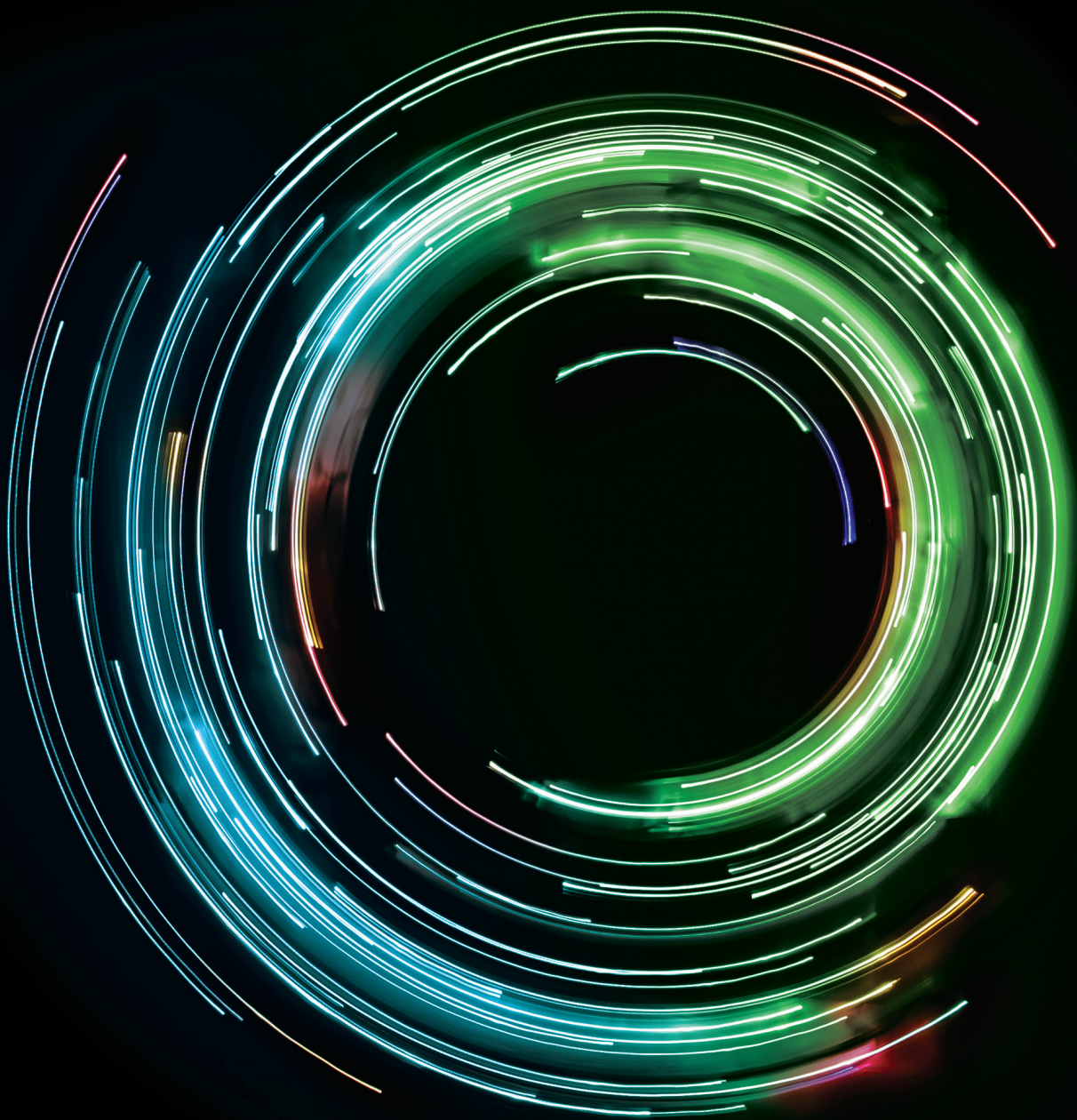

Надійна основа
Вашого розвитку

Каталог послуг

infocom
TRUSTED SECURITY

Компанію Infocom було засновано у 1991 році як спільне товариство Міністерства Зв'язку та німецької IT-компанії Controlware.

Infocom розпочав свою діяльність з побудови першої мережі передачі даних в Україні – UkrPack, яка була зареєстрована в CCITT, як національна мережа України з кодом присвоєння DNIC - 2550. Infocom отримав ліцензію Міністерства Зв'язку України №1 на надання послуг.

Першими міжнародними партнерами Infocom стали Datex-P (Німеччина) та Sprint (США), завдяки яким Україна отримала доступ до більш ніж 120 світових мереж передачі даних та вперше в Україні з'явилася можливість доступу до електронної банківської системи SWIFT.

Сьогодні Infocom є українською IT-компанією, яка динамічно розвивається та має багатий досвід. Infocom забезпечує роботу критичної урядової інфраструктури, надає послуги міжнародним та державним організаціям, енергетичному, фінансовому та приватному секторам.

Наша місія – бути надійною основою для Вашого розвитку.

infocom
TRUSTED SECURITY

infoGuard

СУЧАСНИЙ БАГАТОРІВНЕВИЙ ЗАХИСТ ПЕРИМЕТРУ МЕРЕЖІ ТА РОБОЧИХ МІСЦЬ

Сканування трафіку, як звичайного так і **зашифрованого**, забезпечує захист найвищого рівня від усіх відомих загроз: вірусів, шпигунського програмного забезпечення, троянів, фішинг-програм, системних моніторів, кілоґґерів, рекламного програмного забезпечення та інших. **Система використовує базу даних про загрози, що оновлюється у режимі реального часу** та є спільним ресурсом Cyber Threat Alliance, у який входять основні світові компанії з кібербезпеки.

Головною метою сучасних кіберзлочинців є **викрадення конфіденційної корпоративної та особистої інформації** через вторгнення у мережу завдяки наявним вразливостям встановленого обладнання та програмного забезпечення. **Система запобігання вторгненням** сервісу infoGuard постійно аналізує всі зовнішні запити, що дозволяє попередити можливі атаки та спричинені цим негативні наслідки. Крім того, infoGuard має гнучку систему внутрішнього контролю, яка значно зменшує вірогідність витоку конфіденційної інформації, спричиненого ненавмисними, або навмисними діями співробітників компанії.

Робочі місця дуже часто стають ціллю різноманітних кібератак. Нещодавнє дослідження показало, що **30% атак було скоєно за допомогою ураження кінцевих точок шкідливим ПЗ**. Шляхом встановлення на комп'ютери агентів з інтегрованим засобами відстеження, контролю та запобігання розповсюдження шкідливого ПЗ infoGuard значно посилює безпеку робочих місць.

Сервіс infoGuard містить функцію **динамічної веб-фільтрації в режимі реального часу**, яка блокує відвідування співробітниками компанії скомпрометованих, або навмисно створених ресурсів за допомогою яких злочинці отримують доступ до персональних та корпоративних даних, або завантажують шкідливе програмне забезпечення. За потребою клієнта система дозволяє створити додаткові фільтри та закрити для перегляду співробітниками окремі сайти, або цілі категорії веб-ресурсів: із азартними іграми, онлайн переглядом фільмів, «дорослі» ресурси, тощо.

infocom
TRUSTED SECURITY

Функція контролю додатків infoGuard безперервно класифікує і оцінює трафік програм, якими користуються співробітники компанії. Система контролю дозволяє блокувати, або обмежити доступ до ризикованих програм, цілих категорій програм, оптимізує використання пропускної здатності у Вашій мережі, встановлюючи пріоритети програм чи повністю блокуючи небажаний трафік. Наприклад, перегляд відео у соціальних мережах, залишаючи при цьому можливість перегляду світлин та дописів.

Сервіс infoGuard це:

- Оптимізація Ваших витрат на забезпечення кіберзахисту завдяки **відсутності потреби купувати дороге сучасне обладнання та ліцензії до нього**
- **Безпечне користування мережею Інтернет**
- Зниження ризиків порушення діяльності Вашої компанії
- Можливість оперативно змінювати кількість підключених до сервісу філій/відділень/робочих місць, як у бік збільшення, так і у бік зменшення
- Залучення фахівців Infocom без необхідності у додатковому навчанні власних
- Моніторинг і контроль атак та інцидентів 24x7x365
- Підтримка 24x7x365

infoSDWAN

НАДІЙНА ІНФРАСТРУКТУРА НА БАЗІ ТЕХНОЛОГІЇ SD-WAN

Мережа SD-WAN функціонує як надбудова над транспортним рівнем і повністю незалежна від типу наявної лінії зв'язку, тому послуга **infoSDWAN розгортається на базі доступу до мережі Інтернет будь-яких провайдерів за будь-якою технологією**. Розгортання послуги передбачає встановлення в офісі замовника обладнання компанії Infocom, до якого під'єднується один, або декілька каналів з доступом у мережу Інтернет від різних провайдерів, після чого встановлене обладнання отримує автоматично повну конфігурацію з контролеру сервісу infoSDWAN, що розташований на майданчику компанії Infocom. Час потрібний на **розгортання послуги, як правило, не перевищує кількох днів** і здебільшого залежить тільки від часу доставки необхідного обладнання кур'єрськими службами.

infocom
TRUSTED SECURITY

Послуга infoSDWAN дозволяє **оперативно організовувати віддалений доступ** до корпоративної мережі працівникам, що змушені працювати поза межами офісу. Для цього достатньо встановити на комп'ютер або ноутбук працівника спеціальне програмне забезпечення, яке не потребує жодних налаштувань. Все що потрібно - це ввести наданий компанією Infocom логін та пароль які «прив'язані» до Вашої мережі, після чого програма автоматично отримає всі необхідні налаштування та надасть відповідний доступ.

Система **менеджменту та моніторингу каналів зв'язку** постійно перевіряє якість з'єднання на наявність затримок та втрати пакетів даних. Якщо якість зв'язку погіршується, система автоматично коригує маршрут надсилання даних та проводить їх дублювання, що значно зменшує вірогідність втрати даних. **Інтелектуальна система балансування навантаження** на канали зв'язку забезпечує оптимальне використання наявних ресурсів для якісної роботи додатків та сервісів. При наявності двох чи більше каналів система забезпечує постійне активне резервування.

Системі **контролю додатків** infoSDWAN відомо більш ніж 4500 існуючих програм, що дозволяє у автоматичному режимі, або за попередньо встановленими налаштуваннями контролювати роботу наявних програм, надавати пріоритет та прискорювати критично важливі. Прикладом може бути ситуація коли система контролю автоматично призупинить чи сповільнить швидкість доступу до мережі другорядних сервісів, поки у мережі здійснюється відеоконференція яку визначено пріоритетною.

Технологія SD-WAN, або програмно-конфігурована глобальна мережа, є еволюційним розвитком організації корпоративних мереж, яка дозволяє значно спростити процес побудови мережі та зменшити її вартість, скоротити час на розгортання, підвищити надійність, вдосконалити функції управління, контролю та моніторингу.

Сервіс infoSDWAN це:

- Ваша корпоративна **мережа у будь-якій точці України та світу** як послуга
- Оптимізація Ваших витрат на побудову сучасної **захищеної** корпоративної мережі завдяки **відсутності потреби купувати дороге сучасне обладнання та ліцензії до нього**
- Можливість **оперативно змінювати кількість підключених до сервісу філій/відділень/робочих місць**, як у бік збільшення, так і у бік зменшення
- **Можливість додатково підключити сервіс з інформаційної безпеки infoGuard за унікальною ціною**
- Економія Вашого часу та можливість повністю сконцентруватись на Ваших стратегічних планах та задачах
- Підтримка 24x7x365

infocom
TRUSTED SECURITY

infoDDoS

БЕЗПЕРЕРВНА РОБОТА РЕСУРСІВ ЗАВДЯКИ ЗАХИСТУ ВІД DOS/DDOS АТАК

У сучасному світі **Web-портал є важливим інструментом ведення бізнесу, зупинка якого може призвести до недоотриманого прибутку, репутаційних та прямих фінансових втрат**. Це особливо характерно для **інтернет-торгівлі, банків, платіжних систем** та усіх інших, чия робота глибоко пов'язана, або повністю залежить від взаємодії з клієнтом через власний Web-портал. Зловмисники знають про важливість онлайн-ресурсів для комерційних і державних організацій і регулярно роблять спроби злому за допомогою розподілених DDoS-атак, метою яких є порушення їх працездатності. Такі **атаки можуть здійснювати як звичайні зловмисники, вимагаючи сплати за припинення атаки, так і недобросовісні компанії, які намагаються загальмувати розвиток бізнесу компанії-конкурента.**

Одним із найпоширеніших методів такої кібератаки є насичення інфраструктури клієнта великою кількістю зовнішніх запитів таким чином, що атаковане устаткування не може відповісти справжнім користувачам, або відповідає настільки повільно, що стає, фактично, недоступним. Як правило, відмова атакованого сервісу досягається шляхом:

- примусу до повної зупинки роботи програмного забезпечення/устаткування атакованого сервісу, або до витрат наявних апаратних ресурсів, внаслідок чого устаткування не може продовжувати роботу
- перевантаження комунікаційних каналів між користувачами і атакованим сервісом, внаслідок чого якість передачі даних перестає відповідати будь-яким (навіть мінімальним) вимогам

Завдяки сервісу infoDDoS ми можемо протистояти всім відомим типам DoS/DDoS-атак та забезпечимо безперервну роботу Ваших ресурсів в мережі Інтернет за допомогою багаторівневого захисту, в який входить:

- поведінковий захист
- система запобігання вторгнень
- захист від SYN-флуду
- обмеження одночасних з'єднань
- обмеження трафіку
- технологію SPI (інспекція пакетів зі збереженням стану)
- захист від сканування
- протидію http-атакам

Платформа infoDDoS має **вбудовану систему запобігання зовнішнім вторгненям**, яка є оптимальним рішенням протидії DDoS-атакам та високопродуктивним методом захисту від відомих вразливостей програмного забезпечення. Крім цього, платформа дозволяє уникнути ризиків проникнення «комп'ютерних черв'яків» та з легкістю **виявляє роботу «ботів» на комп'ютерах співробітників**.

infocom
TRUSTED SECURITY

Сервіс infoDDoS це:

- **Надійний захист від DoS/DDoS-атак та безперервна робота Ваших ресурсів** у мережі Інтернет
- Зниження ризиків порушення діяльності Вашої Компанії
- Оптимізація Ваших витрат на забезпечення кіберзахисту завдяки **відсутності потреби купувати дороге сучасне обладнання та ліцензії до нього**
- Економія Вашого часу та можливість повністю сконцентруватись на Ваших стратегічних планах та задачах
- Залучення фахівців Infocom без необхідності у додатковому навчанні власних
- Моніторинг і контроль атак та інцидентів 24x7x365
- Підтримка 24x7x365

infoMail

КОМПЛЕКСНИЙ ЗАХИСТ ЕЛЕКТРОНОЇ ПОШТИ

Сучасну систему кіберзахисту неможливо уявити без її невід'ємної складової – захисту електронної пошти. Згідно з VERIZON 2019 DATA BREACH INVESTIGATIONS REPORT **понад 92% шкідливого програмного забезпечення отримується по Email**. Незважаючи на заходи безпеки, яківживаються компаніями, **49% заражень шкідливим ПЗ відбувається саме через електронну пошту**.

Сервіс infoMail розроблений для боротьби із сучасними загрозами широкого спектру, що виникають в наслідок використання електронної пошти такими як: віруси, шкідливе програмне забезпечення, спам, листи з посиланнями на ресурси що містять шкідливе програмне забезпечення, витік конфіденційної інформації спричинений фішинг технологіями, витік критичної інформації спричинений помилковими, або навмисними несанкціонованими діями працівників компанії.

Щоб ефективно боротися з новими кібернетичними загрозами аналітичний центр сервісу infoMail аналізує по всьому світу мільйони електронних листів на годину і може ідентифікувати новий небезпечний код за лічені хвилини. Усі підозрілі вкладення, виявлені в електронних листах блокуються для аналізу у лабораторіях інформаційної безпеки. Створена база даних постійно доповнюється та є спільним ресурсом CYBER THREAT ALLIANCE, в який входять світові лідери з кібербезпеки.

infocom
TRUSTED SECURITY

Найшвидшим та дієвим механізмом захисту від **спаму та фішингових повідомлень** є використання репутаційних баз даних. Під час отримання повідомлення на електронну пошту, система перевіряє IP-адресу відправника та вміст щодо наявності їх у такій базі. Якщо відповідний відправник має негативну репутацію, то лист блокується.

Сучасний захист не можливо уявити без надійного антивірусу. Сервіс infoMail налічує в своїй базі понад **50 000 сигнатур різних варіантів сімейств вірусів**. Так само як і репутаційна база даних, база даних вірусних сигнатур постійно оновлюється у режимі реального часу. Під час перевірки антивірус аналізує вміст вкладень та за потреби проводить розпакування наявних архівів, розшифровує файли, видаляє активний вміст підозрілих файлів та HTML.

Сервіс infoMail перевіряє електронні листи та надсилає підозрілі файли та посилання у так звану хмарну «пісочницю» для подальшого аналізу. У «пісочниці» створюється віртуальне середовище у якому підозрілий код запускається так, ніби він потрапив у реальну систему отримувача. Під час цієї перевірки аналізуються дії підозрілого коду, чи намагається він зв'язатися для отримання інструкцій, чи запускає будь-які процеси, які суперечать політиці безпеки, тощо. Після перевірки система призначає відповідний рейтинг, згідно якому виконуються подальші дії, такі як дозвіл на доставку отримувачеві, або видалення.

Сервіс infoMail це:

- **Надійний захист Вашої електронної пошти та даних**
- Зниження ризиків порушення діяльності Вашої Компанії
- Оптимізація Ваших витрат на забезпечення кіберзахисту завдяки **відсутності потреби купувати дороге сучасне обладнання та ліцензії до нього**
- Економія Вашого часу та можливість повністю сконцентруватися на Ваших стратегічних планах та задачах
- Підтримка 24x7x365

infocom
TRUSTED SECURITY

Передача даних

ЗАКРИТІ КОРПОРАТИВНІ МЕРЕЖІ

Будь-який бізнес, офіси якого знаходяться на значній відстані один від одного, потребує побудови єдиної масштабованої і безпечної телекомунікаційної інфраструктури, основою якої є корпоративна мережа, що створює єдиний об'єднаний інформаційний простір для всіх територіально розподілених підрозділів та об'єктів.

На базі мережі УкрПак (побудованою за технологіями MPLS/VPN, IP VPN) клієнтам надається можливість будувати власні закриті корпоративні мережі та отримувати послуги доступу до мереж загального користування (Інтернет, мережі надання фінансових послуг, телефонна мережа, аудіо та відеоконференцзв'язок тощо). Використовуючи ресурси мережі MPLS, Infocom надає послуги як другого (L2), так і третього рівня (L3).

Наша компанія має великий досвід у проектуванні та побудові корпоративних мереж з кількістю точок підключення до кількох тисяч. Серед таких: корпоративні мережі Державної служби зайнятості України, банку «Universal Bank», МВС України, Пенсійного фонду України та багатьох інших.

Інтернет

ДОСТУП ДО МЕРЕЖІ ІНТЕРНЕТ

Найшвидший і найпростіший спосіб підключитися до Інтернет саме з тими параметрами, які оптимально відповідають Вашим потребам – звернутися до нас та отримати консультацію спеціаліста. У залежності від Вашого місцезнаходження та технічних вимог щодо доступу до мережі Інтернет, ми допоможемо обрати оптимальний спосіб підключення та тарифний план.

Ми надаємо послуги Інтернет за наступними технологіями: **WiFi**, **WiMAX**, **GPON**, **FTTx** та **ADSL**:

- Технології **WiFi** та **WiMAX** забезпечують отримання швидкісного безлімітного доступу до мережі Інтернет та віртуальних локальних мереж у місцевостях без розвиненої кабельної інфраструктури.
- Послуга доступу до мережі Інтернет за технологією **GPON** передбачає прокладання волоконно-оптичної кабельної лінії безпосередньо до будівлі користувача. Технологія GPON дозволяє мати надійний персональний оптичний канал зі швидкістю доступу до Інтернет до 1 Гбіт/с.
- Послуга доступу до мережі Інтернет за технологією **FTTx** дозволяє споживачам мати постійний доступ до мережі Інтернет по виділеній волоконно-оптичній лінії на швидкості від 5 до 10 Гбіт/с.

В поєднанні з послугами з інформаційної безпеки **infoGuard** та **infoDDoS** Ви отримуєте **безпечне підключення до мережі Інтернет** із захистом від вірусів, шпигунського програмного забезпечення, троянів, фішинг-програм, системних моніторів, кілоґґерів, рекламного програмного забезпечення та DoS/DDoS-атак.

infocom
TRUSTED SECURITY

ManuScan

СИСТЕМА БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

ManuScan – це система біометричної ідентифікації, що використовує метод сканування вен у долоні. Даний метод ідентифікації у сотні разів надійніший, ніж найпоширеніший зараз метод сканування відбитків пальців та є **безконтактним**, що є дуже важливим з огляду на **гігієнічність**. За своєю ефективністю метод складає пряму конкуренцію складнішим та дорогим системам, що використовують технологію сканування сітківки, або зіниці ока, залишаючись при цьому більш комфортним та простим у використанні.

Робота системи ManuScan заснована на зчитуванні відбитого від людської долоні випромінювання в інфрачервоній області спектра. Оскільки відновлений гемоглобін крові поглинає інфрачервоне випромінювання, то від венозних судин долоні відбивається випромінювання меншої інтенсивності, ніж від решти її поверхні. Так формується **унікальний малюнок венозних судин**, і вени стають видимими при скануванні в ІЧ-променях.

Процес ідентифікації системою ManuScan проходить наступним чином:

- Необхідно піднести долоню до сканера системи;
- Камера з сенсором зчитує зображення відбитку вен і конвертує його в унікальний «хеш», що порівнюється зі зразком у захищеній базі даних;
- Спрацьовує алгоритм відповідно до налаштованих профілів, в залежності від застосування системи ідентифікації.

ManuScan це:

- Точна та швидка ідентифікація
- **Гігієнічність** (відсутність контакту с поверхнею сенсора)
- Інтегрованість у більшість систем контролю доступу та індустріальних систем, яким необхідна точна ідентифікація користувачів
- Простота та зручність у користуванні
- Стабільна працездатність за будь-яких погодних і кліматичних умов (від -25°C до + 85°C)
- Потрійна система шифрування
- **Неможливість підробки**
- Простота монтажу
- Підтримка 24x7x365

infocom
TRUSTED SECURITY

Ми надаємо
нові можливості
для Вашого бізнесу

infocom
TRUSTED SECURITY

Карта присутності

1000+
вузлів зв'язку

500+
базових станцій WiFi

9000+
точок присутності в Україні

300+
співробітників, які обслуговують клієнтів по всій країні

22
регіональні офіси

19 000+
клієнтів

СП ТОВ «Інфоком»
+38 (044) 230-52-00
01001, Київ, вул. Володимирська, 8
sales@infocom.ua • **infocom.ua**

infocom
TRUSTED SECURITY