до 3,0 м;
- 2,0 м - при висоті обвалування понад 3,0 м;
- або огорожуюча стіна з негорючих матеріалів, розрахована на гідравлічний тиск рідини, що розлилась.

Висота обвалування або огороджуючої стіни кожної групи резервуарів визначається розрахунком і повинна бути на 0,2 м вище рівня розрахункового об'єму рідини, що розлилась, але не менше 1 м для резервуарів об'ємом менше 10000 м^3 і 1,5 м для резервуарів об'ємом 10000 м^3 і більше.

Вільний від забудови об'єм обвалованої території, що утворюється між внутрішніми відкосами обвалування або огороджуючої стіни, повинен прийняти розрахунковий об'єм рідини, яка розлилась, що дорівнює одному найбільшому по об'єму резервуару в групі. При розташуванні тільки одного резервуару на обвалованій площадці, її вільний об'єм повинен розраховуватись на об'єм цього резервуару.

Відстань від стінок резервуарів до внутрішніх схилів обвалування або до огорожуючих стін належить приймати не менше:

- 3 м - від резервуарів об'ємом менше 10000 м^3;
- 6 м - від резервуарів об'ємом 10000 м^3 і більше (п.3.2.2 НАПБ 05.033-2002).

В межах однієї групи кожний резервуар об'ємом 20000 м^3 і більше або декілька менших резервуарів сумарною місткістю 20000 м^3 повинні відділятись від інших резервуарів групи внутрішнім земляним валом або стінами висотою 0,8 м для резервуарів місткістю менше 10000 м^3 і 1,3 м для резервуарів місткістю 10000 м^3 і більше.

Обвалування підземних резервуарів слід передбачати тільки при зберіганні в цих резервуарах нафти і мазутів. Об'єм, що утворюється між внутрішніми схилами обвалування, слід визнача-

ти з умови утримання рідини в кількості, що дорівнює 10% об'єму найбільшого підземного резервуару в групі.

Для переходу через обвалування або огорожуючу стіну, а також для входу на осипку резервуарів необхідно передбачати сходи-переходи в кількості чотирьох для групи резервуарів і не менше двох для резервуарів, що стоять окремо, і одного входу на осипку.

Вузли засувок слід розташовувати з зовнішнього боку обвалування (огороджуючої стіни) груп або резервуарів, що стоять окремо. Корінний запірний пристрій слід розташовувати безпосередньо біля резервуарів (п.3.2.6 НАПБ 05.033-2002).

Всередині обвалування групи резервуарів допускається прокладання інженерних комунікацій, обслуговуючих тільки резервуари даної групи.

Трубопроводи, прокладені всередині обвалування, не повинні мати фланцевих з'єднань, за винятком місць приєднання арматури з застосуванням негорючих прокладок. Трубопроводи не повинні перетинати обвалування площадки, крім тих, до резервуарів якої вони підведені.

При прокладанні трубопроводів крізь обвалування в місці проходу труб повинна забезпечуватись герметичність.

Установка електрообладнання і прокладання електрокабельних ліній всередині обвалування не допускається за винятком електроприводу корінного запірного пристрою та інших пристроїв (що є обладнанням власне резервуару), контролю і автоматики, приладів місцевого освітлення. Всі ці пристрої повинні виконуватись у вибухозахисному виконанні (п.3.2.9 НАПБ 05.033-2002).

Транзитне прокладання трубопроводів, електропроводок і кабельних ліній через сусідні обвалування групи резервуарів не допускається.

Обвалування (стінки), їх перехідні містки, сходи, огорожі повинні постійно підтримуватись в справному стані. Майданчики всередині обвалувань повинні бути рівними, утрамбованими та посипані піском. Випадково розлиті ЛЗР та ГР слід негайно прибирати, а місця розлиття посипати піском.

Наземні резервуари мають бути пофарбовані білою (сріблястою) фарбою для запобігання дії сонячного проміння.

При прокладці або заміні трубопроводів, які проходять через обвалування наземних резервуарів, прориті траншеї після закінчення робіт повинні бути негайно засипані і обвалування відновлено.

На кожний резервуар необхідно складати технологічну карту, в якій вказується номер резервуара, його тип, призначення, максимальний рівень наливання, мінімальний залишок, швидкість наповнення і випорожнювання.

У процесі експлуатації резервуарів необхідно здійснювати постійний контроль за справністю дихальних клапанів та вогнезагорожувачів.

При температурі повітря вище нуля перевірка повинна проводитись не рідше одного разу на місяць, а нижче нуля - не рідше двох разів на місяць. Взимку дихальні клапани та сітки повинні очищуватися від льоду.

Під час огляду резервуарів, відбирання проб або замірів рівня рідини слід застосовувати пристосування, які виключають іскроутворення в разі ударів.

Люки, що служать для вимірювання рівня та відбору проб із резервуарів, повинні мати герметичні кришки, а отвори для вимірів - кільце з металу, яке виключає іскроутворення.

Підігрівати в'язкі та застигаючи нафтопродукти в резервуарах (у встановлених межах) дозволяється за умови рівня рідини над підігрівниками не менше 0,5 м (п.3.2.17 НАПБ 05.033-2002).

Для резервуарів, де зберігаються сірчисті нафтопродукти, повинен бути розроблений графік планових робіт з очищення від відкладень пірофорного сірчистого заліза.

При виникненні тріщин у швах, стінок або дна, діючий резервуар має бути негайно випорожнений.

Ремонт резервуарів дозволяється проводити лише після повного звільнення резервуара від рідини, від'єднання від нього трубопроводів, відкриття усіх люків, ретельного очищення (пропарювання та промивання), відбирання з резервуарів проб повітря та аналізу на відсутність вибухонебезпечної концентрації (п.3.2.20 НАПБ 05.033-2002).

Перед ремонтом резервуарів необхідно їх накрити повстю, просоченою антипіренами, усі засувки на сусідніх резервуарах та трубопроводах (влітку повстю змочити водою). Електро- та газозварювальну апаратуру дозволяється розміщати на відстані не ближче 50 м від діючих резервуарів.

Електро- та газозварювальні роботи повинні проводитись з оформленням наряду - допуску, а місця їх виконання забезпечуються первинними засобами пожежогасіння (п.3.2.21 НАПБ 05.033-2002).

Стаціонарні установки пожежогасіння наземних металевих резервуарів повинні бути в справному стані.

Зливно-наливні естакади

Площадка, зайнята зливно-наливною естакадою, повинна мати тверде водонепроникне покриття, огороджене по периметру бортиком висотою 200 мм і мати ухил не менше 2% в бік лотків, які в свою чергу повинні передбачатись з ухилом 0,5% до збірних колодязів (приямків), що розташовані на відстані не більше 50 м (п.3.3.1 НАПБ 05.033-2002).

Зливно-наливні естакади слід розміщувати на прямій горизонтальній дільниці горизонтальної колії.

Протяжність залізничних зливно-наливних естакад визначається в залежності від кількості одночасно оброблюваних цистерн, але повинна бути не більше максимальної довжини одного маршрутного состава залізничних цистерн.

Довжину тупикової залізничної колії з зливно-наливними пристроями або естакадою слід збільшувати на 30 м (для можливості розчеплення состава при пожежі), рахуючи від крайньої цистерни розрахункового маршрутного составу до упорного бруса.

Відстань від осі залізничних колій (складу або підприємства), на якій передбачається рух локомотивів, до осі найближчої колії з зливно-наливною естакадою повинна бути не менше 20 м, якщо температура спалаху рідин, що зливається, 120 °С і нижче і не менше 10 м, якщо температура спалаху вище 120 °С і мазутів.

Не допускається передбачати залізничну колію з зливно-наливною естакадою для наскрізного проїзду локомотивів (п.3.3.5 НАПБ 05.033-2002).

Зливно-наливні пристрої для рідин повинні бути закритими, як правило, безшланговими у вигляді систем шарнірно зчленованих труб і телескопічних пристроїв.

Для нафтопродуктів з температурою спалаху вище 120 °С і мазутів допускаються відкриті зливні пристрої з використанням міжрейкових або бокових жолобів, закритих знімними плитами.

Проміжні резервуари для мазуту і масел повинні розміщуватись, як правило, з зовнішньої сторони залізничних колій з зливно-наливною естакадою, так і під залізничними коліями (п.3.3.6 НАПБ 05.033-2002).

Зливно-наливні естакади повинні мати драбини з негорючих матеріалів, що розміщуються в торцях та мають ширину 0,7 м і ухил не більше 45°.

В відкритих зливних пристроях на зливних естакадах необхідно передбачати встановлення гідравлічних затворів.

Для місцевого освітлення під час зливно-наливних операцій можуть застосовуватися акумуляторні ліхтарі у вибухобезпечному виконанні.

Зливні шланги повинні бути споряджені наконечниками з матеріалів, які виключають можливість іскроутворення від удару (п.3.3.10 НАПБ 05.033-2002).

Залізничні шляхи, естакади, трубопроводи, телескопічні труби, наконечники шлангів та зливних пістолетів мають бути заземлені. Опір заземлю-

вальних пристроїв слід перевіряти не рідше одного разу на рік згідно з графіком (п.3.3.11 НАПБ 05.033-2002).

На зливних естакадах рідкого палива (нафтопродуктів) лотки мають бути постійно закритими негорючими плитами, а в місцях зливу залізничних цистерн - відкидними кришками.

Бетоновані площадки естакад і їх бортові огородження (від розтікання нафтопродуктів) слід періодично ремонтувати для запобігання вибоїн і тріщин.

Перед початком зливних операцій необхідно перевіряти правильність відкриття усіх зливних пристроїв і засувок, щільність з'єднань всіх зливних шлангів або труб на причалах, а також берегових пристроїв заземлення нафтоналивних суден.

Після зливних операцій необхідно прибрати розлиті нафтопродукти (п.3.3.14 НАПБ 05.033-2002).

Під час зливу рідких нафтопродуктів повинні використовуватись переносні лотки або кожухи для недопущення розбризкування.

При з'єднуванні або роз'єднуванні трубопроводів, а також при відкритті зливних пристроїв в залізничних цистернах повинні використовуватись інструмент, фланцеві і муфтові з'єднання, які не утворюють іскор (п.3.3.16 НАПБ 05.033-2002).

Забороняється рух тепловозів по залізничних коліях зливних естакад. Залізничні цистерни під злив повинні подаватись і виводитись плавно, без поштовхів і ривків.

Застиглі нафтопродукти повинні підігріватись тільки парою або в спеціальних тепляках.

При розігріві мазуту в залізничних цистернах відкритим паровим пристосуванням, його слід вмикати в роботу тільки після повного занурення шлангу в мазут.

Підігрів в цистернах і в інших ємностях (лотках) повинен бути на 15 °С нижче температури спалаху цих нафтопродуктів, але не вище +90 °С (п.3.3.18 НАПБ 05.033-2002).

При зливі нафтопродуктів і інших горючих рідин, які мають температуру спалаху нижче 120 °С (за винятком мазуту), зливні пристрої повинні бути закритого виконання (гнучкий шланг з наконечником або фланцеве з'єднання). Довжина шлангу має бути такою, щоб можна було опускати його до дна залізничної цистерни. Наконечники (фланці) шлангів повинні виготовлятися із іскробезпечних матеріалів.

Нижній злив ЛЗР (нафтопродуктів) допускається тільки через герметизовані зливні пристрої. Забороняється злив вказаного палива у відкриті лотки (п.3.3.19 НАПБ 05.033-2002).

У випадку надходження на склад рідкого палива з температурою спалаху нижче 45 °С, злив його забороняється.

Забороняється злив мазуту, дизельного палива і інших нафтопродуктів на залізничних зливних естакадах під час грози.

При зливних операціях забороняється:

- виконувати електрогазозварювальні роботи та користуватись відкритим вогнем ближче 30 м;

- застосовувати для освітлення переносні електролампи відкритого виконання, крім акумуляторних в вибухобезпечному виконанні (п.3.3.22 НАПБ 5.033-2002).

Мазутонасосні і мазутопроводи

Пожежна небезпека мазутонасосних і мазутопроводів характеризується наступними ознаками:

- температура спалаху мазуту 120 - 140 °С;

- температура самозаймання - 420 °С;

- температурні межі вибуху 143-170 °С.

В мазутових господарствах електростанцій використовується пара тиском 0,8-1,3 МПа (8-13 кгс/см^2) з температурою 200-250 °С.

Мазутонасосні відносяться до категорії В і виконуються II ступеню вогнестійкості (прил.1 СНіП II-35-76).

Захищаючі будівельні конструкції і двері приміщень мазутонасосних, а також приміщень витратних резервуарів дизельних електростанцій повинні передбачатися з межею вогнестійкості не менше 45 хв. Приміщення масло- і мазутонасосних, розміщених в одній будівлі, повинні розділятися протипожежною стіною і мати окремі входи (п.7.16 НАПБ 05.028-2004).

Підлога в приміщеннях масломазутного господарства повинна бути з матеріалів, що не згоряють, і виконуватися з ухилами не менше 0,5% до приямків для збору нафтопродуктів (п.4.56 СНіП II-58-75).

На всмоктувальних і нагнітальних мазутопроводах не ближче 10 м від стін мазутонасосних (зовні мазутонасосних) повинна передбачатися установка ручних засувок (п. 8.3.6 НАПБ 05.028-2004).

При розміщенні вузлів засувок в окремому приміщенні воно повинно відділяться від приміщення для насосів протипожежною перегородкою 1 типу в будівлях I і II ступеня вогнестійкості і 2 типу в будівлях IIIа ступеня вогнестійкості і мати вихід назовні. Двері між цими приміщеннями повинні бути протипожежними, що самозакриваються, 2 типу.

В місцях розташування вузлів засувок слід передбачати в підлозі лоток для відведення стоків в приямок, глибина якого повинна бути не більше 0,5 м (п.7.15 ВБН В.2.2-58.1-94).

В місцях проходу труб через внутрішні стіни насосних слід передбачати ущільнюючі пристроїв (п.7.17 ВБН В.2.2-58.1-94).

Прокладку кабелів через перекриття в мазутонасосній слід передбачати в трубах, при цьому кінці труб повинні підноситися над рівнем підлоги не менше ніж на 0,1 м і мати ущільнення.

Підлога кабельних споруд розподільних улаштувань, що блокуються з будівлею мазутонасосної, слід передбачати вище рівня заглибленої частини підлоги мазутонасосної не менше ніж на 0,1 м (п.8.3.10 НАПБ 05.028-2004).

Вихідні люки з кабельних споруд і інші отвори в підлозі приміщення установки мазутових насосів слід захищати бортиками висотою не менше 0,1 м (п.8.3.10 НАПБ 05.028-2004).

Прокладку мазутопроводів до котлів слід передбачати усередині котельного відділення за винятком підвальних приміщень (п. 8.3.12 НАПБ 05.028-2004).

В будівлях головних корпусів на вводах мазутопроводів повинна передбачатися установка електрозасувок, управління якими повинне передбачатися з блокового щита і з місця установки цих засувок (п. 8.3.13 НАПБ 05.028-2004).

Мазутопроводи котельні повинні бути покриті негорючою теплоізоляцією і при прокладці з обігріваючим супутником виконується в загальній ізоляції з ним (п. 8.3.13 НАПБ 05.028-2004).

Мазутопроводи котельних установок (від магістралей котельної до пальників) повинні виконуватися з безшовних труб на зварці. Фланцьові з'єднання допускаються лише в місцях установки арматури, вимірювальних діафрагм і заглушок.

На мазутопроводах повинна застосовуватися тільки сталева арматура 1-го класу герметичності по ГОСТ 9544-75 (п. 8.3.7 НАПБ 05.028-2004).

Усі мазутопроводи повинні бути заземлені при установці на них електри-

Пожежа на порожньому нафтеналивному танкері Pablo коло берегів Малайзії

фікованої арматури, а фланцеві з'єднання слід обладнувати струмопровідною перемичкою (п. 8.3.16 НАПБ 05.028-2004).

Мазутопроводи повинні передбачатися з посилених безшовних труб на тиск відповідно (Ру)0,4; 0,6 і 0,8 МПа (40,60 і 80 кгс/см2) при температурі до 200 °С (п. 8.3.9 НАПБ 05.028-2004).

На мазутопроводах повинні застосовуватися фланцеві з'єднання ШИП-ПАЗ, які повинні закриватися кожухами з негорючих матеріалів (п. 8.3.8 НАПБ 05.028-2004).

На відкритих зливних пристроях мазуту на зливних естакадах необхідно передбачати установку гідравлічних затворів (п.8.3.17 НАПБ 05.028-2004).

В приміщеннях мазутонасосних повинна передбачатися установка автоматичних газоаналізаторів, що блокуються з аварійною вентиляцією, з виводом сигналів на щит управління, з постійним перебуванням персоналу (п. 8.3.18 НАПБ 05.028-2004).

Мазутонасосні площею 500 м^2 і більш підлягають устаткуванню установками автоматичної пожежогасіння (додаток 6 НАПБ В.01.034-2005/111).

В продуктових насосних, розміщуваних в будівлях, насосні агрегати можуть застосовуватися з електродвигунами у виконанні, що дозволяє їх установку як в загальному залі з насосами, так і в окремому приміщенні за протипожежною перегородкою. Ця протипожежна перегородка повинна бути газонепроникною, суцільною (без отворів) з межею вогнестійкості не нижче 45 хв. В місцях проходу через перегородку валів, що сполучають двигуни з насосами, повинні бути ущільнюючі пристрої (п. 7.17 ВБН В.2.2-58.1-94).

Приміщення для підготовки і перекачки нафтопродуктів (мазутонасосні, маслонасосні, регенерації масла та ін.) повинні постійно утримуватись у чистоті.

Забороняється для чистки підлоги і обладнання користуватись легкозаймистими рідинами.

Перед пуском устаткування необхідно перевіряти стан обладнання, герметичність засувок і трубопроводів, включення автоматичних систем захисту і блокування.

Підтікання нафтопродуктів на засувках, фільтрах, фланцевих з'єднаннях або ущільненнях обладнання повинно негайно усуватись.

При виявленні значного витоку нафтопродуктів, що порушує нормальний режим роботи обладнання, необхідно включити резервне обладнання або аварійно зупинити установку.

Технічний стан стаціонарних автоматичних газоаналізаторів, пристроїв звукової і світлової сигналізації про наявність у виробничих приміщеннях небезпечної концентрації парів у повітрі належить регулярно перевіряти.

Маслоочисні установки (сепаратори), які встановлені стаціонарно, повинні мати справну дренажну систему, а приймальний бак брудного масла - мірне скло із захисним кожухом.

При очистці масла потрібно вести контроль за його тиском, температурою, вакуумом, безперервністю подавання масла в маслопідігрівачі.

Обладнання маслоочисних установок повинно встановлюватись на негорючих фундаментах (основах).

Пости первинних засобів пожежогасіння потрібно розміщувати раціонально для можливості швидкого і безпечного використання.

У приміщеннях для підготовки і перекачки нафтопродуктів забороняється:

- зберігати різні матеріали і обладнання;
- залишати промаслені (замазучені) обтиральні матеріали;
- сушити на нагрітих поверхнях обладнання і трубопроводах спецодяг;
- обладнувати тимчасові зварювальні пости в приміщеннях насосних та проводити вогневі роботи без попереднього контролю за станом повітряного середовища засобами експрес-аналізів з застосуванням газоаналізаторів;
- захаращувати евакуаційні проходи і виходи із приміщення матеріалами і обладнанням (п.п.10.3.1-10.3.9 НАПБ В.01.034-2005/111).

Масляне господарство

На електростанціях і підстанціях 500 кВ не залежно від потужності встановлених трансформаторів і на підстанціях 330 кВ з трансформаторами потужністю 200 МВ. А і вище, розташованих у віддалених або труднодоступних районах, слід передбачати масляні господарства з устаткуванням для обробки масла.

Склади масла таких маслогосподарств повинні мати:

- на теплових електростанціях - по 4 резервуари турбінного і ізоляційного масла;
- на гідростанціях - по 3 резервуари турбінного і ізоляційного масла;
- підстанціях - 3 резервуари ізоляційного масла.

Об'єм кожного резервуару повинен бути не менше:

- для турбінного масла - об'єму масляної системи одного агрегату і доливання масла у розмірі 45-денної потреби всіх агрегатів теплової станції і 10% об'єму агрегату для ГЕС;
- для ізоляційного масла - об'єму одного найкрупнішого трансформатора із запасом 10% (п.4.2.214 ПУЕ).

Стаціонарні маслопроводи на електростанціях і підстанціях 330 і 500 кВ слід прокладати від майстерні або апаратної маслогосподарства до приміщення для ремонту трансформаторів (до ремонтного майданчика машинного залу на електростанції або трансформаторної башти на підстанціях) і до складу масла, а також до місця зливу масла з цистерн. Стаціонарні трубопроводи масла слід виконувати із сталевих труб, сполучених зварюкою (окрім стиків з арматурою) (п.4.2.218 ПУЕ).

Резервуари для зберігання масла повинні бути обладнані повітросушильними фільтрами, покажчиком рівня масла, пробно-спусковим краном на зливному патрубку (п.4.2.220 ПУЕ).

Відстань від стінок резервуарів відкритих складів масла повинна бути не менше:

- до будівель і споруд електростанцій (у тому числі до трансформаторної майстерні): для складів загальним об'ємом до 100 т масла - 12 м; для складів більше 100 т - 18 м;
- до житлових і громадських будівель - на 25% більше відстаней, вказаних вище;
- до апаратної маслогосподарства - 8 м;
- до складів балонів водню - 20 м (п.4.2.221 ПУЕ).

Встановлені в закритих приміщеннях резервуари для зберігання енергетичних масел повинні мати пристрої для виміру рівня рідини і запобігання її переливання.

Вимоги пожежної безпеки при експлуатації складів ЛЗР і ГР

(п.п. 10.1.5-10.2.14 НАПБ В.01.034-2005/111)

Обвалування (стінки), їх перехідні містки, сходи, огорожі повинні постійно підтримуватись в справному стані. Майданчики усередині обвалувань повинні бути рівними, утрамбованими і засипаними піском. Випадково пролиті ЛЗР і ГР слід негайно прибирати, а місця розливу засипати піском.

Наземні резервуари повинні бути пофарбовані білою (сріблястої) фарбою для запобігання дії сонячного проміння.

Проїзні дороги на резервуарних складах повинні мати освітлення, з'єднуватися з дорогами загального користування, знаходитися в справному стані, взимку очищатися від снігу.

На території складів необхідно періодично скошувати траву і вивозити її за межі складів.

При прокладці або заміні трубопроводів, що проходять через обвалування наземних резервуарів, прориті траншеї після закінчення робіт повинні бути негайно засипаними а обвалування відновленим.

На кожний резервуар необхідно складати технологічну карту, в якій вказується номер резервуару, його тип, призначення, максимальний рівень наливання, мінімальний залишок, швидкість наповнення і спорожнення.

В процесі експлуатації резервуарів необхідно здійснювати постійний контроль за справністю дихальних клапанів і вогнезагороджувачів.

При температурі повітря вище за нуль перевірка повинна проводитися не рідше одного разу на місяць, а нижче за нуль - не рідше двох разів на місяць. Взимку дихальні клапани і сітки повинні очищатися від льоду. Під час огляду резервуарів, відбору проб або вимірі рів-

ня рідини слід застосовувати інструменти та пристосування, які виключають іскроутворення при ударах.

Люки, що служать для виміру рівня і відбору проб з резервуарів, повинні мати герметичні кришки, а отвори для вимірів - кільце з металу, яке виключає іскроутворення.

Підігрівати в'язкі і застигаючі нафтопродукти в резервуарах (у встановлених межах) дозволяється за умови рівня рідини над підігрівачами не менше 0,5 м.

Для резервуарів, в яких зберігаються сірчанисті нафтопродукти, повинен бути розроблений графік планових робіт по очищенню від відкладень піpофорного сірчанистого заліза.

При появі тріщин в швах, в металі стінок або днищі, діючий резервуар повинен бути негайно спорожнений.

Ремонт резервуарів дозволяється проводити тільки після повного звільнення резервуару від рідини, від'єднання від нього трубопроводів, відкриття всіх люків, ретельного очищення (пропарювання і промивки) відбору з резервуару проб повітря і аналізу на відсутність вибухонебезпечної концентрації.

Перед ремонтом резервуарів необхідно прикрити повстю, просоченою антипіренами, всі засувки на сусідніх резервуарах і трубопроводах (в літній час повсть потрібно змочити водою). Електро- і газозварювальну апаратуру допускається розташовувати на відстані не ближче 50м від діючих резервуарів.

Електро- і газозварювальні роботи повинні проводитися з оформленням наряду-допуску, а місця їх виконання забезпечуватися первинними засобами пожежогасіння.

На території складів з нафтопродуктами забороняється:

- встановлювати тимчасові інвентарні будівлі і побутові вагончики, а також зберігати різні матеріали і устаткування, що не відноситься до технології переробки і зберігання нафтопродуктів;

- застосовувати відкритий вогонь для огляду та відігрівання труб, а також палити біля резервуарів, в насосній, в камерах засувок і допоміжних приміщеннях.

Стаціонарні установки пожежогасіння наземних резервуарів повинні бути в справному стані.

У виробничих приміщеннях і на території складів повинні бути встановлений знаки безпеки згідно стандарту ГОСТ 12.4.026-76.

Тунелі, камери засувок і канали трубопроводів слід підтримувати в чистоті, регулярно очищати від пролитих нафтопродуктів, води і інших матеріалів.

Блискавкозахист, електричне освітлення складів нафтопродуктів, а також охоронне освітлення по периметру повинні бути в справному стані.

Для місцевого освітлення під час зливно-наливних операцій можуть використовуватися акумуляторні ліхтарі у вибухобезпечному виконанні.

Зливні шланги повинні бути обладнані наконечниками з матеріалів, що виключають можливість іскроутворення при ударі.

Залізничні колії, естакади, трубопроводи, телескопічні труби, наконечники шлангів і зливних пістолетів повинні бути заземлені. Опір заземлюючих пристроїв слід перевіряти не рідше одного разу на рік згідно графіка.

На зливних естакадах рідкого палива (нафтопродуктів) лотки повинні бути постійно закриті негорючими плитами, а в місцях установки і зливу залізничних цистерн - відкидними кришками.

Бетоновані майданчики естакад і причалів, їх бортові огорожі (від розтікання нафтопродуктів) слід періодично ремонтувати для усунення вибоїн і тріщин.

Перед початком зливних операцій повинні перевірятися правильність відкриття всіх зливних пристроїв і засувок, щільність з'єднання зливних шлангів або труб на причалах, а також берегових пристроїв заземлення нафтоналивних суден.

Після зливних операцій необхідно прибирати пролиті нафтопродукти.

Під час зливу рідких нафтопродуктів повинні застосовуватися переносні лотки або кожухи для виключення розбризкування.

При збірці або розбиранні сполучних трубопроводів на причалах, а також при відкритті зливних пристроїв нафтоналивних суден і залізничних цистерн повинні застосовуватися інструмент фланцеві і муфтові з'єднання або пристосування, що не дають іскроутворення.

Нафтоналивні судна, пришвартовані до причалу, повинні заземлятися до з'єднання трубопроводів із зливними пристроями. Заземлення слід знімати тільки після закінчення зливних операцій і роз'єднання трубопроводів з шлангами причалу і судна.

Обслуговуючі працівники причалу і судна зобов'язані вести постійне спостереження за ходом зливних робіт і станом устаткування.

Трубопроводи для зливу нафтопродуктів з нафтоналивних суден повинні обладнуватися аварійною засувкою, яка встановлюється на відстані не менше 30 м від причалу.

Забороняється рух тепловозів по залізничних коліях зливних естакад. Залізничні цистерни під злив повинні подаватися і виводитися плавно, без поштовхів і ривків.

Застиглі нафтопродукти повинні підігріватися тільки парою або в спеціальних тепляках. При підігріві мазуту в залізничних цистернах відкритим паровим пристроєм, його слід включати в роботу тільки після повного занурення шланга в мазут.

Підігрів в цистернах і інших ємкостях (лотках) повинен бути на 15 °С нижче за температуру спалаху цих нафтопродуктів, але не вище +90 °С.

При зливі нафтопродуктів і інших горючих рідин з температурою спалаху нижче 120 °С (за винятком мазуту), зливні пристрої повинні бути закритого виконання (гнучкий шланг з наконечником або фланцеве з'єднання). Довжина шлангів повинна бути такою щоб можна було опускати їх до дна залізничної цистерни. Наконечники (фланці) шлангів повинні виготовлятися з іскробезпечних матеріалів.

Нижній злив легкозаймистих нафтопродуктів допускається тільки через зливні пристрої, що герметизуються. Забороняється злив вказаного палива у відкриті лотки.

У разі надходження на електростанцію рідкого палива з температурою спалаху нижче 45 °С злиття його забороняється.

Забороняється злиття мазуту, дизельного палива та інших нафтопродуктів на залізничних зливних естакадах і водних причалах під час грози.

При зливних операціях забороняється:

- виконувати електрогазозварювальні роботи і застосовувати відкритий вогонь ближче 30 м;

- застосовувати для освітлення переносні електролампи відкритого виконання, окрім акумуляторних у вибухобезпечному виконанні.

В.В.Косюк
Фахівець з пожежної безпеки
в галузі електроенергетики
Вересень 2024 року

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

Частина III. Виховання доброчесності та скорочення корупційного потенціалу в оборонних структурах

У третій частині компендіуму розглядаються суб'єкти виховання доброчесності та їх ролі. Вона починається з розділу про важливість виховання доброчесності. Наступні розділи досліджують вплив нормативної бази, особистості, виконавчої гілки влади (зосереджуючись на міністерстві оборони), парламентів та органів аудиту, інституту омбудсмена, оборонної промисловості, громадянського суспільства та ЗМІ, а також міжнародних організацій. Кожний розділ пропонує принципи та кращий досвід з питань виховання доброчесності та скорочення корупційних ризиків у оборонних структурах.

Розділ 20. Оборонна промисловість як союзник у зниженні корупції

Для того, щоб система боротьби з корупцією ефективно функціонувала, оборонна промисловість повинна взаємодіяти з нею. Постачальники оборонного відомства добре усвідомлюють важливість корпоративної соціальної відповідальності та легітимізації, які асоціюються з більшою прозорістю. Цей розділ пропонує до розгляду політику виховання доброчесності двох значних оборонних контракторів і визначає подальші заходи, яких може бути вжито оборонною промисловістю та органами державної влади в інтересах зміцнення доброчесності в оборонному секторі.

1. Оборонна промисловість як учасник вирішення питання зменшення корупції: американська перспектива

Існує думка про те, що корупція у певних ринкових ситуаціях є лише додатковою ціною за можливість робити бізнес на цих ринках. Наслідком такого судження стає висновок нібито про те, що зусилля у боротьбі з корупцією є марними і необов'язковими. Однак ця точка зору ігнорує цілком реальні негативні наслідки корупції. Вона руйнує громадську довіру до урядів і корпорацій, знижує якість продукції та послуг, які закуповуються за народні гроші, а також підриває ефективність функціонування вільного ринку. На щастя, такий погляд стає менш авторитетним у сьогоднішньому взаємозалежному світі, де факти широкомасштабної корупції, що рано чи пізно майже завжди викриваються, оприлюднюються і критикуються, завдаючи шкоди всім залученим сторонам.

Протягом останніх років оборонна промисловість неодноразова піддавалася звинуваченням щодо корумпованої поведінки в різних країнах світу. Це суттєво послабило довіру до цього сегменту промисловості, який залежить переважно від публічних коштів. При цьому може здаватися неадекватною теза про те, що партнерство між промисловістю та урядом є єдиним ефективним засобом боротьби з корупцією. Однак, якщо трохи відступити назад, то стає очевидним, що на проблему корупції потрібно вести наступ з обох боків – як з боку постачальників, а це, як правило, оборонна промисловість, так і з боку замовників, яких в основному представляють урядові відомства і посадові особи.

Ця частина досліджує корупцію з боку постачальників, зосереджуючись на кращому досвіді найбільших оборонних корпорацій США, зокрема, Локхід Мартін, щодо забезпечення ведення бізнесу відповідно до високих етичних стандартів.

Ініціатива оборонної промисловості (ІОП)

Більшість основних оборонних підрядників всередині Сполучених Штатів приєдналися до ІОП. Цю ініціативу було започатковано у 1986 році у відповідь на ерозію громадської довіри до промисловості, спричиненої широко оприлюдненими випадками обману, марнотратства і зловживань як усередині промисловості, так і в міністерстві оборони. Всі підписанти ІОП погодилися прийняти й дотримуватися шести принципів самоврядування, наведених у Вставці 20.1.

Кожний підписант ІОП погоджується заповнити детальний щорічний опитувальник стосовно їх етичних програм і практики. Результати опитування узагальнюються і згодом публікуються у щорічній Доповіді публічної підзвітності ІОП. *(Починаючи з 2003 року, щорічні доповіді можна знайти на веб-сайті ІОП: www.dii.org.)*

Незважаючи на те, що всі члени ІОП запроваджують свої власні підходи до виконання цих шести принципів, з плином часу та врахуванням поширення досвіду щодо етичних програм основних оборонних контракторів США з'явилися певні спільні елементи.

Вставка 20.1. Принципи самоврядування Ініціативи оборонної промисловості

1. Кожний підписант повинен мати в наявності й дотримуватися письмового кодексу бізнесової поведінки. Кодекс встановлює високі етичні цінності, яких мають дотримуватися всі співробітники організації-підписанта.

2. Кожний підписант повинен організувати підготовку всіх співробітників з питань їх персональної відповідальності за дотримання положень кодексу.

3. Підписанти повинні заохочувати внутрішні доповіді про порушення кодексу, при цьому має виконуватися умова непокарання за такі доповіді.

4. Підписанти беруть зобов'язання щодо самоврядування шляхом застосування механізмів контролю для моніторингу дотримання федеральних законів та запровадження процедур добровільних доповідей у відповідні інстанції щодо інформації про порушення федерального законодавства з питань закупівель.

5. Кожний з підписантів повинен прийняти зобов'язання перед іншими підписантами стосовно поширення кращого досвіду дотримання принципів ІОП; кожний підписант має брати участь у щорічному форумі передового досвіду.

6. Кожний підписант має бути підзвітним суспільству.

Джерело: Charter of the Defense Industry Initiative, Article III: www.dii.org.

Елементи ефективної етичної програми

а. Кодекси етики або поведінки

Кожний з підписантів ІОП запровадив кодекс етики, який також іноді називають кодексом поведінки. Кодекс поведінки встановлює цінності і стандарти, яких компанія та її співробітники мають дотримуватися. Щоб бути ефективним, кодекс повинен відображати особливі традиції компанії та відповідальне ставлення до доброчесності. Багато кодексів, прийнятих у компаніях США, на додаток до визначення переліку цінностей компанії, встановлюють стандарти відповідності. Кодекси членів ІОП зазвичай включають стандарти, які стосуються широкого кола питань – від дискримінації і залякування до бізнесового протоколу ввічливості, протидії корупції та відкатів.

Кодекс компанії Локхід Мартін «Встановлення стандарту, кодекс етики та бізнесової поведінки» *(Можна*

завантажити з веб-сайту: www.lockheedmartin.com/data/assets/corporate/documents/ethics/setting-the-standard.pdf.) існує з самого початку діяльності корпорації. Кодекс підкреслює зобов'язання компанії Локхід Мартін щодо дотримання найвищих стандартів доброчесності, а також важливої ролі кожного співробітника у дотриманні цих зобов'язань. Він ознайомлює співробітників із важливими для Локхід Мартін цінностями та їх роллю у дотриманні цих цінностей. Кожний співробітник повинен засвідчити отримання кодексу, а також підтвердити факти прочитання, розуміння і готовності дотримуватися.

Таким чином, наприклад, один з розділів кодексу, який називається «Роби бізнес етично за межами Сполучених Штатів», декларує, що Локхід Мартін бере зобов'язання щодо глобального застосування високих стандартів етичної поведінки. Кодекс також зазначає:

Хабарництво, порушення експортно-імпортного законодавства, участь у незаконних бойкотах руйнують довіру до ринку, підривають демократію, псують економічний і соціальний розвиток, а також шкодять кожному, хто залежить від довіри й прозорості під час здійснення бізнесових операцій. *(Lockheed Martin, Setting the Standard: Code of Ethics and Business Conduct (Bethesda, MD: Lockheed Martin Corporation, October 2008), 12.)*

Це відображає головну цінність Локхід Мартін: «Робити як належить». Також у цьому розділі від працівників компанії вимагається дотримуватися загальнонаціонального і місцевого законодавства тих країн, де відбуваються операції Локхід Мартін. Розділ недвозначно спрямовує працівників компанії приділяти виключну увагу питанням дотримання антикорупційного законодавства, включаючи акти, прийняті відповідно до Конвенції з протидії хабарництву серед іноземних посадових осіб Організації з економічного співробітництва і розвитку (ОЕСР), а також, серед інших міжнародних антикорупційних конвенцій, Закону США про іноземну корупційну практику. *(Там само, 12.)*

б. Організації формальної етики

Більшість великих підрядників міністерства оборони США мають у своєму складі організації формальної етики, які відповідають за менеджмент й імплементацію етичної програми компанії.

Програми формальної етики сприяють забезпеченню дієвості кодексу поведінки компанії. Як правило, така програма виконує принаймні дві важливі функції: (1) комунікація, тренування й інформаційне супроводження виконання всього, що стосується цінностей компанії, відданості кодексу, а також дотриманню його положень; і (2) забезпечення виконання кодексу.

Під час реалізації своїх функцій комунікації та інформаційного супроводження організація в основному намагається забезпечити ситуацію, коли відданість дотриманню стандартів доброчесності буде невід'ємною частиною культури компанії. З різних точок зору, це найбільш важливі функції, які може здійснювати програма формальної етики. Найбільш ефективним шляхом попередження порушень або корупції є забезпечення такого стану, коли створюється культура розуміння всіма працівниками невідворотності відповідальності за недостойні дії.

Однак, культура доброчесності не пустить коріння, якщо працівники вважатимуть, що цінності та кодекс організації – це просто слова на папері, які не відображають реального стану діяльності компанії. Відповідно, надзвичайно важливим є балансування потреби захисту приватних інтересів працівників з потребою інформувати їх про наслідки для тих, хто ігноруватиме кодекс компанії.

Вибір місця цієї організації в структурі органів управління компанії також має важливе значення. Воно має бути достатньо високим в структурі всієї організації, щоб забезпечувати дотримання важливих норм етики і доброчесності та мати необхідний рівень незалежності.

Зокрема, у США більшість етичних програм підзвітні керівному органу або безпосередньо особисто управляючому компанією. Більшість також підтримує канали зв'язку або звітування з радою директорів.

Нарешті, найбільш ефективні етичні організації мають повноцінних або частково зайнятих відповідальних посадових осіб (офіцерів) з питань етики, які знаходяться в гущі виробничих або управлінських процесів. Посадовці з питань етики фактично є людським обличчям етичних організацій і можуть надавати консультації та поради, а також розслідувати випадки звинувачень у порушеннях. Оскільки вони знаходяться в гущі бізнесових проектів, то ці посадовці також можуть давати певні поради з поточних питань бізнесової діяльності.

У складі Локхід Мартін етична організація доповідає голові, управляючому та президенту компанії, а також раді директорів. Організація нараховує понад шістдесят п'ять посадовців з питань етики, з повною і частковою зайнятістю, які працюють всередині основних бізнесових операцій.

в. Гарячі лінії, лінії допомоги або канали доповідей

Невід'ємним елементом більшості етичних програм США є засоби, за допомогою яких працівник може повідомити про своє занепокоєння або запитати про керівні вказівки етичну організацію.

Більшість етичних програм США встановили для своїх працівників багато різних каналів для звернень з проблемних питань або отримання керівництва до дій з етичних питань. Ці канали включають особисті зустрічі з посадовцями з питань етики, звернення через електронну пошту безпосередньо до певного посадовця або через загальну корпоративну електронну адресу, залишення повідомлень на визначеному веб-сайті або відправку листів факсом чи поштою. Однак, найбільш важливими каналами зв'язку є гарячі лінії або лінії допомоги. Зазвичай це безкоштовний номер телефону, по якому працівник може безпосередньо з'єднуватися з етичною організацією. Такі гарячі лінії загалом дозволяють працівникам звертатися зі своїми проблемами анонімно, якщо вони не бажають називати себе. Вони також мають встановлені засоби спілкування, що дозволяють працівникам, які залишили анонімну доповідь, подзвонити ще раз по тій самій телефонній лінії й отримати відповідь стосовно реагування етичної організації на їх запити.

Ефективні канали спілкування забезпечують можливість для тих працівників, які побачили певні порушення або відчувають тиск щодо залучення до участі у корупційних схемах, отримати канал спілкування, який допоможе їх почути й відреагувати на їх стурбованість. Ефективність компанії визначається також її здатністю неухильно забезпечувати такий стан, за якого вона не дозволяє помсти проти працівників, які скористалися цими каналами зв'язку з найкращими намірами. Боязнь помсти є однією з найвагоміших причин, через яку працівники не доповідають компанії про проблемні випадки.

г. Підготовка та інформаційне супроводження

Більшість етичних програм США також включають тренінги з питань дотримання та з питань кодексу поведінки компанії. Навчання з питань дотримання є концентрованим курсом підготовки, що стосується окремих сфер регуляторних або правових ризиків, які постають перед компанією в конкретних умовах промислової діяльності. Тренінги з питань кодексу поведінки компанії, яке у Локхід Мартін називають «тренінгами усвідомлення», можуть включати питання дотримання, але більше фокусуються на цінностях компанії, її культурі та етиці прийняття рішень. Ні навчання з питань дотримання, ні підготовка з питань кодексу поведінки компанії не ставлять за мету перетворити працівників на експертів щодо конкретного закону чи настанови. Вони створені для підняття рівня свідомої відповідальності й допомогти працівникам зрозуміти, де можна отримати пораду перед тим, як почати діяти.

У компанії Локхід Мартін працівники проходять через комп'ютерне

навчання з питань дотримання, що базується на врахуванні тих функцій, які працівники виконуватимуть під час роботи в організації. Наприклад, нам не потрібно, щоб механік, який працює на збірці літака, проходив підготовку з питань експорту/імпорту, оскільки його повсякденні обов'язки не передбачають знання цього предмету. З іншого боку, всі працівники повинні пройти через курси з питань умов праці, оскільки статус компанії, як контрактора уряду США, вимагає від усіх працівників певного рівня знань у цій сфері. Нарешті, певні особливі умови створюються для тих працівників, які не мають доступу до комп'ютера або мають певні особливі потреби.

Тренінг усвідомлення проводиться щорічно. На відміну від комп'ютерного навчання з питань дотримання, більша частина тренінгу усвідомлення у Локхід Мартін проводиться через особисте спілкування з керівником працівника. Це відбувається так званим «каскадним методом», коли, наприклад, Боб Стівенс, управляючий компанією Локхід Мартін, навчає своїх підлеглих, які, у свою чергу, навчають їхніх підлеглих і так далі, вниз по структурних східцях організації, доки всі працівники не отримають цю підготовку. Курс підготовки зазвичай триває протягом години і ґрунтується на відеосценаріях та обговоренні певних питань.

д. Комунікація

Ефективні етичні програми також докладають значних зусиль для створення інноваційних методів комунікації для того, щоб усі працівники пам'ятали про важливість дотримання етичних стандартів компанії. Компанії використовують дайджести новин, електронні листи, плакати поштові картки та веб-сайти для доведення до працівників важливих повідомлень, які стосуються питань етики і доброчесності, протягом усього року. Креативні способи комунікації привертають увагу працівників часто навіть краще, ніж обов'язкові навчальні курси. Багато компаній у США інтенсивно використовують сучасні технології для розвитку нових засобів доведення етичних повідомлень до своїх працівників. Наприклад, компанії розміщують відеосюжети щодо нестандартних етичних ситуацій на YouTube і потім обговорюють у блогах ці ситуації або поточні події, що стосуються етичних успіхів або невдач.

У Локхід Мартін найбільш популярним методом, яку використовує етична організація, є Хвилина доброчесності. Цей метод – Хвилина доброчесності Локхід Мартін – має вигляд коротких серій відеосюжетів, що надсилаються електронною поштою працівникам Локхід Мартін з метою доповнення щорічного курсу з тренінгу усвідомлення шляхом стимулювання уваги до питань етики, етнічної різноманітності та відповідального лідерства протягом усього року. Локхід

Мартін випускає три серії Хвилин доброчесності протягом кожного року. Вони спеціально підібрані до конкретних ситуацій, які відбуваються на робочих місцях у компанії. Кожна серія висвітлює важливі теми, такі, як належне ведення міжнародного бізнесу, агресивність, конфлікт інтересів, дискримінація та інші випадки невідповідної поведінки працівників. Сценарії демонструються двохвилинними сегментами протягом трьох тижнів. Перші два сегменти закінчуються оголошення про те, що працівників запрошують налаштуватися на перегляд наступного сегменту, який покажуть на наступному тижні і тоді можна буде дізнатися про остаточну розв'язку подій попередніх сегментів.

Спеціальні методи боротьби з корупцією

На основі дієвих етичних програм, які забезпечують, щоб доброчесність була невід'ємною частиною культури компанії, нижче пропонується узагальнений виклад деяких методів, які в Локхід Мартін вважаються ефективними у боротьбі з корупцією:

- Розділи кодексу поведінки, в яких визначені питання протидії корупції, надання й отримання бізнесових стимулів, а також конфліктів інтересів.
- Детальне викладення політики компанії стосовно відкатів, бізнесових стимулів і конфліктів інтересів.
- Керівництво для врахування національних особливостей знаків гостинності, яке встановлює відповідні обмеження для бізнесових стимулів у країнах, де ми проводимо свою діяльність. Це керівництво є легкодоступним для наших працівників.
- Регулярні доповіді вимагаються у всіх випадках бізнесових подарунків, що перевищують ліміти гостинності, вказані у керівництві, та у випадках оплати витрат як прояву гостинності іншої сторони.
- Навчання з питань дотримання і тренінги з питань кодексу поведінки компанії, які тісно пов'язані з практикою антикорупційної діяльності компанії.
- Аудит усіх аспектів наших антикорупційних заходів.
- Ретельне вивчення інформації про всіх представників третьої сторони і консультантів ще до того, як залучати їх до надання послуг. Це включає, як мінімум, вивчення відкритих джерел інформації, перевірку наданих документів, направлення запитів до посольств у цих країнах, а також особисті інтерв'ю.
- Від представників третьої сторони і консультантів вимагається дотримання кодексу поведінки компанії Локхід Мартін «Дотримання стандартів» і, більш конкретно, антикорупційних стандартів Локхід Мартін.
- Домовленості стосовно представників третьої сторони і консультантів є предметом періодичних перевірок, включаючи проведення процедури ретельного вивчення інформації.

2. Політика доброчесності: приклад Європейського оборонного підрядника

Протягом останніх років основні міжнародні компанії прийшли до розуміння того, що суворі етичні стандарти і дотримання міжнародного законодавства повинні бути невід'ємною частиною їх стратегічного бачення. Відповідаючи на основні зміни у глобальному економічному й геополітичному контексті та на зростання глобальних аспектів у їх операціях, компанії змушені були уважно подивитися на те, як вони вирішують окремі питання свого бізнесу, від менеджменту людських ресурсів до маркетингу і продажів, промислових операцій та відносин власності. У 2001 році компанія Талес була однією з перших Європейських компаній, що запровадили власну політику корпоративної відповідальності і таким чином офіційно сприяли цим суттєвим змінам.

Складна, мінлива обстановка

Протягом своєї історії французька компанія Талес успішно адаптувалася до змін у навколишньому середовищі. Поточні трансформації інституційних підвалин, що визначають «суверенітет промисловості» на початку 21 століття, є принаймні настільки ж важливими, як і будь-які інші зміни.

Талес разом із придбаними в інших країнах (Сполучене Королівство, Нідерланди, Австралія тощо) бізнесовими структурами протягом десятиріч діяла у жорстких національних рамках під прискіпливим контролем держави. В якості головного споживача продукції, а часом і співвласника, держава також брала участь у формуванні корпоративної стратегії, фінансуванні науково-дослідних робіт, наданні експортних дозволів та інших аспектах бізнесу.

Тепер, коли Талес стала багатонаціональною компанією, вона вже не діє в єдиних, чітко визначених і послідовних національних рамках, а, скоріше, у стратегічному середовищі з глобальними параметрами. У цьому новому контексті такі завдання, як менеджмент людських ресурсівабо міжнародні бізнесові операції, стають як ніколи складними.

Незважаючи на отриманий глобальний статус, бізнес цієї компанії продовжує покладатися на технології, які є чутливими, стратегічними і принциповими для національного суверенітету кожної держави. Це структурне проти-

річчя створює багато викликів і для транснаціональних компаній, і для їх контролерів, а також заохочує до прийняття інших методів менеджменту, які ґрунтуються на інноваційних концепціях корпоративного врядування.

Більше прозорості і пунктуальності

На додаток до вже існуючої складності цього міжнародного економічного середовища, міжнародні організації і національні законодавці продовжують створювати нові правила та приймати нові закони, і не завжди послідовно, в той час, як зацікавлені представники громадянського суспільства, разом з неурядовими організаціями, продовжують вимагати нових і вищих стандартів від бізнесового співтовариства.

За відсутності глобальної моделі врядування, самі лише кількість і складність цих різних правил і вимог роблять бізнесове середовище навіть більш нестійким, зокрема, враховуючи ту обставину, що певні «м'які закони» типу кодексів і стандартів, багато з яких мають британське або американське походження, перебувають у складних стосунках з правовими системами інших держав. В умовах зростання глобалізації бізнесу та складного законодавчого і нормативного контексту, створюваного багатьма органами, вимога щодо прозорості постійно зростає, змушуючи компанії запроваджувати набагато вищий рівень відкритості і пунктуальності у своїх бізнесових операціях.

Етичний менеджмент

У той час, як тиск на урядові методи діяльності збільшується у всьому світі, сфера впливу офіційних структур – єдиних органів, що мають повноваження запроваджувати «тверді закони», – поступово звужується, тому що жодний з цих твердих законів не може бути адекватним економічним реаліям довгий час. Часті перегляди та внесення змін потрібні для того, щоб підтримувати закон у належній відповідності, однак, чим більше їх переглядають, тим більше закони можуть стати розпливчастими. В результаті серед законодавців спостерігається зростаюча тенденція вкладати в закони лише основні законодавчі принципи, залишаючи на розсуд компаній визначення їх власних кодексів, основ і стандартів етичної поведінки. Концепція етики і корпоративної відповідальності починається там, де закінчується закон.

Зміни у середовищі управлінської діяльності накладають більшу відповідальність на компанії, безпосередньо впливаючи на їх менеджерську діяльність та моделі бізнесу. Декілька років тому компанія Талес запровадила всеохоплюючу політику з питань етики й корпоративної відповідальності, яка стала частиною загальних зусиль адаптації до нових умов. В умовах жорсткого нормативно-правового поля від менеджерів постійно вимагається робити вибір щодо застосування різних стандартів. Вони зобов'язані знаходити баланс між мінімальними і оптимальними зусиллями, орієнтуючись на можливі варіанти забезпечення стійкого зростання бізнесу та збільшення його дохідності упродовж довгого часу. Ці пошуки вибору є ключовою частиною відповідальності менеджера, і вони стають ще важчими, коли число задіяних учасників збільшується, а їх вимоги стають більш конкретними.

Менеджмент також має зрозуміти і врахувати моральні очікування всіх працівників компанії, вихованих у різних культурних середовищах, а їх традиції відрізняються тим більше, чим більше компанія розширює свої закордонні представництва. Щоб ефективно управляти компаніями у контексті глобалізації, важливо рухатися від очікувань до конкретики, від усних традицій до письмових правил, від самочинного прийняття рішень до поведінки, керованої прийнятним передовим досвідом. Тобто, виникла нова парадигма менеджменту.

Менеджмент ризиків

Будь-який бізнесовий проект пов'язаний з певною долею ризику. Водночас, широке розповсюдження чутливих технологій по всьому світу, зростання складності нормативно-правових актів, нові вимоги в суспільствах та як ніколи інтенсивна конкуренція роблять справу визначення та менеджменту ризиків важливою як ніколи. На додаток, питання цивільної і кримінальної відповідальності компаній та їх керівництва все частіше виявляються у центрі уваги, оскільки бізнесовий світ стає все більш залежним від сфери діяльності судової влади.

Як наслідок, а також з огляду на специфіку своєї основної діяльності, корпоративна відповідальність у компанії Талес ґрунтується не лише на поглибленому аналізі ризиків недотримання, але й на правилах етичної поведінки й доброчесності, за виконанням яких слідкує вище керівництво компанії, яке з цього приводу регулярно спілкується з усіма працівниками.

Такий підхід посилює усвідомлення менеджментом важливості відповідних питань і забезпечує в межах всієї компанії клімат постійного вдосконалення, який визначає подальший розвиток вже сформованих підходів.

Управління процесами

У Талес вважають, що відповідальне ставлення до бізнесової діяльності означає, в першу чергу й понад усе, дотримання правил міжнародної торгівлі та, зокрема, вжиття заходів щодо попередження експорту чутливих технологій і озброєнь та військової техніки до визначених ризикованих країн, щоб таким чином допомогти знайти відповіді на виклики розповсюдження зброї масового ураження та глобального тероризму. Процедури внутрішнього контролю посилюються по всій компанії з метою боротьби з корупцією настільки ефективно, наскільки це можливо, зокрема, у тих секторах, де відбуваються фінансові транзакції на значні суми, а також у випадках взаємодії з країнами, що відрізняються низькими етичними стандартами.

Жорсткі процедури попередження корупції

Добре опрацьований пакет директив і жорсткі процедури делегування відповідальності допомагають забезпечити дотримання національного та міжнародного антикорупційного законодавства. Зокрема, було вжито заходів з метою недопущення самостійного започаткування оперативними підрозділами стосунків по контракту з агентами або зовнішніми структурами з метою полегшення міжнародних бізнесових операцій. Всі структури, що забезпечують підтримку експортних продаж і маркетингових зусиль оперативних підрозділів, перебувають під керівництвом визначених організацій, у даному випадку Талес Інтернешнел. Лише ці організації мають акредитацію від компанії для супроводження зазначених складних питань у жорстких нормативних рамках. Така політика покращує ефективність продажів і маркетингових зусиль Талес, а також забезпечує неухильний моніторинг дотримання під час виконання міжнародних комерційних операцій.

Зазначені процедури і директиви стосуються всіх, хто надає зовнішні послуги, включаючи окремих осіб, консультативні фірми і компанії, які підтримують Талес в операціях з маркетингу й продажу, що виконуються як з державними, так і з приватними замовниками. Консультанти повинні мати визнаний експертний статус у сфері своєї діяльності на регіональному та міжнародно-

му рівнях. До них застосовуються суворі процедури: обов'язкове заповнення анкети, надання копій реєстраційних документів компанії та всіх інших офіційних документів, зокрема, щорічних доповідей, а вище керівництво повинно взяти зобов'язання дотримуватися всіх вимог законодавства стосовно етичної поведінки у міжнародній торгівлі. Вся ця інформація аналізується й підтверджується зовнішнім органом. Підозра у наявності чинників ризику виникає тоді, коли отримана інформація потребує більш глибокого дослідження, а також звертання до менеджера вищого рівня для прийняття рішення. Певні типи інформації класифікуються як неприйнятні і призводять до негайної зупинки процесу відбору. Оплата цих послуг також є предметом жорстких процедур. Наприклад, операції не можуть проводитися на адресу фінансової установи, зареєстрованої в офшорі, а всі виплати повинні чітко відповідати реально наданим послугам і точно відображати наданий тип послуги.

Всі ці процедури викладені у Настанові з передового досвіду, яку розробило й затвердило корпоративне керівництво Талес. Відбувається процес постійного вдосконалення з метою підвищення дієвості процедур та заходів їх дотримання.

Напрацювання передового досвіду

Компанія ризикує програти конкурентам, які здатні забезпечити відповідність мінімальним законодавчим вимогам і при цьому вирішувати менше етичних дилем. Тому потрібно застосовувати єдині підходи в усьому секторі для розроблення і прийняття загальних стандартів в якості передового досвіду всіма компаніями, щоб таким чином зрівняти умови для всіх учасників.

Талес брав участь у започаткуванні саме такої ініціативи в рамках Європейської асоціації аерокосмічної та оборонної промисловості (Aerospace and Defence Industries Association of Europe – ASD).

Етика й корпоративна відповідальність у компанії Талес

Корпоративний менеджмент Талес визнає, що ефективна політика дотримання повинна виходити за межі міжнародних маркетингових операцій та продажів і має включати всі операції компанії. Політика Талес щодо етики й корпоративної відповідальності викладена у Кодексі етики, екземпляр якого видається кожному працівникові, а також у декількох загальних процесах і процедурах компанії з питань комерції, навколишнього середовища, праці та соціального забезпечення. Також було створено відповідну систему, в якій Комітет з питань етики й корпоративної відповідальності формулює політику Талес, а визначений корпоративний департамент відповідає за імплементацію цієї політики. Місцева імплементація – на рівні підрозділу та на рівні країни – забезпечується через мережу посадовців з питань етики.

Водночас, широкомасштабні кампанії з питань усвідомлення, інформування і навчання, у т.ч. програма дистанційної освіти, були розроблені для підтримки зусиль із залучення працівників компанії та забезпечення такого стану, коли всі працівники поділяють етичні цінності компанії.

3. Подальші заходи з поліпшення стану доброчесності в оборонній промисловості

Нещодавно основні підрядники у Західній Європі і Північній Америці почали демонструвати прогрес у прийнятті та забезпеченні дотримання кодексів етики й стандартів нетерпимості до проявів корупції у всіх її формах. Промислові асоціації стали ретельніше ставитися до підведення підсумків і покращання промислових стандартів. У Вставці 20.2 пропонується приклад діяльності в рамках Європейської асоціації аерокосмічної та оборонної промисловості.

Звертаючись до пропонуючої сторони корупції, основні підрядники і асоціації оборонної промисловості мають намір продовжувати оцінювання й намагатися підвищити ефективність кодексів і стандартів доброчесності, залучити постачальників оборонної продукції, включаючи малі та середні підприємства, а також розширити географічне покриття таких підходів. Рівні умови і справедлива конкуренція можуть бути гарантовані лише через застосування послідовних і гармонізованих стандартів серед усіх компаній-експортерів.

Основні оборонні підрядники також повинні забезпечувати, щоб субпідрядники, оборонні консультанти, а також всі інші посередники, яких вони залучають, дотримувалися такого самого кодексу етики, що й самі основні підрядники. Лише забезпечивши повний контроль «ланцюга постачання» вони можуть переконливо стверджувати, що запропонований ними продукт є вільним від корупції.

Вставка 20.2. Діяльність з питань етики й боротьби з корупцією в

Європейській асоціації аерокосмічної та оборонної промисловості У 2006 році управляючі компаніями, які входять до Ради Асоціації, підтвердили свою постійну підтримку зусиль зі створення вільного від корупції ринку продуктів оборонної промисловості, таким чином дозволяючи всім учасникам міжнародного ринку конкурувати в рівних і справедливих умовах.

Промисловість заявила про взяті на себе зобов'язання дотримуватися правил, упроваджених у національне законодавство на виконання Конвенції ОЕСР 1997 року з питань боротьби з хабарами для іноземних посадових осіб під час міжнародних бізнесових операцій, а також на виконання інших відповідних законів. Асоціація створила Робочу групу з питань етики і боротьби з корупцією. Ця група провела спеціальні навчання для оцінки існуючих підходів серед компаній-учасників. Внутрішні кодекси етики цих компаній було проаналізовано незалежним юристом, який також очолює Комісію з боротьби з корупцією Міжнародної Торговельної Палати (МТП).

У результаті цієї діяльності було створено «Загальні промислові стандарти для Європейської аерокосмічної промисловості і оборони», затверджені у квітні 2007 року. Члени Асоціації з числа національних асоціацій отримали пропозицію затвердити стандарти, а компанії-учасниці – підписати Заяву компанії про дотримання. З жовтня 2008 року затвердження стало обов'язковим і тепер, для того, щоб заохотити й переконати компанії затвердити стандарти, здійснюється постійний моніторинг прогресу із застосуванням відповідних індикаторів.

За підтримки Міжнародної Торговельної Палати, Асоціація сприяє ініціативам з розширення географії своєї етичної та антикорупційної діяльності за межами країн-членів ОЕСР.

Джерела: *Aerospace and Defence Industries Association of Europe, Annual Report 2007 (Brussels: ASD, 2008), 20, www.asd-europe.org; Стандарти «Common Industry Standards for European Aerospace and Defence» також є на сайті: www.asd-europe.org/Objects/2/Files/WEB Common Industry Standards.pdf.*

Урядам рекомендується допускати до фінальної частини тендерних процедур лише тих учасників, які прийняли загальні стандарти оборонної промисловості з питань доброчесності і боротьби з корупцією. Крім цього, вони повинні відсікати тих постачальників оборонної продукції, які застосовували корупційні методи для отримання контрактів, і ділитися цією інформацією з урядами інших країн. У такому разі від асоціацій оборонної промисловості очікується, що вони повинні позбавляти порушників статусу членства.

Такі міжнародні організації, як НАТО, можуть сприяти розробці ефективної, збалансованої і всеохоплюючої стратегії з метою зміцнення доброчесності у сфері оборонних постачальників.

Вони також можуть заохочувати до більшої прозорості в оборонній промисловості, включаючи прозорість власності, а також підтримувати постачальників оборонної продукції у виконанні ними вимог доброчесності.

Лише співробітництво між урядами й постачальниками, міжурядовими організаціями й промисловими асоціаціями може перетворити оборонні компанії в надійних союзників у спільній боротьбі проти корупційного потенціалу в секторі оборони.

Розділ 21
Роль громадянського суспільства і засобів масової інформації

Вступ

Цей розділ розглядає ту надзвичайно важливу роль, яку громадянське суспільство і засоби масової інформації (ЗМІ) відіграють у вихованні доброчесності та зниженні рівня корупції у секторі оборони та безпеки. Головним чином, він розглядає питання «виховання доброчесності» через призму реформи сектору безпеки, тобто концепції, яка виникла у 1990х роках у відповідь на визнання того факту, що розвиток і безпека є двома сторонами однієї медалі і що зусилля з покращення безпеки мають докладатися в рамках зміцнення демократичного й ефективного врядування. По своїй суті ефективне врядування має бути зосередженим на потребах людей, справедливим, підзвітним і прозорим. Воно передбачає широке залучення і консультації на етапах планування та прийняття рішень, ефективний і економічний менеджмент державного сектору, а також активне залучення і сприяння участі громадянського суспільства. Іншими словами, ефективне врядування легітимізується за рахунок процесів, у яких приділяється значна увага антикорупційним зусиллям та підзвітності. Воно акцентує увагу на ефективному й економічному використанні ресурсів і заохочує активне залучення приватного сектору до взаємодії з питань важливих інтересів. *(Hans Born, Philipp H. Fluri and Simon Lunn, eds., Oversight and Guidance: The Relevance of Parliamentary*

Oversight for the Security Sector and its Reform. Збірка статей з фундаментальних питань парламентського контролю над сектором безпеки (DCAF/NATO Parliamentary Assembly, January 2003), Glossary, 240–241.)

У 2004 році Комітетом з питань підтримки розвитку Організації з економічного співробітництва і розвитку (ОЕСР) було запропоновано аналітичну доповідь, з висновками і пропозиціями якої погодились усі члени Організації. Зокрема, у доповіді наголошувалося, що потрібно «переглянути ставлення до безпеки і зрушити дискусію з позицій реалізму до більш всеохоплюючого і кооперативного підходу». *(Комітетом з питань підтримки розвитку ОЕСР (OECD Development Assistance Committee), Security System Reform and Governance: Policy and Good Practice (Париж: ОЕСР, 2004 р.)* Цей комітет ОЕСР визначив реформу сектору безпеки як «трансформацію системи безпеки (яка включає учасників, їх ролі, відповідальність і дії) шляхом спільних зусиль, направлених на створення такого менеджменту і такого типу діяльності системи, які більш суттєво відповідали б демократичним нормам і ключовим принципам ефективного врядування, що дозволило б створити набагато кращі умови діяльності у безпековому середовищі». *(OECD, Security System Reform and Governance: A DAC Reference Document (Париж: OECP, 2005 p.), www.oecd.org/dataoecd/8/39/ 31785288.pdf.)* Отже, намагаючись створити «інституційну культуру доброчесності» (Розділ 24), треба мати на увазі, що не потрібно видумувати ще одне концептуальне колесо – цілі й стандарти, визначені у згаданій доповіді комітету ОЕСР для реформування сектору безпеки, вже є доволі прийнятними. А чого не вистачає, так це, головним чином, ефективного запровадження багатьма урядами існуючих стандартів, особливо з питань прозорості й підзвітності, *(У цьому контексті «підзвітність» головним чином означає «під-відповідальність» – у тому сенсі, що мова йде про зобов'язання відповідати на запитання про те, що робиться, що буде робитися і чому. Це визначення використовується групою авторів у аналітичній доповіді Світового банку, див.: William Byrd and Stephane Guimbert in The World Bank, "Public Finance, Security, and Development: A Framework and an Application to Afghanistan", Policy Research Working Paper 4806 (The World Bank South Asia Region Poverty Reduction, Economic Management, Finance and Private Sector Development Department, January 2009), сноска 11.)* а також повного використання потенційного внеску ключових учасників, особливо громадянського суспільства.

Оскільки ситуація у сфері реформування сектору безпеки протягом останніх років помітно змінювалася, громадянське суспільство відігравало важливу роль у забезпеченні цілісності такого підходу, і, окрім цього, серед багатьох країн і в Організації Об'єднаних Націй спостерігається зростаючий рівень визнання того, що неурядові учасники, ЗМІ та парламентарі можуть виконувати важливі функції цивільного контролю і моніторингу. Самі лише парламентарі не можуть гарантувати ефективний контроль та забезпечити підзвітність уряду з питань всіх рішень і діяльності у секторі безпеки, оскільки у них недостатньо часу, ресурсів і навичок, щоб це робити.

Як зазначається в доповіді комітету ОЕСР, «залучення громадянського суспільства до програм реформування сектору безпеки є передумовою для створення більш широкої і всеохоплюючої місцевої бази реформ, а отже й для довготривалості зусиль». *(OECD, OECD DAC Handbook on Security System Reform: Supporting Security and Justice (2007).* Як уже зазначалось у попередніх розділах цього видання *(Див., наприклад, розділи 5 і 6 про національні підходи та офсетні механізми, відповідно. Обидва автори аргументують, що організації громадянського суспільства відіграють важливу роль у забезпеченні прозорості й підзвітності.)*, незалежний контроль з боку організацій громадянського суспільства та ЗМІ є необхідним елементом виховання доброчесності, а також відіграє принципову роль у ефективній імплементації ініціатив з реформування сектору безпеки, направлених на зміцнення ефективного врядування в оборонних відомствах і обмеження корупційних ризиків.

Однак, загалом, практична роль організацій громадянського суспільства і ЗМІ в питаннях реформування сектору безпеки та виховання доброчесності є доволі обмеженою, причому, не лише в нестійких державах або тих, які перебувають у стадії трансформацій (часто з причин природи авторитарних режимів та слабкості громадянського суспільства), але також й у більш демократичних суспільствах і особливо всередині НАТО (де можливості для залучення громадянського суспільства у певних випадках залишаються обмеженими, про що буде сказано нижче). Цей розділ має на меті сприяти стимулюванню обговорення причин зазначеного стану, а також того, що потрібно зробити для зміцнення ролі громадянського суспільства і ЗМІ у моніторингу й реформуванні оборонних відомств.

Він починається з розгляду ролі окремо громадянського суспільства і ЗМІ, а також труднощів з тим, як відігравати ці ролі в рамках трьох конкретних сценаріїв: в нестійкій державі, в державі у стадії трансформації та всередині НАТО. Розділ завершується пропозиціями стосовно можливих варіантів і рекомендацій щодо захисту й посилення здатності громадянського суспільства і ЗМІ у вихованні доброчесності й зниженні рівня корупційного потенціалу в оборонних відомствах.

Роль громадянського суспільства

Дієве громадянське суспільство є ключовою вимогою до демократії. Воно має потенціал створювати противагу потужності держави, чинити опір авторитаризму і, завдяки своєму плюралізмові, не дозволити, щоб держава контролювалася приватними інтересами. Протягом останніх десятиліть політичний простір у багатьох частинах світу, а не лише в розвинутих демократіях, набув більшої відкритості завдяки розвитку і розширенню діяльності груп громадянського суспільства. Не існує єдиного погодженого визначення громадянського суспільства.

У зазначеній вище доповіді комітету ОЕСР «громадянське суспільство» визначається як «політичний простір між особистістю і урядом, виражений через членство в неурядових організа-

ціях (НУО), соціальних групах, асоціаціях та інших організаціях і мережах. Організації громадянського суспільства включають НУО на національному рівні, місцеві організації, релігійні групи, професійні групи та групи за інтересами, такі як профспілки, ЗМІ, приватні бізнесові компанії, асоціації правників, групи захисту прав людини, незалежні консультанти, університети і незалежні дослідницькі організації». *(OECD, OECD DAC Handbook on Security System Reform.)*

«Група видатних особистостей» при Генеральному Секретареві ООН стосовно відносин між ООН та громадянським суспільством пропонує більш вузьке визначення громадянського суспільства як такого, що включає асоціації громадян (поза межами сім'ї, друзів, уряду і бізнесу), що зв'язали себе добровільними відносинами задля просування своїх інтересів, ідей та ідеологій. *(Див. документ Генеральної Асамблеї Організації Об'єднаних Націй: United Nations General*

Assembly, We the Peoples: Civil Society, the United Nations and Global Governance: Report of the Panel of

Eminent Persons on United Nations-Civil Society Relations, A/58/817 (New York, 11 June 2004), 13.) Однак, у цьому розділі в якості вихідних даних для обговорення питань громадянського суспільства досліджуються три секторальні моделі, в яких держава розглядається як сукупність уряду, ринку і громадян. У цьому контексті громадянське суспільство належить до третього сектору, і воно існує паралельно та у взаємодії з державою і прибутковими організаціями (включаючи й ЗМІ) у формі соціальних рухів, НУО, релігійних органів, груп захисту прав жінок і молоді, організацій підтримки корінного населення, професійних асоціацій, науково-дослідних центрів, союзів тощо, які здійснюють діяльність в межах окремої країни або у міжнаціональному просторі.

Таке визначення громадянського суспільства виключає прибутковий бізнес (у тому числі більшість основних ЗМІ) та організації, що представляють урядовий сектор. Водночас, як стане ясно пізніше, кордони між цими трьома секторами стають все більш розмитими. Відбувається певне перетинання, наприклад, між функціями організацій громадянського суспільства, приватним бізнесом і ЗМІ, особливо у випадку зростаючого використання неурядовими організаціями так званих «нових медіа» *(Термін «нові медіа» означає ті ЗМІ, які почали широко використовувати нові цифрові технології, а також комп'ютеризовані або мережеві та комунікаційні технології, такі як Інтернет або веб-сайти, у період наприкінці 20-го сторіччя. Відповідно, до «старих медіа» відносять телевізійні програми, художні фільми, журнали, книги та паперові публікації.)*, щоб здійснювати роль захисників та моніторинг. У наступних параграфах розглядається питання про те, чому громадянське суспільство має відігравати таку роль у вихованні доброчесності та зниженні рівня корупції у сфері оборони, що саме включає ця роль, поточний досвід реформування сектору безпеки і сучасні проблеми діяльності НУО.

Громадянське суспільство і «нова дипломатія»

Громадянське суспільство складається з суміші організацій і рухів, що мобілізують соціальну енергію для того, щоб голосно заявляти про свої принципові цінності й переконання. *(L. David Brown, Creating Credibility: Legitimacy and Accountability for Transnational Civil Society (Sterling, VA: Kumarian Press, 2008), 1.)* НУО є серцевиною громадянського суспільства. Вони можуть бути (але можуть і не бути) засновані на формальному членстві або формально зареєстровані, однак, як правило, вони незалежні від урядів і політичних партій, а також часто фінансуються з незалежних джерел. Вони беруть участь у наданні суспільних послуг (безпека також є важливою послугою, яку потрібно надавати), *(Безпека як суспільна послуга має певні специфічні ознаки, які визначають спосіб надання цієї послуги та варіанти підзвітності й організацію фінансування. Моніторинг діяльності тих, хто надає послуги з безпеки, може бути нелегким, оскільки структури безпеки озброєні й потенційно можуть загрожувати цивільним спостерігачам. При цьому рівень готовності цих структур у мирний час буває важко оцінити, а критерії оцінки часто можуть викликати незгоду з отриманими результатами. Для більш детального ознайомлення див. дискусію: William Byrd and Stephane Guimbert in The World Bank, "Public Finance" (January 2009).* політичному сприянні та розвитку, заходах громадської освіти та інших формах неприбуткової діяльності, і можуть суттєво відрізнятися за розмірами – від величезних міжнародних структур на зразок Транспаренсі Інтернешнел, до якої входять понад 2,2 мільйони членів та підписувачів у понад 150 країнах і регіонах, до невеликих місцевих самодіяльних організацій. Стосовно ж дослідницьких інститутів, то вони можуть бути або НУО, або центрами академічної науки, незалежними від влади, або, навпаки, бути пов'язаними з урядом, наприклад, через державне фінансування або залучення колишніх міністрів та інших офіційних осіб (або в якості членів, або співробітників).

У минулому стосунки між НУО та органами державної влади багато в чому були напруженими або по-справжньому ворожими. У багатьох частинах світу вони такими залишаються й сьогодні (або знову повертаються до цього стану, як про це буде сказано пізніше). Однак, за останні два десятки років з ряду питань та у зростаючій кількості місць (включаючи майже всю Європу і обидві Америки, значну частину Південної Азії й Африки, а також у окремих місцях на Близькому Сході) ці стосунки змінилися – від конфлікту до зростаючого співробітництва. Деякі коментатори охарактеризували конструктивні стосунки між НУО та владою як «нову дипломатію». *(David Davenport, "The New Diplomacy, Policy Review 116 (December 2002 & January 2003).* До певної міри це стало результатом зростаючого розуміння багатьма урядами того, що важливі складові національної безпеки й стабільності забезпечуються шляхом посилення ролі людської складової безпеки (human security). *(Традиційною метою «національної безпеки» завжди була оборона держави від зовнішніх загроз. І навпаки, фокусом безпеки людини є захист окремих осіб. Див.: Human Security Brief 2006 (University of British Columbia, Human Security Centre).*

Контроль оборони з боку громадянського суспільства

У контексті основної теми цього видання представники громадянського суспільства – головним чином вузьке коло НУО та дослідницьких інститутів – можуть (і в окремих, обмежених випадках уже це роблять) підтримувати співпрацю з владою, парламентами і суспільством у п'ять основних способів:

- Освіта суспільства і сприяння зростанню усвідомлення: Попередження суспільства про депресивну ціну корупції, як це описано у Розділі 1, і, відповідно, мобілізація підтримки ініціатив державної влади та міжнародних зусиль з виховання доброчесності, підвищення прозорості та покращення підзвітності є принциповими видами діяльності НУО (та ЗМІ). Головною метою сприяння зростанню усвідомлення є забезпечення того, що імплементація внутрішніх зусиль з реформування сектору безпеки буде сприйматися як сучасний, але довгостроковий процес, і що суспільство усвідомить пов'язаність цього питання з власними інтересами та інтересами окремих громад. НУО успішно використовували свій статус активної причетності та застосовували стратегію «називай і засуджуй» в якості засобу прямої дії проти специфічних випадків і порушень.

- Діючи в якості каталізаторів та посередників: НУО та інші організації громадянського суспільства, такі як аналітичні центри, університети і науково-дослідні інститути, можуть відігравати посередницьку або «мостобудівну» ролі. У цьому контексті Женевський центр демократичного контролю над збройними силами (ДКЗС) й організація Транспаренсі Інтернешнел протягом більш ніж десяти років були двома провідними джерелами світла,

які зробили величезний внесок у розвиток парламентської компетентності та формування відповідних спроможностей шляхом підготовки аналітичних доповідей і проведення курсів підготовки й семінарів. Багато груп громадянського суспільства з Латинської Америки, а також Центральної та Східної Європи наприкінці 1980х і протягом 1990х років також відігравали важливу роль у налагодженні діалогів у час, коли щойно обрані цивільні уряди починали реструктуризацію своїх збройних сил. Ці діалоги спочатку допомогли зруйнувати ізольованість збройних сил і відкрили дорогу до професійних дискусій між представниками громадянського суспільства, обраними посадовими особами та військовим командуванням. Однак, загалом, до спілкування має бути залучено більше представників громадянського суспільства, особливо у нестійких державах і таких, що перебувають на стадії трансформації, для того, щоб бути посередниками між владою (особливо – їх оборонними відомствами) та певними секторами суспільства, які є або байдужими, або потенційно антагоністичними до уряду.

- Підтримання кількісного рівня експертного та інтелектуального середовища: Значна кількість різних місцевих НУО та організацій громадянського суспільства створили умови для зростання кількості груп експертів і окремих активістів, які мають необхідні знання й навички з питань методологій, необхідні для реформування сектору безпеки та реформи ефективного врядування. Наприклад, НУО співпрацювали з військовими з питань підвищення безпеки зберігання небезпечних речовин, надавали поради щодо розвитку програм маркування зброї та її пошуку, а також відігравали критичну роль у пост-конфліктному роззброєнні, програмах демобілізації та реінтеграції. Незважаючи на те, що іноді наявність достатніх знань та потрібного персоналу може бути замалою у деяких специфічних випадках стосовно потреб сектору оборони, про які йдеться у Частині II цього видання, проте вони однаково існують і потенційно можуть бути затребувані національними урядами або міжурядовими організаціями для того, щоб підтримати ініціативи з питань протидії корупції та недолікам у сфері оборони. Наявність більш глибоких знань з питань реформування сектору безпеки може допомогти налагодженню ефективного врядування, а також використанню спеціальних знань однієї сфери у менеджменті сектору оборони. Водночас, незважаючи на те, що певне обмежене використання досвіду й технічних знань відбувається, наприклад, під час парламентських слухань, але загалом цей ресурс використовується мало. Також суттєвим чинником є недостатня довіра з обох сторін і конкуруючі пріоритети в умовах обмежених ресурсів для різних НУО у гуманітарній сфері, захисті прав людини та сфері розвитку.

- *Проведення важливих досліджень і формування пропозицій до політичного курсу:* Одним з найбільш вагомих внесків організацій громадянського суспільства є дослідження і документування стану так званого «прокляття корупції» (Розділ 1), від викриття недоліків і протиріч у процесі прийняття рішень щодо застосування збройних сил – у контексті як рішення про участь у вже триваючому конфлікті, так і рішення про початок проведення воєнної операції – до недоречних, неефективних та іноді незаконних способів оборонного менеджменту, закупівель і експорту. Шляхом покращення розуміння цих питань в суспільстві та органах державної влади, громадянське суспільство і ЗМІ відіграють важливу роль у створенні можливостей для формування адекватних відповідей. З такими дослідженнями тісно пов'язана діяльність аналітичних НУО та дослідницьких інститутів, які намагаються запропонувати нові підходи і стратегічні варіанти у справі виховання доброчесності та зниження рівня корупції у сфері оборони. Така робота включає порівняння найкращого досвіду різних регіонів світу, розробку нових підходів та висування практичних пропозицій стосовно зміни існуючих підходів.

- *Проведення моніторингу:* З моменту, коли політика щодо реагування на «прокляття корупції» буде прийнята урядом, НУО також отримують важливу роль працювати «сторожовим псом» – проводити моніторинг імплементації рішень політиків та відслідковувати діяльність уряду на предмет будь-яких недоліків і провалів, які можуть трапитися. При цьому НУО, особливо національні та міжнародні організації захисту прав людини, такі, як Міжнародна Амністія і Товариство захисту прав людини, відіграють важливу роль у моніторингу діяльності структур безпеки та збройних сил з метою попередження порушень ними прав людини і міжнародного гуманітарного права.

Нижче буде обговорюватися та обставина, що на шляху до виконання громадянським суспільством своєї ролі існує багато труднощів і перешкод. Як мінімум ефективні уряди й парламенти мають забезпечити доступ до всіх відповідних політичних документів, а також стимулювати існування і функціонування незалежного третього сектору, включаючи контроль сектору оборони. Одним із дієвих шляхів досягнення останнього є, наприклад, залучення незалежних аналітичних структур, дослідницьких інститутів, університетів та НУО до проведення досліджень і аудиту у специфічних сферах сектору безпеки та оборони (наприклад, з питань злочинності, закупівель і кадрової політики). Однак, якщо громадянське суспільство повинне відігравати певну активну роль у питаннях виховання доброчесності та, особливо, у заохоченні альтернативних обговорень серед громадян, то незалежні НУО повинні бути здатними залучати й утримувати необхідний рівень експертної думки, яка має забезпечувати добре поінформовані погляди на урядову політику з питань безпеки, оборонний бюджет, закупівлі та варіанти використання ресурсів. На сьогодні потрібний рівень експертних знань є недостатнім навіть у розвинутих демократіях і потребує більше зусиль для підвищення спроможностей і більшого бажання спонсорів їх фінансувати.

Представники громадянського суспільства були особливо активними протягом десятків років у розповсюдженні принципів міжнародного законодавства, як це вбудовано у Хартію ООН та інші багатосторонні угоди й інституції. Багато країн бачать у них можливість отримання підтримки та надійного партнерства. Громадські рухи та НУО стали головними захисниками інтересів громадян у багатьох сферах, включаючи права людини, навколишнє середовище, розвиток, демократичне врядування та попередження конфліктів. Вони надавали допомогу у поширенні міжнародних норм і договорів, а також допомагали сформулювати основоположні моральні та політичні стандарти, які пізніше були покладені в основу політики й актів законодавства.

Приклади дієвих рухів громадянського суспільства включають боргову кампанію «Ювілей 2000», яка переконала уряди країн «Великої сімки» скасувати $100 мільярдів доларів боргів бідних країн, Оттавську кампанію із заборони протипіхотних мін, *(Див., наприклад: Kenneth Anderson, "The Ottawa Convention Banning Landmines: the Role of International Non-Governmental Organizations and the Idea of International Civil Society", European Journal of International Aff airs 2:1 (2000),* а також опозицію до вторгнення коаліції під проводом США на територію Іраку у 2003 році. Також НУО відіграли принципову роль у створенні Міжнародного кримінального суду, прийнятті рішення щодо доповнення додаткового протоколу до Конвенції з прав дитини (визначивши поза законом призов на військову службу дітей віком до 18 років), а також просування заходів боротьби з розповсюдженням стрілецької зброї.

Громадянське суспільство та реформування сектору безпеки

Завдяки процесові, очолюваному Міністерством міжнародного розвитку Сполученого Королівства та Директоратом розвитку і співробітництва ОЕСР, у 2007 році було розроблено по-

сібник, який мав забезпечити «керівництво з питань запровадження рекомендацій ОЕСР щодо реформування сектору безпеки, а також закрити розрив між рішеннями, що приймаються, і реальною практикою». *(OECD DAC Handbook on Security System Reform (OECD, 2007).*

Стосовно залучення громадянського суспільства до реформування сектору безпеки посібник наголошує, що «організації громадянського суспільства можуть виступати в ролі отримувачів допомоги, неформальних контролерів, партнерів та захисників реформ, а також надавати послуги.

Допомога у реформуванні сектору безпеки також може бути надана міжнародними представниками громадянського суспільства, які можуть відігравати важливу роль у створенні спроможностей, а також у розробці, захисті, виконанні, моніторингу та оцінці реформ». *(Там само, с. 226.)*

НУО пропонують підходи знизу, які часто бувають більш доречними й ефективними, ніж заходи, що ініціюються зверху, наприклад, шляхом організації каналів комунікації з місцевими громадами, з якими держава часто має обмежений контакт чи обмежений вплив на них. Посібник також наголошує, що:

Програми реформування сектору безпеки повинні включати глибокий аналіз контексту, ролі й позицій організацій громадянського суспільства, оскільки їх спроможності, ефективність та рамки діяльності суттєво відрізняються у різних країнах. Оцінки стосовно громадянського суспільства повинні брати до уваги всю сукупність місцевих учасників, а не лише тих, хто «визнається» державою, і виділяти тих, хто щиро зосереджений на покращенні безпеки бідних, жінок, дітей і молоді, а також інших груп, які часто бувають виключені з дискусій на теми безпеки. *(Там само.)*

Окрім цього, у посібнику дискутуються можливі сфери залучення громадянського суспільства, такі як миротворчі процеси, національні бюджетні процеси та огляди безпеки і оборони. Теоретично, громадянське суспільство може виконувати багато важливих функцій, зокрема: моніторинг заходів, що стосуються безпеки й оборони; дослідження ефективності заходів боротьби з тероризмом на предмет того, чи вони передбачають дотримання прав людини та принципів верховенства права; контроль діяльності збройних сил, правоохоронних органів та інших структур безпеки й оприлюднення порушень законодавства і визначених підходів, або негативних наслідків у разі прийняття неадекватних законів і підходів; проведення досліджень щодо вірогідних корупційних та інших зловживань; підготовка пропозицій з питань поліпшення заходів реформування сектору безпеки. Однак, на практиці, організації громадянського суспільства часто бувають відсунуті на консультативні ролі, *(Див.: Daniel Bendix and Ruth Stanley, "Deconstructing Local Ownership of Security Sector Reform: A Review of the Literature", African Security Review 17:2 (June 2008): 93–104.)* а високопарні принципи, які проголошуються в посібнику, постійно ігноруються.

Навіть наявність активного громадянського суспільства не є чарівною паличкою або гарантом успіху. Наприклад, напередодні геноциду 1994 року в Руанді, країна мала один з найбільш розвинутих в Африці неурядових секторів, однак її суспільство було роз'єднаним за етнічною ознакою і швидко опустилося до насилля і хаосу. *(Більшість НУО в Руанді у 1994 році були щойно створеними, майже повністю залежними від зовнішніх донорів і держави, причому, там було дуже мало програм стримування расизму та етнічної ненависті. Див.: Peter Uvin, Aiding Violence: The Development Enterprise in Uganda (West Hartford, CT: Kumarian Press, 1998),164–176.)*

Реакція проти НУО?

Той ентузіазм до громадянського суспільства, який виник наприкінці 1980х та у 1990х роках після падіння Берлінської стіни й поширення демократичних режимів, згідно з окремими дослідженнями, змінюється протягом останніх років на реакцію протидії на багатьох рівнях і фронтах. Ця реакція відбувається в діапазоні від поновлених, систематичних репресій проти громадянського суспільства в авторитарних державах, з одного боку, до більш загального ставлення під сумнів неупередженості організацій громадянського суспільства, особливо НУО, з іншого боку. *(Jude Howell, et al., "The Backlash against Civil Society in the Wake of the Long War on Terror", Development in Practice 18:1 (2008): 82–93. Стосовно останнього пропонується відмітити, наприклад, нібито невинне речення з Розділу 4 цього Компендіуму: "Відповідальні організації громадянського суспільства повинні розглядатися як партнери і помічники на шляху до спільної мети – інституційної доброчесності" [акцент додано]. Однак, немає схожого визначення для використання при описанні або ідентифікації інших учасників.)*

Громадськість, науковці, рядові активісти, міжурядові організації (МУО), ЗМІ, корпорації та уряди все більш активно ставлять під питання природу повноважень НУО говорити від імені інших громадян та намагатись впливати на внутрішні й міжнародні процеси. (В принципі, це цілком законне запитання, але відповідь на нього лежить за межами змісту цього розділу. *(Для більш глибокого вивчення цього питання див.: Lisa Jordan and Peter van Tuijl, eds., NGO Accountability: Politics, Principles and Innovations (Sterling, VA: Earthscan, 2006); and Jem Bendell, Debating NGO Accountability, UN-NGLS Development Dossier (United Nations, 2006).)* Не можна також не сказати й про те, що питання доброчесності та підзвітності всередині організацій громадянського суспільства й ЗМІ є принциповими передумовами прийнятності для суспільства і влади їхньої контролюючої ролі та статусу провідників потрібних змін.) Мова йде про реакцію, яка лише загострилася після терористичного нападу 11 вересня 2001 року та наступного розгортання глобальної війни проти тероризму. Бачення недержавних структур як загроз національній безпеці призвело до обмежувальних законодавчих і регуляторних заходів, які ускладнили для багатьох НУО можливості діяти вільно й ефективно. *(Наприклад, у США, де ворожість до залучення НУО в питаннях глобального врядування стала визначальною рисою позиції неоконсерваторів, такі обмежувальні підходи визначені в президентському указі №13224, у так званому законі «Патріотичний Акт», та у добровільному антитерористичному фінансовому керівництві для благодійних організацій, виданому міністерством фінансів США. Водночас, схожі регуляторні підходи, направлені на розширення повноважень поліції, розвідки та структур безпеки з питань розслідування діяльності та арешту підозрюваних, причому без суттєвої уваги до контролю судової влади або захисту прав особистості, спостерігалися й у багатьох інших країнах світу.)* НУО, а також організації та рухи, які кидають виклик репресивним режимам, напевне провокують невдоволення представників влади, але протягом останніх років демократичні держави, МУО та транснаціональні корпорації (ТНК) пристосувалися до мови антитероризму для інтенсифікації свого наступу на критиків з боку громадянського суспільства. Негативні наслідки були особливо відчутними у зонах конфліктів та серед груп, які кидають виклик урядовій політиці через свою діяльність у сферах миротворчості, демократизації та прав людини. *(Для більш глибокого ознайомлення з прикладами див.: Alistair Millar with David Cortright, Linda Gerber-Stellingwer and George A. Lopez, Oversight or Overlooked? Civil Society's Role in Monitoring and Reforming Security Systems and the Practice of Counterterrorism, A report to Cordaid from the Fourth Freedom Forum and Kroc Institute for International Peace Studies at the University of Notre Dame (March 2009).* Так, ніби зазначеного вище недостатньо, уряди (та значною мірою й приватний сектор) іноді створюють «авторитетні» НУО, які працюють на підтримку позицій істеблішменту і затруднюють можливість почути справжній голос громадянського суспільства. *(Moises Naim, "What Is a Gongo? How Government-Sponsored Groups Masquerade as Civil Society", Foreign Policy (May/June 2007): 96.)* У декількох виняткових випадках корпорації та уряди ще й заси-

лали «шпигунів» всередину НУО. *(Saeed Shah, "BAE Ordered to Identify 'Mole' Who Passed Details on Arms Protesters", The Independent (27 February 2007); George Monbiot, "A Parallel State", The Guardian (13 February 2007)*. Таким чином, спостерігається напружений сучасний контекст, у якому від громадянського суспільства очікується сприяння у вихованні доброчесності та зниженні рівня корупції у сфері оборони.

Замість того, щоб безперешкодно виконувати свою роль «сторожового пса», численні НУО опинилися під підозрою і стали предметом підвищеного моніторингу їхньої діяльності з боку держави й приватного сектору.

Роль засобів масової інформації

Принциповою контролюючою функцією журналістів є викриття порушень і недостойної поведінки.

Поза цим механізмом підзвітності незалежні ЗМІ також можуть функціонувати як інструмент ефективного врядування шляхом надання точної, збалансованої та своєчасної інформації з важливих для суспільства питань. Це дозволяє громадянам приймати свідомі поінформовані рішення стосовно того, хто ними керує та як ними керують. Іншими словами, гарна журналістика «грає принципово важливу роль у визначенні ключових моментів у конкретній політиці або рішенні, формуванні проблем для громадськості, аналізі питань та визначенні можливих рішень і альтернатив». *(Для більш детального ознайомлення із стосунками між ЗМІ й сферою безпеки та управлінням нею див.: Marina Caparini, ed., Media in Security and Governance: The Role of the News Media in Security (Geneva: DCAF, 2004), chapter 1)*

Прискіпливий нагляд з боку ЗМІ широко визнається як важливий елемент контролю над збройними силами. Однак, стосунки між «четвертою владою» і політикою безпеки є складним предметом з багатьма нюансами і цей розділ лише торкається декількох ключових тенденцій і питань.

Багато з традиційних засобів передачі інформації поступово стають неконкурентоспроможними в умовах швидкого розвитку передових сучасних технологій. Майже кожний традиційний вид ЗМІ та розповсюдження інформації має сучасного двійника: поверхневе телебачення проти супутникового телебачення; електронні публікації проти традиційних публікацій, а також голосовий зв'язок через Інтернет-протокол проти звичайного телефонного зв'язку. Експоненціальне зростання видань електронних новин (як за обсягами випуску, так і за споживанням) стали особливо значущою тенденцією. Наприклад, протягом 1990х років число користувачів супутникового та кабельного телебачення зросло з 85 мільйонів до 300 мільйонів, а дюжина чи більше регіональних каналів новин з'явилися вперше. У поєднанні з Інтернетом, яким зараз у світі користується майже 1,8 мільярда осіб (понад 25% всього населення планети), все це дозволило багатьом громадянам отримати регулярний доступ до «іноземних ЗМІ» як альтернативного джерела новин про події у світі. Багато з цих передових технологій також пропонують журналістам суттєві потенційні переваги у намаганнях підтримувати й зміцнювати їхню «свободу слова», хоча деякі уряди відповідають на виклики, створені новими медійними технологіями шляхом застосування своїх власних надзвичайно ефективних технологій (відомим прикладом є спроби Китаю встановити контроль за допомогою контрольованої державою Служби Інтернет провайдера, яка має контролювати доступ до Інтернету).

Журналісти наштовхуються на численні перепони і виклики під час виконання своєї загальної функції «сторожового пса», а ці виклики часто є загостреними або дуже чутливими під час здійснення репортажів на теми, що стосуються оборони. Зокрема, контрольні функції ЗМІ стосовно органів безпеки та розвідки часто виявляються слабкими, особливо у мирний час. *(На противагу репортажам про військові справи у мирний час, репортажі періоду війни, як виявляється, приваблюють більшу кількість журналістів. Наприклад, близько 5 тис. журналістів інформували про воєнні дії під час війни у Косово у 1999 році.)*

Частково це відбувається через те, що порівняно мало журналістів спеціалізуються у цій сфері – більшість з яких перебуває або у складі великих медійних організацій (таких, як БіБіСі, основні мережі в США, та інші найбільші національні газети і мережі), або у складі спеціалізованих оборонних видань (таких, як Група Джейнс) – а також через зниження рівня журналістики з питань державного управління та загальне «отупіння» новин протягом останніх близько десяти років.

Водночас, існує багато інших чинників, які потенційно можуть загрожувати ефективності ЗМІ під час виконання ними контрольних функцій у сфері оборони. Так зване «публічне інформаційне поле бою» після подій 11 вересня 2001 року нараховує багато таких перешкод і викликів, так само, як це відбулося з організаціями громадянського суспільства, про що зазначалося вище. *(Carl Conetta, "Disappearing the Dead: Iraq, Afghanistan, and the Idea of a 'New Warfare'", Project on Defense Alternatives Research Monograph, No.9 (18 February 2004).)*

Найважливішим загальним принципом є те, що ЗМІ повинні дотримуватися належного рівня незалежності, особливо від держави та діючого уряду, а також і від інших зацікавлених сторін.

Однак, після подій 11 вересня 2001 року основні джерела західної преси почали критикувати за їхню патріотичність і послужливість. Зростання концентрації власності (яке лише частково було збалансоване зростанням різноманітних «нових медіа») лише загострює таку стурбованість. Ця тісна взаємодія між корпоративними інтересами, певними політичними елітами та медійними монополіями призводить до обмеження незалежного й критичного журналізму. Вона також може звузити спектр висловлюваних думок, особливо щодо важливих суспільних питань. Отже, так само, як антиєвропейські газети-таблоїди у Сполученому Королівстві відіграють важливу роль у підтримці широкого, однак малопоінформованого євроскептицизму в публічній дискусії, подібний вплив застосовується до параметрів дискурсу з питань національної безпеки. Як зауважив один з критиків підтримки американською пресою інтервенцій в Ірак і Афганістан, «багато впливових американських журналістів і дописувачів продовжують нагадувати придворних писак на зразок тих, яких тримали монгольські імператори». *(Pankaj Mishra, "Kissinger's Fantasy is Obama's Reality", The Guardian (11 December 2009)*

Ця тенденція до співпраці (відтворення офіційних заяв і поглядів замість застосування до них критичного аналізу) вочевидь є найбільш поширеною у сфері безпеки – так само, як і ризик прийняття як керівництва до дій офіційної лінії або дозвіл маніпулювати собою для певних інсайдерів (включно з державними посадовими особами). Наприклад, у більшості країн НАТО ставлення до ЗМІ сьогодні загалом таке саме, як і в будь-якій іншій великій організації, яка має директорат комунікацій та спеціалістів у сфері зв'язків з громадськістю. Також сьогодні для зацікавлених сторін стає майже звичайною практикою під час військових операцій залучати послуги фірм-лобістів для презентації своєї позиції. Така практика вперше була популяризована урядом Кувейту у 1990 році, вона продовжувалася у період дезінтеграції Югославії і нещодавно використовувалася урядами Грузії та Афганістану. *(Jaimy Lee, "National Security Council of Georgia hires Public Strategies", PR Week (19 November 2009)*

Журналістам також потрібен необхідний рівень захисту для того, щоб їх несправедливо не звинувачували в упередженості, не засуджували, не кидали до в'язниці чи навіть не вбивали за те, що вони викривають відомих офіційних осіб у корупційних діях. Водночас, більше третини населення планети проживає у країнах, де немає свободи преси, і нові типи конфліктів між етнічними, ідеологічними, релігійними і просто кримінальними інтересами зробили журналістські розслідування надзвичайно небезпечними.

Іншою ключовою тенденцією є зростаюча спроможність глобальних ЗМІ розпалювати «чуттєвість до втрат» з метою або підтримки, або протидії іноземній інтервенції. Цей так званий «CNN ефект» став предметом суттєвої стурбованості в оборонному середовищі, починаючи з 1990х років. *(Іноді це означало будь-яке залучення ЗМІ, однак, цей вираз більш точно відображає переконання у тому, що, зокрема, телевізійні репортажі в реальному масштабі часу здійснюють небезпечний вплив на кризовий менеджмент та розгортання військ за межами демократичних країн. Див.: Margaret H. Belknap, "The CNN Effect: Strategic Enabler or Operational Risk?" Parameters (Autumn 2002): 100–114.)* Початок і закінчення операції США в Сомалі, а також швидке закінчення війни в Перській Затоці у 1990-1991 роках (після розповсюдження репортажів про так званий інцидент на «Шосе смерті») в обох випадках частково підтвердили цей ефект. Це, у свою чергу, призводило до більших зусиль уряду щодо менеджменту стосунків з пресою, посилення контролю за розповсюдженням інформації та формувало підходи до репортажів про військові операції у період після 11 вересня 2001 року шляхом, наприклад, «вживляння» журналістів у бойові порядки військ під час війни в Іраку у 2003 році та скоординованого формування основних випусків новин і їх розповсюдження. Незважаючи на продовження такої обмежувальної політики в Афганістані – включаючи обмеження щодо «негативних» вживлених журналістів *(Charlie Reed, "Pentagon Hires PR firm to Weed out 'Negative' Embedded Journalists", Stars and Stripes (25 August 2009), www.reclaimthemedia.org/propaganda_and_war/pentagon_hires_pr_firm_weed_ou2535.)* – стратегічна література була заповнена домислами щодо здатності Талібану та Аль-Каїди використовувати в якості "CNN ефекту" й чутливість до втрат у пошуку асиметричних переваг над Сполученими Штатами та їх союзниками з НАТО. *(Див., наприклад: Peter Singer, "Winning the War of Words: Information Warfare in Afghanistan" (The Brookings Institution, 23 October 2001); Thomas Elkjer Nissen, "The Taliban's Information Warfare – A Comparative Analysis of NATO Information Operations (Info Ops) and Taliban Information Activities", Brief (Royal Danish Defence College, December 2007); Tim Foxley, "Winning the Information War", Blog entry, SIPRI website (12 May 2009), www.sipri.org/blogs/Afghanistan/winning-the-information-war.)*

Вставка 21.1. Журналістські розслідування виявляють випадки корупції у сфері оборони

Контрактування «чорної діри» в Іраку

Комбінований вплив журналістських розслідувань, добровільних викривачів, урядових аудиторів та стривожених законодавців поступово ліквідували порочну практику контрактування з боку США в Іраку. Розслідування програми БіБіСі «Панорама» у 2008 році нібито виявило аж $23 мільярди, які могли бути втрачені, вкрадені або неточно враховані в Іраку.

Звинувачень у неналежному менеджменті, обмані та перевитратах було більш ніж достатньо:

- підрядники вибиралися з огляду на їх зв'язки в уряді США без змагання під час проведення тендерів;

- підрядники завищували вартість своїх послуг і вдавалися до подвійних обрахунків, щоб збільшити свої прибутки, і також були підозри, що декілька мільярдів доларів на відбудову Іракської армії опинилися в кишенях окремих урядовців Іраку.

Джерела: *Ed Harriman, "Where Has all the Money Gone?", London Review of Books 27:13 (7 July 2005):3-7; Daylight Robbery: BBC Panorama (10 June 2008), http://news.bbc.co.uk/1/hi/programmes/panorama/7438372.stm.*

Фінансування Талібану в Афганістані

У 2009 році Арам Ростон, який спеціалізується на журналістських розслідуваннях, відслідкував, як цивільні підрядники Пентагону в Афганістані дійшли до того, що заплатили групам повстанців, щоб захистити від нападів маршрути постачання американських військ. Військові офіційні особи США в Кабулі сказали Ростону, що мінімум десять відсотків логістичних контрактів Пентагону складають виплати Талібану.

Джерело: *Aram Roston, "How the US Funds the Taliban", The Nation, 30 November 2009.*

Справа Айткена – Сполучене Королівство

У квітні 1995 року колишній заступник міністра оборони Сполученого Королівства Джонатан Айткен пообіцяв застосувати «меч правосуддя» проти газети Гардіан і подав проти неї судовий позов за наклеп щодо його оборудок з торгівцями зброєю з Саудівської Аравії. У 1999 році він був засуджений до семи місяців тюрми за неправдиве свідчення після того, як був викритий у неодноразовому обмані.

Джерело: "The Aitken Aff air", Special Reports, The Guardian, www.guardian.co.uk/aitken.

Файли BAE – Сполучене Королівство

У лютому 2010 року британська фірма з виробництва зброї BAE Системз визнала себе винною та погодилася виплатити штраф у США та Сполученому Королівстві загальним обсягом у декілька мільйонів доларів для залагодження всіх довготривалих звинувачень у корупції проти неї, що вперше були оприлюднені газетою Гардіан у 2003 році.

Джерело: *"The BAE Files", The Guardian, www.guardian.co.uk/world/bae.*

Операція «Західний край», Індія

Операція «Західний край» була спеціальною операцією проти корупції, що заполонила сферу великих збройових контрактів Індії. Початковий матеріал розслідування журналу Тегелка (незалежного тижневого журналу новин Індії) у 2001 році був спрямований проти декількох членів тогочасної правлячої урядової коаліції. Він викривав декілька політичних фігур, а також старших армійських офіцерів, у змові з метою отримання хабарів за затвердження оборонних контрактів. Після того, як плівки з розмовами були опубліковані, міністр оборони подав у відставку, але пізніше його відновили на посаді. Спочатку уряд, замість того, щоб діяти відповідно до отриманих свідчень, звинуватив Тегелка у фабрикації звинувачень. Однак, через п'ять років, у жовтні 2006 року, Центральне бюро розслідувань Індії висунуло звинувачення проти керівних осіб у випадку ракети Барак, стверджуючи, що мали місце достатні підґрунтя для підозр у корупції та злочинній змові.

Джерела: *Tarun J. Tejpal, "The Tehelka Expose", www.taruntejpal.com/TheTehelkaExpose.htm; V. Venkatesan, "Dubious Deal", Frontline 23:21 (2006), http://www.hinduonnet.com/fl ine/fl 2321/stories/20061103001804100.htm.*

Останнім і давнім складним питанням є секретність. У той час, як уряди можуть законно закривати певну інформацію, якщо вони вважають, що її оприлюднення може зашкодити суспільним або національним інтересам, вони також можуть використовувати поняття «національної безпеки» як підґрунтя для втаємничення інформації, яка б призвела до незручностей або

скандалу з огляду на наявність корупції чи неефективного менеджменту. Обстановка посиленої уваги до питань безпеки, яка з'явилася після подій 11 вересня 2001 року, також призвела до поновлення уваги до урядової секретності і часткового розвернення назад розпочатих після закінчення «холодної війни» тенденцій щодо більшої прозорості, громадської підзвітності та доступності офіційної інформації.

Громадянське суспільство і ЗМІ у нестійких державах, перехідних державах і НАТО

У багатьох нестійких державах *(Нестійкі держави (які також іноді називають державами, що не відбулися, або слабкими державами) – це ті, які загалом не здатні забезпечити безпеку своїх громадян, або своєї території, і які є корумпованими й нелегітимними в очах своїх громадян)* надмірно жорсткі дії служб безпеки надзвичайно ускладнюють або роблять небезпечними для громадянського суспільства та ЗМІ навіть спроби моніторингу і просування ідеї виховання доброчесності в національних оборонних відомствах. Створення спеціальних сил безпеки та інтенсифікація операцій проти повстанців і тих, кого вважали злочинцями і терористами, призвели до різкого зростання числа не розслідуваних випадків таємних вбивств та викрадень співробітників організацій боротьби за права людини і політичних активістів у багатьох нестійких державах, до яких відносять певний перелік (який, безумовно, не є вичерпним) таких країн, як Бангладеш, Ефіопія, Кенія, Пакистан, Уганда та Зімбабве. При цьому, в Колумбії, Непалі, Палестинських Територіях, Сомалі, Шрі-Ланці та інших зонах конфліктів, НУО іноді розглядаються і владою, і повстанцями однаково як політичні противники. У деяких зонах конфліктів НУО не дозволяють доступу, а в інших – таких, як Могадішо та окремі частини Іраку й Афганістану – діяльність організацій громадянського суспільства іноді просто припиняється через надзвичайну небезпеку. *(Див., наприклад: Millar, Cortright, Gerber-Stellingwerf and Lopez, Oversight or Overlooked? (2009)*

Схожим чином у багатьох «перехідних державах» *(Цей термін зазвичай вживається стосовно колишніх радянських республік, які стали незалежними державами, але він також іноді застосовується й до будь-якої держави, що здійснює перехід від авторитарного чи військового правління до демократичного врядування.)* бюрократичні бар'єри на шляху до законної реєстрації НУО, погана історія політичної свободи та загалом слабкі громадянські суспільства вказують на те, що стосовно реформування сектору безпеки і оборони недержавні суб'єкти відіграють лише мінімальну роль у формуванні політики. *(З питань громадянського суспільства і реформування сектору безпеки у посткомуністичних країнах див.: Marina Caparini, Philipp Fluri and Ferenc Molnar, eds., Civil Society and the Security Sector: Concepts and Practices in New Democracies (Berlin: LIT, 2006).)* Як було попередньо зазначено, репресивне законодавство і тиск на громадянське суспільство зросли після подій 11 вересня 2001 року. Антитерористичне законодавство та заходи проти «екстремізму» використовувалися для нападок на НУО й політичних активістів, що критикували політику влади у багатьох перехідних державах, включаючи (і, знову ж, не обмежуючись) Китай, Єгипет, Ель-Сальвадор, Індонезію, Йорданію, Філіппіни, Росію, Судан, Туніс, Узбекистан та Ємен. *(Див., наприклад: Millar, Cortright, Gerber-Stellingwerf and Lopez, Oversight or Overlooked? (2009)*.

Незважаючи на те, що 1990-ті роки бачили значний обсяг оптимістичних доповідей про реформування сектору безпеки в Росії, однак протягом останніх років російське громадянське суспільство й ЗМІ виглядають значно ослабленими. Водночас, залучення громадянського суспільства та нагляд за сектором безпеки все ще іноді можливі у перехідних державах, особливо завдяки зовнішній допомозі з боку МУО. Наприклад, на пострадянському просторі Організація з безпеки і співробітництва в Європі (ОБСЄ) зробила багато для того, щоб стримати такі негативні тенденції шляхом сприяння стабільності через зміцнення ефективного врядування, громадянського суспільства і свободи ЗМІ. Подібним чином ЄС також, з перемінним успіхом, показував добре розуміння ролі недержавних суб'єктів як певних альтернативних точок дотику у нестійких та перехідних державах. Європейська ініціатива з прав людини (ЄІПЛ) і Механізм швидкого реагування (МШР) унікальні тим, що вони фінансують громадянське суспільство, демократію, права людини й проекти попередження конфліктів без необхідності отримання дозволу від своїх урядів.

Також існують приклади важливого внеску у справу реформування сектору безпеки, зробленого суб'єктами громадянського суспільства у середовищі перехідних держав.

Наприклад, Південноафриканська мережа оборони та безпеки є спонсорованим видом діяльності у секторі безпеки, яка має на меті підвищення професіоналізму й підзвітності широкого спектру суб'єктів (включаючи громадянське суспільство) і взаємодію між ними. Однак, незважаючи на окремі приклади, коли місцеві організації громадянського суспільства відіграють важливу роль у нагляді та моніторингу на «м'якшому» краю реформування сектору безпеки (зокрема, дії поліції та судова реформа), на важчому боці (пов'язані з обороною місії та інституції, що висвітлюються у цій книзі) активність організацій громадянського суспільства майже непомітна. *(Edward Rees, "Security Sector Reform (SSR) and Peace Operations: 'Improvisation and Confusion' from the Field", External Study for the UN Department of Peacekeeping Operations (March 2006)*.

Один огляд декількох випадків дійшов до висновку: «у всіх досліджуваних країнах громадянське суспільство рідко буває повноцінним партнером, а його програми залишаються більше сфокусованими на тих, хто забезпечує безпеку і право, ніж на тих, хто їх потребує». *(Christopher Stone, Joel Miller, Monica Thornton and Jennifer Trone, "Supporting Security, Justice, and Development: Lessons for a New Era" (Vera Institute of Justice, June 2005), 9, www.dfid.gov.uk/Pubs/files/security-justice-development.pdf.)*

А інший огляд інтегрованих місій в Бурунді, Демократичній Республіці Конго, Гаїті та Косово прийшов до висновку, що у кожному випадку «незначна увага приділяється розвитку парламентських механізмів контролю над сектором безпеки або відповідних механізмів громадянського суспільства. Підтримка зміцнення спроможностей парламентів і суб'єктів громадянського суспільства, таких як ЗМІ та НУО, загалом надається з боку ПРООН, хоча вона рідко буває сфокусованою на секторі безпеки» *(Heiner Hanggi and Vincenza Scherrer, "Recent Experience of UN Integrated Missions in Security Sector Reform (SSR): Review and Recommendations" (Geneva: DCAF, November 2007), www.dcaf.ch/un_ssr_ pcpb/recent-experience-un-integrated-missions-071203.pdf.)* Іншою слабкістю порядку денного, який включає реформу сектору безпеки та ефективне врядування, є те, що вона напевне виглядає як щось таке, що інші держави мають виконувати. Таким чином, наприклад, у той час як один з провідних союзників, Міністерство міжнародного розвитку Сполученого Королівства багато зробило для заохочення реформ у секторі безпеки та залучення НУО у перехідних і нестійких країнах, власний нещодавній *(Див., наприклад: UK Department for International Development, "Understanding and Supporting Security Sector Reform", www.dfid.gov.uk/Pubs/files/supportingsecurity.pdf)*. досвід Британії вважається суперечливим: провідний виробник озброєнь в країні постав перед суттєвими звинуваченнями в корупції стосовно збройових контрактів у Африці, на Близькому Сході та у Східній Європі. *(Див.: "BAE Faces Corruption Charges", New York Times (1 October 2009). Для більш детального ознайомлення див.: "The BAE Files", The Guardian, www.guardian.co.uk/world/bae. Цікаво, що у даному випадку мова йде про скоординовану акцію громадянського суспільства між організацією Корнер Хаус (Corner House) та рухом Кампанія проти торгівлі зброєю (Campaign Against Arms Trade), яка призвела до судового перегляду рішення Офісу надзвичайних фальсифікацій (Serious Fraud Offi ce) про припинення розслідування щодо контрактів*

ВАЕ з Саудівською Аравією). Національний офіс аудиту охарактеризував програму оборонних закупівель Британії як «непідйомну» після того, як були оприлюднені підозри в існуванні «чорної діри» в планах витрат міністерства оборони розміром від 6 до 36 мільярдів фунтів. *(Nicholas Timmins, "Warning of 'Black Hole' in Defence Budget", Financial Times (15 December 2009); Jeremy Lemer, Alex Barker and James Blitz, "Damning UK Defence Equipment Review", Financial Times (15 October 2009)*. Отже, ключовим уроком із зазначеного досвіду Британії є те, що виховання доброчесності та зниження рівня корупції у сфері оборони починається вдома. Хоча, звичайно, у порівнянні з ситуацією в нестійких та перехідних державах ситуація в Британії набагато менш критична.

Вставка 21.2. Участь та партнерство громадянського суспільства у процесі реформування сектору безпеки і контролю оборонного сектору

Ряд організацій і мереж громадянського суспільства подають приклади успішної участі у реформуванні сектору безпеки та здійсненні контролю за сферою оборони. Серед них є такі:

Африканська мережа сектору безпеки *(The African Security Sector Network (ASSN), www.africansecuritynetwork.org) і Південноафриканська мережа оборонного та безпекового менеджменту (Southern African Defense and Security Management Network (SADSEM), www.sadsem.org).*

Африканську мережу було створено в Гані у 2003 році з метою надання допомоги і сприяння врядуванню у секторі безпеки в Африці шляхом докладання зусиль, які включали б дослідження, захист, розвиток спроможностей та забезпечення умов для взаємодії й обміну інформацією з партнерами та іншими учасниками. Африканська мережа залучила учасників з усього спектру реформування сектору безпеки (зокрема, політиків, професіоналів, донорів та громадянське суспільство), а також запровадила курси з питань врядування у секторі безпеки, які, наприклад, були запропоновані Південноафриканській мережі. А Південноафриканська мережа – це діяльність у секторі безпеки, що підтримується за рахунок донорської допомоги і має на меті підвищення професіоналізму й підзвітності широкого кола учасників діяльності у секторі безпеки (включаючи громадянське суспільство) та взаємодії між ними. Цінність обох мереж полягає у тому, що вони пропонують площадку для спілкування офіційних осіб з сектору безпеки та представників академічної науки й громадянського суспільства, і таким чином відіграють важливу роль у порозумінні та створенні спроможностей.

Сейфеуолд, Сполучене Королівство *(Saferworld – UK, www.saferworld.org.uk)*

Академія миру та розвитку, Сомалі *(Academy for Peace and Development, Somalia, www.apd-somaliland.org).*

Центр дослідження розвитку Пунтланд, Сомалі *(Puntland Development Research Centre – Somalia, www.pdrcsomalia.org).*

Центр досліджень і діалогу, Сомалі *(Centre for Research and Dialogue – Somalia, www.crdsomalia.org).*

Понад 15 років тому Сейфеуолд почав працювати над створенням регіональної угоди з питань торгівлі зброєю у Європейському Союзі – тобто, розпочав рух, який призвів до підписання в межах ЄС зобов'язуючої угоди з питань контролю над експортом озброєнь. На початку тисячоліття у Сполученому Королівстві законодавство, яке регулювало питання безвідповідальних поставок озброєнь, було змінене вперше з часів Другої світової війни, і в результаті воно ускладнило виробникам озброєнь та їх агентам збут зброї до тих регіонів, де вона може завдати найбільшої шкоди.

У Сомалі, де не існувало ефективного врядування понад 18 років, Сейфеуолд працював з місцевими організаціями, бізнесовим сектором та іншими групами громадянського суспільства, щоб донести їхні ідеї з питань безпеки та розвитку країни до уваги міжнародних політичних діячів, включаючи представництво Ради Безпеки ООН у Джибуті. Місцеві сомалійські партнери включають Академію миру та розвитку, Центр дослідження розвитку Пунтланд та Центр досліджень і діалогу. Хоча залишаються величезні виклики, однак, перші цеглини вже закладено, що дозволить організаціям громадянського суспільства робити внесок у мирні процеси та розвиток, а також допомогти у досягненні консенсусу стосовно того, як дати мир Сомалі.

Для того, щоб НАТО продовжував існувати на тому самому підґрунті, на якому він був створений – *для захисту свободи, спільної спадщини та цивілізації своїх народів, заснованих на принципах демократії, індивідуальної свободи і верховенства права* (Північноатлантичний Договір, 1949 рік) – від нього очікується здатність бути відкритим, прозорим та підзвітним суспільству. Система колективного прийняття рішень в НАТО може бути достатньо підзвітною, якщо члени парламенту будуть постійно і повністю поінформованими про рішення НАТО та якщо вони матимуть фінансовий контроль. Однак, цього немає у обох випадках. Нагляд, безумовно, існує у національних законотворчих органах і парламентських комітетах, також відбулися окремі високоефективні розслідування діяльності НАТО (наприклад, стосовно Боснії, Косово та Афганістану). Водночас, такі зусилля часто ускладнювались проблемами в отриманні доступу до відповідної інформації. Окрім цього, роль національних парламентів у їхній безперечно найважливішій функції узгодження політики є не досить розвиненою. Багато парламентів просто не мають достатніх повноважень щодо попереднього узгодження військових операцій або визначення часового терміну для майбутньої місії.

Так само й Парламентська асамблея НАТО не була задумана таким чином, щоб мати формальний вплив або контроль за процесом прийняття рішень в альянсі. Рішення з питань оборони, безумовно, не повинні бути виключною прерогативою виконавчої гілки влади або впливових міжурядових бюрократій. Це, наприклад, стосується рішень з питань закупівель, які приймаються в рамках Конференції національних директорів озброєнь – вищого органу НАТО, відповідального за співробітництво між країнами-членами з питань проектів оснащення та проведення досліджень.

Громадяни (і парламентарі) у країнах-членах НАТО до цього часу діють в рамках правил збереження таємниці, які були запроваджені у цілком інший час – коли суспільство мало інші очікування стосовно участі у формуванні питань оборони та зовнішньої політики, коли дуже мало членів альянсу прийняли закони стосовно права доступу до інформації і коли загроза для країн Заходу була набагато більш суттєвою і безпосередньою. Всі ці обставини змінилися, але режим секретності, який регулює поширення інформації, залишається незмінним за багатьма параметрами. Як наслідок, все ще залишаються утрудненими можливості для парламентарів і громадян брати участь у формуванні варіантів політики, які мають глибокий вплив на їхні свободи та безпеку.

Щоб якось виправити цей недолік, у квітні 2009 року було створено нову мережу громадянського суспільства «НАТО Уотч» (NATO Watch). «НАТО Уотч» має на меті: заохочувати НАТО до прийняття політики інформаційної відкритості, яка б відповідала духу законів про доступ до інформації, вже прийнятих у всіх 28 країнах-членах альянсу; сприяти незалежному моніторингу й аналізу оперативної та адміністративної діяльності в рамках НАТО; підвищити прозорість, стимулювати залучення парламенту та ознайомлення й залучення широких верств суспільства до процесу прийняття рішень в НАТО. Учасники мережі «НАТО Уотч» з різних країн-членів, країнпартнерів та контактних країн будуть заохочуватися до підтримки цілей проекту шляхом використання своїх власних парламентських представників і національних мереж, до яких входять відповідальні керівники та впливові особи. *(Для кращого ознайомлення з деталями див.: www.natowatch.org)*. Зустріч груп громадянського суспільства на Тіньовому самміті НАТО в Брюсселі також закликала НАТО до «відновлення зв'язків з громадянами», заявивши, що «поглиблення й розширення спільних ціннісних основ в рамках Альянсу... означає оновлений, більш відкритий, прозорий та підзвітний Альянс, який відповідатиме очікуванням 21 століття». *(Див. «Декларація громадян з питань безпеки Альянсу» ("Citizens Declaration of Alliance Security"), яка прийнята на Тіньовому самміті НАТО в Брюсселі 31 березня – 1 квітня 2009 р., www.isis-europe.org/pdf/2009_artrel_308_natoshadow_execsum_v5.pdf; див. також: "The Shadow NATO Summit Report", www.isis-europe.org/pdf/2009_ artrel_309_natoshadow_v11.pdf)*. Окрім цього, «П'ять прин-

ципів відкритого й підзвітного НАТО», сформульованих групою «Аксесс Інфо» (Access Info), закликають НАТО до встановлення стандартів оприлюднення ключової інформації, які передбачали б механізм направлення громадянами запитів про інформацію та створення незалежного спостережного органу для розгляду звернень з приводу відмов у наданні або оприлюдненні інформації протягом короткого терміну. *(Див.: NATO Shadow Summit Report, "Five Principles for an Open and Accountable NATO", Appendix 4. «Аксесс Інфо» (Access Info) (www.access-info.org) є організацією захисту прав людини, яка базується у Мадриді та працює над заохоченням і захистом дотримання прав доступу до інформації шляхом сприяння прозорості національних та наднаціональних офіційних структур. «НАТО Уотч» та «Аксесс Інфо» запропонували створення спільної експертної групи з числа представників громадянського суспільства і НАТО з метою перегляду політики альянсу з питань розкриття інформації).*

Висновки: покращення партнерства між НУО та урядами у вихованні доброчесності

Громадянське суспільство відіграє фундаментальну роль у вихованні доброчесності та зниженні рівня корупції у сфері оборони. Багато урядів вже зрозуміли важливість внеску НУО, інших секторів громадянського суспільства та незалежних ЗМІ. Організації громадянського суспільства і ЗМІ можуть підтримувати здатність до ефективного нагляду шляхом постійного оприлюднення та протистояння випадкам зловживань у оборонному секторі, а також шляхом організації громадської підтримки у питанні створення більш відповідального врядування, що ґрунтується на верховенстві права. Однак, у тих країнах, де такого взаємовигідного партнерства не вистачає або воно відсутнє, владі потрібно створити відповідні умови, щоб таке партнерство стало реальним і ефективним.

Формування такого суспільного клімату, в якому зазначеним питанням буде приділятися суттєва увага, вимагає зміни психології та закріплення в повсякденному житті суспільства норм відкритості, консультування, співробітництва й довіри як з боку влади, так і з боку тих таки НУО та структур громадянського суспільства. Окрім цього, потрібно залучати до участі й більш широкі верстви активних представників громадянського суспільства від ЗМІ, НУО, академічної науки, профспілок і жіночих організацій – а не лише «дружніх до істеблішменту» оборонних «мозкових трестів». На жаль, доволі часто до голосів з цього більш широкого представництва громадянського суспільства, як і до їхньої ролі, увага виявляється обмеженою, а іноді вони просто ігноруються. Потрібні зміни не відбудуться протягом однієї ночі. Однак потенційні вигоди для суспільства і влади (див. Розділ 14) роблять ці зміни на користь посилення ролі громадянського суспільства бажаними і потрібними.

З часу терористичних нападів 11 вересня 2001 року, Сполучені Штати та декілька їх союзників почали вважати себе у стані війни, тому цілком зрозуміло, що під час воєнного стану стосунки між ЗМІ–громадянським суспільством і владою–збройними силами регулюються за іншими правилами. У більшості демократичних суспільств переважна частина людей добре розуміє, що під час війни влада буде застосовувати як секретність, так і обман. Однак, якщо стосовно доцільності обмежень на дії ЗМІ та громадянського суспільства під час війн за виживання нації практично немає дискусії, то випадки застосування цих правил до «війн по вибору» (до яких,зокрема, можна віднести операцію в Іраку та інші операції в рамках «війни з тероризмом») отримали набагато меншу підтримку суспільства.

У відповідь на тиск і обмеження, застосовані до груп громадянського суспільства з 11 вересня 2001 року, окремі НУО забезпечили свої власні права діяти вільно без втручання й тиску з боку влади. Заснований у США Міжнародний центр за неприбуткові права, наприклад, сформулював перелік принципів захисту громадянського суспільства, які ґрунтуються на універсальних конвенціях прав людини і деклараціях, які визнаються практично всіма урядами. *(International Center for Not-for-Profi t Law and World Movement for Democracy, "Defending Civil Society", The International Journal of Not-for-Profi t Law 10:2 (April 2008): 31-33).* Держави не лише повинні уникати необережного втручання у питання прав людини та основних свобод, але вони повинні ще й захищати ці права й гарантувати їх упорядковане дотримання. Принципово важливо, щоб держави створювали сприятливе середовище, в якому структури громадянського суспільства можуть діяти без обмежень.

У свою чергу, групи громадянського суспільства й особливо товариства з питань розвитку, прав людини та громадянських свобод повинні бути більш тісно залучені до суспільної дискусіїз питань стратегій безпеки та вибору належного підходу до подолання ризику корупції в оборонній сфері. Ці структури громадянського суспільства можуть утворити інтернаціональну мережу для того, щоб говорити єдиним голосом і брати участь у погоджених заходах з метою протидії тим викликам, про які говориться у цій книзі. Організації громадянського суспільства можуть допомогти сформувати та заохотити підтримку в такому непростому питанні, як забезпечення оптимального балансу між зусиллями у вихованні доброчесності, прозорістю й підзвітністю, з одного боку, та підтриманням ефективності й невитратності збройних сил, з іншого (див. Розділ 2). НУО разом з досвідом організацій громадянського суспільства виявилися добре пристосованими до цих викликів. Багато з них має значний досвід перебування у зонах конфліктів та виконання своїх загальних місій, наприклад, у подоланні соціального відчуження, і можуть забезпечити цінний внесок у справу створення середовища, несприятливого для розвитку корупції у сфері оборони.

Дослідження досвіду Південної Кореї, описане у Розділі 19, показує, чого можна було б досягти. Після численних проблем з доброчесністю й корупцією у сфері оборонних закупівель уряд Південної Кореї з 2003 року започаткував процес реформ. Трьома роками пізніше було запроваджено систему омбудсмена, яка стала першою в Кореї, що була законодавчо визначеною, та першим випадком участі громадянського суспільства у моніторингу оборонних закупівель. Організації громадянського суспільства мають бути більш активними у донесенні свого досвіду та мудрості до більш широкої аудиторії політиків і суспільства, а також повинні шукати можливості для своєї провідної ролі у реформуванні політичних підходів до виховання доброчесності на всіх рівнях обговорення питань оборони і безпеки. Групи громадянського суспільства повинні допомагати у формуванні нової тематики дискусій шляхом більш практичних та водночас більш етичних підходів. Організації громадянського суспільства повинні створювати нові ЗМІ та нові засоби для комунікації такого бачення і протидії фальшивим намаганням та дезінформації. Для забезпечення повної реалізації потенціалу громадянського суспільства можливі спонсори заохочуються до передачі ресурсів для посилення спроможностей НУО у виконанні зазначених вище ролей.

НУО не повинні нехтувати вимогами щодо більшої прозорості та підзвітності у своїх власних фінансових питаннях і операціях. Легітимність і громадська доброчесність мають важливе значення для організацій громадянського суспільства у контексті ефективності виконання ними своєї місії. Якщо прозорість і підзвітність вимагаються від НУО, то такі ж самі прозорість і підзвітність потрібні й урядові та його відомствам, а також і НАТО. Протягом всієї історії НАТО, коли члени національних парламентів запитували про рішення НАТО, то їм напевне відповідали, що такі рішення є конфіденційними. А коли такі ж запитання задавали Генеральному Секретареві, то він напевне відповідав, що НАТО є альянсом суверенних держав. Ця ситуація замкненого кола може й мала б сенс у часи «холодної війни», однак сьогодні вона вже не є прийнятною. Всередині НАТО потрібно терміново створювати адекватні механізми прозорості та підзвітності.

Розділ 22
Роль міжнародних організацій

Міжнародні організації грали ключову роль у тому, що за останні двадцять років відбулося величезне зрушення у всьому світі у питанні ставлення до корупції. Вони також відігравали головну роль у практичних зусиллях щодо подолання корупції шляхом запровадження міжнародних конвенцій і стандартів, сприяння встановленню ефективного врядування, моніторингу та громадської дії. У той час, як більша частина цієї роботи була зосереджена у сферах міжнародного бізнесу та розвитку, сьогодні спостерігається зростання уваги до проблеми корупції в оборонному та безпековому секторах. Це природне розширення зростаючої уваги до оборонного врядування протягом останнього десятиліття було ініційовано саме зростаючим розумінням у таких інституціях, як, наприклад, НАТО, того, що ефективний менеджмент ресурсів є життєво важливим питанням для забезпечення успіху операцій.

Міжнародні організації (в інтересах цього розділу до них віднесено й міжурядові організації) мають величезні ресурси й передові технології, які можуть знадобитися тим офіційним особам і простим громадянам, хто бажає зробити внесок у справу боротьби з корупцією у своїх відомствах або суспільстві. Цей розділ має на меті допомогти таким читачам краще зрозуміти питання наявних ресурсів, доступу до них та можливості їх ефективного використання. Спершу буде розглянуто різні ролі та підходи у боротьбі з корупцією, якими користуються міжнародні організації взагалі та у сфері оборони зокрема. Після цього більш глибоко буде досліджено декілька важливих інституцій з метою визначення, як найкраще використати спроможності цих інституцій, щоб прискорити зміни у національному контексті.

Роль міжнародних організацій: широкий контекст

Принаймні до початку 1990х років корупція розглядалася переважною більшістю міжнародного бізнесу та співтовариством розвитку як постійна (можливо, навіть «прийнятна») додаткова частина вартості контрактів. У деяких країнах Заходу вважалося іноді прийнятним навіть включати корупційні виплати до переліку легітимних витрат у податкових деклараціях. Однак, уже протягом декількох десятиліть спостерігалося зростаюче розуміння величезного навантаження, яке корупція накладає на програми розвитку, а також на руйнівний економічний вплив корупції. Дебати навколо закону США «Про корупційні іноземні практики» від 1977 року, наприклад, показали, що понад 400 американських корпорацій визнали виплати у понад $300 мільйонів своїх корпоративних фондів іноземним посадовим особам. Цей реальний факт виглядав не лише неетичним, але також і поганим для бізнесу, руйнуючи довіру до корпорацій, які це робили, та (з огляду на перевагу приватних оборудок над ефективністю) підриваючи цілісність системи вільного ринку загалом. *(Unlawful Corporate Payments Act of 1977, Legislative History – House Report, http://10.173.2.10/ criminal/fraud/fcpa/ history/ 1977/houseprt.html)*. Величезний руйнівний ефект корупції також утворювався в результаті перетворень у напрямі «вільного ринку» в Росії та інших пострадянських країнах, в яких приватизаційні програми, рекомендовані щирими (однак наївними) західними експертами, дегенерували у повномасштабне розкрадання державної власності.

Створення у 1993 році організації Транспаренсі Інтернешнел, батьками якої були офіційні особи з безпосереднім досвідом отримання руйнівних наслідків корупції для розвитку, дало цій зростаючій стурбованості свій голос. З того часу зростаюча мережа національних і міжнародних інституцій використовувала освіту, лобіювання та цілеспрямовані дослідження для того, щоб напевне внести проблему корупції (та необхідність боротьби з нею) до світового політичного порядку денного.

Сьогодні десятки відомих міжнародних, міжурядових та глобальних неурядових організацій активно залучені до зусиль з подолання корупції. Вони заповнюють ряд важливих ніш у антикорупційній екосистемі (прохання враховувати, що через обмежений обсяг розділу тут згадуються лише окремі організації в інтересах презентації ніш, а не їх повного представлення):

Розробка й запровадження антикорупційних угод і стандартів на світовому та регіональному рівнях. Сьогодні вже існує більше десятка таких угод, найбільш відомими з яких є Конвенція ООН проти корупції (UN Convention against Corruption (UNCAC)), яка вступила в дію у грудні 2005 року, а також Конвенція ОЕСР з питань боротьби з хабарництвом серед іноземних державних посадовців (OECD Convention on Combating Bribery of Foreign Public Offi cials in International Business Transactions), підписана у грудні 1997 року. Моніторинг імплементації таких конвенцій відіграє важливу роль для таких інституцій, як ОЕСР, так само, як і виявлення та розповсюдження передового досвіду. У цій роботі підтримка часто надходить через мережу організацій, наприклад, в Європі: Рада Європи, Група держав проти корупції (Group of States against Corruption (GRECO), Європейська Комісія та Координатор ОБСЄ з питань економічної та екологічної діяльності. На континентах обох Америк Організація американських держав забезпечує підтримку Міжамериканській конвенції проти корупції. Також потрібно зазначити важливу нішеву роль таких організацій, як: Група з розробки фінансових заходів боротьби з відмиванням коштів (FATF) – провідна організація з питань боротьби з відмиванням коштів шляхом розвитку й імплементації міжнародних стандартів; Світова організація торгівлі, що виконуєантикорупційну функцію у рамках Робочої групи з питань прозорості та урядових закупівель.

Парламентські асамблеї можуть допомогти у розвитку міжнародних угод і підходів до боротьби з корупцією, лобіюванні адаптації всередині країн та подальшій імплементації. Парламентська асамблея Ради Європи (ПАРЄ) є найкращим прикладом в контексті своєї роботи в рамках Цивільної та Кримінальної конвенцій Ради Європи про боротьбу з корупцією. Інша видатна організація – Глобальна організація парламентарів проти корупції (Global Organisation of Parliamentarians against Corruption (GOPAC) зі штаб-квартирою в Канаді – підтримує членів національних парламентів у питаннях захисту їх власної доброчесності в рамках дотримання кодексу поведінки, а також для ефективного розуміння та виконання своєї наглядової функції. Зазвичай, для цього потрібні індикатори стану виконання цієї функції. Інші регіональні парламентські асамблеї, наприклад, Парламентська асамблея країн Азії, також звертають увагу на проблеми корупції.

Банки розвитку стали провідними учасниками антикорупційних заходів – як з метою підтримання цілісності своїх власних програм, так і, у більш широкому контексті, щоб прибрати корупцію як серйозну перешкоду на шляху економічного і соціального розвитку; корупція розмиває верховенство права, ослаблює інституції, які потрібні для економічного зростання, і підриває служби соціального забезпечення, на які покладаються бідні люди. Програми банків розвитку часто застосовують різнопланові підходи до протидії корупції, допомагаючи створити корпоративне врядування й менеджмент у інституціях, що отримують кредити, підвищуючи політичну відповідальність за витрачання ресурсів, а також зміцнюючи здатність громадянського суспільства вимагати вжиття заходів та контролювати їх виконання. Світовий банк та Міжнародний валютний фонд є двома найбільшими світовими гравцями. Окрім них, регіональні банки розвитку, такі, як Європейський банк реконструкції та розвитку, Азійський банк розвитку та Міжамериканський банк розвитку, також мають антикорупційні програми.

Провідні позабанкові міжнародні (й національні) організації розвитку також активно борються з корупцією в рамках зростаючих зусиль щодо забезпечення ефективного врядування, яке відіграє життєво важливу роль у питаннях людського розвитку. З корупцією все більше борються відкрито й безпосередньо, оскільки її руйнівний вплив на врядування став краще зрозумілим.

Інституціями, що докладають зусиль для виявлення й розповсюдження передового досвіду, є Програма розвитку ООН, Женевський центр демократичного контролю над збройними силами та Глобальна мережа сприяння реформуванню сектору безпеки (Global Facilitation Network for Security Sector Reform (GFN-SSR).

У цьому сенсі НАТО також працює як організація з питань «розвитку», прив'язуючи свої антикорупційні програми до власного інтересу щодо ефективного врядування у секторі безпеки та демократичного цивільного контролю.

Координація правоохоронних заходів. Глобальні інституції, такі, як Інтерпол та Офіс ООН з питань боротьби з наркотиками й злочинністю (United Nations Offi ce on Drugs and Crime (UNODC), відіграють значну роль у координації та доповненні національних антикорупційних зусиль.

Звертаючись до цієї однієї із шести пріоритетних сфер боротьби зі злочинністю, Інтерпол розробив кодекси етики й поведінки для правоохоронців, стандарти для офіцерів поліції та запитальник поліцейської доброчесності для того, щоб краще виділити спроможності, зібрані у Бібліотеці передового досвіду, з метою надання допомоги слідчим у розслідуванні корупційних справ, а також створив групи національних координаторів з питань боротьби з корупцією. Він також курує Групу експертів Інтерполу з питань корупції (Interpol Group of Experts on Corruption (IGEC)) з метою сприяння, спільно з іншими міжнародними партнерами, у питаннях координації й гармонізації національних і регіональних підходів до боротьби з корупцією. Офіс ООН UNODC та Інтерпол домовилися відкрити першу в світі Антикорупційну Академію, що буде розташована поблизу Відня, Австрія. Європейська Комісія також має потужні антикорупційні програми, й так само їх мають окремі регіональні інституції, наприклад, правоохоронні робочі групи у регіоні Балтійського моря та на Балканах.

Вставка 22.1. Перелік міжнародних організацій та їх веб-сайтів

Азійський банк розвитку http://www.adb.org/Anticorruption/unit.asp

Азійська організація вищих аудиторських інститутів http://www.asosai.org

Парламентська асамблея країн Азії http://www.asianparliament.org

Рада Європи http://www.consilium.europa.eu

Європейський банк реконструкції та розвитку http://www.ebrd.com

Європейська Комісія http://ec.europa.eu

Група з розробки фінансових заходів боротьби з відмиванням коштів (FATF) http://www.fatf-gafi .org

Женевський центр демократичного контролю над збройними силами http://www.dcaf.ch

Глобальна мережа сприяння реформуванню сектора безпеки http://www.ssrnetwork.net

Глобальна організація парламентарів проти корупції http://www.gopacnetwork.org

Група держав проти корупції http://www.coe.int/t/dghl/monitoring/greco/

Міжамериканський банк розвитку http://www.iadb.org

Міжнародна асоціація суддів http://www.iaj-uim.org

Міжнародна асоціація прокурорів http://www.iap-association.org

Міжнародна асоціація адвокатів http://www.ibanet.org

Антикорупційна комісія Міжнародної торговельної палати http://www.iccwbo.org/policy/anticorruption

Міжнародна комісія юристів http://www.icj.org

Міжнародний валютний фонд http://www.imf.org

Інтерпол http://www.interpol.int

Організація Північноатлантичного договору (НАТО) http://www.nato.int

Організація економічного співробітництва і розвитку (ОЕСР) http://www.oecd.org

Організація американських держав http://www.oas.org

Координатор ОБСЄ з питань економічної та екологічної діяльності http://www.osce.org/eea

Парламентська асамблея Ради Європи (ПАРЄ) http://assembly.coe.int

Транспаренсі Інтернешнел http://www.transparency.org

Організація Об'єднаних Націй http://www.un.org

Глобальна антикорупційна мережа профспілок (UNICORN) http://www.againstcorruption.org

Офіс ООН з питань боротьби з наркотиками та злочинністю (UNODC) http://www.unodc.org

Програма розвитку ООН (ПРООН) http://www.undp.org

Світовий банк http://www.worldbank.org

Світова організація торгівлі (СОТ) http://www.wto.org

Робоча група СОТ з питань прозорості державних закупівель http://www.wto.org/english/tratop_e/gproc_e/ gproc_e.htm#plurilateral

Міжнародні професійні організації часто мають програми підтримання доброчесності й боротьби з корупцією у сфері своєї відповідальності. До прикладів глобальних організацій відносять Міжнародну асоціацію суддів, Міжнародну комісію юристів, Міжнародну асоціацію адвокатів та Міжнародну асоціацію прокурорів. Також існує ряд регіональних організацій з питань аудиту, зокрема, Азійська організація вищих аудиторських інститутів.

Сприяння і моніторинг. Ряд міжнародних неурядових організацій працюють над підвищенням рівня усвідомлення небезпеки корупції та заохоченням до антикорупційних дій, використовуючи для цього як політичний, так і соціальний тиск. Маючи міжнародну мережу та понад 90 національних розділів, Транспаренсі Інтернешнел є провідною організацією у цій сфері. Її зусилля доповнюються іншими інституціями, такими, як антикорупційна організація профспілок UNICORN та Міжнародна торговельна палата – бізнесова асоціація, що підтримує таке функціонування глобальної економіки, яке характеризується вільною і справедливою конкуренцією. У складі Міжнародної торговельної палати є Антикорупційна комісія, головним завданням якої є заохочення до саморегуляції бізнесу щодо протистояння рекету і хабарництву, а також забезпечення врахування інтересів бізнесу у міжнародних ініціативах боротьби з корупцією.

Зв'язок з обороною

Підвищення уваги до важливості ефективного врядування, яке спостерігається в оборонному середовищі, та усвідомлення прямої загрози для нього з боку корупції відбувається паралельно з такими ж процесами у середовищі розвитку. Досвід програми «Партнерство заради миру» у країнах Центральної та Східної Європи добре ілюструє цю ситуацію. У 1990х роках спостерігалися сподівання на швидкі демократичні ринкові перетворення у посткомуністичних державах. Міжнародне військове співробітництво доповнювало ці процеси шляхом надання можливості військовим професіоналам спілкуватися один з одним під час виконання спільних завдань миротворчості та гуманітарної допомоги. Тому головним завданням програм допомоги й співробітництва тих часів була взаємосумісність – здатність збройних формувань до розвитку спільних (або принаймні узгоджених) підходів, процедур та технічних спроможностей, необхідних для того, щоб діяти пліч-о-пліч під час спільних операцій. Демократичний контроль над збройними силами в якості окремого питання розглядався переважно у сенсі оперативного контролю.

Протягом наступного десятиліття спостерігався значний прогрес у розвитку оперативної взаємосумісності. Водночас, вже у 1990х роках ставало зрозумілим, що взаємосумісність – це лише половина справи, а інша половина – це розвиток нових спроможностей і методів, які відповідали б потребам ведення сучасних операцій. Ця тенденція до нових трансформацій була ще більш прискорена з урахуванням важливих антитерористичних місій після подій 11 вересня 2001 року. На відміну від взаємосумісності,

трансформаційні процеси не можуть відбуватися ізольовано на зразок заходів міжнародного військового співробітництва. Навпаки, вони потребують нових бачень зі сфери політики, інноваційного планування та збільшення бюджетних ресурсів. Однак, якщо демократичний цивільний контроль вже існував у оперативному сенсі (тобто, президент був «верховним головнокомандувачем»), то оборонні інституції, відповідальні за питання воєнної політики, планування, забезпечення ресурсами тощо, були все ще слабкими у багатьох країнах. Без ефективного цивільного міністерства оборони, яке б забезпечувало керівні вказівки й лобіювання інтересів військових, останні ставали жертвами власної інерції та апатії політичного класу до питань національної безпеки (і оборонних бюджетів).

Зазначене поставило питання врядування у секторі безпеки в центр уваги оборонного співробітництва – ця тенденція отримала підтвердження через прийняття у 2004 році програми «Будівництво оборонних інституцій» (Defence Institution Building) в рамках Програми НАТО «Партнерство заради миру». А коли вже питання ефективного врядування впевнено зайняли місце у порядку денному оборонного співробітництва, то увага до проблеми боротьби з корупцією стала лише питанням часу. Це якраз і проявилося у вигляді програми НАТО «Виховання доброчесності та зниження рівня корупції у сфері оборони» (яка є спонсором цього компендіуму). Ця програма розглядає боротьбу з корупцією як невід'ємну частину процесу реформ, однак продовжує зосереджуватися на розвитку позитивної динаміки у питаннях доброчесності, прозорості та підзвітності як найбільш важливих для ефективного оборонного менеджменту.

Вибрані установи та програми

Роль *Організації Об'єднаних Націй* у протидії корупції зосереджена загалом навколо імплементації Конвенції ООН проти корупції, яка вступила в дію у грудні 2005 року. Метою конвенції є розвиток спільної глобальної мови з питань корупції та ефективної системи індикаторів для цілеспрямованого виконання відповідних стратегій. Вона формує чотирьохкомпонентний підхід до боротьби з корупцією, який включає превентивні заходи, криміналізацію, міжнародне співробітництво та повернення цінностей.

Офіс ООН з питань боротьби з наркотиками і злочинністю втілює Глобальну програму проти корупції в якості каталізатора й ресурсу, який допомагає державам ефективно виконувати положення Конвенції. Він допомагає державам із вразливим станом економіки (що розвивається або перебуває у перехідному стані) шляхом заохочення антикорупційних заходів у державному та приватному секторах, у тому числі високі фінансові й політичні кола. Сфери застосування включають кодифікацію передового досвіду й політики, технічну допомогу у поширенні цього передового досвіду у державному й приватному секторах та ознайомлення суспільства.

Конкретні знаряддя для цього включають Групу доброчесності судової влади, запитальник самооцінки і законодавче керівництво для підписантів Конвенції.

Протягом останніх декількох років під тиском з боку ЗМІ та урядів країн-членів Департамент миротворчих операцій ООН також посилив свої антикорупційні зусилля, провівши декілька розслідувань та, в окремих випадках, відмовившись від залучення військ з країн, що мали проблеми з корупцією в минулому.

Організація економічного співробітництва та розвитку (ОЕСР) є міжнародною організацією, до складу якої входить 31 країна, кожна з яких поділяє цінності плюралістичної демократії, засновані на верховенстві права та повазі до прав людини, дотриманні відкритих і прозорих принципів ринкової економіки та спільних цілей стабільного розвитку. *(До складу ОЕСР входять: Австралія, Австрія, Бельгія, Канада, Чилі (приєдналася у січні 2010 року), Чеська Республіка, Фінляндія, Франція, Німеччина, Греція, Угорщина, Ісландія, Ірландія, Італія, Японія, Корея, Люксембург, Мексика, Нідерланди, Нова Зеландія, Норвегія, Польща, Португалія, Словацька Республіка, Іспанія, Швеція, Швейцарія, Туреччина, Сполучене Королівство та Сполучені Штати).*

ОЕСР стала одним з найбільш впливових форумів для діалогу з глобально важливих питань і робить суттєвий внесок у створення сильнішої, чистішої та справедливішої світової економіки. Використовуючи одне з найбільших у світі та найбільш надійне джерело порівняльної статистики, вона здійснює моніторинг тенденцій, аналізує і прогнозує економічний розвиток, а також досліджує соціальні зміни або еволюційні процеси у торгівлі, навколишньому середовищі, сільському господарстві,технологіях, податковій системі та державному управлінні.

Однією з важливих сфер діяльності організації є боротьба з корупцією. Остання є загрозою для ефективного врядування, демократичного процесу, стабільного розвитку т а справедливості у бізнесовій діяльності. Шляхом застосування багатокомпонентного підходу ОЕСР торкається проявів корупції у бізнесі, податковій системі, наданні допомоги з питань розвитку та у врядуванні всередині країн-членів та за їх межами. Це включає протидію тій стороні корупції, що представляє «пропозицію», запобігаючи хабарництву через експортні кредити, унеможливлюючи зменшення оподаткування за рахунок хабарів, заохочуючи відповідальну поведінку бізнесу, попереджуючи корупцію у сфері державного управління шляхом створення дієвої системи підтримки доброчесності та покращення врядування через підтримку розвитку. *(Для отримання більш детальної інформації див.: www.oecd.org/corruption).*

ОЕСР допомагає країнам у попередженні конфліктів інтересів і корупції у системі державної служби. Вона зосереджує увагу на таких вразливих сферах, як державні закупівлі та менеджмент контрактів, лобіювання і стан справ у політико-адміністративних стосунках. На основі перегляду й аналізу передового досвіду різних країн ОЕСР розробила відповідні інструменти для проведення своєї політики, настанови з питань їх імплементації та практичні рекомендації, щоб допомогти керівникам і менеджерам зміцнювати доброчесність і посилювати опір корупції у сфері державного управління.

Ключовим документом антикорупційних зусиль ОЕСР стала прийнята у 1997 році Конвенція з питань боротьби з хабарництвом серед іноземних державних посадовців (так звана «антихабарницька конвенція») та інші відповідні документи, які стосуються питань оподаткування, експортних кредитів, двосторонньої допомоги, багатонаціональних проектів і державних закупівель. *(OECD, "Key OECD Anti-Corruption Documents," www.oecd.org/document/42/0,3343,en_2649_37447_ 41799402_1_1_1_1,00.html.)* Ця конвенція є обов'язковим до виконання міжнародним договором, що розглядає «активну корупцію» – окремих осіб чи компанії, які обіцяють, пропонують або дають хабарі іноземним посадовим особам для того, щоб отримати або зберегти бізнесові преференції. Всі країни-члени ОЕСР плюс 7 економік країн - не членів є учасниками цієї «антихабарницької конвенції», і вони зобов'язалися у своєму національному законодавстві визнавати хабарі іноземним посадовим особам у міжнародному бізнесі кримінальним злочином, а також вживати ефективних заходів з метою попередження, виявлення, розслідування та покарання іноземного хабарництва.

Своєю боротьбою за викорінення хабарництва іноземних посадових осіб зі сфери конкуренції за контракти й інвестиції ОЕСР робить важливий внесок у запровадження рівних умов у сфері транснаціонального бізнесу, включаючи й оборонну промисловість.

Унікальність впливу антикорупційних інструментів ОЕСР полягає в тому, що вони вимагають від усіх учасників суворого контролю, за ефективність якого відповідає Робоча група ОЕСР з питань хабарництва. Детальні звіти про моніторинг оцінюють якість виконання країною антикорупційного законодавства.

Процес взаємної оцінки створює «дружній» тиск всередині Робочої групи і мотивує країни до найвищого рівня дотримання цієї конвенції.

Вставка 22.2. «Антихабарницька конвенція» ОЕСР та інтереси національної безпеки

Відповідно до статті 5 «антихабарницької конвенції» ОЕСР, питання розслідування фактів хабарництва іноземних посадових осіб та переслідування за них не повинні бути мотивовані національними економічними інтересами, потенційним впливом на відносини з іншою державою або особливостями причетної фізичної чи юридичної особи. Стаття 5 визнає можливість певних рамок прокурорської позиції, але обмежує ці рамки лише професійними мотивами (тобто вагою доказової бази), виключаючи неприйнятний вплив підходів політичного характеру. Дієвість статті 5 цієї Конвенції ОЕСР було піддано випробуванню у Сполученому Королівстві, коли розслідування надзвичайного випадку підозри у дачі хабара іноземній посадовій особі було зупинено нібито з причини необхідності забезпечення національної та міжнародної безпеки.

Факти. У період між липнем 2004 року та груднем 2006 року Офіс надзвичайних фальсифікацій (Serious Fraud Offi ce (SFO) Сполученого Королівства розслідував підозри у хабарництві з боку компанії BAE Системз під час реалізації контрактів «Аль-Ямамах» на поставку військових літаків до Королівства Саудівська Аравія. У жовтні 2005 року компанія BAE намагалася переконати генерального прокурора та SFO зупинити розслідування на підставі того, що його продовження може негативно вплинути на відносини між Сполученим Королівством і Саудівською Аравією, а також не дозволить Сполученому Королівству отримати, як було заявлено, найбільший експортний контракт за останнє десятиліття. У липні 2006 року, коли SFO впритул наблизився до отримання доступу до рахунків у швейцарському банку, раптом з'явилися особи, яких дехто вважає «саудівськими представниками», і висунули недвозначну погрозу керівникові апарату прем'єр-міністра Джонатану Пауеллу: якщо розслідування не буде припинено, то не відбудеться контракт на експорт літаків типу Тайфун, а також припиниться тісне розвідувальне й дипломатичне співробітництво. З цього приводу міністри висловили думку про те, що заявлені погрози може бути виконано, а це призведе до надзвичайно негативних наслідків для торгівлі озброєннями та для безпеки британських громадян і військовослужбовців. Вважаючи, що зазначені загрози життю були реалістичними, у грудні 2006 року директор SFO вирішив зупинити розслідування. У квітні 2008 року, після запиту від двох НУО щодо проведення розгляду в судовому порядку, Вищий Суд Сполученого Королівства прийшов до висновку, що розслідування у справі контрактів «Аль-Ямамах» було зупинене незаконно і у спосіб, який голова суду Мозес та член суду Салліван

визначили як «успішна спроба з боку іноземного уряду вплинути на судовий процес у Сполученому Королівстві». У липні 2008 року Палата Лордів, найвища апеляційна інстанція в країні, підтримала апеляцію SFO і призупинила рішення Вищого Суду, погодившись із тим, що директор SFO діяв у межах своїх повноважень, тому, з урахуванням можливості застосування статті 5 до питань національної безпеки, було прийнято остаточне рішення про те, що подальший розгляд потрібно залишити лише у компетенції Робочої групи ОЕСР з питань хабарництва.

Доповідь ОЕСР. У своїй доповіді про вивчення стану справ у Сполученому Королівстві Робоча група ОЕСР з питань хабарництва зробила висновок про неприйнятність інтерпретації статті 5 у контексті зазначеної вище ситуації, що стала предметом розгляду доповіді. Зокрема, у доповіді увагу зосереджено на процедурах застосування статті 5 та зроблено такі висновки:

i) в разі, коли припинення розслідування ставиться в залежність від положень статті 5, слідчі повинні застосовувати чіткий, суто принциповий підхід з метою з'ясування дійсних інтересів у прийнятті рішень посадовцями в рамках наявних повноважень; ii) справу не можна закривати на підставах інтересів національної безпеки допоки всі альтернативні рішення не будуть старанно досліджені і весь уряд не прийде до спільної позиції. Таким чином, випадок незавершеного розслідування у справі контрактів «Аль-Ямамах» висвітлив у Сполученому Королівстві ряд недоліків у системі розслідування і доведення до суду справ, які торкаються інтересів національної безпеки, зокрема, щодо умов застосування прокурорської позиції. Також він загострив необхідність глибокої реформи застарілого антихабарницького законодавства у Сполученому Королівстві. Він також показав необхідність подальших академічних досліджень та авторитетної інтерпретації статті 5 Конвенції ОЕСР з метою роз'яснення рамок очікуваного покарання за хабарі для іноземних посадових осіб.

Джерела: OECD Working Group on Bribery, Phase 2bis Report on the UK, www.oecd.org/dataoecd/23/20/ 41515077.pdf; The UK High Court judgment, www.bailii.org/ew/cases/ EWHC/ Admin/2008/714.html; The UK House of Lords judgment, http://www.publications.parliament.uk/pa/ld200708/ldjudgmt/jd080730/corner.pdf; TI 2009 Progress Report on the OECD Anti-Bribery Convention, http://www.transparency.org/ news_room/in_focus/2009/ oecd_pr_2009.

Група держав проти корупції (GRECO) під егідою Ради Європи працює над підтриманням і зміцненням плюралістичної демократії, прав людини та верховенства права. Зусилля Ради у справі боротьби з корупцією ґрунтуються на розумінні загрози, яку корупція становить самим основам цих ключових цінностей. Підхід Ради Європи у цій справі складається з трьох взаємопов'язаних елементів: (1) запровадження європейських норм і стандартів; (2) моніторинг дотримання цих стандартів; (3) пропозиція допомоги для окремих країн і регіонів у створенні необхідних спроможностей шляхом виконання програм технічного співробітництва.

Рада Європи розробила ряд правових інструментів для вирішення таких питань, як криміналізація корупції у державному та приватному секторах, відповідальність та компенсації за шкоду, заподіяну корупційними діями, поведінка державних посадових осіб і фінансування політичних партій. Ці інструменти направлені на підвищення спроможності держав у боротьбі з корупцією як усередині країни, так і на міжнародному рівні.

Моніторинг дотримання цих стандартів доручено проводити Групі держав проти корупції (GRECO). Цю Групу було створено Радою Європи у 1999 році з метою забезпечення моніторингу дотримання державами-членами антикорупційних стандартів. На сьогодні до її складу входять 46 членів, 45 європейських держав та Сполучені Штати Америки. Головним завданням Групи є підвищення здатності держав-членів боротися з корупцією. Це досягається шляхом підтримання динамічного процесу взаємних оцінок і «дружнього» тиску під час роботи моніторингових місій, які оцінюють дотримання державами стандартів Ради Європи, знаходять недоліки у національних антикорупційних підходах, а потім пропонують необхідні законодавчі, інституційні й практичні реформи. Група GRECO також забезпечує форум для обміну передовим досвідом у попередженні та виявленні корупції.

У липні 2008 року НАТО започаткував Трастовий фонд з метою виховання доброчесності та скорочення рівня корупції в оборонних структурах. Ця програма призначена для того, щоб підвищити національні спроможності у застосуванні трьох принципових інструментів:

- інструменту самооцінки, призначеного для оцінки поточного стану доброчесності та антикорупційних програм у оборонних структурах;
- курсів з питань виховання доброчесності для військового й цивільного персоналу;
- розробки компендіуму для сприяння поширенню передового досвіду (який саме зараз ви читаєте).

Трастовий фонд виховання доброчесності впроваджується спільно з такими партнерами, як Оборонна академія Сполученого Королівства, Женевський центр демократичного контролю над збройними силами, Женевський центр політики безпеки та Транспаренсі Інтернешнел.

Цей Трастовий фонд є природнім продовженням Плану дій НАТО з питань будівництва оборонних інститутів (Partnership Action Plan for Defence Institution Building (PAP/DIB), який було започатковано у липні 2004 року з метою надання допомоги країнам-партнерам у розвитку та утриманні ефективних оборонних інститутів, що діють під демократичним цивільним контролем. План PAP/DIB визначив десять цілей (див. Вставку 22.3) для країн, які будують оборонні структури, і запропонував три головні кроки, щоб

допомогти цим країнам у досягненні цих цілей:

- інтеграція процесу будівництва оборонних інститутів у процес оборонного планування ПЗМ (так званий «Процес планування та оцінки сил» – ППОС);
- розробка заходів для полегшення обміну досвідом; наприклад, модельна програма навчання пропонує детальний набір навчальних завдань та матеріал для допомоги у розробці програми навчання;
- допомога у формуванні двосторонніх оборонних і безпекових програм допомоги.

Трастовий фонд також покликаний допомогти державам виконати свої міжнародні зобов'язання, включаючи виконання Конвенції ООН проти корупції, «антихабарницької конвенції» ОЕСР, стратегії Світового банку з питань корупції, а також антикорупційних інструментів інших міжнародних і регіональних організацій.

Інтенсивне безпекове й оборонне співробітництво між НАТО та Україною під егідою Хартії про особливе партнерство створювало своєрідний інкубатор для інноваційних проектів. Цей приклад містить корисний досвід, який може бути застосований більш широко.

Вставка 22.3. Цілі Плану дій ПЗМ з питань будівництва оборонних інститутів

Цілями Плану дій є такі:

- створення ефективних і прозорих умов для демократичного контролю за оборонною діяльністю;
- участь цивільних у розробці питань політики оборони і безпеки;
- ефективний та прозорий законодавчий і судовий нагляд за сектором оборони;
- поглиблений аналіз безпекових ризиків та вимог національної оборони, які забезпечуються шляхом створення й підтримання посильних і взаємосумісних спроможностей;
- оптимізація менеджменту міністерств оборони та інших відомств, що мають споріднені організаційні структури;
- дотримання міжнародних норм і практики у секторі оборони, включаючи й експортний контроль;
- ефективні й прозорі процедури фінансування, планування та забезпечення ресурсами у сфері оборони;
- ефективний менеджмент оборонних витрат, а також соціально-економічних наслідків оборонної реструктуризації;
- ефективні і прозорі системи кадрового менеджменту у збройних силах;
- ефективне міжнародне співробітництво та добросусідські відносини з питань оборони і безпеки.

Джерело: *Partnership Action Plan for Defence Institution Building, www.nato.int.*

Одним з найбільш успішних інноваційних кроків було створення у 1998 році Спільної робочої групи між Україною і НАТО з питань оборонної реформи (СРГ-ОР). За понад десятирічний термін своєї діяльності СРГ-ОР допомогла Україні залучити досвід країн-членів НАТО з питань реформування секторів безпеки й оборони у різних форматах: від експертних семінарів до щорічних консультацій на рівні міністрів. Це виявилося особливо цінним у сенсі допомоги Україні в розробці програм реформування за рахунок отримання кращого міжнародного досвіду та практичної можливості працювати разом з країнами НАТО і залучати міжнародну допомогу, включаючи й розробку ряду інноваційних програм, створених спеціально під потреби України.

Цей спільний менеджмент також передбачав регулярні оцінки досягнутого прогресу.

Ряд конкретних ініціатив, що виникли в результаті співробітництва в рамках СРГ-ОР, заслуговують на увагу:

- експертна допомога у розробці ключових документів національної безпеки, що створюють дорожню карту реформ, зокрема, це Оборонні огляди у 2003 та 2009 роках, а також Стратегія національної безпеки у 2006 році;
- експертна допомога в розробці «Білих Книг», що забезпечували публічність оборонної політики та політики у секторі розвідки/безпеки й стану їх виконання;
- залучення багатьох технічних радників від країн-членів НАТО до роботи у Міністерстві оборони України, а також створення Об'єднаного координаційного комітету для координації цієї діяльності;
- співробітництво з парламентом у питаннях демократичного контролю, включаючи проведення семінарів, експертизу законодавчих актів і публікацію збірника нормативних документів з питань безпеки та оборони;
- створення Робочої групи між НАТО й Україною з питань демократичного контролю у секторі розвідки, в рамках якої вдалося зібрати разом десятки офіційних осіб і експертів з питань розвідки з країн НАТО й України для обговорення діяльності розвідувальних відомств у демократичних країнах;
- створення Програми професійного розвитку, в рамках якої отримали підготовку сотні цивільних службовців від оборонного та безпекових відомств України;
- створення мережі партнерства для розвитку експертизи у громадянському суспільстві з питань оборони і безпеки шляхом налагодження зв'язків між експертами з України та країн НАТО.

Багато з цих зусиль було імплементовано у тісній координації з Женевським центром демократичного контролю над збройними силами.

Женевський центр демократичного контролю над збройними силами (ДКЗС) є однією з провідних світових організацій з питань реформ сектору безпеки та управління сектором безпеки. Заснований урядом Швейцарії у 2000 році, він діє як міжнародна фундація, до якої входять 53 країни. ДКЗС розробляє і сприяє впровадженню відповідних демократичних норм на міжнародному й національному рівнях, пропагує передовий досвід і проводить дослідження з питань політики у сфері реформування сектору безпеки, а також надає дорадчу допомогу та проводить програми практичної допомоги. Він забезпечує виконання таких програм:

- Програма врядування у секторі безпеки;
- Програма дорадчої допомоги урядам;
- Програма допомоги парламентам;
- Програма громадянського суспільства;
- Програма оборонних реформ;
- Програма реформування поліції;
- Програма прикордонної безпеки;
- Програма підзвітності розвідки;
- Програма гендерних, дитячих та інших аспектів безпеки.

Виховання доброчесності та боротьба з корупцією в оборонному секторі. Збірник прикладів (компендіум) позитивного досвіду

(продовження в наступному номері)

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

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»