

# Інформаційна безпека

GRI 418-1

**Технологічний прогрес супроводжується як можливостями, так і загрозами для нашого бізнесу. У зв'язку з переходом до онлайн-формату дедалі більше поширюються кібератаки, тому Група Метінвест запроваджує комплекс заходів із підвищення інформаційної безпеки.**

Ми забезпечуємо конфіденційність даних та дотримуємося чинних законів щодо збору, використання та захисту особистої інформації.

Також у Групі діє і постійно вдосконалюється система внутрішніх документів, зокрема стратегія та політика з інформаційної безпеки, а також регламенти та інструкції, що регулюють окремі процеси. Основні положення щодо захисту конфіденційної інформації викладено в нашій [Політиці конфіденційності](#), яка востаннє оновлювалася у березні 2020 року.

Група Метінвест керується визнаними галузевими стандартами та підходами у питаннях кібербезпеки. З метою загального управління інформаційною безпекою ми використовуємо стандарт ISO 27001. Задля вдосконалення процесів Група впроваджує підходи NIST SP 800, а для захисту персональної інформації – GDPR та українські нормативно-правові

акти. Ми використовуємо MITRE для вдосконалення можливостей виявлення загроз, а технічні аспекти регулюються згідно з найкращими практиками й конфігураціями CIS Security Benchmarks security library.

Захист інформаційних ресурсів у Групі Метінвест забезпечує комплекс технічних і організаційних заходів. Багатошаровий захист IT-інфраструктури забезпечується завдяки використанню сучасних рішень, таких як: міжмережеві екрани (Firewall), системи захисту від вторгнень (Intrusion Prevention System), захист хмарної інфраструктури (Azure Security Center, Web Application Firewall), аналіз мережевого трафіку (Network Traffic Analysis), аналіз нетипових операцій та активності (User Behavior Analytics) та

централізований моніторинг і керування IT-компонентами (Configuration Management, Vulnerability Management).

Важливою складовою нашого інформаційного захисту є Центр кібербезпеки. Він особливо допомагає у випадках, коли ми маємо справу з висококваліфікованими зловмисниками, які застосовують методи обходу автоматизованих механізмів захисту. Робота центру передбачає моніторинг IT-інфраструктури та виробничих процесів Метінвесту, виявлення і реагування на кібернетичні атаки на Групу та координацію роботи IT-підрозділів під час інцидентів.

## Система захисту конфіденційної інформації Data Leakage Prevention

Інвентаризація і визначення категорій конфіденційної інформації та оцінка ризиків витоку критичної для бізнесу інформації відбувається за допомогою:

- Маркування та шифрування інформації
- Виявлення та блокування спроб несанкціонованого передавання інформації
- Навчання співробітників щодо безпечної роботи з інформацією
- Моніторингу ризикових операцій та ролей
- Ревалідації прав доступу і повноважень
- Захищеного підключення до корпоративних ресурсів
- Корпоративних засобів для відеоконференцій та спільної роботи з документами





Група Метінвест розвиває комплексний захист (Identify, Protect, Detect, Respond, Recover) із широким використанням автоматизації та машинного навчання. Для підвищення обізнаності наших співробітників у питаннях інформаційної безпеки ми впроваджуємо початковий інструктаж щодо базових правил ІТ-безпеки, періодичні мінікурси з окремих аспектів безпечної роботи з інформацією, тренінги з інструктором для персоналу, який працює з автоматизованою системою управління процесами, та періодичні навчальні кібератаки для перевірки готовності до них співробітників Групи Метінвест.

Для розуміння свого поточного рівня інформаційної безпеки і визначення пріоритетів розвитку в цьому напрямі Група Метінвест систематично проводить внутрішні аудити ефективності функції та цільові зовнішні аудити. Для кожного процесу ми використовуємо операційні метрики та проводимо самооцінку на відповідність найкращим практикам. У 2020 році ми впровадили щорічні перевірки надійності нашого захисту через багатовекторне тестування на проникнення «білих хакерів» (penetration testing). Такі перевірки максимально наближені до реальних хакерських атак та дають нам змогу правильно розставляти пріоритети в налагодженні систем безпеки, постійно вдосконалюватися і тренувати команду в умовах потенційної небезпеки.

У 2020 році Метінвест підтвердив високий рівень інформаційної безпеки: в рейтингу від Microsoft Secure Score ми отримали оцінку 49%, що на 15 відсоткових пунктів вище, ніж в інших компаній галузі.