ЦИФРОВІ ІНІЦІАТИВИ

ГНУЧКА ПІДТРИМКА

У 2024 році Метінвест продовжував демонструвати стійкість і гнучкість, впроваджуючи важливі для бізнесу цифрові проєкти. Група посилила заходи з кібербезпеки завдяки оновленим протоколам і регулярним перевіркам, а також покращила технічні можливості через цільові тренінгові програми.

НАДІЙНИЙ ПОСТАЧАЛЬНИК ПОСЛУГ

У 2024 році цифровий порядок денний Метінвесту був зосереджений на основних пріоритетах, що відповідають за розвиток Групи: підвищення якості управління даними, розширення застосування технологій штучного інтелекту (ШІ) та посилення інформаційної безпеки.

Зусилля у сфері управління даними були спрямовані на підвищення ефективності завдяки автоматизації процесів і впровадженню цільових проєктів, як-от консолідація даних по торговельній діяльності, звітність за CBAM і HR-аналітика. Інструменти ШІ були впроваджені серед виробничих й адміністративних функцій, зокрема машинний зір, що забезпечував контроль якості та моніторинг безпеки. Ці ініціативи супроводжувалися навчанням персоналу, що охопило понад 3 000 співробітників. Інформаційну безпеку було посилено з метою захисту цифрової інфраструктури від кіберзагроз, як описано нижче.

Цифрова дорожня карта, ухвалена у 2020 році, залишалася головним орієнтиром діяльності Метінвесту в цій сфері. Її напрями було узгоджено з основними бізнес-функціями, проте обмеження воєнного часу вплинули на перехід на менші, короткострокові проєкти. Протягом звітного періоду основний фокус дорожньої карти був на основних операціях гірничо-збагачувальних комбінатів і підприємствах Групи поза межами України.

Метінвест продовжував послідовно впроваджувати довгострокову цифровізацію підприємств за кордоном. У звітному періоді Група завершила впровадження системи SAP CRM у Metinvest Polska, що дозволило підвищити ефективність операцій зі збуту.

Підтримка дистанційної роботи набрала обертів протягом року, адже цифрова платформа Metapolis перейшла від пілотного етапу до масштабного розгортання на дев'яти підприємствах Метінвесту в Україні. Покриття програми значно зросло, оскільки дедалі більше працівників перейшли з режиму тестування до активного користування, що стало важливим етапом цифрової трансформації Групи. Також впроваджено додаткові функціональні можливості, які підвищили доступність та ефективність робочих процесів. Серед основних результатів:

- доступ через мобільні, веб- та чат-боти
- розширене використання електронного документообігу з кваліфікованими електронними підписами
- подальша відмова від окремих паперових процесів.

ПОСИЛЕННЯ ПИЛЬНОСТІ

Метінвест керується у своїх діяльності Стратегією кібербезпеки на 2022–2026 роки. Вона спрямована на зниження ризиків, пов'язаних із витоками інформації та збоями систем, що можуть вплинути на критичне обладнання та процеси Групи. Стратегія також забезпечує дотримання відповідного законодавства, зокрема Загального регламенту захисту даних (GDPR).

Стратегія кібербезпеки підкріплена Політикою інформаційної безпеки та понад 15 внутрішніми регламентами, які охоплюють ключові напрями, зокрема безпеку даних і конфіденційність. Ці документи визначають процедури контролю доступу, оцінки ризиків та реагування на інциденти інформаційної безпеки.

Метінвест забезпечував відповідність системи інформаційної безпеки стандартам ISO 27001[1] та NIST[2], що підтверджується щорічними зовнішніми аудитами. Крім того, Група отримала сертифікацію за стандартом ISO 20000-1:2018, що підтверджує якість і надійність системи управління IT-послугами.

Основні дії з кібербезпеки у 2024 році були зосереджені на профілактиці, реагуванні на інциденти та зміцненні внутрішніх стандартів.

Метінвест забезпечував цілодобовий захист і впроваджував заходи, щоб підтримувати високий рівень кібербезпеки у Групі, а саме:

- регулярне тестування на вразливість, оцінку ризиків та оновлення чинних внутрішніх політик
- цілодобову роботу центру кібербезпеки для виявлення кіберзагроз, реагування й забезпечення стабільності систем
- впровадження засобів безпеки та мінімізації відомих вразливостей
- стримування спроб атак без фінансових втрат і з мінімальними перебоями.

Щоб підвищити обізнаність співробітників, протягом звітного періоду проводилися очні тренінги на теми, пов'язані з запобіганням шахрайству, захистом даних та кіберризиками в промислових системах. Для розробки протоколів реагування проводили симуляції фішингових атак. Щомісячні звіти для керівництва забезпечували постійний контроль і дозволяли відстежувати прогрес у зниженні ризиків.

[1] Цю сертифікацію пройшли Метінвест Діджитал та Метінвест Холдинг.
[2] Стандарти безпеки NIST, розроблені Національним інститутом стандартів і технологій (NIST), містять рекомендації, контрольні заходи й базуються на найкращих практиках для посилення кібербезпеки та забезпечення відповідності державним стандартам і регламентам.