Надійна основа Вашого розвитку

Каталог послуг

infocom
TRUSTED SECURITY

Структура послуг Infocom

Бути надійною основою Вашого розвитку - не просто місія Infocom, але насамперед філософія нашої компанії. З моменту заснування Infocom, у 1991 році, ми безперестанно вдосконалюємо та доповнюємо перелік наших послуг у відповідь на сучасні потреби та безпекові виклики з якими стикаються як бізнес, так і державні установи. Наші послуги органічно доповнюють одна одну, що дозволяє не тільки побудувати чи вдосконалити тій чи інший аспект телекомунікаційної складової наших клієнтів, але й забезпечити максимально можливий захист від наявних кіберзагроз на усіх рівнях. Саме оптимальне поєднання безпекових та телекомунікаційних послуг є запорукою надійної та якісної роботи інформаційної інфраструктури, яка в сучасному світі є невід'ємною частиною будь-якої компанії чи організації.

АУТСОРСИНГ

У складних економічних умовах ведення бізнесу вимагає від менеджменту та співробітників компанії максимальної зосередженості, скрупульозного аналізу ринкової ситуації та пошуку можливостей для розвитку. Делегування наявних непрофільних завдань стороннім підрядникам дозволяє компаніям та організаціям зосередитись виключно на профільній діяльності та спрямувати всі свої внутрішні ресурси на досягнення поставлених цілей.

infoStructure

web-сторінка послуги

АУТСОРСИНГ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

infoStructure - послуга комплексного аутсорсингу спрямована на зменшення витрат та адміністративних і IT-ресурсів компанії шляхом делегування різноманітних організаційних та технічних завдань стосовно проектування, розбудови, підключення, оптимізації, модернізації, підтримки та захисту інформаційної інфраструктури із залученням спеціалістів та технічних ресурсів Infocom.

Утримання власної IT-інфраструктури на перший погляд виглядає привабливіше з точки зору економії коштів і контролю над процесами, але при глибшому аналізі усіх супутніх витрат та врахуванні частих змін на ринку такий підхід далеко не завжди виявляється доцільним, особливо для компаній, які швидко зростають або мають розподілені офіси, або філії. Кожна локація потребує надійного підключення до мережі «Інтернет» чи корпоративної мережі, закупівлі та встановлення необхідного для роботи мережевого та офісного обладнання, його відповідного налаштування, захисту та підтримки в робочому стані, резервуванні, адміністративного обліку, тощо. Все це неминуче призводить до значних додаткових витрат, адже чимала частина затрат на підтримку власної IT-інфраструктури є, на перший погляд, непомітною або вважається несуттєвою, але в довгостроковій перспективі може значно накопичитися, роблячи аутсорсинг вигіднішим та більш ефективним рішенням.

Концепція послуги infoStructure спрямована на зменшення витрат на розбудову та підтримку IT-інфраструктури, на спрощення і пришвидшення процесу підключення до неї нових локацій через відсутність необхідності залучення власних ресурсів на пошук та придбання відповідного обладнання, його налаштування та обслуговування. З іншого боку, користування послугою усуває також багато труднощів пов'язаних із закриттям філіалів або відділень. Користувачу послуги не потрібно шукати нових, або скорочувати наявних співробітників, не потрібно купувати нове, або думати, що робити з наявним зайвим обладнанням. Все що потрібно - це подати заявку на збільшення або зменшення обсягу послуг.

Основні аспекти, які варто врахувати при виборі між власною IT-інфраструктурою та відповідною послугою аутсорсингу Infocom:

- ПОЧАТКОВІ ІНВЕСТИЦІЇ

  Розбудова власної IT-інфраструктури потребує значних початкових витрат на закупівлю обладнання, програмного забезпечення, пошук та навчання відповідного персоналу. З іншого боку, послуга infoStructure дозволяє значно знизити початкові витрати, оскільки наша інфраструктура вже готова до використання.

- ЗМІННІ ВИТРАТИ

  Утримання власної IT-інфраструктури пов'язане з постійними витратами на обслуговування, підтримку та оновлення обладнання і програмного забезпечення. Такі витрати можуть створювати невизначеність у бюджеті компанії, оскільки несподівані проблеми, наприклад, з мережею через вихід з ладу її важливих компонентів, можуть призвести до неочікуваного та значного перевищення суми, запланованої на її підтримку. Аутсорсинг IT-інфраструктури може допомогти вам уникнути цих проблем, адже Infocom пропонує фіксовані ціни на свої послуги, що спрощує планування вашого бюджету.

- МАСШТАБОВАНІСТЬ

  При зростанні бізнесу власна IT-інфраструктура може потребувати значних змін та модернізації як технічно, так і організаційно. Аутсорсинг дозволяє легко та швидко масштабувати інфраструктуру, додавати нові локації та різноманітні послуги без жодних зусиль шляхом простої подачі відповідних заявок на зміни. Це забезпечує гнучкість та ефективність у відповідь на нові потреби вашого бізнесу та дозволяє бути більш конкурентоспроможним у змінному середовищі.

- ІНФОРМАЦІЙНА БЕЗПЕКА

  Однією з ключових переваг аутсорсингу Infocom є доступ до передових технологій та професійного персоналу, який спеціалізується на кібербезпеці. Використання спеціалізованого програмного забезпечення та рішень для захисту мережі, інтелектуальних систем виявлення інцидентів та реагування на них, допомагає запобігати потенційним загрозам і забезпечує високий рівень захисту від різноманітних кібератак.

- АКТУАЛЬНІСТЬ ТЕХНОЛОГІЙ

  Infocom підтримує та постійно оновлює свою інфраструктуру, щоб відповідати найсучаснішим вимогам і стандартам. Це дозволяє нашим клієнтам користуватися новітніми технологіями без необхідності постійних інвестицій у навчання технічного персоналу, оновлення власного обладнання та програмного забезпечення.

- ЄДИНИЙ КОНТАКТ

  У якості аутсорсингового партнера, Infocom надає компанії-клієнту єдиний контактний номер для вирішення питань, пов'язаних з інформаційною інфраструктурою. Це значно спрощує управління інфраструктурою, звільняючи від необхідності постійно контактувати з локальними операторами, різноманітними постачальниками обладнання та комплектуючих тощо. Наша компанія забезпечує повний спектр послуг, що дозволяє клієнту зосередитися на своїх головних ділових завданнях, маючи впевненість, що захист та підтримка інформаційної інфраструктури знаходяться в надійних руках.

- ЮРИДИЧНА ВЗАЄМОДІЯ

  Обираючи аутсорсинг інформаційної інфраструктури, ваша компанія позбавляється складних і множинних юридичних відносин. Замість того, щоб укладати окремі договори з різними постачальниками та постійно підключати юристів для перевірки умов кожного контракту, наші клієнти мають можливість укласти один єдиний договір з Infocom. Це значно спрощує процес юридичних формальностей, забезпечуючи зручність та ефективність в управлінні інфраструктурними послугами.

У рамках послуги аутсорсингу інформаційної інфраструктури пропонується не лише одна єдина опція яка б обов'язково включала повний перелік послуг необхідних для функціонування інфраструктури, але й можливість вибору вами часткового аутсорсингу в залежності від ваших потреб. Концепція infoStructure дозволяє нам підтримати ваш бізнес на кожному етапі зручним та ефективним способом. Наприклад, ми готові взяти на себе підключення всіх ваших офісів до мережі «Інтернет» за єдиним контрактом та стандартом якості, або забезпечити всі філії резервними каналами зв'язку для надійної роботи. Наша команда може розбудовувати та адмініструвати корпоративну мережу, використовуючи для цього як обладнання Infocom, так і ваше наявне обладнання, або забезпечити сучасний інформаційний захист вашої вже існуючої інфраструктури, гарантуючи конфіденційність та цілісність критичної інформації.

Наші послуги можуть бути адаптовані до ваших унікальних потреб, незалежно від обсягу аутсорсингових послуг, які ви оберете. Ми прагнемо стати вашим надійним партнером у розвитку та оптимізації інфраструктури, щоб ви могли зосередитися на стратегічних аспектах вашого бізнесу та досягненні успіху.

Послуга infoStructure це:

- Скорочення витрат адміністративних та IT-ресурсів
- Зменшення сукупних витрат на розбудову та підтримку інформаційної інфраструктури
- Прогнозовані щомісячні витрати у вигляді фіксованої абонентської плати
- Можливість оперативно змінювати кількість підключених до сервісу філій/відділень, як у бік збільшення, так і у бік зменшення
- Зниження ризиків порушення діяльності вашої компанії.
- Підтримка 24x7x365

КОРПОРАТИВНІ МЕРЕЖІ

Основою кожної інформаційної інфраструктури є корпоративна мережа, яка дозволяє створити єдиний інформаційний простір всередині компанії або організації між територіально розподіленими підрозділами. З щоденним зростанням рівня використання цифрових технологій та все більшим покладанням їх у основу ведення діяльності саме швидке масштабування та надійність корпоративної мережі стають не просто її бажаними властивостями, а критичною необхідністю яка безпосередньо впливає на всі виробничі, фінансові, організаційні або будь-які інші процеси всередині компанії.

infoSDWAN

web-сторінка послуги

КОРПОРАТИВНА МЕРЕЖА НА БАЗІ ТЕХНОЛОГІЇ SD-WAN

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

Перехід від корпоративних мереж побудованих за технологією MPLS (багатопротокольна комутація за мітками) на мережі SD-WAN є на цей час одним із найпопулярніших глобальних трендів у галузі мережевих технологій. MPLS VPN – це традиційна технологія побудови закритих корпоративних мереж, яка використовується для зв'язку між офісами компаній та централізованого надання доступу до мережі «Інтернет» вже понад два десятиліття, однак зі стрімким розвитком хмарних технологій, електронної комерції та майже тотальною діджиталізацією усіх процесів у різноманітних галузях, мережеві вимоги багатьох компаній стали змінюватися і технологія SD-WAN завдяки своїм очевидним перевагам стала більш привабливою альтернативою.

Корпоративна мережа SD-WAN розгортається на базі доступу до мережі «Інтернет». Розгортання передбачає передачу в офіси замовника обладнання, яке підключається до одного або декількох каналів з Інтернет-доступом від різних провайдерів, що своєю чергою забезпечує додаткове резервування та значно підвищує надійність. Після підключення до інтернету відбувається автоматичне завантаження необхідних налаштувань з контролеру сервісу infoSDWAN та подальше об'єднання обладнання у єдину корпоративну мережу. Час потрібний на розгортання подібної захищеної мережі, як правило, не перевищує кількох днів і здебільшого залежить від часу доставлення необхідного устаткування кур'єрськими службами.

Послуга infoSDWAN дозволяє оперативно організовувати захищений віддалений доступ до корпоративної мережі працівникам, які змушені працювати поза межами офісу. Для цього достатньо встановити на комп'ютер або ноутбук співробітника 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 SD-WAN мережі постійно перевіряє якість з'єднання на наявність затримок та втрати надісланих 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 забезпечення якісної роботи додатків та сервісів.

В базі даних системи контролю додатків infoSDWAN є інформація про більш ніж 5000 існуючих програм, що дозволяє у автоматичному режимі, або за попередньо встановленими налаштуваннями контролювати їх роботу, надавати пріоритет та прискорювати критично важливі. Прикладом може бути ситуація коли система контролю у випадку нестачі ресурсів каналу зв'язку автоматично призупинить чи сповільнить швидкість доступу до мережі другорядних процесів, поки здійснюється відеоконференція яку визначено пріоритетною.

SD-WAN є сучасною технологією, яка надає численні переваги в порівнянні з традиційними WAN рішеннями серед яких варто виділити наступні:

- ПІДВИЩЕНА ПРОДУКТИВНІСТЬ

  SD-WAN забезпечує автоматичне перенаправлення трафіку між будь-якими наявними каналами зв'язку, включаючи MPLS та мобільний Інтернет. Це дозволяє підвищити продуктивність вашої мережі та забезпечити максимальну доступність сервісів.
- ГНУЧКІСТЬ ТА ШВИДКІСТЬ МАСШТАБУВАННЯ

  SD-WAN дозволяє додавати нові філії, офіси або користувачів без значних зусиль. Мережа легко масштабується відповідно до змін потреб вашого бізнесу, що дозволяє швидко реагувати на зростання або зміну розмірів вашої компанії.
- ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ

  Корпоративна мережа побудована по технології SD-WAN має єдину точку управління, що дозволяє швидко налаштовувати правила мережі, розв'язувати будь-які проблеми та забезпечувати її безпеку.

Послуга infoSDWAN це:

- Ваша корпоративна мережа у будь-якій точці України та світу як послуга
- Безпечне та швидке підключення до ваших хмарних сервісів
- Можливість оперативно змінювати кількість підключених до сервісу філій/відділень/робочих місць, як у бік збільшення, так і у бік зменшення
- Оптимізація та повна передбачуваність Ваших витрат
- Можливість додатково підключити послуг з інформаційної безпеки за унікальною ціною
- Підтримка 24x7x365

infocom
TRUSTED SECURITY

infoVPN

web-сторінка послуги

КОРПОРАТИВНА МЕРЕЖА НА БАЗІ ЗАГАЛЬНОНАЦІОНАЛЬНОЇ ІНФРАСТРУКТУРИ INFOCOM

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, яка створює єдиний об'єднаний інформаційний простір для всіх територіально розподілених підрозділів та об'єктів. Завдяки корпоративній мережі, всі віддалені працівники можуть працювати як в одному приміщенні, обмінюватися даними, спілкуватися та здійснювати спільну роботу над проектами в режимі реального часу, що дозволяє компаніям зменшити час, необхідний для реалізації нових проектів, зробити комунікацію між підрозділами ефективнішою та знизити ризики витоку конфіденційної інформації.

На базі інформаційної інфраструктури Infocom клієнтам надається можливість розбудовувати 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 власної мережі, Infocom надає послуги як другого (L2), так і третього рівня (L3).

У першому варіанті, замовник послуги отримує у розпорядження групу каналів рівня L2 за допомогою яких реалізує бажану топологію своєї віртуальної корпоративної мережі для зв'язку своїх географічно рознесених локальних мереж. Послуга infoVPN рівня L2 надається у наступних варіантах:

- Віртуальний канал Ethernet у конфігурації точка-точка (point-to-point) за технологією MPLS або Ethernet

- Віртуальний канал Ethernet у конфігурації точка-багатоточка (point-to-multipoint) за технологією MPLS або Ethernet

Віртуальна корпоративна мережа побудована на рівні L3 бачиться замовником як власна WAN-інфраструктура за допомогою якої забезпечується зв'язок між корпоративними локальними мережами, розташованими в різних географічних місцях.

Наша компанія має великий досвід у проектуванні та побудові корпоративних мереж різних рівнів 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.

Послуга infoVPN це:

- Ваша корпоративна мережа у будь-якій точці України як послуга
- Можливість оперативно змінювати кількість підключених до сервісу філій/відділень/робочих місць, як у бік збільшення, так і у бік зменшення
- Оптимізація та повна передбачуваність ваших витрат на побудову та підтримку приватної корпоративної мережі
- Можливість додатково підключити послуги із захисту периметру мережі infoGuard за унікальною ціною
- Підтримка 24x7x365

ІНТЕРНЕТ

Інтернет є одним із найважливіших винаходів у всій сучасній історії. Це революціонізувало спосіб нашого спілкування, навчання та роботи. З його здатністю формувати наш світ і змінювати спосіб життя він став для нас необхідністю. Державний сектор, банківський сектор, комерція, виробництво, транспортна сфера, навчання, сфера розваг та глобальна соціальна взаємодія – усі ці аспекти життя були б кардинально іншими без нього.

Інтернет

web-сторінка послуги

ДОСТУП ДО ВСЕСВІТНЬОЇ МЕРЕЖІ «ІНТЕРНЕТ»

Найшвидший і найпростіший спосіб підключитися до всесвітньої мережі «Інтернет» саме з тими параметрами, які оптимально відповідають вашим потребам - звернутися до нас та отримати консультацію нашого спеціаліста. В залежності від вашого місцезнаходження та технічних вимог, ми допоможемо обрати оптимальний спосіб підключення та відповідний тарифний план.

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

- Технологія WiFi забезпечує отримання швидкісного безлімітного доступу до мережі «Інтернет» та корпоративних 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 всесвітньої мережі по виділеній волоконно-оптичній лінії на швидкості від 5 до 10 Гбіт/с.

В поєднанні з послугами з інформаційної безпеки Infocom ви отримуєте безпечне підключення до мережі «Інтернет» із захистом від вірусів, шпигунського програмного забезпечення, троянів, фішинг-програм, моніторів, кілоґґерів, рекламного програмного забезпечення та DoS/DDoS-атак.

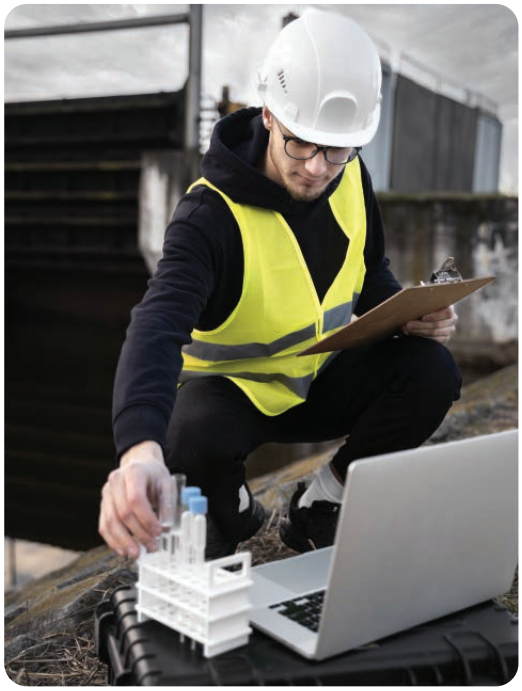
БЕЗДРОТОВИЙ ДОСТУП

Бездротові технології дозволяють будувати захищені канали передачі даних у місцях, де традиційні дротові мережі є недоступними, або якщо побудова та експлуатація традиційних каналів зв'язку є недоцільною з економічної чи технічної точки зору. За допомогою технології long-range Wi-Fi та використовуючи наявні в Україні мережі стільникового зв`язку клієнтам надається можливість підключатись до своїх закритих корпоративних мереж, отримувати послуги з доступу до інтернету та організувати резервування наявних каналів зв'язку на всій території країни.

Пілігрим

web-сторінка послуги

ЗАХИЩЕНИЙ МОБІЛЬНИЙ КОМПЛЕКС

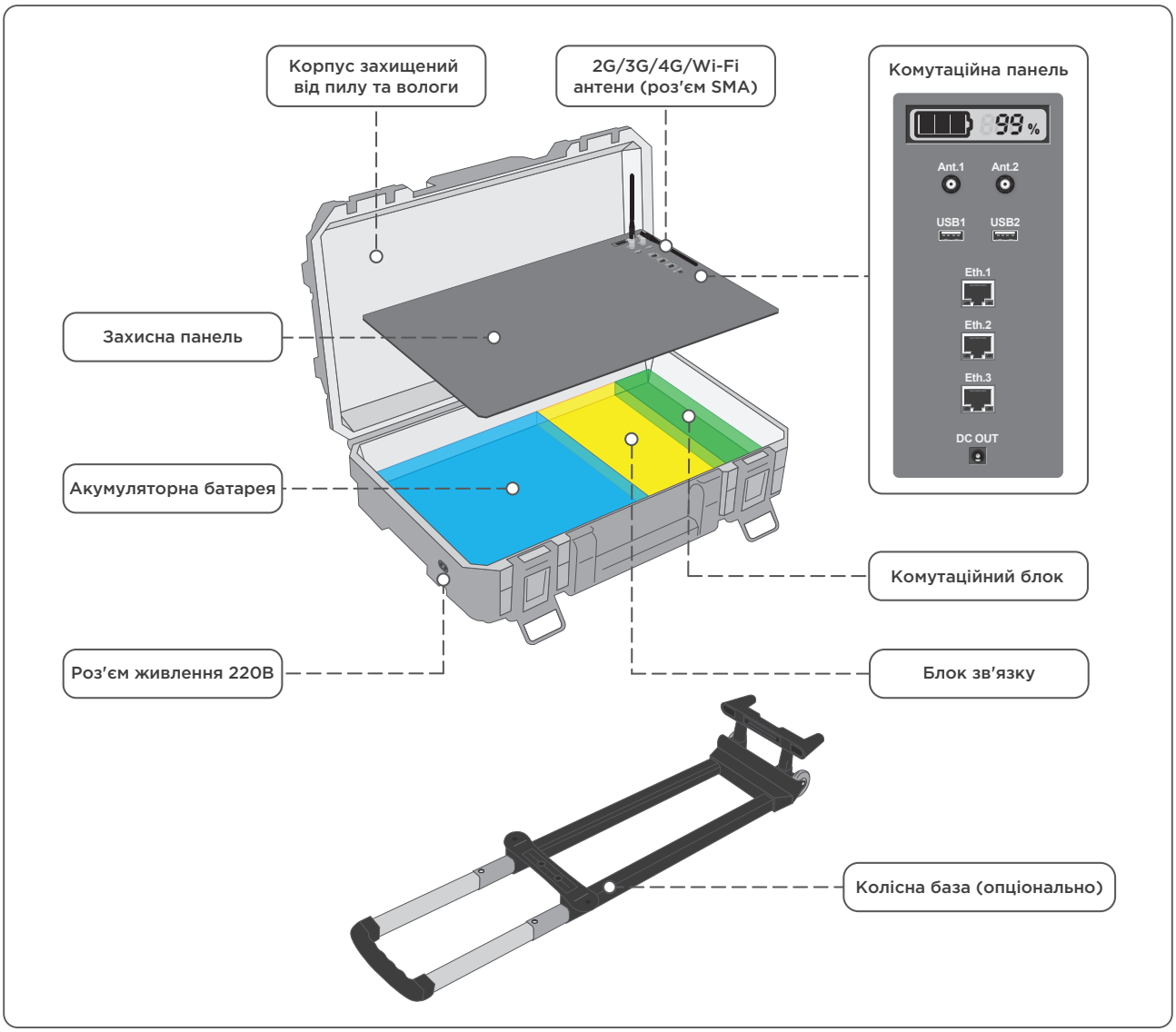


Пілігрим – це пересувний мобільний комплекс, оснащений VPN-маршрутизатором бездротового/дротового зв'язку та вбудованим акумулятором. Комплекс дозволяє створити захищені канали передачі даних, які надають змогу працювати у закритих корпоративних мережах і забезпечує тривалу автономність портативних персональних комп'ютерів та роботу інших пристроїв завдяки акумулятору.

Мобільний комплекс використовується у разі необхідності забезпечення високої мобільності та незалежності користувачів комплексу від традиційних дротових мереж зв'язку та електромереж, у випадках коли робота проводиться у віддалених районах без розвиненої інформаційної інфраструктури, відбувається часта зміна робочих локацій впродовж дня, відсутнє надійне електропостачання або існує потреба у оперативному та швидкому встановленні захищених каналів зв'язку без огляду на наявну можливість підключення на місцевості. Пілігрим може використовуватись для швидкого розгортання оперативних центрів служб екстреного порятунку, штабів збройних сил або сил МВС, тощо.

Основним призначенням пересувного комплексу Пілігрим є організація автономного підключення користувачів до корпоративних мереж та мережі «Інтернет». Для реалізації цієї функції маршрутизатор комплексу може бути обладнаний двома незалежними 2G/3G/4G - модемами з можливістю поділу наявних каналів передачі даних на основний та резервний, або вбудованими модемом та модулем Wi-Fi. Окрім бездротового підключення, Пілігрим обладнано трьома портами Gigabit Ethernet, що дає змогу використовувати систему супутникового зв'язку Starlink*, підключати комплекс до мережі у разі наявності дротового зв'язку, або використовувати порти для забезпечення зв'язком інших пристроїв.

* підключення супутникової системи Starlink потребує спеціального Ethernet-адаптеру (Starlink Ethernet Adapter). У разі живлення Starlink від вбудованого акумулятору загальний час автономної роботи комплексу Пілігрим може становити до 5 годин в залежності від ємності акумулятору та за умови вимкненого підігріву поверхні супутникової антени.



Конструкція пересувного комплексу Pilgrim

Комплекс Пілігрим являє собою жорсткий пластиковий кейс захищений від пилу та вологи розміром 35x56,4x16,5 см з відокремленим, від основного об'єму захисною панеллю, службовим відділенням. Основний об'єм комплексу дозволяє вільно розмістити до двох стандартних 15.6-дюймових портативних персональних комп'ютерів або інше вимірювальне чи комунікаційне обладнання. Службове відділення комплексу розташоване у нижній частині кейсу та призначене для розміщення акумуляторної батареї, VPN-маршрутизатора та комутаційного блоку. Комутаційна панель комплексу містить дисплей індикації рівня заряду акумуляторної батареї, роз'єми для підключення SMA-антен та три порти Gigabit Ethernet. Для живлення зовнішніх пристроїв панель опціонально може бути обладнана USB-роз'ємами та роз'ємами постійного чи змінного струму з необхідною вихідною напругою.

Мобільний комплекс Пілігрим це:

- Тривала автономність, висока мобільність, швидке розгортання
- Можливість створення L2/L3 VPN мережі: 12tp, ipsec, openvpn, pptp, gre, eoip
- Доступ до мережі «Інтернет», зокрема, через Захищений Вузол Інтернет Доступу (ЗВІД)
- Протоколи маршрутизації: BGP, OSPF, RIP, фільтрація мережевого трафіку, NAT, брандмауер
- Живлення зовнішніх пристроїв: USB, Постійний/Змінний струм (опціонально)
- Акумуляторна батарея 120-600 Вт·год (32 000 - 162 000 мАч / 3.7В)

infocom
TRUSTED SECURITY

Бездротові канали

web-сторінка послуги

БЕЗДРОТОВІ КАНАЛИ ПЕРЕДАЧІ ДАНИХ

Infocom пропонує два варіанти побудови бездротових каналів для організації доступу до корпоративної мережі чи мережі «Інтернет» – за допомогою технології long-range Wi-Fi та на базі VPN-маршрутизатора дротового та бездротового зв'язку RDT-33.

Канали передачі даних, побудовані за допомогою технології long-range Wi-Fi, дозволяють передавати дані на значні відстані, які можуть вимірюватися десятками, або у деяких випадках навіть сотнями кілометрів зі швидкістю до 150 Мб/с. Використання бездротового зв'язку, дозволяє підключати користувачів до корпоративних мереж чи мережі «Інтернет» у місцевостях зі складними географічними умовами (гори, ліси, ущелини, річки, болотиста місцевість), де прокладання оптоволоконних магістралей є неможливим, або є економічно невигідним. Даний тип побудови каналів зв'язку відрізняється швидкістю розгортання, оскільки для запуску бездротової лінії потрібно лише встановити прийомопередаючі станції в початковій, кінцевій і, за необхідності, у проміжних точках без потреби прокладання кабелю впродовж всієї лінії зв'язку та тривалого узгодження цих робіт з місцевими органами влади.

Перехід операторів стільникового зв'язку на нові швидкісніші стандарти передачі даних та зростання їхнього сукупного покриття до загальнонаціонального рівня зумовили нові спроможності у побудові бездротових захищених каналів. Використання ресурсів стільникових мереж у якості транспортних, дозволяє розгортати сервіс скрізь де є відповідне покриття та додатково надає користувачу послуги виняткову можливість вільно переміщатись. Для організації подібних каналів передачі даних, інженерами Infocom був створений багатофункціональний VPN-маршрутизатор дротового та бездротового зв'язку RDT-33, який являє собою компактний пристрій промислового типу, розроблений з урахуванням побажань користувачів та багаторічного досвіду експлуатації попередньої власної моделі RD-010. Два вбудованих модема з підтримкою стандартів 2G/3G/4G та функцією активного резервування дають змогу використовувати VPN-маршрутизатор для забезпечення надійним зв'язком мобільних пересувних пунктів, або у місцях де традиційні дротові мережі є недоступними чи побудова і використання дротових каналів є недоцільними. Канали передачі даних на базі RDT-33 широко використовують для організації зв'язку між банкоматами та терміналами самообслуговування з головними процесинговими центрами банків, для забезпечення резервного доступу користувачів до корпоративних мереж та для організації захищеного зв'язку державного та військового спецтранспорту.

Резервування каналів

web-сторінка послуги

РЕЗЕРВУВАННЯ КАНАЛІВ ПЕРЕДАЧІ ДАНИХ

Безперебійність з'єднання з корпоративною мережею чи мережею «Інтернет» це безумовно ключова необхідність кожної сучасної компанії. Простота та відносно низька собівартість безпровідних каналів дозволяють використовувати цей тип зв'язку у якості резервного, забезпечуючи резервування наявних наземних ліній передачі даних.

У сучасному світі резервні канали передачі даних є своєрідною «страховкою» на випадок втрати зв'язку, адже його відсутність навіть впродовж години може призвести до відчутних проблем у роботі державних установ, або негативно вплинути чи повністю зупинити бізнес-процеси значної частини компаній. Крім очевидної основної функції резервного каналу саме слугувати запасним підключенням, його наявність додатково дає можливість розвантажувати основний канал передачі даних під час великих навантажень, шляхом розподілу трафіку між основним та резервними каналами, що дозволяє уникати збоїв та збільшує загальну продуктивність мережі. Важливо зазначити, що під час пошуку постачальника послуг для організації резервного підключення до мережі «Інтернет», або корпоративної мережі, необхідно перевірити, чи не використовує обрана компанія одну й ту саму фізичну лінію зв'язку що й ваш поточний провайдер, оскільки підключення каналів зв'язку від різних постачальників, але таких які використовують ту ж лінію, за великим рахунком, не є резервуванням - при пошкодженні кабелю, або за інших технічних проблем обидва канали однаково перестануть працювати. На жаль, цієї обов'язкової умови під час організації резервування буває важко дотриматися, оскільки підключення окремих будівель, комерційних комплексів, бізнес-центрів чи навіть деяких населених пунктів іноді здійснюється за допомогою однієї фізичної лінії. Саме через це, використання бездротових каналів зв'язку може виявитися не тільки доступним, але й ефективним методом резервування, оскільки використання радіоміста long-range Wi-FI з підключенням до іншого комунікаційного вузла, або задіяння ресурсів національних стільникових операторів за допомогою багатофункціонального VPN-маршрутизатору дротового та бездротового зв'язку RDT-33 гарантують повну незалежність резервного каналу від основного.

infocom
TRUSTED SECURITY

ІНФОРМАЦІЙНА БЕЗПЕКА

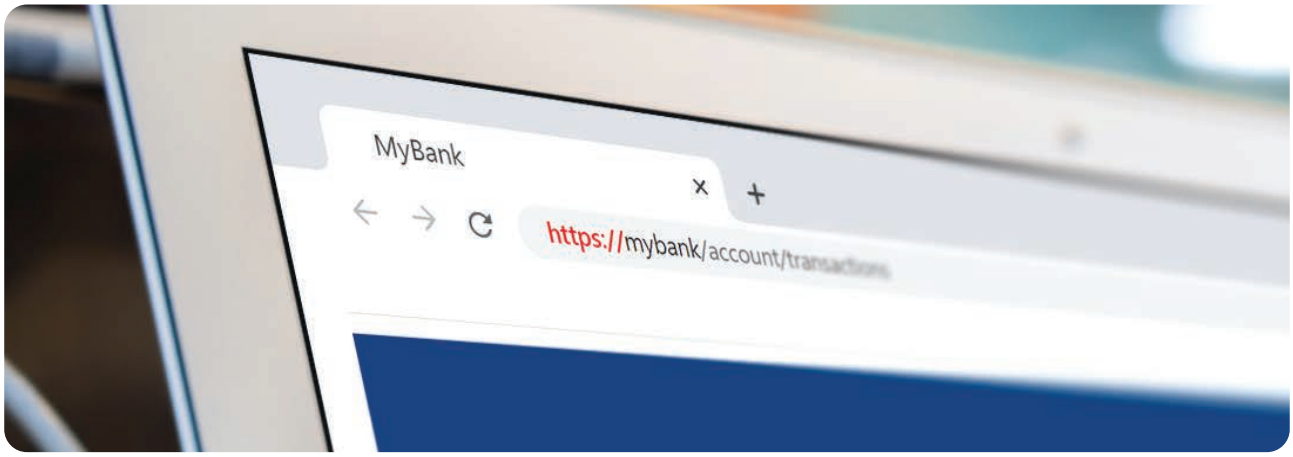
Робота державної чи фінансової установи, великого або малого бізнесу, навчального чи медичного закладу нерозривно зв'язана з використанням цифрових інформаційних технологій, які, в значній мірі, дозволяють спростити, впорядкувати, автоматизувати та значно підвищити ефективність усіх наявних організаційних, фінансових, виробничих або будь-яких інших процесів. Будь-яке несанкціоноване втручання у роботу відповідної інформаційної інфраструктури збоку зловмисників або недоброчесних конкурентів може не тільки тимчасово зупинити важливі робочі процеси але й через виток конфіденційної внутрішньої інформації призвести до значних репутаційних або фінансових втрат.
Послуги Infocom з інформаційної безпеки покликані мінімізувати будь-які ризики несанкціонованого доступу у вашу інформаційну інфраструктуру та забезпечити її надійне та безперервне функціонування завдяки всебічному захисту як зовнішнього так і внутрішнього периметру.

infoGuard

web-сторінка послуги

БАГАТОРІВНЕВИЙ ЗАХИСТ ПЕРИМЕТРУ МЕРЕЖІ

infoGuard — це перша лінія захисту вашої інформаційної інфраструктури. Це важливий елемент, який запобігає несанкціонованому сторонньому втручанню у корпоративну мережу, контролює та відстежує діяльність співробітників, приймає, відхиляє або припиняє доступ ззовні водночас дозволяючи вам бути гнучкими та динамічними у виконанні ваших бізнес-задач.



Широке використання безпечного протоколу передачі даних HTTPS, який унеможливлює «прослуховування» мережевого з'єднання під час відвідування веб-сторінок різноманітних онлайн-сервісів, значно знижує ризик перехоплення приватної конфіденційної інформації третіми особами, але в той самий час приховує від звичайних систем захисту увесь потік даних між користувачем та веб-порталом. Це створює не тільки можливість проникнення всередину корпоративної мережі вірусів, шпигунського програмного забезпечення, системних моніторів, кілоґґерів та іншого шкідливого програмного забезпечення через комп'ютер співробітника, але й скриває вихідний потік даних, який може містити конфіденційну корпоративну інформацію. Оскільки об'єм трафіку з використанням протоколу HTTPS, за статистикою, складає понад 80% від загального, аналіз системами безпеки зашифрованих даних стає однією з основних складових сучасного інформаційного захисту. Послуга infoGuard дозволяє перевіряти зашифровані дані, виступаючи

своєрідним посередником між користувачами та веб-порталами, таким чином значно знижуючи ризики проникнення шкідливого ПЗ у корпоративну мережу завдяки аналізу на наявність загроз усього, без виключення, вхідного та вихідного трафіку.

- Основною 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. Окрім аналізу зовнішніх запитів, infoGuard має гнучку систему внутрішнього контролю, яка завдяки аналізу вихідних даних значно зменшує вірогідність витоку конфіденційної інформації, спричиненого ненавмисними, або злочиними діями співробітників компанії.

- Послуга 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.

- 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, infoGuard дає можливість заблокувати перегляд відео чи прослуховування аудіофайлів у соціальних мережах, залишаючи при цьому доступ до світлин та дописів.

Розгортання та спосіб підключення послуги infoGuard залежить від того чи є замовник користувачем послуг Infocom, а саме телекомунікаційних послуг infoSDWAN чи infoVPN, або послуг з доступу до мережі «Інтернет». В цьому разі підключення послуги займає мінімальний проміжок часу, а усі комутаційні роботи та відповідне налаштування відбуваються всередині Infocom без додаткових робіт та налаштування на боці замовника (крім встановлення на робочі комп'ютери сертифікатів infoGuard для аналізу зашифрованого трафіку). Якщо замовник не є користувачем вищезгаданих послуг Infocom на боці замовника або створюється GRE-тунель, який спрямовує увесь вхідний трафік на обладнання infoGuard яке встановлене у Infocom, або замовнику послуги надається окрема кількість устаткування яке встановлюється у кожній кінцевій точці та здійснює перевірку трафіку безпосередньо на боці замовника.

У рамках послуги infoGuard спеціалісти Infocom можуть взяти на себе функції адміністрування клієнтського устаткування, якщо у нього немає власної команди з інформаційної безпеки. Це означає, що наша команда забезпечить ефективний моніторинг та захист ваших мереж та систем від зловмисних атак та інших загроз 24/7 використовуючи ваше обладнання.

Послуга infoGuard це:

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

infoEP

web-сторінка послуги

ЗАХИСТ ВНУТРІШНЬОГО ПЕРИМЕТРУ МЕРЕЖІ

infoEP є важливим доповненням infoGuard яке дозволяє ефективно захистити корпоративну мережу «зсередини». Послуга розгортається шляхом встановлення спеціального програмного забезпечення (агентів) на робочі комп'ютери та мобільні пристрої співробітників компанії.

Робочі місця часто стають ціллю різноманітних кібератак, адже дослідження показують, що 30% від усіх атак на корпоративні мережі було здійснено за допомогою успішного ураження шкідливим програмним забезпеченням саме кінцевих точок. Як правило, основною причиною яка дозволяє кіберзлочинцям проводити подібні атаки є не тільки нехтування елементарними правилами з інформаційної безпеки та загальна низька обізнаність співробітників у цій сфері, але й поширена практика використання офісних комп'ютерів, ноутбуків та мобільних пристроїв як у робочих, так і у приватних цілях поза межами захищеного периметру у публічних місцях або вдома.

infoEP дозволяє значно знизити ризики ураження робочих комп'ютерів та мобільних пристроїв шкідливим ПЗ шляхом поширення повного захисту згідно корпоративних правил безпеки на усі кінцеві точки який включає брандмауер програм, антивірусне/антишпигунське сканування, веб-фільтрацію, сканування вразливостей тощо. Окрім інструментів які забезпечують безпеку у незахищеному мережевому середовищі, послуга дозволяє обмежувати чи повністю блокувати роботу зі знімними накопичувачами інформації такими як USB флеш-накопичувач, або зовнішні жорсткі диски, які можуть містити потенційно небезпечні файли, або програмне забезпечення.

Послуга infoEP це:

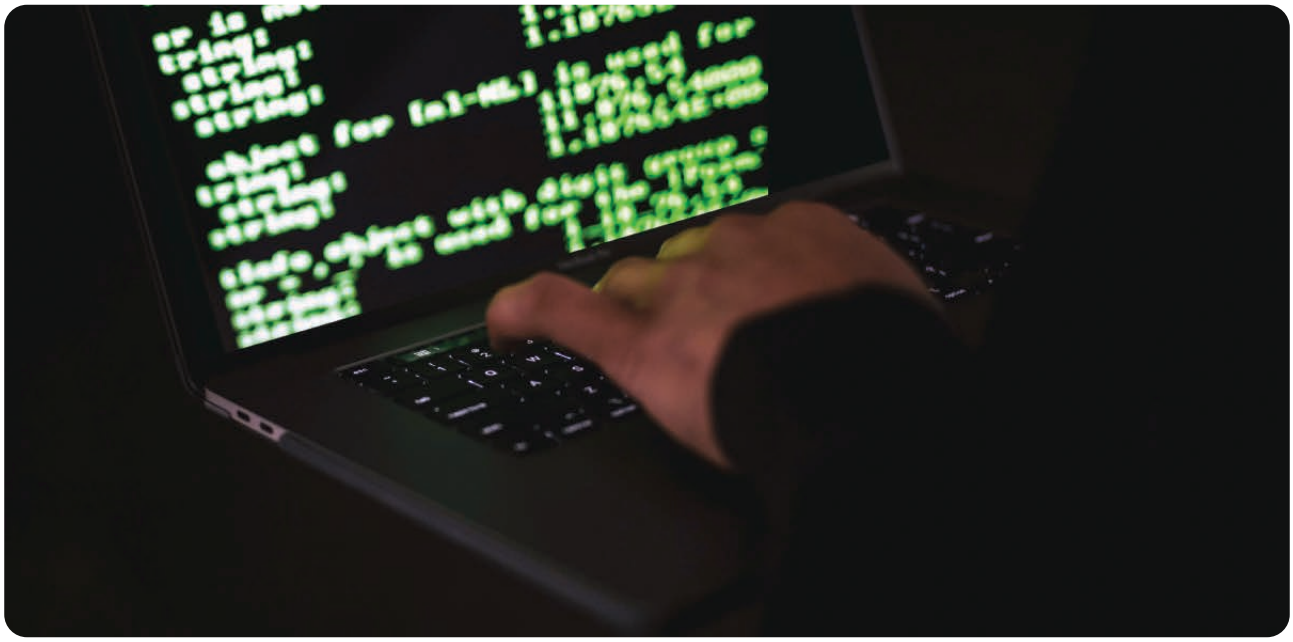
- Інтеграція будь-якого пристрою – локального чи віддаленого, стаціонарного чи мобільного у єдину систему корпоративної безпеки
- Безпечне користування комп'ютерами та мобільними пристроями поза межами офісу
- Захищений віддалений доступ до корпоративної мережі
- Підтримка 24x7x365

infoDDoS

web-сторінка послуги

БЕЗПЕРЕРВНА РОБОТА РЕСУРСІВ ЗАВДЯКИ ЗАХИСТУ ВІД DOS/DDOS АТАК

У сучасному світі веб-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 веб-портал. Зловмисники знають про важливість онлайн-ресурсів для комерційних та державних організацій і регулярно роблять спроби злому за допомогою атак на відмову в обслуговуванні, метою яких є порушення їх працездатності. Такі DoS/DDoS-атаки можуть здійснювати як звичайні зловмисники, вимагаючи сплати за припинення атак, так і недобросовісні компанії, які намагаються причинити шкоду або 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 швидкість передачі даних припиняє відповідати будь-яким вимогам для забезпечення нормального функціонування відповідного веб-порталу

Послуга infoDDoS може протистояти всім відомим типам DoS/DDoS-атак та забезпечує безперервну роботу Ваших ресурсів в мережі «Інтернет» за допомогою багаторівневого захисту у який входить увесь спектр сучасних засобів протидії атакам на відмову в обслуговуванні. У перелік засобів окрім поведінкового захисту, обмеження одночасних з'єднань, обмеження трафіку, захисту від SYN-флуду та інших, входить вбудована система запобігання зовнішнім вторгненням, яка є високопродуктивним методом протидії атакам з використанням відомих вразливостей програмного забезпечення, яке може використовуватися на вашому веб-порталі. Крім цього, платформа послуги infoDDoS дозволяє уникнути ризиків проникнення «комп'ютерних черв'яків» та з легкістю виявляє роботу «ботів» на комп'ютерах співробітників.

infocom
TRUSTED SECURITY

Послуга infoDDoS це:

- Безперервна робота ваших ресурсів у мережі «Інтернет»
- Зниження ризиків порушення діяльності вашої Компанії
- Оптимізація ваших витрат на забезпечення захисту від DoS/DDoS-атак 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

infoWAF

web-сторінка послуги

БЕЗПЕКА ВАШИХ ВЕБ-РЕСУРСІВ

Великий попит на веб-додатки призвів до виникнення великої кількості спеціалізованих компаній та приватних розробників, які займаються створенням програм з різноманітними функціональними можливостями. Проте, у своєму прагненні задовольнити потреби ринку, багато з них звертають недостатньо уваги чи просто нехтують аспектами безпеки, що призводить до появи серйозних вразливостей у додатках та створенню загроз для їх роботи. Ситуація ускладнюється тим, що вразливий веб-додаток може бути легко скомпрометований вправними зловмисниками без використання спеціалізованих інструментів, навіть за допомогою звичайного веб-браузера.

Складність боротьби з кібератаками на веб-ресурси полягає в тому, що вони, як правило, відбуваються одночасно з сесіями легітимних користувачів і, в більшості випадків, використовують стандартні порти. Оскільки блокування всього трафіку на рівні порту призведе до повного закриття доступу усіх користувачів до веб-додатків, а використання традиційних брандмауерів є малоефективним через їх обмежені можливості розпізнавання та фільтрації HTTP-трафіку ефективний захист веб-ресурсів можливий тільки завдяки використанню спеціального програмно-технічного забезпечення - брандмауера веб-додатків (англ. Web Application Firewall або WAF).

В рамках послуги infoWAF, Infocom пропонує просте та ефективне рішення для захисту ваших веб-додатків. Використання нашого програмно-технічного комплексу гарантує захист від широкого спектру загроз, таких як SQL-ін'єкції, крос-сайтові скрипти, перехоплення сесій тощо. Комплекс дозволяє ефективно усунути наявні вразливості та, як результат, забезпечити надійну та безперервну роботу усіх ваших онлайн-проектів. Робота послуги infoWAF базується на аналізі усіх вхідних та вихідних даних, фільтрації шкідливих запитів та блокуванні атак на різних рівнях, а постійні оновлення бази загроз забезпечують високу ефективність, завдяки можливості оперативно реагувати на нові типи атак та нові вразливості, що виникають у сучасному цифровому середовищі.

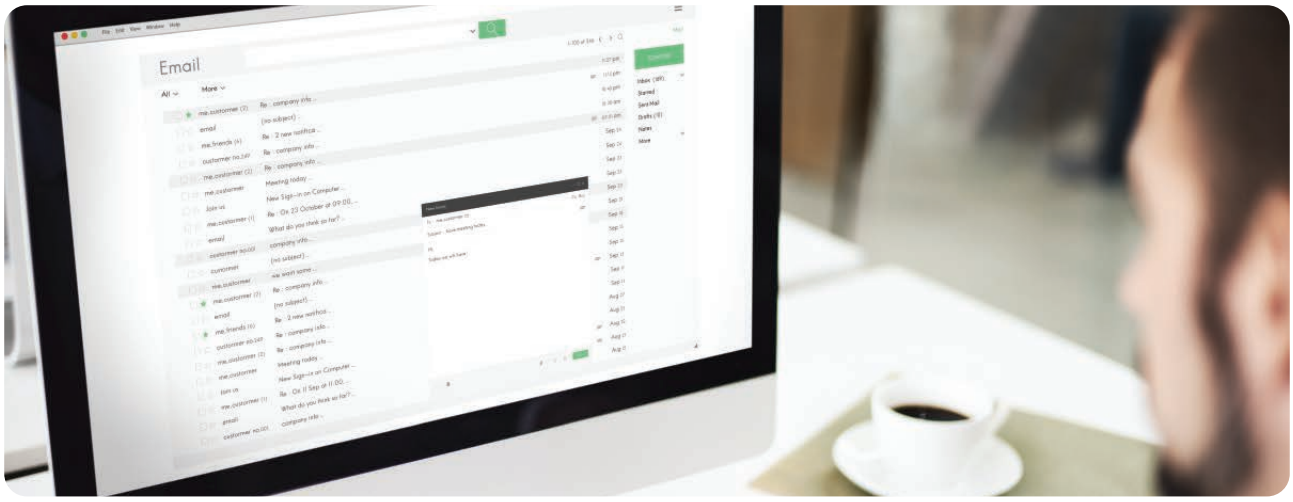
Послуга infoWAF це:

- Ефективний захист ваших веб-ресурсів
- Безперервний доступ клієнтів до ваших інтернет-послуг
- Оптимізація ваших витрат на забезпечення захисту 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

infoMail

web-сторінка послуги

ЗАХИСТ ЕЛЕКТРОННОЇ ПОШТИ



Електронна пошта залишається інструментом номер один за допомогою якого кіберзлочинці досягають своїх цілей із зараження комп'ютерів користувачів, проникнення у мережі, викрадення приватної чи корпоративної інформації. Переважно, подібні атаки починаються з «приманки» або «розвідувальних» електронних листів, які служать двом цілям: вони перевіряють існування облікового запису електронної пошти жертви та намагаються зібрати більше інформації про жертву, яку кіберзлочинець може використати для здійснення цілеспрямованіших комбінованих атак у майбутньому. Згідно зі звітом VERIZON 2022 DATA BREACH INVESTIGATIONS REPORT 82% успішних атак було здійснено саме завдяки вдалому використанню отриманої інформації чи здобутому обманним шляхом доступу до комп'ютера користувача чи до корпоративної мережі.

- Послуга infoMail розроблена 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 загрозами аналітичний центр виробника обладнання, на якому розгорнуто послугу infoMail, аналізує по всьому світу мільйони електронних листів на годину і може ідентифікувати новий небезпечний код за лічені хвилини та заблокувати усі підозрілі вкладення, виявлені в електронних листах для подальшого аналізу у лабораторіях інформаційної безпеки.

- 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. Платформа послуги infoMail налічує в своїй базі десятки тисяч 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.

- 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 зі сторонніми серверами 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.

Послуга infoMail це:

- Надійний захист вашої електронної пошти та даних
- Оптимізація ваших витрат на забезпечення кіберзахисту завдяки відсутності потреби купувати дороге сучасне обладнання та ліцензії до нього
- Зниження ризиків порушення діяльності вашої компанії
- Економія вашого часу та можливість повністю сконцентруватись на ваших стратегічних планах та задачах
- Підтримка 24x7x365

infoScan

web-сторінка послуги

НЕЗАЛЕЖНИЙ АУДИТ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

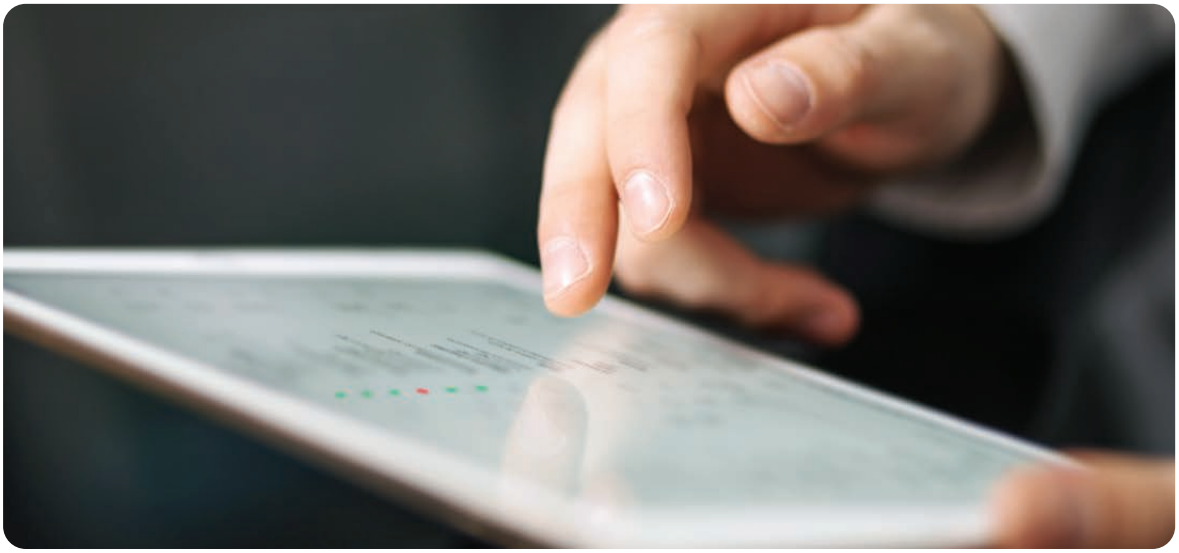
Аудит захищеності інформаційної інфраструктури - комплекс заходів спрямований на пошук будь-яких вразливостей та потенційних загроз, які можуть призвести до несанкціонованого проникнення сторонніх осіб у вашу мережу. Періодичне проведення аудиту є важливим для забезпечення ефективності заходів безпеки та виявлення нових загроз, які можуть виникнути внаслідок змін у вашій інформаційній інфраструктурі та застосованих технологіях.

Наявність вразливостей у вашій мережі дає можливість зловмисникам реалізовувати загрози і таким чином отримувати доступ до конфіденційних даних, завдавати шкоди поточним робочім процесам або зупиняти їх повністю. Своєчасне виявлення таких вразливостей та їх відповідне усунення є критично важливими для забезпечення безпеки інформаційної інфраструктури.

Інформаційна інфраструктура може бути вразлива з багатьох причин. Серед основних видів вразливостей, які можуть існувати в інформаційних системах слід виділити наступні:

- Вразливості програмного забезпечення: помилки в програмному забезпеченні або застаріле програмне забезпечення, яке може бути використано зловмисниками
- Вразливості мережі: слабкі місця в мережі, обумовлені неправильною конфігурацією мережного обладнання, недостатнім рівнем захисту від зовнішніх атак або недостатня захищеність пристроїв, які підключені до мережі
- Вразливості управління доступом: використання слабких паролів, втрата або крадіжка пристроїв, проблеми управління правами доступу тощо
- Вразливості фізичної інфраструктури: недостатній рівень захисту приміщень, де зберігаються сервери та інші пристрої, які містять конфіденційну інформацію.

Якщо вразливості пов'язані з фізичною інфраструктурою та управлінням доступом великою мірою є питаннями адміністративними та організаційними, які можуть бути, здебільшого, вирішені компаніями чи організаціями власними силами, то вразливості програмного забезпечення та мережеві вразливості є суто технічними та потребують аналізу спеціалістів з кібербезпеки.



Першим та ключовим етапом аудиту захищеності інформаційної інфраструктури є аналіз наявних ризиків. Цей аналіз передбачає тісну співпрацю між представниками Infocom та компанією чи організацією яка проходить аудит. Під час цього етапу визначаються потенційні загрози, проводиться оцінка ймовірності та наслідків їх реалізації, а також визначення пріоритетів захисних заходів. У процесі такого аналізу, до уваги беруться такі фактори як потенційне джерело загроз (із середини периметру або ззовні), можливі методу впливу (мережні, апаратні або соціальні) та об'єкти загрози (корпоративні дані, робочі процеси тощо). Після визначення усього спектру можливих загроз спеціалістами Infocom проводиться перевірка мережевої інфраструктури (конфігурація обладнання, схема підключення, тощо) та здійснюється «сканування» з використанням спеціалізованого програмного забезпечення. Отримані таким чином дані дозволяють виявляти всі слабкі місця в інформаційній системі, такі як відкриті порти, застарілі версії програмного забезпечення, слабко захищені мережеві протоколи, неправильно налаштоване або підключене обладнання. Після проведення аудиту, представниками Infocom формується звіт, в якому відображаються всі виявлені вразливості та детальні рекомендації щодо їх усунення, а також пропозиції щодо покращення загального рівня безпеки інформаційної інфраструктури. За бажанням компанії чи організації, Infocom може провести додатковий повторний аудит для перевірки рівня імплементації раніше наданих рекомендацій та пропозицій.

СКУД / БІОМЕТРИЧНА ІДЕНТИФІКАЦІЯ

Системи контролю та управління доступом (СКУД) та біометрична ідентифікація відіграють важливу роль у забезпеченні безпеки та захисту конфіденційної інформації. Використання СКУД допомагає контролювати доступ до приміщень, комп'ютерів, мереж та інших ресурсів, обмежуючи доступ невповноваженим особам. Біометрична ідентифікація, яка використовує унікальні фізіологічні характеристики ще більше підвищує рівень безпеки, завдяки унеможливленню використання вкрадених паролів або фізичних засобів доступу таких як ключі чи ID-картки.

ManuScan

web-сторінка послуги

СИСТЕМА БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

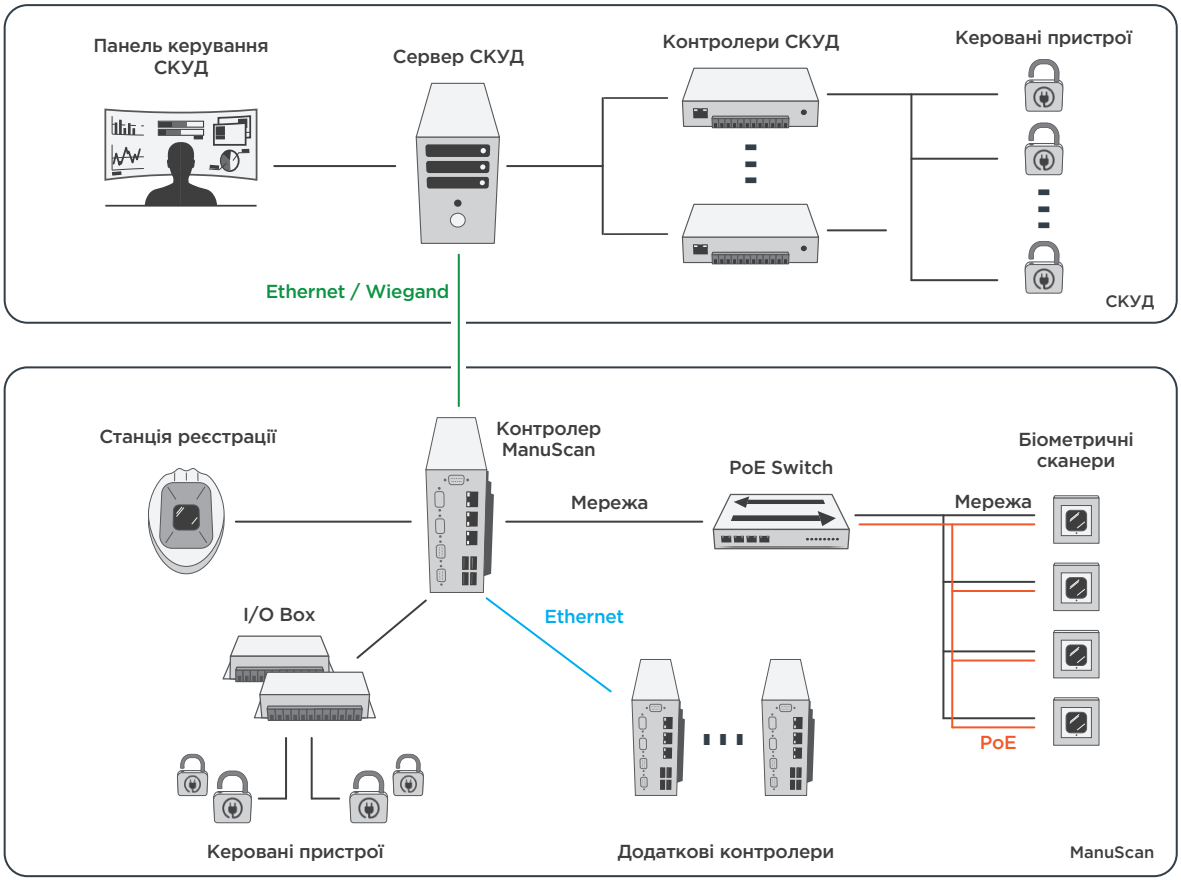
ManuScan - це система біометричної ідентифікації , яка використовує метод сканування вен у долоні. Система значно підвищує рівень безпеки завдяки високій точності ідентифікації користувачів, неможливості втрати, копіювання, крадіжки та передачі ідентифікатора третім особам. Метод сканування вен долоні 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.

Система ManuScan може бути обладнана двома типами сканерів – зовнішніми або внутрішніми. Зовнішні сканери встановлюють на фасадах будівель та/або при в'їзді на територію, а внутрішні – на входах в окремі приміщення. Обидва типи мають одне й те саме призначення – ідентифікувати людей, які входять у приміщення або на територію та обмежувати несанкціонований доступ.

Окрім контролера системи ManuScan та сканерів зовнішнього та внутрішнього розміщення до складу системи входить станція реєстрації, яка разом зі спеціальним програмним забезпеченням використовується для реєстрації нових користувачів.

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. Це дозволяє системі під час сканування розпізнавати унікальний для кожної людини малюнок венозних судин долоні та використовувати його у якості ідентифікатора.

Система ManuScan може використовуватися як у складі системи контролю і управління доступом та обліку робочого часу так і у автономному режимі. В автономному режимі контролер ManuScan може самостійно керувати чотирьома пристроями через USB - I/O Box (замки, сигналізація, тощо), отримуючи дані з чотирьох окремих сканерів. У разі потреби, керувати більшою кількістю пристроїв, або встановлення більшої кількості біометричних сканерів, необхідна кількість контролерів ManuScan об'єднується в одну спільну мережу. Після об'єднання всі контролери отримують доступ до всіх встановлених біометричних сканерів та збережених баз даних, що дозволяє вносити дані нових користувачів за допомогою станції реєстрації тільки в один із контролерів без необхідності внесення даних окремо у кожний.



Використання ManuScan у поєднанні з системою контролю та управлінням доступом

У складі системи контролю і управління доступом, ManuScan проводить біометричну ідентифікацію користувачів та передає на сервер СКУД відповідні дані, при цьому кожне додаткове збережене положення долоні лівої чи правої руки (або одразу двох) окремого користувача відносно біометричного сканера має власний унікальний ідентифікатор. Це дозволяє реалізовувати різноманітні алгоритми на рівні СКУД в залежності від пред'явленої руки та положення долоні (відкриття чи закриття дверей, увімкнення чи вимкнення сигналізації, виклик охорони тощо), що розширює стандартні можливості системи контролю і управління через можливість реалізації додаткових алгоритмів керування та сповіщення.

ManuScan у складі СКУД зберігає можливість автономного керування чотирма пристроями, які можуть бути підключені до контролера напряму, що дає можливість створення повністю автономної та незалежної від загальної системи управління додаткової відокремленої зони контролю та доступу (серверна кімната, банківське сховище, кімната зберігання зброї тощо).

ManuScan це:

- Точна та швидка ідентифікація
- Інтегрованість у більшість систем контролю доступу та індустріальних систем, яким необхідна точна ідентифікація користувачів
- Потрійна система шифрування / Неможливість підробки ідентифікатора
- Простота та зручність у користуванні
- Гігієнічність (відсутність контакту с поверхнею сенсора)
- Простий та швидкий монтаж

СКУД

web-сторінка послуги

СИСТЕМА КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

Система контролю та управляння доступом, є важливою частиною безпеки будь-якої компанії або організації. Ця система дозволяє обмежити доступ до різних зон та приміщень, що забезпечує високий рівень безпеки та захисту проти несанкціонованого доступу до окремих приміщень або цінних ресурсів. СКУД забезпечує можливість точно ідентифікувати особу, яка намагається отримати доступ до зони з обмеженим доступом, що забезпечується за допомогою використання різних ідентифікаторів, таких як картки доступу, ключі, відбитки пальців або інші біометричні характеристики. Крім того, система контролю доступу дозволяє вести детальний облік та контроль над рухом працівників на території компанії або в будівлі. Наприклад, зберігати інформацію про час прибуття та вибуття працівників, складати їхні маршрути переміщення, а також іншу необхідну для адміністрації підприємства та служби безпеки корисну інформацію, яка може бути використана для оптимізації робочих процесів чи підвищення загального рівня безпеки.

Infocom є партнером компанії ZKTeco, яка є всесвітньо відомим виробником систем контролю та управлінням доступом, систем обліку робочого часу та різноманітних систем біометричної ідентифікації. Наші спеціалісти допоможуть вам підібрати оптимальне обладнання СКУД, що найбільше відповідає вашим потребам та виконають установку і налаштування з врахуванням особливостей вашого бізнесу, наявного обладнання та специфіки об'єктів.

ХМАРНІ ПОСЛУГИ

Хмарні послуги – це сучасне рішення для розміщення та управління інформацією, яке дозволяє компаніям отримувати високу надійність, продуктивність та масштабованість без необхідності купівлі та підтримки власного обладнання. Infocom пропонує гнучкий підхід щодо необхідної технічної реалізації обраної послуги, високу швидкість роботи та безпеку даних, а також цілодобову технічну підтримку для забезпечення оптимальними умовами використання наших хмарних послуг.

VPS

web-сторінка хмарних послуг

ВІРТУАЛЬНИЙ ПРИВАТНИЙ СЕРВЕР

Віртуальний приватний сервер (англ. virtual private server, VPS) або віртуальний виділений сервер - це послуга хмарного хостингу, яка дозволяє розмістити на одному фізичному сервері постачальника послуг кілька віртуальних клієнтських серверів. Кожен з цих віртуальних серверів функціонує незалежно від інших та має власні виділені ресурси, включаючи процесорні потужності, обсяг оперативної пам'яті, простір на жорсткому диску та мережевий трафік. В результаті, користувач VPN послуги одержує свій ізольований віртуальний сервер, який є повноцінною альтернативою фізичному серверу, проте, з кількома суттєвими перевагами, серед яких варто відзначити наступні:

- Швидке розгортання
  VPS можна швидко створити та розгорнути, що дозволяє розпочати роботу з ним практично миттєво. Власний сервер вимагає значно більше часу та ресурсів для його налаштування та розгортання.
- Гнучкість та масштабованість
  Володіння власним фізичним сервером може виявитися дорогим та складним для масштабування. VPS, з іншого боку, надає більш гнучкі можливості масштабування ресурсів, щоб задовольнити зростаючі потреби бізнесу.
- Надійність
  VPS має багато механізмів для забезпечення надійності, таких як моніторинг 24/7, автоматичне резервне копіювання та відновлення.
- Зручність
  Управління власним фізичним сервером може виявитися складним, особливо для невеликих компаній без спеціального IT-персоналу. Послуга VPS пропонує зручний інтерфейс керування та цілодобову підтримку, що значно полегшує роботу.
- Економія
  Володіння власним сервером потребує значних інвестицій в обладнання, програмне забезпечення, встановлення та налаштування, технічну підтримку та в забезпечення безпеки як інформаційної так і безпосередньо фізичної. Віртуальний приватний сервер надає багато з цих можливостей у рамках самої послуги, або за меншу вартість.

Infocom пропонує послугу віртуального приватного сервера з різними технічними параметрами, такими як: обсяг оперативної пам'яті, процесорні потужності та дисковий простір, щоб задовольнити індивідуальні потреби кожного нашого клієнта. Ми також надаємо широкий вибір операційних систем, включаючи Windows та різні дистрибутиви Linux, а також можливість вибору рівня доступу до сервера, що дозволяє користувачеві мати бажаний рівень контролю над встановленими додатками та даними. Послуга VPS також включає статичну IP-адресу та безлімітний канал передачі даних до 1 Гбіт/с, що дає можливість у стислі терміни розгорнути необхідне клієнтське рішення та запустити його в роботу якомога швидше.

Хостинг

ХОСТИНГ ВЕБ-РЕСУРСІВ

Хостинг веб-ресурсів - це послуга, у рамках якої клієнту надається можливість розмістити свій веб-портал, веб-сайт, веб-додаток або будь-який інший веб-ресурс на серверах Infocom без потреби у самостійному створенні та підтримки необхідної для його функціонування інфраструктури. У рамках послуги, наша компанія надає свої технічні ресурси для зберігання вашого веб-порталу чи додатку, забезпечуючи його безперервним якісним доступом до мережі «Інтернет», фізичну безпеку, можливість резервного копіювання та інші пов'язані з роботою ресурсу додаткові послуги такі як захист від DoS/DDoS-атак або інші послуги з інформаційної безпеки. Ми надаємо користувачам необхідний для належної роботи дисковий простір, гарантуємо необхідну пропускну здатність Інтернет-каналу та забезпечуємо повну технічну підтримку 24/7.

Крім послуги хостингу веб-ресурсів, Infocom також надає послуги реєстрації та підтримки доменних імен. Ця послуга включає в себе реєстрацію доменного імені в обраній вами зоні (ua, com, com.ua, kiev.ua, net.ua, org.ua, gov.ua, net, org, info, biz тощо), а також його подовження в майбутньому.

Сховище

ХМАРНЕ СХОВИЩЕ ДАНИХ

Хмарне сховище даних - це послуга Infocom, яка дозволяє користувачам зберігати свої дані в безпечному та надійному хмарному середовищі. Замість того, щоб зберігати дані на власних пристроях, на знімних носіях інформації чи на комп'ютерах або серверах у своєму офісі, користувачі можуть зберігати свої файли, документи та інші важливі дані на серверах Infocom, до яких вони можуть отримати доступ з будь-якого пристрою будь-де де є підключення до мережі «Інтернет». Хмарне сховище даних є ідеальним рішенням для користувачів, які шукають безпечне та зручне рішення для зберігання своїх даних, а також для команд, які потребують спільного доступу та роботи з даними.

Хмарні послуги Infocom це:

- Висока доступність вашіх ресурсів у мережі «Інтернет»
- Швидка маштабованість обраних послуг
- Можливість підключення послуг з інформаційної безпеки за спеціальною ціною
- Оптимізація та повна передбачуваність ваших витрат
- Залучення фахівців Infocom без необхідності у навчанні власних
- Цілодобова підтримка 24x7x365

Ми надаємо
нові можливості
для Вашого бізесу

infocom
TRUSTED SECURITY

Карта присутності

КИЇВ — Головний офіс

Львів — Регіональний офіс

Основні вузли

22

регіональні офіси

300+

співробітників

9000+

точок присутності

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

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

infocom TRUSTED SECURITY