
С П Е Ц В И П У С К
спеціально для
МІСЯЦЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ
1 – 31 ЖОВТНЯ
2020 року
the Cyber Review
Security
KYIV CHAMBER OF COMMERCE AND INDUSTRY
Ж У Р Н А Л
К И Ї В С Ь К О Ї
ТОРГОВО-ПРОМИСЛОВОЇ
П А Л А Т И
ЖОВТЕНЬ
2020
kiev-chamber.org.ua

SMART technologies

www.smarttechnologies-ua.com

З М І С Т

the CyberSecurity Review

журнал Київської торгово-промислової палати

КИЇВСЬКА ТОРГОВО-ПРОМИСЛОВА ПАЛАТА –
найбільша у системі ТПП в Україні, працюючи у всіх напрямках,
пропонує новий інформаційний продукт –
онлайн–журнал **The CyberSecurity Review**

Електронний журнал
The CyberSecurity Review
це інтерактивний майданчик для розміщення
інформації з актуальних питань та її обговорення.

Матеріали авторів публікуються після схвалення
редакційною радою електронного журналу.

Матеріали повинні відповідати оголошеній тематиці.

Якщо Ви хочете стати автором статті в електронному журналі –
надсилайте свої матеріали на адресу kopetska@kcci.org.ua

Для передплати – надішліть запит на kopetska@kcci.org.ua
Послуга для членів Київської ТПП – безкоштовна.

КИЇВСЬКА ТОРГОВО-ПРОМИСЛОВА ПАЛАТА

Kyiv Chamber of Commerce and Industry
kiev-chamber.org.ua

UKRAINIAN CHAMBER OF COMMERCE AND INDUSTRY

ГЕННАДІЙ ЧИЖИКОВ

президент ТПП України

Від імені Торгово-промислової палати України вітаю усіх з Місяцем кібербезпеки в Україні!

ІТ зараз застосовуються в кожній сфері людської життєдіяльності: чи то політика, економіка, наука, культура, охорона здоров'я і т.д. Все більше даних міститься на цифрових носіях. Інформаційна інфраструктура сьогодні забезпечує функціонування не тільки державного апарату, а й більшості великих підприємств. Враховуючи все це, збільшується також і кількість загроз, які впливають на інформаційну безпеку. Наразі кіберризики посідають одне з провідних місць серед ризиків, які загрожують бізнесу.

Торгово-промислова палата України надає великого значення питанням кібербезпеки наших членів. За ініціативи **ТПП України**, при підтримці **РНБО України**, **Держспецзв'язку**, **Кіберполіції МВС** Україна приєдналась до європейської традиції і вже втретє проводить **Місяць кібербезпеки**, що надало можливість організувати навчання заходам кібергігієни більш ніж 7000 школярів в м. Києві, підвищити рівень навичок безпекової поведінки в кіберпросторі більш 300 представників бізнесу під час практичних семінарів в м. Запоріжжя, Миколаїв, Херсон, акцентувати увагу державних структур, бізнесу і громадянського суспільства на актуальності проблем кіберзахисту бізнесу підтвердило ефективність державно-приватної взаємодій в розбудові безпечного кіберпростору в Україні. Проте кіберзагрози не втихають.

Ще в листопаді 2019 року ми розпочали підготовку і планували в 2020 році розширити географію проведення заходів, присвячених питанню кібербезпеки. На жаль, COVID-19 не тільки вніс корективи в наші плани, але і відкрив нові проблеми безпечного ведення бізнесу, в яких питання безпеки набувають нової значимості.

Цього року в рамках Місяця кібербезпеки ми плануємо проведення 3 форумів, 2 міжнародних науково-практичних конференцій, тренінгів, навчальних семінарів, 2 круглих столів. Це дозволить обговорити питання взаємодії влади і бізнесу по створенню реальної і ефективної екосистеми кібербезпеки в Україні та вибудувати стратегію співпраці, що сприятиме підвищенню рівня цифрової безпеки компаній, організацій і громадян.

Бізнес має бути обізнаним!
А ми маємо бути поруч, щоб надати необхідну підтримку.

ВОЛОДИМИР КОЛЯДЕНКО

Голова Комітету з електронних комунікацій,
Антикризового центру кібернетичного захисту бізнесу
при ТПП України, віце-президент Київської ТПП

Вітаю усіх із початком третього Місячника кібербезпеки в Україні!

Подальше збільшення цифровізації бізнесу викликає у компаній необхідність протистояти все більшій кількості викликів і загроз у кіберпросторі. На жаль, сьогодні ризики кібербезпеки займають друге місце серед ризиків для бізнесу.

Надійність і конкурентоздатність України в сфері кібербезпеки залежить від рівня фахової підготовки молоді та формується у вишах, на кафедрах, лабораторіях та полігонах. Тому зв'язок і взаємодія бізнесу, влади і суспільства з молоддю, з навчальними закладами, яку ми поклали в основу Місяця кібербезпеки, є ключовими. Наше спільне завдання – підняти рівень поінформованості суспільства і рівень компетентності і мотивації молоді.

Торгово-промислова палата України через Комітет з електронних комунікацій, Антикризовий центр кібернетичного захисту бізнесу при ТПП України, регіональні торгово-промислові палати, за підтримки державних органів, виступає в якості координатора Місяця кібербезпеки в Україні в 2020 році.

Досвід проведення Місячника минулих років продемонстрував ефективність державно-приватної взаємодії в розбудові безпечного кіберпростору в Україні, надав можливість акцентувати увагу державних структур, бізнесу і громадського сектору на актуальності розробки першочергових напрямків діяльності у сфері кібербезпеки і вирішенні комплексу проблем, пов'язаних із розбудовою національної екосистеми кібербезпеки.

Цього року Торгово-промислова палата України виступає з ініціативою прийняття рішення на державному рівні про проведення Місяця кібербезпеки в Україні як щорічного загальнонаціонального заходу.

Сподіваємось, що Місяць кібербезпеки стане Національним майданчиком для ознайомлення з потенціалом України в сфері кіберзахисту, обміну досвідом і дієвою взаємодією влада-бізнес у кіберпросторі, буде сигналом бізнесу і громадськості про особливу увагу України до нової кібербезпекової реальності, формуванню нової культури поведінки у кіберпросторі.

Головна мета наших активностей – виявити шляхи допомоги компаніям будь-якого масштабу в оцінці, розробці і зміцненні своїх програм кібербезпеки для захисту бізнесу, просвіти та обміну досвідом, виявлення кращих практик в сфері інформаційної безпеки, надання дійсного поштовху в українському суспільстві щодо підвищення уваги до кібернетичних загроз та шляхів їх подолання.

1-31 ЖОВТНЯ

МІСЯЦЬ КІБЕРБЕЗПЕКИ

МІСЯЦЬ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Багато країн світу ведуть цілеспрямовану роботу, щоб зробити кібербезпеку частиною культури суспільства.
У 2004 році **Міністерство внутрішньої безпеки** і **Національний альянс з кібербезпеки** оголосили **Національний місяць обізнаності про кібербезпеки**, щоб допомогти американцям залишатися в безпеці в Інтернеті.

У 2012 році **Європейський місяць кібербезпеки** вперше пройшов в якості пілотного проекту по всій Європі.

В 2018 році, за ініціативи **Торгово-промислової палати України** та **Держспецзв'язку**, Україна приєдналася до європейської традиції та вперше провела **МІСЯЦЬ КІБЕРБЕЗПЕКИ**.

2018

У рамках **МІСЯЦЯ КІБЕРБЕЗПЕКИ 2018** відбулися:

- Конференція **Cybersecurity Legal Conference;**
- **PKI Forum UA-2018;**
- 4-5 жовтня 2018 року, в м. Гаага (Нідерланди), відбувся форум по кібербезпеці **Cyber security Week**, виставка та конференція **«CSW Congress and Expo»**.
  Посольство України в Королівстві Нідерланди спільно з ТПП України організували український павільйон за участі вітчизняних компаній галузі кібербезпеки – **«AVTOR»**, **«CyberDesk»**, **«10Guards»**;

– Київська мала Академія наук України, за участі експертів Google, при підтримці компанії Lucy Net і ТПП україни, провели **DIGITAL WORKSHOP** з кібербезпеки для вчителів;

– **ГО «Українська академія кібербезпеки»** спільно з **Департаментом освіти КМДА** провели для адміністраторів коледжів і профтехучилищ з кібербезпекової освіти і розвитку продуктивних сил **Конференцію і тренінгові курси Cyberedua-18;**

– Антикризовий центр кібернетичного захисту бізнесу при ТПП України спільно з Київською ТПП підготувати випуск журналу **«Кібербезпека»** та ін.

Під час першого місяця кібербезпеки було проведено більш 20 заходів, 10 з яких були зареєстровані як заходи у рамках заходів ЄС.

1-31 ЖОВТНЯ

ДРУГИЙ МІСЯЦЬ КІБЕРБЕЗПЕКИ В УКРАЇНІ

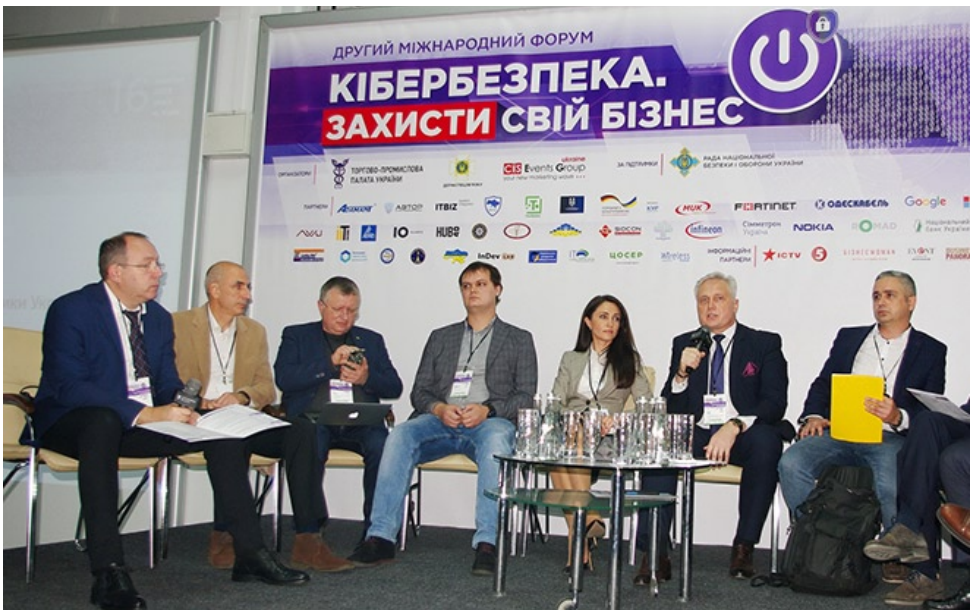
Торгово-Промислова Палата України, Комітет з електронних комунікацій, Державна служба спеціального зв'язку та захисту інформації України, за підтримки **Ради національної безпеки і оборони України** **1 - 31 жовтня 2019** року провели **Місяць кібербезпеки в Україні**

2019

Проведені спеціалізовані форуми «LEGAL CYBERSECURITY FORUM», «PKI форум».
Ключовою подією став II міжнародний форум «КІБЕРБЕЗПЕКА. ЗАХИСТИ СВІЙ БІЗНЕС!».

На форумі виступили понад **30 профільних експертів** з державних установ та бізнесу з України, США, Німеччини та Ізраїлю. Загалом участь у заході взяли **636** представників центральних та місцевих органів влади, державних підприємств і установ, освітніх закладів, бізнесу з усіх регіонів України та інших країн, асоціацій підприємців, ЗМІ, дипломатичних установ, акредитованих в Україні з 19 країн, викладачів вузів та НАН України.

У рамках форуму відбулася **спеціалізована виставка «КІБЕРБЕЗПЕКА 2019»** - перший захід такого рівня і масштабу в на якому було представлено потенціал України у сфері кібербезпеки.



Під час роботи форуму було підписано **«Меморандум про партнерство та співпрацю між Департаментом кіберполіції Національної поліції України та Торгово-промисловою палатою України»**

Під час **Другого Місяця кібербезпеки** було проведено більш **20** заходів (2 з яких були зареєстровані як заходи в рамках програми ЄС):

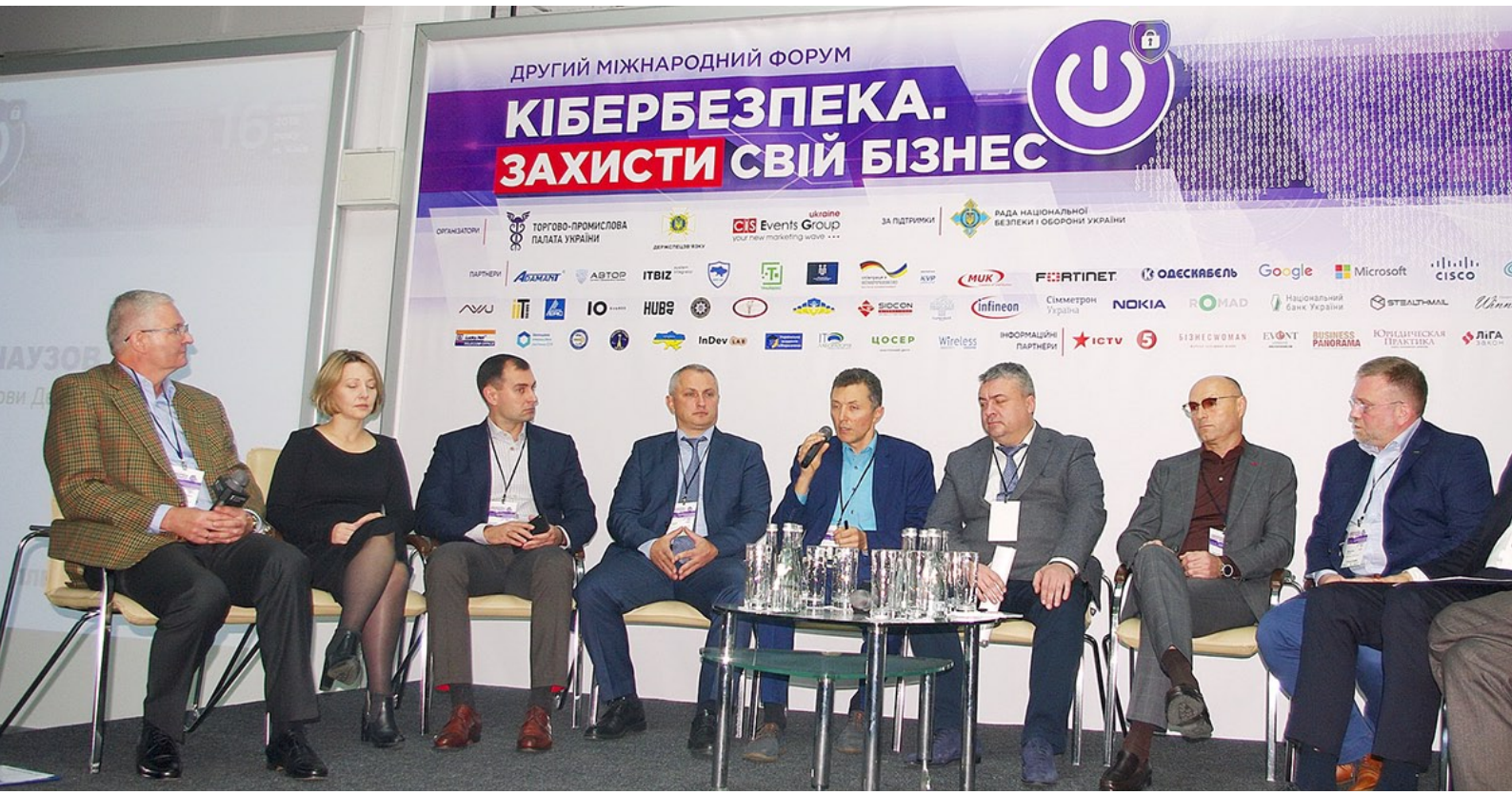
– **Київська ТПП спільно з Департаментом кіберполіції Національної поліції України** провели Круглий стіл **«Наскільки ефективні засоби протидії шахрайству Кіберполіції, судової системи, законодавства, бізнесу»**;

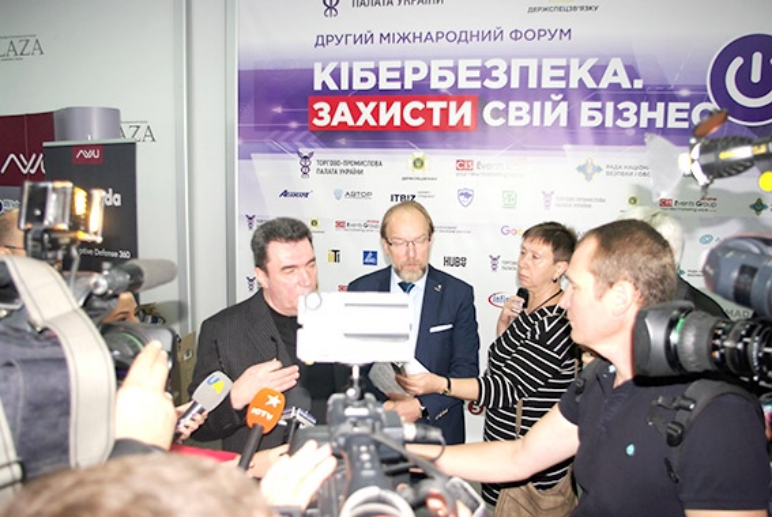
– **Херсонська торгово-промислова палата** за підтримки **ТПП України**, **Держспецзв'язку**, компанії **10Guards** провела семінар-тренінг **«Безпека бізнесу в кіберпросторі що формується»**;

– **Державного центру кіберзахисту CERT-UA**, Держспецзв'язку та захисту інформації України провели засідання науково-технічного семінару на тему «Концепція розвитку організаційно-технічної моделі кіберзахисту»;

– **Мала Академія наук України**, за участі експертів Google, при підтримці компанії **«АДАМАНТ»** і **ТПП України**, провели **DIGITAL WORKSHOP** з кібербезпеки для вчителів та стрім-трансляція із залученням педагогів з усіх регіонів України;

– **Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського»** провів в закладах освіти України відкриті уроки на тему **«Вступ до кібергігієни»**;

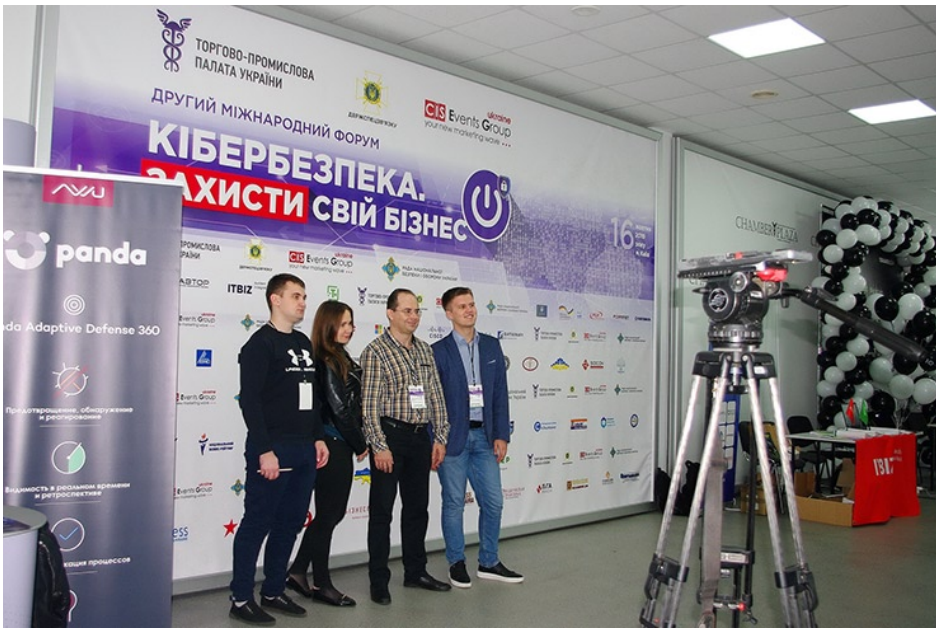




Секретар РНБО **Олексій ДАНІЛОВ:**

«Сьогодні питання кібербезпеки є питанням номер один для кожної сучасної країни, а спільне завдання бізнесу й влади – створити реальну дієву систему кіберзахисту, щоб жоден агресор не мав можливості зазіхати на безпеку держави».

– **Антикризовий Центр кібернетичного захисту бізнесу при ТПП України спільно з Київською ТПП** підготували випуск журналу **«КІБЕРБЕЗПЕКА»** присвячений тематики Місяця кібербезпеки в Україні.



НКЦК

УКРАЇНА РОЗГОРНУЛА РОБОТУ ГЛОБАЛЬНОГО КІБЕРЦЕНТРУ, СТВОРЕНОГО ПРИ РНБО

СЕРГІЙ ДЕМЕДЮК

заступник Секретаря Ради національної безпеки і оборони України

+380 **44 290 03 41**

report@ncscc.gov.ua
Facebook: https://www.facebook.com/ncsccUA
Twitter: https://twitter.com/ncsccua

Кібератаки сьогодні – потужна зброя і щороку вона стає все більш досконалою. Вона завдає мільярдних збитків та може спричинити нищівного удару інфраструктурі усієї країни. Саме тому питання забезпечення надійного кіберзахисту – важливе питання, що постоїть перед керівництвом будь-якої сучасної держави. Атаки минулих років, які пережила Україна, і досі відчутні. Вони дали розуміння того, наскільки може бути ефективною кіберзброя в руках ворога.

У відповідь сучасним викликам 27 січня 2016 року в Україні було створено **Національний координаційний центр кібербезпеки (НКЦК)**.

Центр є першим робочим органом Ради національної безпеки і оборони України. НКЦК покликаний координувати роботу усіх державних

інституцій, які займаються питаннями кіберзахисту країни, а також формувати нові шляхи вдосконалення системи кіберзахисту.

Три роки потому, у 2019 році, указом **Президента України Володимира Зеленського** було внесено зміни до діяльності НКЦК, чим суттєво підсилено спроможності Центру – розширено його завдання, функції та штат.

Олексій Данілов,
Секретар Ради національної безпеки і оборони України – керівник Національного координаційного центру кібербезпеки

Національний координаційний центр кібербезпеки став сучасним «хабом» із захисту держави від кіберзагроз. Оновлений і значно підсилений Національний координаційний центр кібербезпеки є ключовим суб'єктом в національній системі

кібербезпеки, координує та контролює діяльність суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку у відповідних сферах – Держспецзв'язку, СБУ, Національної поліції, Національного банку, Генерального штабу ЗСУ та ін.

Більше того, до роботи в НКЦК залучено висококваліфікованих спеціалістів у галузі кібербезпеки, кібероборони та кіберрозвідки: правоохоронні органи, державні суб'єкти забезпечення кібербезпеки, представники власників та операторів критичної інфраструктури, компаній з кібербезпеки, а також розробники, інтегратори, вендори та експерти.

Основними пріоритетами в роботі НКЦК є: прогнозування, виявлення, реагування на потенційні та реальні кіберзагрози, розробка стандартів кібербезпеки та інформаційної безпеки, а також розбудова системи цифрової освіти. Крім того, Центр є першим державним майданчиком, який об'єднує зусилля держави та приватного сектору у протидії загрозам національній кібербезпеці.

Важливий акцент у побудові роботи НКЦК відіграє саме державно-приватне партнерство. Більшість кібератак, які можна виявляти у реальному часі, спрямована саме на приватний сектор. Проте, співпраця між суб'єктами приватного та державного секторів до цього часу була недостатньою.

Відсутність адекватної комунікації та захисту з боку держави спричиняли недовіру суб'єктів приватного сектору до владних органів та призводили навіть до «замовчування» кіберінцидентів. Відтак, розслідування цих справ могло бути неефективним, або і взагалі не розпочиналося через відсутність звернення до правоохоронних органів.

Переважна більшість кіберінцидентів, і які є цікавими для усіх суб'єктів сектору безпеки і оборони, котрі забезпечують кібербезпеку, сталися у приватному секторі, який атакують і на якому випробовують шкідливе програмне забезпечення. В цьому випадку обмін на постійній основі даними щодо актуальних кіберзагроз й інструментів боротьби з ними, формування відносин довіри між регуляторами кібербезпеки і керівництвом приватних підприємств – сприяє створенню ефективної системи кібербезпеки держави у цілому.

Налагодження плідного контакту з приватним сектором, початок формування єдиної бази обміну інформацією про кіберінциденти дозволяє вчасно і професійно виявляти і локалізувати виявлені кібератаки, розробляти алгоритм підготовки до них, координувати на високому рівні діяльність усіх суб'єктів кібербезпеки.

Крім того, наразі на базі НКЦК державні суб'єкти сектору безпеки і оборони разом з представниками приватного сектору працюють над розробкою унікального програмного забезпечення для виявлення кібератак ще на початковому етапі.

Ми хочемо закріпити на законодавчому рівні стандарти послуг із кіберзахисту і обов'язковість їх надання, працюємо над створенням бази фахівців з приватного сектору, кваліфікованих Держспецзв'язком і НКЦК, які можуть надавати відповідну консультаційну допомогу. Ми плануємо також використовувати приватний сектор для тестування різного роду програмного забезпечення на предмет виявлення вразливостей чи шкідливого коду, а також нових методів захисту систем, щоб надалі ці знання використовувати для захисту державних установ.

Серед пріоритетів діяльності НКЦК – також провадження освітницької діяльності у сфері кібергігієни, оскільки відсутність у людей відповідних знань є чи не найголовнішою причиною вразливості для кібератак.

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Наша адреса:
03110, Київ, вул. Солом'янська, 13

Наші телефони:

Приймальня Голови Держспецзв'язку
281-90-00 (тел.)
281-94-83 (факс)

Щодо опрацювання вхідних документів
281-92-27 (тел.)
281-92-30 (тел./факс)

Щодо опрацювання вихідних документів
281-94-32 (тел.)
281-94-41 (тел./факс)

Щодо розгляду заяв, скарг та пропозицій
281-92-83 (тел.)

Щодо розгляду запитів
на отримання публічної інформації
281-92-81 (тел./факс)

Електронна пошта:

Для листів
info@dsszzi.gov.ua

Адміністратор
admin@dsszzi.gov.ua

Для ЗМІ
press@dsszzi.gov.ua

STATE SERVICE OF SPECIAL COMMUNICATION AND INFORMATION PROTECTION OF UKRAINE

https://cip.gov.ua

ЗАХИСТ ІНТЕРЕСІВ ОСОБИ, СУСПІЛЬСТВА, БІЗНЕСУ ТА ДЕРЖАВИ ЯК НАРІЖНИЙ КАМІНЬ ДІЯЛЬНОСТІ У СФЕРІ КІБЕРБЕЗПЕКИ

ЮРІЙ ЩИГОЛЬ

Голова Державної служби спеціального зв'язку та захисту інформації України, підполковник

Нова Стратегія національної безпеки «Безпека людини – безпека країни», введена в дію Указом Президента України від 14 вересня 2020 року № 392/2020, визначила одним з пріоритетів національних інтересів України посилення спроможностей національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі. Шляхи реалізації цього пріоритету полягають у розробці адекватної стратегії забезпечення кібербезпеки України, яка має визначити окресленої законодавством України напрями розвитку національної системи кібербезпеки з урахуванням загроз, що постають перед суспільством в умовах розвитку інформаційних технологій, підвищення їх ролі у сучасному постіндустріальному суспільстві, особливо у тих умовах, коли глобальні виклики, на кшталт різного роду пандемій, що змущують людство змінити звичні правила спілкування та взаємодії, виводять кіберпростір на роль особистого та суспільно значущого фактору.

Як зазначають американські дослідники, кіберпростір є середовищем, яке принципово відрізняється від нормального фізичного світу. І тим не менш, насправді кіберпростір є надзвичайно фізичним середовищем: він створений фізичними мережами та системами, поєднаними між собою та підпорядкованими певним правилам, що проявляються через програмне забезпечення та комунікативні протоколи. Більш того, сама основа роботи кіберпростору – це суто фізичні закони електромагнетизму та світла. Саме вони створюють його основну особливість – глобальні комунікації через кіберпростір, які здійснюються майже миттєво, а масштабні обсяги даних передаються на великі відстані, ігноруючи географічні і політичні кордони. Саме швидкість і незалежність від фізичних перешкод дає основну перевагу і одночасно створює проблему, оскільки можливості кіберпростору можуть бути використані будь-ким і з будь-якою метою.

Таким чином, кіберпростір як основа глобальних процесів цифрової трансформації та як середовище, яке реально існує поряд з суходолом, морем, повітрям і космосом, вимагає дедалі більше уваги приділяти питанням його безпечного використання, розвитку і сталості, тобто питанням його безпеки і захисту.

Кіберзахист – це мистецтво захисту мереж, пристроїв, даних від несанкціонованого доступу або злочинного використання, це практика забезпечення конфіденційності, цілісності і доступності інформації, яка циркулює в кіберпросторі, який розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтер-

активний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадянського суспільства до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади і одночасно стає джерелом виникнення нових загроз національній та міжнародній безпеці. Сьогодні поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб. В умовах, коли світ переходить на нові форми навчання, спілкування та взаємодії ці загрози стають актуальними. Нові виклики потребують прийняття відповідних заходів, спрямованих на забезпечення безпеки людини, громадянина, суспільства та держави у кіберпросторі.

Серед таких заходів – заходи з підвищення рівня усвідомлення як окремими громадянином, так і суспільством і бізнесом тих ризиків, які пов'язані із невиконанням правил і базових вимог безпечного застосування сучасних інформаційних технологій в умовах поширення процесів цифровізації суспільних взаємовідносин, а також заходи, які мають впроваджуватись задля захисту особистості, її життя, розвитку, діяльності і бізнесу як потенції розвитку економіки будь-якої країни, громадянського суспільства і власне держави як інструменту і механізму організації процесів розвитку країни.

Ці заходи відповідають кращим світовим практикам у сфері кібербезпеки і викладені у постанові КМУ №518 «Про затвердження Загальних вимог

до кіберзахисту об'єктів критичної інфраструктури». Цей нормативно-правовий акт, який імплементує світові підходи і стандарти з кібербезпеки допомагає широкому колу українських фахівців захищати власні інформаційні ресурси своїх компаній та установ від кібератак та кіберінцидентів.

Унікальною ситуацією є потужний поштовх використання кіберпростору в умовах поширення коронавірусної хвороби (COVID-19). Його поширення змусило світ перейти до роботи, навчання, спілкування on-line та призвело до швидкого розвитку нових технологій віддаленого доступу, що, у свою чергу спровокувало появу нових ризиків кібербезпеки через неусвідомлення користувачами важливості виконання навіть елементарних заходів захисту.

Тому донесення до широких верств населення, до бізнесових кіл, важливості питань кіберзахисту на сьогодні розглядається у світі як основа політики кібербезпеки і як головний стрижень національної безпеки будь-якої країни та захисту особи, суспільства і держави у кіберпросторі. Формування нової моделі поведінки у кіберпросторі, необхідність постійної роботи над зміною поведінки усіх користувачів кіберпростору та створення умов для ознайомлення їх з ризиками, що пов'язані з новими технологіями, зокрема технологіями 5G, M2M, IoT, адитивного виробництва, технології доповненої реальності, хмарних обчислень, штучного інтелекту тощо, вимагають проведення широкої інформаційної компанії, передусім на рівні держави із залученням бізнесу і професійних освітніх кіл як ресурсної бази для формування майбутнього сучасного навченого і обізнаного суспільства, яке не тільки користується перевагами інформаційного світу, але й дбає про захист критичної інфраструктури своєї держави в інтересах країни і світу в цілому.

Місячник кібербезпеки, який втретє поспіль відбувся в Україні у жовні 2020 року став майданчиком широкого поширення знань і навичок у сфері кібербезпеки серед усіх верств населення,

ДЕРЖСПЕЦЗВ'ЯЗКУ У ОСОБІ ІНСТИТУТУ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ НТУУ «КПІ» ІМ. ІГОРЯ СІКОРСЬКОГО ВЖЕ НЕ ПЕРШИЙ РІК БУДЕ ПРОВОДИТИ ВІДКРИТІ ЗАНЯТТЯ З КІБЕРГІГІЄНИ САМЕ В ШКОЛАХ, ТАМ, ДЕ СЬОГОДНІ ВИХОВУЄТЬСЯ МАЙБУТНЄ НАШОЇ КРАЇНИ

серед бізнесу, який є основою стабільного розвитку країни та її інтеграції у світовий інформаційний простір, у безпекові європейські і світові організації. Саме формування нової парадигми безпечної поведінки в мережі є нашим загальним завданням. **Тому Держспецзв'язку у особі Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ» ім. Ігоря Сікорського вже не перший рік буде проводити відкриті заняття з кібергігієни саме в школах, там, де сьогодні виховується майбутнє нашої країни.** У минулому році такі заняття були проведені у 120 школах по всій Україні, до них було залучено понад 7 тис. учнів.

На сьогодні здійснюється поступовий перехід із існуючої нормативно-правової бази системи технічного захисту інформації на міжнародну. Зокрема, в Закон України **«Про захист інформації в інформаційно-телекомунікаційних системах»** внесені зміни, які забезпечують можливість сучасним компаніям будувати системи управління інформаційною безпекою у відповідності до вимог міжнародних стандартів та найкращих світових практик. Розробляється пакет документів, вимоги яких спираються на вимоги стандартів провідних країн світу, зокрема США. Це дозволить в перспективі забезпечити можливість вибору заходів для кіберзахисту та створити умови для бізнесу застосовувати прийнятні для нього рішення, забезпечуючи при цьому виконання вимог держави із захисту населення України від можливих наслідків реалізації кіберзагроз на об'єктах критичної інфраструктури.

Держава продовжує розбудову організаційно-технічної моделі, яка забезпечує повний цикл заходів щодо кіберзахисту, спрямовані на виявлення кіберзагроз, реагування на них та відновлення систем у разі їх реалізації. Галузеві центри реагування на кіберзагрози мають стати ключовим елементом для подальшого ефективного розвитку організаційно-технічної моделі кіберзахисту. Показовими є приклади роботи таких центрів, які побудовані у Мінінфраструктурі, Національній енергетичній компанії «Укренерго», які не лише розпочали свою роботу та прагнуть взаємодії не тільки з державними центрами, але готові співпрацювати із представниками приватного сектору. Розгортається потужний проєкт з побудови у Міненерго галузевого Центру забезпечення кібербезпеки, розробки та затвердження галузевої Стратегії та Концепції кібербезпеки, а також низки галузевих нормативно-правових актів. Особиста зацікавленість та небайдужість Міністра енергетики суттєво пришвидшує реалізацію цього проєкту.

Суттєвий внесок у забезпечення кіберзахисту України у кіберпросторі робить бізнес. Ряд компаній успішно завершили проєкти з розгортання власних центрів реагування, здійснюють збір та обробку даних щодо кіберінцидентів на власних підприємствах, відповіді на кібератаки та кіберінциденти. Безумовно, результати діяльності таких центрів мають стати основою державно-приватної взаємодії в сфері кібербезпеки, яка ґрунтується на принципах довіри. Тим більше, що державі є що запропонувати бізнесу, і зокрема це фахова допомога команди реагування на комп'ютерні інциденти CERT-UA, обмін інформацією через платформу MISP. Держспезв'язку завжди відкрита для такої взаємодії та запрошує до співробітництва всі заінтересовані компанії.

Здійснюються заходи із покращення взаємодії основних суб'єктів забезпечення кібербезпеки, розгортаються платформи для швидкого обміну інформації щодо інцидентів.

Кроки, які виконуються сьогодні, законодавча база, яка формується, організаційні заходи, які впроваджуються, дозволяють Україні імплементуватися у світовий економічний простір на засадах рівності і безпеки.

Зважаючи на те, що Україна стала однією з перших країн світу, яка розробила рекомендації по забезпеченню кібербезпеки при роботі в умовах віддаленого доступу як для органів центральної влади, так і для приватного сектора і бізнеса, впевнений, що цьогорічна інформаційна кампанія, заходи, які у рамках її проведення заплановані, державно-приватна взаємодія, яка налагоджується у ключових сферах національної безпеки, дозволять значно просунути за підтримки та на умовах взаємодопомоги наше суспільство та бізнес на шляху створення безпечного і захищеного інформаційного суспільства в Україні.

ДЕПАРТАМЕНТ КІБЕРПОЛІЦІЇ
НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

КІБЕРПРОСТІР ЯК П'ЯТА СФЕРА ЖИТТЯ.

ЙОГО ВИКЛИКИ – НАШІ ЗАВДАННЯ

ОЛЕКСАНДР ГРИНЧАК

начальник **Департаменту кіберполіції Національної поліції України**, полковник

callcenter@cyberpolice.gov.ua
https://cyberpolice.gov.ua

Повсякденне життя українських громадян все сильніше залежить від сучасних інформаційних сервісів. Із впровадженням державою цифрових технологій у сферу надання послуг зростає кількість громадян, що їх споживають і сплачують. Все це посилює ризики від діяльності кіберзлочинців, які стають дедалі активнішими. Така проблема, як виток персональних даних громадян України із автоматизованих систем державних органів та приватних компаній стає пріоритетом діяльності злочинів. Ситуація ускладнюється, оскільки з'являються нові форми приховування кіберзлочинцями не лише своїх комунікацій (Darknet та Deepweb), але й інструментів виведення коштів (криптовалюти).

У свою чергу Держава стикається із низкою загроз та викликами у сфері кібербезпеки. На сьогоднішній день існує понад 100 державних та єдиних реєстрів, які містять конфіденційну (у т. ч. про особу) інформацію. Більшість з них використовує авторизацію за допомогою логіну та паролю, що у свою чергу має певні вразливості. Зокрема, у такий спосіб не можливо достовірно ідентифікувати особу, яка отримує інформацію з реєстру (логін та пароль легко надати іншій особі, чи підібрати, тощо).

Разом з цим, гостро стоїть проблема із захистом інформації, яка зберігається у розпорядників (держателів) реєстрів чи баз даних. Здебільшого мережева інфраструктура має застаріле та вразливе програмне забезпечення. Переважно користувачі, а деколи і адміністратори поряд з доступом до реєстрів мають доступ в мережу Інтернет, що в рази збільшує ризики зовнішнього ураження та подальшої кібератаки на системи зберігання інформації.

За період незалежності України, переважна більшість інформації накопичена на паперових носіях. З метою її цифрової трансформації залучаються

приватні компанії. Вони тимчасово отримують доступ до інформації, що містить персональні данні. Тобто у рази зростають ризики витоку конфіденційних даних. На противагу накопиченню, обробка та зберігання більшої кількості інформації потребує збільшення цифрової інфраструктури (сервери, мережі, дата центри), а їх збільшення та розростання потребує підвищеної уваги до забезпечення безпеки цих об'єктів.

Збирання, опрацювання та накопичення даних вимагає реалізації принципу прозорості. Будь-яка інформація та опрацювання персональних даних повинні бути доступними, зрозумілими та захищеними. Крім цього період, протягом якого зберігаються персональні дані, має реалізовувати принцип «дані не зберігаються довше, ніж це необхідно». Чітко визначений період зберігання та знищення це ще один чинник, який убезпечить від несанкціонованого витоку інформації.

Національною поліцією встановлено, що на спеціальних форумах та у закритих спільнотах циркулюють різні бази даних. Деякі дійсно актуальні та постійно оновлюються, інші мають застарілий характер, однак містять персональну інформацію.

Наявність такої циркулюючої інформації, створює підґрунтя для вчинення протиправних дій у кіберпросторі метою, яких є отримання прибутку від продажу персональних даних. Так, злочинцями створюються спеціальні сервіси для перевірки інформації чи безпосереднього продажу баз даних.

Більш широка сфера – шахраї. Вони під приводом продажу інформації, баз даних здійснюють заволодіння коштами. Великий суспільний розголос, а також інше привертання уваги до будь-яких витоків інформації активізує злодіїв. Латентність таких злочинів значна, а їх розслідування переважно не розпочинається з заяви потерпілої сторони, більшість таких фактів розкривається ґрунтуючись на оперативній інформації.

Наразі, Національною поліцією на постійній основі забезпечено відслідковування активності учасників російськомовного сегменту хакерської спільноти.

Зокрема, на закритих онлайн майданчиках **«darknet»**, **«tor»**, на закритих каналах «skype», «telegram». Відслідковуються публікації приватних дослідників з інформаційної безпеки щодо витоку персональних даних громадян України із автоматизованих систем державних органів та приватних компаній. За наявною інформацією, такі витоки відбуваються щонайменше раз на 2 місяці.

Найпопулярнішими серед таких майданчиків є закриті веб-форуми **«exploit.in»**, **«phreaker.pro»**, **«peers.fm»** та **«xss.io»** доступ до участі в яких здійснюється на підставі числених перевірок кандидатів. Наявності в них хакерських навичок та поручителів, а також за вступними внесками, що в деяких випадках перевищують 150 доларів США.
У Національній поліції протидія таким видам злочинів забезпечується системними заходами особистого пошуку, які здійснюються найдосвідченішими працівниками, агентурною роботою з учасниками хакерської спільноти, роботою із власними оперативними обліками, які напрацьовані у ході збору

вмісту закритих онлайн майданчиків **«darknet»**, **«tor»**, та у тому числі завдяки активній участі поліції у співпраці із правоохоронцями інших держав.

З метою стабілізації криміногенної ситуації, виявлення та вилучення з незаконного обігу баз даних, що містять інформацію з обмеженим доступом Кіберполіцією у поточному році проведено низку відповідних профілактичних заходів. Зусилля кіберполіцейських спрямовано на досягнення якісного результату, а не штучного збільшення кількісних показників.

Під час практичного етапу, який тривав лише один тиждень Кіберполіцією виявлено 34 факти неправомірних дій, пов'язаних з розповсюдженням чи збутом даних з обмеженим доступом, відомості про які внесені до ЄРДР.

Зокрема встановлено осіб, які упродовж тривалого часу збирали інформацію з обмеженим доступом (особисті дані) та реалізовували її у Телеграм каналах, соціальних мережах, тематичних форумах.

Проведено 36 обшуків на території понад 10 регіонів України та здобуто докази протиправної діяльності 25 фігурантів, у тому числі відносно групи до складу якої входить 7 осіб, які під приводом продажу баз даних комерційних та державних установ, вчиняли шахрайські дії.

За результатами проведених слідчих дій з незаконного обігу вилучено ресурси, що містять персональні дані громадян України, фрагменти баз даних та бази даних електронних поштових адрес, аккаунтів платіжних систем ігрових сервісів.

Крім цього, оголошено про підозру мешканцю однієї з областей України у вчиненні 8-ми фактів несанкціонованого доступу до облікових записів користувачів онлайн-магазинів.
Так, в Україні за останні 5 років кількість кіберзлочинів зросла у 2,5 рази. Кіберполіція фіксує зростання таких видів, як:

- втручання в роботу інформаційних систем та їх навмисне пошкодження;
- незаконне збирання, зберігання, використання, знищення, поширення персональних даних та інформації з обмеженим доступом;
- створення каналів розповсюдження зброї та наркотиків;
- незаконні фінансові операції, у тому числі з цифровими валютами, крадіжки та шахрайства у мережі Інтернет: кардінг (використання реквізитів чужих карток), фішинг (отримання реквізитів, персональних даних кардхолдерів), скімінг (зчитування інформації з банківської картки);
- спам та вірусні програми: криптолокери (шифрувальники-вимагачі), стіллери (збір персональних даних ті іншої інформації).

Більш того, крім небезпеки для людини та шкоди для бізнесу, кіберпростір несе загрози й національній та міжнародній безпеці. Сьогодні ми змушені констатувати, що він стає п'ятою сферою ведення бойових дій, поряд із традиційними: Земля, Повітря, Море та Космос.

Потужна національна система кібербезпеки є надважливою складовою системи Національної безпеки України, а МВС, та безпосередньо Департамент кіберполіції Національної поліції України є однією з ключових структур у цій системі.

Кіберполіція України ефективно протистоїть сучасним загрозам, але кіберпростір постійно розвивається, і разом з ним з'являються нові виклики.

Вже сьогодні Кіберполіція, з урахуванням світових тенденцій приступила до формування та розробки нових стратегій та візій кібербезпеки, підготовки методології протидії кіберзагрозам та надання методичної допомоги правоохоронним органам, з метою – посилення системи Національної безпеки України!

Тому, сьогодні Кіберполіція готова перейти на новий рівень боротьби із кіберзлочинністю у кооперації з IT-бізнесом, науковим середовищем і міжнародними партнерами.

МІФИ ЩОДО ПОБУДОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У БАНКАХ ТА ФІНАНСОВИХ УСТАНОВАХ

ОЛЕКСАНДР ДРЕЛІНГ

к. т. н., старший науковий співробітник,
екс-заступник голови правління банку

+380 50 311 57 49

Маючи великий досвід роботи, зокрема, у банківському секторі, хочу розказати про існуючі у суспільстві міфи щодо галузі інформаційної безпеки. А також хочу висловити аргументи й докази щодо розвінчання цих міфів.

Міф №1. Стосується того, що більшість банків та фінансових установ досі не вважають інформаційну безпеку чимось доцільним, у що треба вкладати гроші. Це їх помилкова точка зору.

Наведу один із «свіжих» прикладів. Нещодавно сайт Національної поліції піддався хакерській атаці, у результаті якої на сторінках декількох обласних управлінь зловмисники встигли розмістити фейковий контент. Про це всі ми дізналися із масс-медіа. Чекаємо результатів розслідування. Інший приклад – приблизно півроку тому невеликі компанії та банки України зазнали значних втрат після хакерської атаки, яка визначалася у шифруванні критичних файлів. Ті, хто проводив ці атаки, вимагали гроші за надання коду дешифрування. Я знаю, що багато організацій заплатили гроші. Проте за висновками антивірусних лабораторій, файли практично було зруйновано і знищено, тобто їх реанімація була не можливою. Компаніям та банкам було нанесено фінансових та репутаційних втрат.

Наступна прикра подія сталася декілька років тому. Хочу зупинитися детальніше на цьому прикладі, оскільки він був унікальним. Це факт хакерських атак на SWIFT-ресурс банків. SWIFT – міжнародна платіжна система. Зараз вона називається CRISP і нині гарантує потрійне дублювання ресурсів та найвищий рівень захисту своєї технології. Але у той час у двох українських банках цю технологію було зламано й вкрадено мільйони доларів. Це була дуже потужна та «цікава» атака, яка досі не розслідувана. Отже величезні фінансові втрати для банківської спільноти примусили замислитися над вирішенням подібних проблем.

Наступний приклад – всім відомий і дуже розповсюджений вірус «Петя». Тут я можу із задоволенням зазначити, що ті банки, де я працював, зберегли стабільність та працездатність головних фінансових бізнес-процесів. Втім багато інших банків та фінансових установ ще досі не оговталися.

Можна згадати про blackenergy, що мала критичний вплив на об'єкти критичної інфраструктури України. Що може статися завтра, враховуючи нашу загальну нестабільну ситуацію, ніхто не знає. Точно, – не спокійніше.

Мій висновок щодо першого міфу, – треба вкладати в інформаційну безпеку максимально ресурсів, як професійних, так й фінансових.

Рівень інформаційної безпеки у світі постійно зростає. З точки зору фінансування інформаційної безпеки в компаніях, ще 10 років тому вважалося, що її бюджет повинен складати приблизно 5-10 відсотків від загального бюджету на послуги IT. Нині до 30 відсотків, а то й більше – у залежності від ступеню критичності об'єктів та існуючого стану захисту інформації в цих компаніях.

Міф №2 про те, що інформаційна безпека не повинна мати високого рівня і статусу в організації. Це – дуже помилково, тому що досвід показує: для того, щоб успішно захищатися від зовнішніх атак і, особливо, від внутрішніх атак, фахівці інформаційної безпеки повинні бути на рівень вище тих, хто атакує. На 95 відсотків внутрішні хакери – це фахівці IT з високим рівнем знань та повноважень.

Тому, практичний висновок щодо цього міфу – рівень і статус підрозділа з інформаційної безпеки повинен бути на тому ж рівні, що й бізнес-підрозділи у компанії. Спеціалісти з інформаційної безпеки повинні мати повноваження і такий самий рівень заробітної плати і соціальний пакет, а, іноді, навіть більший, як і ключові працівники компанії.

Міф №3 – про те, що інформаційною безпекою може керувати у компанії, хто завгодно. Якщо звернути увагу на те, які оргмоделі використовують деякі банки, у тому числі досить солідні, можна здивуватися не на жарт. Інформаційною безпекою керують юридичний департамент, голова правління, бізнес. Хто завгодно... Це шлях у «нікуди».

У житті існують дві перевірені часом моделі. Модель номер один (якої дотримувався я), – коли IT та інформаційна безпека перебуває під контролем одного з членів правління. Разом з цим, ця конкретна людина повинна мати відповідний фах і відповідний досвід роботи за цими напрямками, бути здатною вирішувати робочі конфлікти збалансовано, не втратити стабільність IT-ресурсів з одного боку, та забезпечити необхідний рівень інформбезпеки, з іншого боку. Це дуже складна робота. Особливості полягають у тому, що найбільше конфліктів при побудові інформаційної безпеки, якраз виникає між IT та службою безпеки. І член правління, маючи відповідний досвід, повинен збалансувати цю ситуацію.

Друга модель, яка має місце на практиці, – коли інформаційна безпека знаходиться під контролем загальної служби безпеки. Але тут, у більшості випадків, керівники служби безпеки – це люди, які знаються на технічному захисту інформації, що складає не більше 10 відсотків від необхідних знань з інформбезпеки. Важливо, щоб людина, яка очолює службу безпеки, теж мала технічну освіту та мала змогу вирішувати усі проблеми.

Висновок? Вибирайте правильну модель та професійного CISO. Тільки у такому разі ви отримаєте фактор сильної інформбезпеки у компанії.

Наступне про що хотів би наголосити – це важлива роль держави у створенні відповідних законів та розробки стратегій. Насамперед, мова йде про основні засади кібербезпеки, про захист інформації та про об'єкти критичної інфраструктури. Це вкрай необхідні речі. Але більш важливіше те, що вони повинні бути не просто прийнятті, а практично реалізовані.

Я маю на увазі те, що на підставі цих документів насамперед повинен бути проведений аудит існуючих об'єктів критичної інфраструктури, як державних, так і в комерційних галузях, зроблено SWOT аналіз, розроблено відповідні плани, проведено оцінку необхідних ресурсів та бюджетів, виділено їх та розпочато практичну реалізацію.

А держава через відповідні комітети та комісії повинна здійснювати постійний моніторинг ситуації. Це те, що ми всі очікуємо і те, що має реально практичну цінність.

Хочу підкреслити важливу роль підготовки професійних кадрів з інформбезпеки в Україні. Звичайно це завдання у першу чергу профільних вишів держави. Треба уживати також заходів щодо навчання пересічних громадян. Важливо поглиблювати спілкування та нетворкінг між професіоналами та студентами.

Все це сукупно дасть результати на користь держави та бізнесу. ■

СПЕЦІАЛІЗОВАНИЙ СИСТЕМНИЙ ІНТЕГРАТОР УКРАЇНИ

СМАРТ ТЕХНОЛОДЖІС:

ВИРІШУЄМО IT-ЗАДАЧІ КОРПОРАТИВНИХ КЛІЄНТІВ НА НАЙВИЩОМУ РІВНІ

Компанія СМАРТ ТЕХНОЛОДЖІС модернізує та впроваджує необхідні інфраструктурні рішення. Створює та розробляє концепцію, аналізує та удосконалює IT- інфраструктуру та IT безпеку. Обслуговує та підтримує корпоративні інформаційні мережі та системи. Ми зустрілися з комерційним директором Максимом АЛЕКСЄЄНКО, щоб запитати про напрямки роботи і переваги, які може надати компанія своїм партнерам- клієнтам.

– Ми йдемо в ногу з ринком IT-технологій, є партнерами світових віробників та лідерів IT- індустрії, обираємо інноваційні шляхи. Ми залучаємо лише компетентних IT-практиків, впроваджуємо оптімальні решення, что впливають на розвиток та розширення бізнесу замовника та его захист.

МАКСИМ АЛЕКСЄЄНКО

комерційний директор

СМАРТ ТЕХНОЛОДЖІС

+380 44 331 47 89

www.smarttechnologies-ua.com

– Які основні напрямки з кіберзахисту від СМАРТ ТЕХНОЛОДЖІС Ви пропонуєте?

– Їх досить багато. Я їх просто перерахую:
Ми забезпечуємо захист мережі **Network Access Contro**l. В нашому арсеналі – методи протідії **DoS / DDoS**- атак та антивірусні решення.

Пропонуємо системи моніторингу та аналізу мережевий трафіку, системи управління вразливостями (Vulnerability Management).

Можемо захищати середовища віртуалізації та БД (бази даних, - *прим. ред.*).

Здійснюємо:

- Оцінку рівня захіщеності IT- інфраструктури
- Впроваджуємо стандарт ISO/IEC 27001, ISO/IEC 27002 та GDPR
- Налаштовуємо DLP- систему
- Здійснюємо мультифакторну аутентіфікацію
- Захищаємо дані від неавторізованого доступу
- Забезпечуємо безпеку Endpoint Protection.

Можемо відповідати за контроль прівілейованих користувачів та паролей.
У нашій компетенції – сканування вразливостей та Penetration test, а також:

- Впровадження і аудит управлінням **IT- технологіямі Cobit**;
- Побудова системи збору и кореляції подій (**SIEM**);
- Захист від атак «нульового дня»;
- Побудова IPS і системи міжмережевого екранування (**NGFW/NGIPS**);
- Установка системи Web- фільтрації контенту (**Secure Web Gateway, Secure Email Gatewa**y);
- Захист Web-Додатків (**Web Application Firewall**).

– Про який із продуктів, який пропонує Ваша компанія клієнтам, Ви хотіли б розказати трошки більше сьогодні?

– **Imperva SecureSphere** – найкраще в своєму класі рішення із захисту даних і аудиту. Це – вибір преміум-класу для захисту критичних для бізнесу даних і додатків в хмарних середовищах і на власних майданчиках клієнтів.

Рішення з захисту даних SecureSphere покриває всі аспекти безпеки баз даних і відповідності регулюючим вимогам, використовуючи кращі в індустрії механізми аудиту баз даних, захисту в реальному часі, що не приводять до втрати продуктивності або доступності.

За допомогою багатоланкової архітектури Imperva SecureSphere може масштабуватися для підтримки найбільших баз даних і систем великих обсягів даних. З огляду на автоматизацію захисту даних і дотримання відповідності регулюючим вимогам, не дивно, що тисячі компаній вибирають Imperva SecureSphere для забезпечення безпеки своїх найцінніших активів.

IMPERVA

SecureSphere

ЗАХИЩАТИ ДАНІ В ЇХ ДЖЕРЕЛІ

Imperva SecureSphere

забезпечує моніторинг захисту даних і незалежне журнал аудиту на відповідність регулюючим вимогам:

• Запис в журнал тільки необхідної інформації про активність при проведенні моніторингу всіх дій на предмет порушення безпеки;

• Моніторинг та захист баз даних з високим рівнем транзакцій;

• Блокування підозрілих дій в момент, коли вони відбуваються, проведення контекстного розслідування;

• Виконання багатовекторних сигналів безпеки, усуваючи вузькі місця і затримки;

• Взаємозв'язок захисту бази даних фаєрволом вебдодатків SecureSphere Web Application Firewall, системою захисту Account Take-over Protection і рішенням по захисту від шкідливого ПО для забезпечення багатофакторної безпеки.

Відповідність регулюючим вимогам SecureSphere допомагає організаціям виконати регулюють вимоги, в тому числі такі як PCI DSS, SOX, My Number і HIPAA.

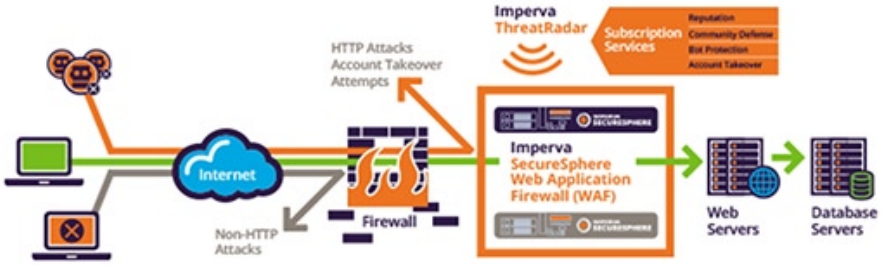
• За допомогою визначених політик і звітів покриває регулюючі вимоги для баз даних.

• Здійснює швидку конфігурацію і розгортання модифікованих політик.

• Забезпечує поділ ролей з використанням захищених від підробки даних аудиту.

• Оновлення в режимі «на ходу» і «дзвінок додому» мінімізують необхідність перезапуску системи і викликаних ними прогалин в даних аудиту.

• Завдяки SecureSphere стає можливою гнучкість і адаптивність для відповідності нестабільних IT-середовищах і регулюючим вимогам.



the CyberSecurity Review

ЖУРНАЛ
КИЇВСЬКОЇ
ТОРГОВО-ПРОМИСЛОВОЇ
ПАЛАТИ

1-31 ЖОВТНЯ 2020

МІСЯЦЬ КІБЕРБЕЗПЕКИ В УКРАЇНІ

вул. Б. Хмельницкого, 55
Київ, 01054, Україна
тел: **+380 44 482 03 01**
факс: **+380 44 482 39 66**

KYIV CHAMBER OF COMMERCE AND INDUSTRY
info@kcci.org.ua
kiev-chamber.org.ua

ВЛАДИСЛАВ МАСЛО

CEO

AM Integrator Group

+380 **44 394 86 07**
+380 **44 394 86 09**

mail@amintegrator.com
https://amintegrator.com/

ХОЧЕТЕ БУТИ ЗАХИЩЕНИМИ, ЯК GOOGLE, HP, MICROSOFT?

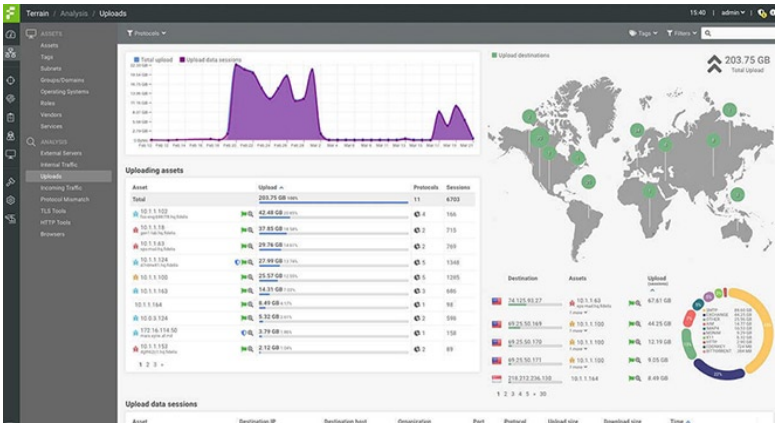
Активна руйнівна діяльність зловмисників у кіберпросторі України відома навіть людям, не пов'язаним з IT-галуззю. Державні органи, корпорації, приватні підприємства змушені робити серйозні кроки з інформаційної безпеки. Втім традиційних заходів із захисту виявляється недостатньо.

Компанія «АМ Інтегратор» склала концепт кіберзахисту з найнадійніших та новітніх платформ кібербезпеки.

Що робити, коли зловмисники знаходять нові можливості для проникнення у корпоративну мережу та отримують доступ до ресурсів, при цьому довго залишаючись непоміченими? Важливо захищати зовнішній периметр від загроз, але не менш важливо бути готовим оперативно реагувати на загрози і витік інформації із середини організації.

Також важливо контролювати роботу персоналу, який часто стає цим самим каналом витоку цінної інформації із структури.
Для того, щоб якісно відпрацьовувати виникаючі загрози, необхідно мати досвідчену команду з кіберзахисту.

«АМ Інтегратор» входить в ТОП 3 IT-Інтеграторів України та має 28 років досвіду у сфері безпеки.



ПРОГРАМА, ЯКА ВИЯВИТЬ БУДЬ-ЯКІ ЗАГРОЗИ ТА КОНТРОЛЮЄ МЕРЕЖУ

Основне завдання кібербезпеки – автоматичне виявлення загроз після їх проникнення всередину інфраструктури та швидке (за лічені хвилини) реагування на загрозу.

Яскравий приклад – американська **платформа кібербезпеки Fidelis Elevate**, яка нещодавно з'явилася на ринку України та встигла добре зарекомендувати себе у низці державних та приватних підприємств.

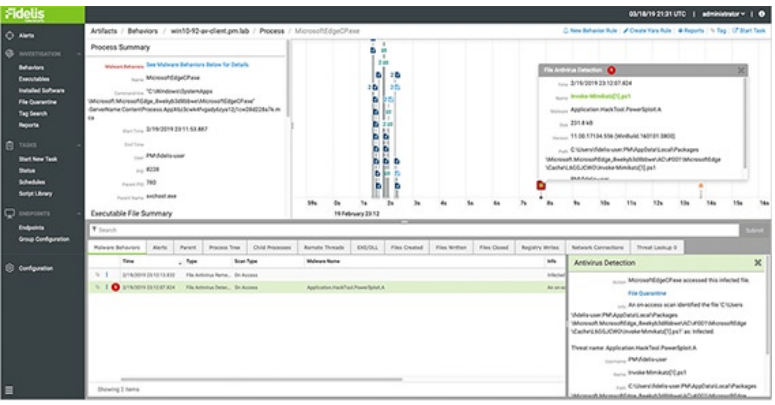
Платформа Fidelis Elevate складається з трьох основних компонентів – Network module, Endpoint Module та Deception module – які відповідно забезпечують безпеку внутрішньої мережі, безпеку кінцевих точок (серверів та робочих станцій), та пошук загроз, які не були помічені рештою існуючих засобів забезпечення безпеки у корпоративній мережі.

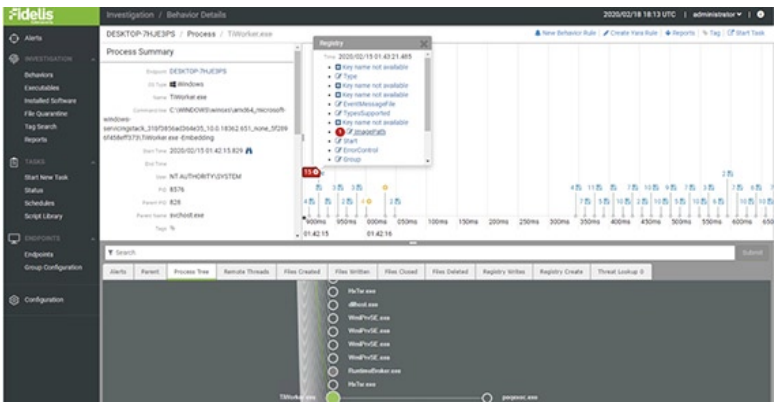
Для захисту від кіберзагроз, реагування на них та аналізу Fidelis використовується в більшості держсектору США, у структурах Google, US CERT, NATO, HP, Microsoft та багато інших.

Network module (являє собою NTA технологію – Network Traffic Analysis) здійснює аналітику мережевого трафіку та надає користувачу повний контроль за безпекою мережі будь-якої складності.

Endpoint module (EDR) – працює за принципом контролю процесів та керування ними, не навантажуючи кінцеву точку та не конфліктуючи з програмним забезпеченням.

Deception module (Post breach detection технологія) – виявлення атак та нелегітимної активності після проникнення у корпоративну мережу.





ПРОГРАМА, ЯКА ДОПОМОЖЕ КОНТРОЛЮВАТИ ПЕРСОНАЛ КОМПАНІЇ

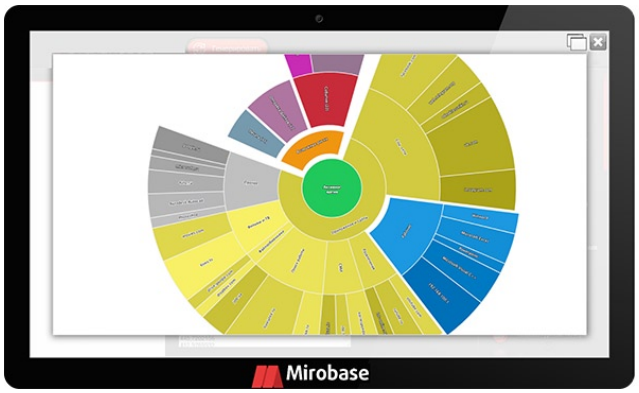
Важливо контролювати роботу персоналу. Який, до речі, нерідко неусвідомлено виносить цінну інформацію. А в умовах пандемії і віддаленої роботи, корисно розуміти ефективність роботи співробітників.

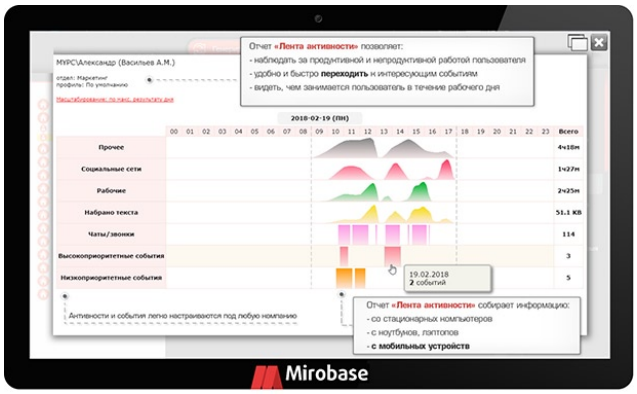
Розумна **система контролю активності в робочий час Mirobase** – це програма, яка моніторить всі дії співробітників на комп'ютері та надає керівництву та службі безпеки звіти про ефективність загрузки персоналу, загрози та витоки інформації. Це цифровий помічник, який збирає та обробляє статистику, проводить аналіз і видає готовий звіт про відхилення поведінки, гнучко настроюється під різні відділи або індивідуально під кожного співробітника, розпізнає і попереджає фішинг, виявляє інсайдера, бачить запуск небезпечного ПЗ, сигналізує про надзвичайну подію службі безпеки.

Mirobase стане у нагоді керівництву та HR-відділу для підвищення ефективності роботи організації.

Програма дозволяє моніторити внутрішні процеси та знайти, що гальмує зростання компанії. Контролює співробітників і не дає їм знижувати темпи за відсутності начальства.

Mirobase допомагає виявити ефективних співробітників, визначити реальний рівень завантаження штату, демонструє, як нові співробітники справляються з роботою, здатна передбачити, хто збирається звільнитися.





КІБЕРПОЛІГОН

Щоб співробітники були готові якісно відбити викаючі загрози, мало мати надійні і функціональні сервіси, важливі ще досвід і кваліфікація співробітників.

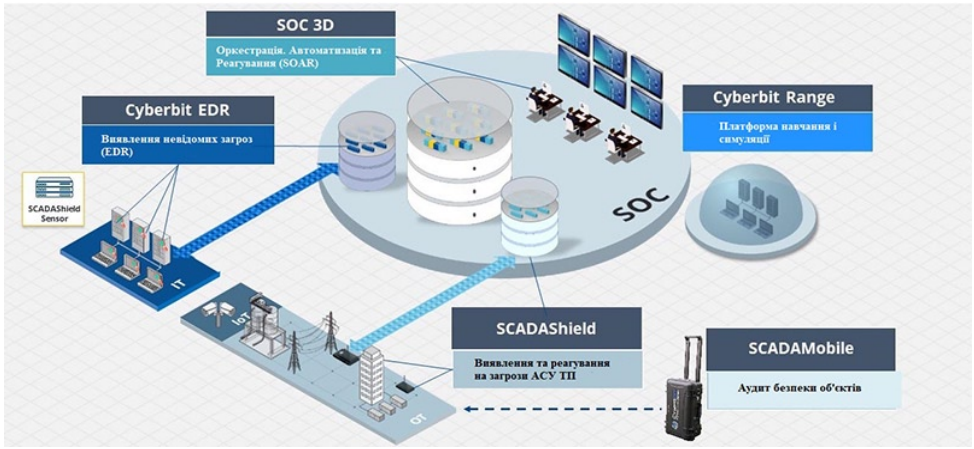
Для цього є відмінне рішення **CyberBit Range – платформа з двох навчальних класів, яка дозволяє моделювати атаки і тренувати навички персоналу в захисті від цих різноманітних атак**.

У розпорядження компанії може бути наданий кіберполігон з гіперреалістичними сценаріями навчання, моделювання мережевого трафіку і кібератак.

З ним можна згенерувати будь-які сценарії атаки з вибором інструментів із багатьма блоками.

Фактично використовується принцип, подібний до тренування пілотів винищувачів! Практикантам забезпечується реальний досвід протидії загрозам та інцидентам.

За допомогою кіберполігону можна підготувати фахівців різного рівня та навичок – від студентів до інструкторів з підтримкою як індивідуальної, так і командної підготовки. У Центрі навчання здійснюється підготовка команд реагування на інциденти інформаційної безпеки, підвищення кваліфікації, скорочення термінів сертифікації та актуалізації знань та навичок персоналу з кіберзахисту, оцінка ефективності впроваджуваних продуктів в області корпоративної інформаційної безпеки.



AM INTEGRATOR GROUP

04070, м. Київ, вул. Іллінська, 14/6
тел./факс: (044) 394-86-07, 394-86-09

AM INTEGRATOR SOFT

04070, м. Киев, вул. Братська, 6
тел./факс: (044) 394-86-08

Регіональні представництва:
Дніпро, Запоріжжя, Маріуполь, Одеса, Полтава, Харків.

Номер безкоштовної лінії технічної підтримки:
0 (800) 218-609

ОЛЕКСАНДР РАПП

системний інженер компанії
Palo Alto Networks, США

orapp@paloaltonetworks.com

PALO ALTO NETWORKS

ML-POWERED NEXT- GENERATION FIREWALL –

ПЕРШИЙ У СВІТІ МІЖМЕРЕЖЕВИЙ ЕКРАН З ЕФЕКТИВНИМИ МОДЕЛЯМИ МАШИННОГО НАВЧАННЯ ДЛЯ БЛОКУВАННЯ НЕВІДОМИХ ЗАГРОЗ

Інфраструктура підприємств постійно змінюється. При цьому, атаки постійно і автоматично поліморфуються. Нові пристрої розповсюджуються швидко і без попередження. Ваші бізнес-потреби зумовлюють швидкі зміни. Типові продукти безпеки змушують вас реагувати на ці зміни вручну, напружуючи свої ресурси та залишаючи свою організацію відкритою до нових атак.

Світ потребує нового типу міжмережевого екрану – з машинним навчанням та аналітикою в своїй основі, здатного ідентифікувати нові загрози та нові пристрої, не покладаючись тільки на сигнатури та хеш-суми. Він повинен постійно оновлювати моделі машинного навчання шляхом аналізу да-

них за допомогою необмежених хмарних обчислень. Він повинен постійно збирати телеметрію та рекомендувати політики та конфігураційні зміни для зменшення ризику та зменшення шансів на помилку.

Захистіть цифрову трансформацію своєї організації з першим у світі та єдиним у галузі, інноваційним міжмережевим екраном нового покоління, що опирається на Машинне Навчання (МН).

Використовуйте найновіші технології машинного навчання, щоб забезпечити захист вашого підприємства від невідомих шкідливих файлів на фішингових атак.

Забезпечте безсигнатурну ідентифікацію некерованих пристроїв Інтернету речей (Internet of Things, IoT).

Використовуйте телеметрію для оптимізації політик безпеки та усунення ризиків пов'язаних з неправильною конфігурацією.

Використовуйте послідовну, інтегровану і найкращу реалізацію платформи мережевої безпеки, доступної в апаратному, віртуальному, контейнерному та хмарній форм-факторах і керуйте всім цим централізовано.

ОСНОВА СТРАТЕГІЇ МЕРЕЖЕВОЇ БЕЗПЕКИ

Наші міжмережеві екрани наступного покоління перевіряють весь трафік, включаючи всі застосунки, вміст та загрози, і прив'язують цей трафік до користувача, незалежно від місцезнаходження або типу пристрою. Користувач (User), застосунки (Application) та вміст (Content) – елементи, що керують вашим бізнесом – стають невід'ємними компонентами вашої корпоративної політики безпеки. Як результат, ви можете узгодити безпеку зі своєю бізнес-політикою, а також написати правила, які легко зрозуміти та підтримувати.

ІДЕНТИФІКАЦІЯ КОРИСТУВАЧІВ

Технологія User-ID™ дозволяє нашим NGFW ідентифікувати користувачів всюди, не зважаючи на тип ОС та місцезнаходження користувача. Вона дозволяє будувати політики на основі користувачів і груп користувачів, а не IP-адрес, що дозволяє створювати бізнес орієнтовані політики.

Наприклад, ви можете дозволити тільки адміністраторам використовувати такі інструменти як SSH, Telnet, та FTP. При цьому політики слідують за користувачами, незалежно звідки вони підключається – філії чи користувацької мережі в центральному офісі.

БЕЗПЕЧНЕ ВИКОРИСТАННЯ ЗАСТОСУНКІВ

Технологія App-ID™ дозволяє нашим NGFW ідентифікувати застосунки, що є в мережі, на будь-якому порту з однаковою точністю, дозволяючи лише необхідні бізнесу застосунки та блокуючи всі інші недозволені та високоризикові застосунки відповідно до політик безпеки.

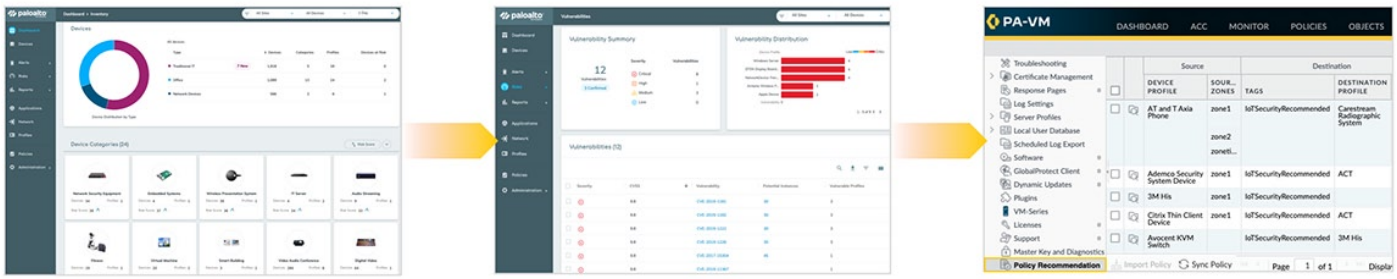
Функціонал Policy Optimizer дозволить вам швидко ідентифікувати застосунки та швидко перейти від застарілих правил (Layer-4) до правил на основі застосунків (Layer-7).

ІНСПЕКЦІЯ ШИФРОВАНОГО ТРАФІКУ

Наші політики дешифрування дозволяють інспектувати потенційно шкідливий трафік та блокувати відповідні загрози. Серед підтримуваних протоколів - TLS 1.3 та HTTPS/2.

ДЕТЕКТУВАННЯ ТА ПОПЕРЕДЖЕННЯ ПРОДВИНУТИХ ЗАГРОЗ

Кібератаки збільшилися в обсязі та вдосконалилися, використовують сучасні технології для транспортування атак або експлуатування вразливостей, обходячи пристрої та інструменти мережевої безпеки. Тож, скористайтеся передовими техноло-



Complete Visibility

Accurately identify and classify all devices with ML, including those never seen before

In-depth Risk Analysis

Quickly understand anomalies, vulnerabilities and severity to make confident decisions

Built-in Enforcement

Safely automate enforcement on your next-gen firewall with a new Device-ID policy construct

гіями на ринку і захистіть свою організацію від найдосконаліших та передових загроз.

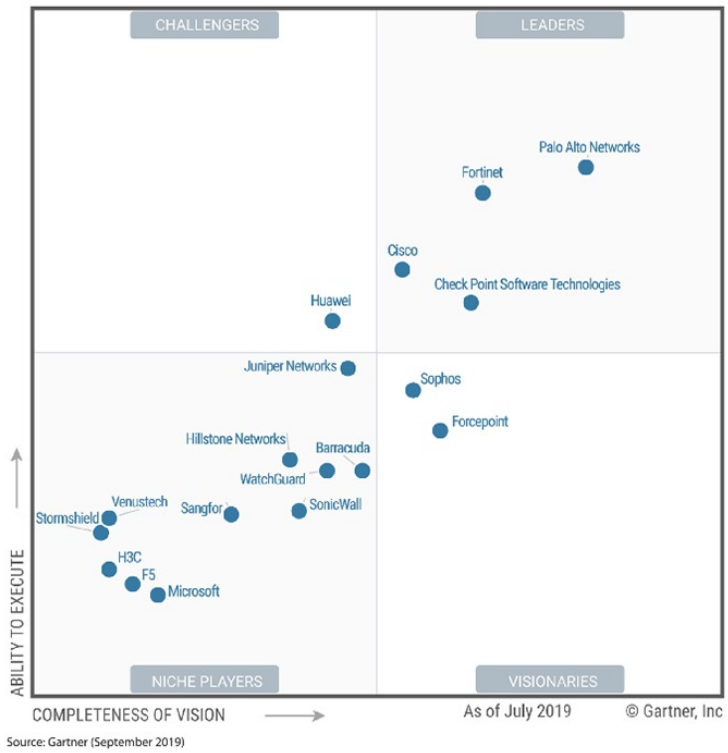
Threat Prevention – виходить за рамки типової технології системи запобігання вторгненню (IPS). Ця підписка дозволяє перевіряти весь трафік на наявність загроз – незалежно від порту, протоколу чи шифрування, і автоматично блокувати відомі вразливості, шкідливі файли, експлойти, шпигунське програмне забезпечення та трафік командних центрів управління ботами (C2).

URL Filtering – захищає організації від веб-загроз, таких як фішинг, зловмисне програмне забезпечення та командний контроль ботами (C2). Вбудоване машинне навчання миттєво визначає та запобігає появі нових та невідомих шкідливих веб-сайтів, перш ніж користувачі зможуть отримати до них доступ.

Сервіс попередження невідомих загроз WildFire® - використовує хмарні методи виявлення шкідливого програмного забезпечення та багаторазові методи аналізу для виявлення та захисту від невідомих файлових загроз. WildFire застосовує вбудовані модулі машинного навчання на міжмережевих екранах наступного покоління для виявлення, а також запобігання появі нових і невідомих файлових загроз, захищаючи користувачів, перш ніж загроза може навіть потрапити у вашу мережу.

DNS Security – застосовує прогнозну аналітику, машинне навчання та автоматизацію для блокування атак, що використовують DNS протокол. інтеграція з NGFW надає вам автоматизований захист, перешкоджає зловмисникам обходити заходи безпеки та усуває необхідність у незалежних інструментах або змінах маршрутизації DNS.

Figure 1. Magic Quadrant for Network Firewalls



Source: Gartner (September 2019)

IoT Security – є першим у галузі повноцінним рішенням безпеки IoT, що забезпечує підхід, заснований на машинному навчанні, для виявлення всіх некерованих пристроїв, виявлення поведінкових аномалій, рекомендування політики на основі ризику та автоматизації застосування без необхідності в додаткових датчиках або інфраструктурі. Ця унікальна комбінація видимості IoT та брандмауера наступного покоління дозволяє забезпечити контекстну сегментацію мережі для зменшення ризику та застосовує наші провідні підписки на безпеку, щоб захистити IoT та IT-пристрої від усіх загроз.

ЧОМУ PALO ALTO NETWORKS NEXT-GENERATION FIREWALLS?

Наші міжмережеві екрани наступного покоління, з функціоналом машинного навчання, надають вам змогу бути на крок попереду нових загроз, контролювати та захищати ваше підприємство, включаючи IoT, а також підтримувати швидкість змін та зменшення помилок за допомогою автоматичних рекомендацій щодо існуючих політик.

Понад 75 000 клієнтів у понад 150 країнах використовують нашу архітектуру, орієнтовану на попередження. Ми вісім разів поспіль були визнані лідером у Magic Quadrant® від Gartner для Enterprise Networks Firewalls і наші NGFW регулярно отримують Рекомендовану оцінку від NSS Labs – найвищий рейтинг, який пропонує NSS Labs.

Ласкаво просимо в еру інтелектуальної безпеки, захищаючи своє підприємство від завтрашніх загроз.

1-31 ЖОВТНЯ 2020

МІСЯЦЬ КІБЕРБЕЗПЕКИ В УКРАЇНІ

KYIV CHAMBER OF COMMERCE AND INDUSTRY

the CyberSecurity Review

ЖУРНАЛ КИЇВСЬКОЇ ТОРГОВО-ПРОМИСЛОВОЇ ПАЛАТИ

вул. Б. Хмельницкого, 55
Київ, 01054, Україна
тел: **+380 44 482 03 01**
факс: **+380 44 482 39 66**
info@kcci.org.ua
kiev-chamber.org.ua

ДЛЯ ТРАНСПОРТУВАННЯ ВИСОКОШВИДКІСНОГО ТРАФІКУ ПОТРІБЕН DWDM

СЕРГІЙ ЧОРНОУС

керівник департаменту
промислових рішень компанії
IT Biz Solutions

+380 **44 597 10 90**
sales@itbiz.com.ua

www.itbiz.ua

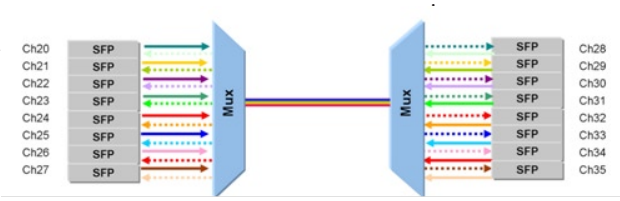
Реальність сьогодення полягає в тому, що постійно з'являються типи сервісів і нові користувальницькі додатки, які створюють дедалі більше навантаження на магістральну транспортну мережу. Це означає, що для транспортування високошвидкісного трафіку потрібні технології передачі даних, які, з одного боку, мають достатню продуктивність, з іншого – надають оператору можливість масштабування мережі без зміни інфраструктури. Цим вимогам задовольняє технологія спектрального мультиплексування (WDM – Wavelength Division Multiplexing), яка досить давно є основною технологією побудови магістральних волоконно-оптичних мереж зв'язку.

WDM – це технологія фізичного рівня, яка дозволяє передавати одночасно кілька інформаційних каналів по одному оптичному волокну. Для цього використовуються різні довжини світлових хвиль. Канали можуть додаватися поступово і мати різну швидкість і формати передачі, що дає можливість користувачам нарощувати ємність мережі і розвивати різні типи сервісів на існуючій мережі без прокладки додаткових оптичних волокон.

Перші WDM-системи були двоканальними з передачею на довжинах хвиль 1310/1550 нм та 1270/1330 нм. Трохи пізніше з'явилися багатоканальні рішення: CWDM (Coarse Wavelength Division Multiplexing – грубе спектральний ущільнення) та DWDM (Dense Wavelength Division Multiplexing – щільне спектральний ущільнення), де назви говорять про щільності розташування інформаційних каналів в оптичному діапазоні.

Саме CWDM та DWDM-системи дозволили більш раціонально використовувати існуючу кабельну інфраструктуру.

DWDM – це технологія щільного спектрального мультиплексування. Оптичні канали розташовуються в діапазоні від 1530 до 1565 нм з кроком 0,4 нм (50 ГГц) або 0,8 нм (100 ГГц). Використання великого числа несучих з мінімальним кроком між



Мал. 1

Технологія передачі DWDM створює основу для організації гнучких високошвидкісних інтелектуальних мереж, забезпечуючи прозору передачу постійно зростаючого трафіку, в тому числі чутливого до затримок. Технологія підтримує швидкості від 150 Мбіт/с до 400 Гбіт/с на одну довжину хвилі. На тепер в компанії **DWDM.me** в активній розробці знаходяться 400-гігабітні рішення.

Переваги DWDM при використанні в державних структурах:

- **Висока пропускна здатність**
- **Можливість значного розширення ємності та масштабування мережі**
- **Передача трафіку широкого спектру рішень**
- **Поєднана гнучкість управління потоків в основних магістралях**
- **Надійність та відмовостійкість**
- **Можливість передачі великих обсягів даних на дальні відстані.**

Обладнання DWDM.me – це повноцінна система, яка дозволяє побудувати DWDM-мережу. Модельний ряд обладнання DWDM.me складається з кількох моделей.

Основою системи **DWDM.me** є шасі (розміром 1, 2 та 5U), яке дозволяє встановити окремі модулі, що виконують певні функції. Одними з таких модулів є плати транспондерів – 200G OTN Muxponder. Для максимальної безпеки і збереження переданих даних система побудована з використанням ідеології «гарячої» заміни модулів. Слід зазначити – система **DWDM.me** дозволяє здійснювати централізоване управління, що значно спрощує налаштування та контроль за роботою обладнання.

Оптична транспортна система 1U *(мал.2)*
Ця платформа DWDM в основному використовується в мережі доступу.

Мал.2

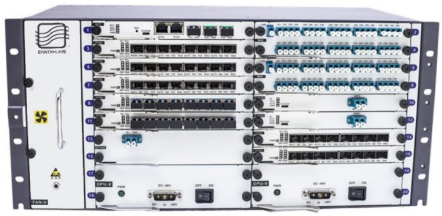
Живлення: AC: 90 ~ 260 В або DC: -36 ~ -72 В (підтримка 1 + 1 резервного джерела живлення).

Оптична транспортна система 2U *(мал. 3)*

Мал.3

Найчастіше використовується для організації магістральних DWDM-мереж.
Живлення: AC: 90 ~ 260 В або DC: -36 ~ -72 В (підтримка 1 + 1 резервного джерела живлення).

Оптична транспортна система 5U *(мал.4)*



Мал.4

Використовується для організації магістральних DWDM-мереж.
Живлення: AC: 90 ~ 260 В або DC: -36 ~ -72 В (підтримка 1 + 1 резервного джерела живлення).

Сервісна карта Muxponder 200G (***мал.5***), виробництва **DWDM.me,** підтримує мультиплексування/демультиплексування електричного сигналу 2x100G (2 модулі форм-фактору QSFP28) в оптичний DWDM-сигнал 200G зі стандартною довжиною хвилі.

Мал.5

Компанія «Айті Бізнес Солюшн» (IT Biz) має великий досвід в побудові DWDM-мереж, поставках активного та пасивного DWDM-обладнання для наших замовників. Серед реалізованих проєктів:

- побудова DWDM-магістралі Київ – Харків зі швидкістю 200 ГБіт/с для одного з провідних українських інтернет провайдерів на обладнанні **DWDM.me**
- модернізація DWDM-мережі (з'єднання студій та офісів) однієї з найбільших медіа-груп України
- поставки DWDM-обладнання багатьом українським провайдерам та операторам
- консультативні послуги з розбудови та модернізації DWDM-мереж в корпоративному сегменті.

За додатковою інформацією по обладнанню **DWDM.me** просимо звертатись в компанію **«Айті Бізнес Солюшн» (IT Biz).**

ЩО ДАСТЬ ПОСЛУГА VIRTUAL SECURITY TEAM ДЛЯ ВАШОЇ КОМПАНІЇ?

ВІТАЛІЙ ЯКУШЕВ

операційний директор компанії
10Guards

+380 **44 39 39 000**
+380 **67 556 97 95**
vy@10guards.com

Кіберзагрози – головний біль для діджиталізованих бізнесів, незалежно від сфери їх діяльності. З кожним роком компанії перебувають у постійному пошуку відповідних рішень для підвищення рівня своєї кібербезпеки. Питання ускладняється тим, що забезпечити належний рівень захисту інформації та активів повною мірою не можна, покладаючись лише на технологічні рішення. Необхідно постійно підтримувати кваліфікацію співробітників, які координують питання із забезпечення кібербезпеки в компанії, що є не таким простим завданням, як здається на перший погляд. До того ж, на ринку відчувається нестача кваліфікованих кадрів, відсутня спеціалізація у галузі кібербезпеки. Галузь розвивається динамічно й персоналу, навіть молодим спеціалістам, необхідно опановувати великі обсяги нових знань.

Щоб йти у ногу із трендами, компанії намагаються взяти у штат керівника з кібербезпеки **(Chief Information Security Officer, CISO)**. Але дуже часто така вакансія набуває значення «Універсальний

спеціаліст у сфері безпеки», а опис обов'язків однієї людини включає практично весь можливий спектр задач і робіт:

- створення та управління стратегією кібербезпеки
- планування та створення програми кібербезпеки
- управління ризиками кібербезпеки
- моніторинг відповідності законодавчим нормам
- розробка документації
- підвищення обізнаності співробітників в сфері інформаційної безпеки
- управлення інцидентами безпеки та підготовка по реагуванню на них
- моніторинг безпеки та активів, фізичної й мережевої безпеки
- контроль і супроводження впровадження програмних та апаратних засобів кібербезпеки, тощо

Щоб відповідати таким вимогам, людині потрібні навички не тільки досвідченого керівника і знання специфіки конкретної індустрії, але й досвід написання документації та глибокі технічні знання у сфері створення і супроводження комплексної системи управління кібербезпекою. Звісно, таких спеціалістів вкрай мало і оплата їх праці дуже висока. Саме тому, для малого та середнього бізнесу залучення кваліфікованого CISO в штат може бути просто неможливим або нерентабельним. Однак, навіть якщо компанія має таку можливість, такого спеціаліста важко знайти, не дивлячись на запропоновані умови праці.

Необхідно також взяти до уваги, що у наші дні через пандемію COVID-19 різні уряди і регулюючі органи зобов'язують як державні, так і приватні організації переводити діяльність у формат віддаленої роботи та дотримуватись соціальної дистанції.

Вищеперераховані фактори посприяли тому, що послуга **CISO as a Service (CISOaaS)**, або **аутсорсинг послуг інформаційної безпеки**, набуває популярності.

Замовляючи таку послуги, компанія залучає «віртуального» CISO, що вирішує наступні проблеми реального CISO:

- **вузький профіль:** компанія отримує команду експертів із досвідом в багатьох сферах та на різних позиціях (від менеджменту до технічного спеціаліста)
- **навантаження:** всі задачі рівномірно розподіляються між членами кваліфікованої команди, а не доручені одній людині
- **відсутність на робочому місці:** забезпечення безперервності бізнес-процесів (штатний CISO з будь-яких причин (лікарняний, від-

пустка) може бути недоступним для вирішення питань)
- **витрати на персонал:** в залежності від специфіки бізнесу, CISOaaS часто коштує до 75% дешевше, ніж штатні співробітники
- **необхідність замовлення додаткових зовнішніх послуг:** стають доступними компетенції (кваліфікації) для реалізації усіх задач та процесів (наприклад, періодичні тести на проникнення).

А завдяки сьогоднішнім можливостям віддаленої роботи CISOaaS не відрізняється від діяльності «локального» CISO, за винятком фізичної відсутності в офісі.

Аутсорсинг послуг інформаційної безпеки може стосуватись не лише позиції CISO, а й команди з кібербезпеки в цілому. Тепер, замість пошуку співробітників до власного відділу кібербезпеки, можна скористуватися пропозицією «віртуальна команда кібербезпеки» **– Virtual Cybersecurity Team**.

Безпека як послуга – новий, але популярний підхід, що має попит в багатьох сферах: банківська справа, фінансові послуги і страхування (BFSI); урядові організації та оборонні підприємства; роздрібна торгівля; охорона здоров'я; IT та телеком; енергетика та комунальні послуги; виробництво тощо. Експерти «віртуальної команди» виконують наступні задачі:
- моніторинг стану кібербезпеки;
- підтримка процесів захисту даних, реагування на певні інциденти, управління загрозами та вразливостями;
- управління IT активами;
- забезпечення відповідності законодавчим нормам та міжнародним стандартам безпеки (compliance);
- побудова і впровадження процесів управління кіберризиками;
- управління внутрішніми контролями інформаційної безпеки;
- підтримка в створенні і оновленні документації в сфері кібербезпеки.

Virtual security team має значні переваги над штатною командою, адже допомагає позбутися: труднощів у пошуку кадрів, витрат на заробітну платню, підвищення кваліфікації та на час «простою» команди.

Таким чином, якщо компанія вирішує скористатися послугами віртуальних CISO або команди з кібербезпеки, вона отримує сертифікованих спеціалістів, які виконують усю необхідну роботу в сфері інформаційної безпеки, а сплачує тільки за реальні трудовитрати. Це дозволяє компанії:

1. **Отримати необхідну експертизу** у всіх областях, не наймаючи великий штат вузькопрофільних співробітників.

2. **Радикально знизити витрати.** Компанія сплачує лише за те, що їй необхідно, неважливо, пораду спеціаліста по підвищенню обізнаності персоналу або проведення технічної оцінки захищеності.

3. **Знизити бізнес-ризики.** Прийом на роботу ключового співробітника – важливе рішення та серйозна інвестиція. Помилка може вартувати компанії багатократної зарплати CISO. При правильному виборі постачальника послуг «віртуального» CISO чи команди, ризик невеликий, так як можна вибрати оптимальний рівень обслуговування з пропонованих та розірвати відношення у будь-який момент, якщо це необхідно.

10 GUARDS

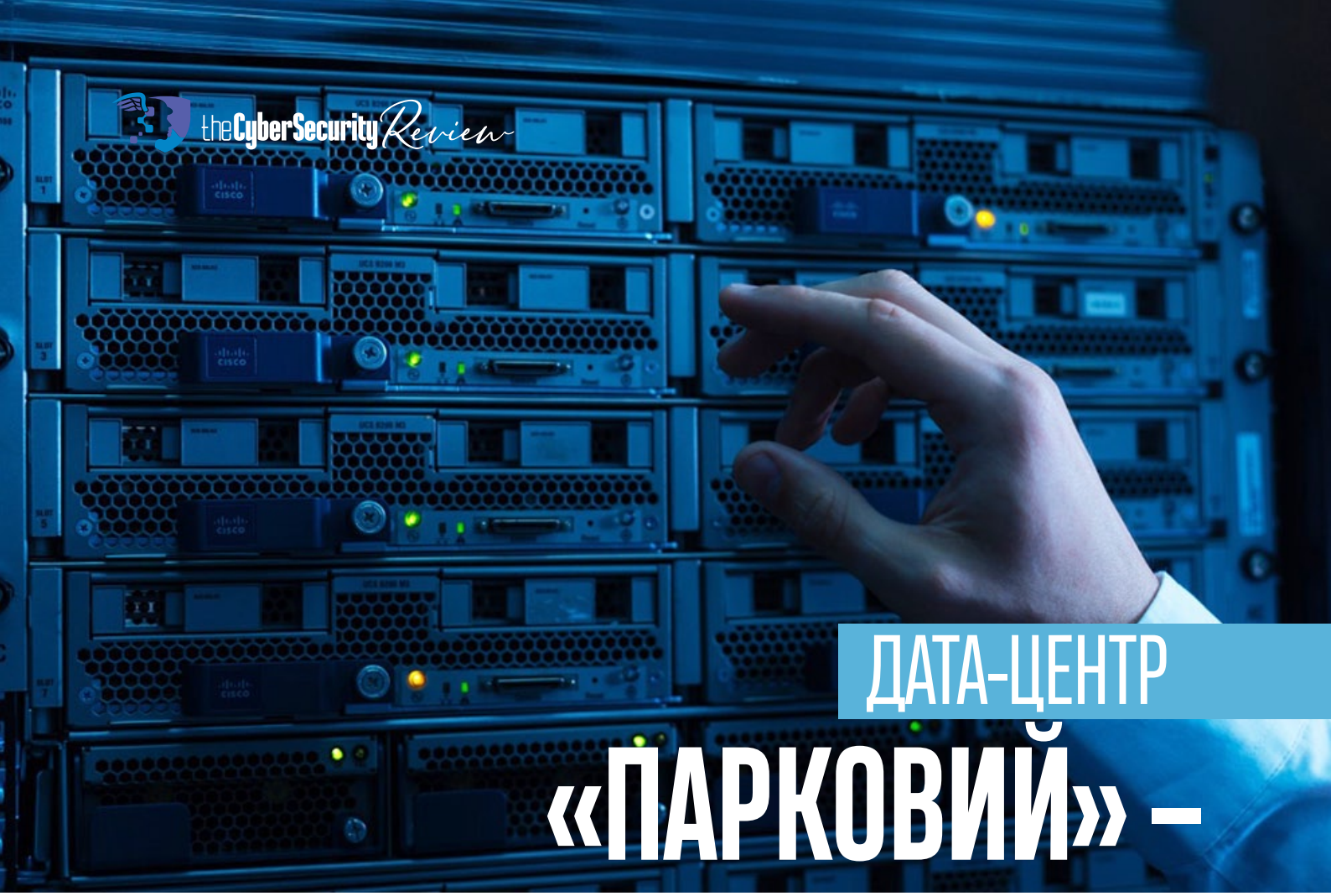
КОНСАЛТИНГОВА КОМПАНІЯ З КІБЕРБЕЗПЕКИ

ТОВ ТЕНГАРДЗ УКРАЇНА

Круглоуніверситетська, 3-5,
Київ, Україна

besecure@10guards.com

+38 044 3939 000



ДАТА-ЦЕНТР «ПАРКОВИЙ» – НАДІЙНІСТЬ ПОНАД УСЕ

Цей рік ще раз довів, що для виживання бізнесу необхідно бути діджиталізованним і автономним. При цьому все, що пов'язано з онлайн, вимагає підвищеної безпеки і контролю, адже елементарний збій у роботі обладнання може призвести до колосальних фінансових та репутаційних втрат. Самостійна підтримка продуктивності та надійності функціонування IT-інфраструктури вимагає великих капітальних вкладень, не кажучи вже про людські ресурси. Тому все більше компаній довіряють зберігання обладнання і даних професійним дата-центрам.

Одним з найбільш важливих критеріїв, на який звертають увагу при виборі технологічного партнеру є відповідність дата-центра певному рівню TIER.

Д О В І Д К А

У світовому співтоваристві найавторитетнішою організацією, яка оцінює показники ефективності роботи дата-центрів відповідно до глобальної класифікації **TIER** визнана **Uptime Institute**.

Кожен рівень **TIER** класифікує ЦОДи з точки зору їх продуктивності та безвідмовності роботи.

Оптимальним і достатнім рівнем, який гарантує надійність комерційного дата-центру є рівень TIER III. Він означає, що клієнтське обладнання буде працювати постійно (відмовостійкість 99,982%), незалежно від зовнішніх або внутрішніх обставин.

На прикладі єдиного дата-центру України, який отримав сертифікат Uptime Institute стандарту TIER III – «Парковий» – розповідаємо завдяки яким характеристикам досягається високий рівень надійності.

ДЖЕРЕЛО ЖИВЛЕННЯ

Єдиним по-справжньому надійним джерелом живлення для дата-центру є дизель-генераторна установка, яка автоматично приймає на себе все навантаження без обмеження часу роботи.

У дата-центрі «Парковий» побудовано окреме приміщення з чотирма дизель-генераторами FG Wilson P1700. Резерв палива складає 40 т. в підземних танках і по 1000 літрів підігрітого палива в кожній дизель генераторній машині, що гарантує тривалу безперервну роботу всієї системи.

РЕЗЕРВНЕ ОБЛАДНАННЯ

Безперебійне функціонування системи можливо лише при наявності резервного обладнання, яке автоматично розподіляє навантаження в разі відключення одного з компонентів інфраструктури.

«Парковий» працює за формулою «N + 1», тобто для кожного елемента інженерної системи є дублюючий елемент в паралельній роботі. Як тільки один з критичних компонентів вийде з ладу – його замінить дублюючий, який запобіжить зупинці функціонування ЦОД.

ОХОЛОДЖЕННЯ

Завдання системи охолодження і вентиляції підтримувати оптимальну температуру і вологість у приміщенні для ефективної і безпечної роботи обладнання.

Зовнішній контур охолодження представлений шістьма чиллерами APC Uniflair BREF 2802A. Холодильні машини працюють за двоконтурною схемою і оснащені функцією фрікулінга, що в умовах Києва дозволяє використовувати для охолодження зовнішнє повітря в холодну пору року. Це гарантує високі показники енергоефективності для всього ЦОД.

ПОЖЕЖНА БЕЗПЕКА

Система автоматичного пожежогасіння, яка зможе або запобігти виникненню спалаху, або ліквідувати пожежу, що виникла.

У кожному машинному залі дата центру встановлені автономні системи пожежогасіння. Спеціальні вогнетривкі конструкції гарантують, що клієнтські системи не постраждають від високої температури. У газовій системі пожежогасіння використовується інноваційний газ Novec 1230, який ліквідує займання в лічені секунди, при цьому є абсолютно безпечним для обладнання, електроніки і людини. Контроль за системою ведеться цілодобово.

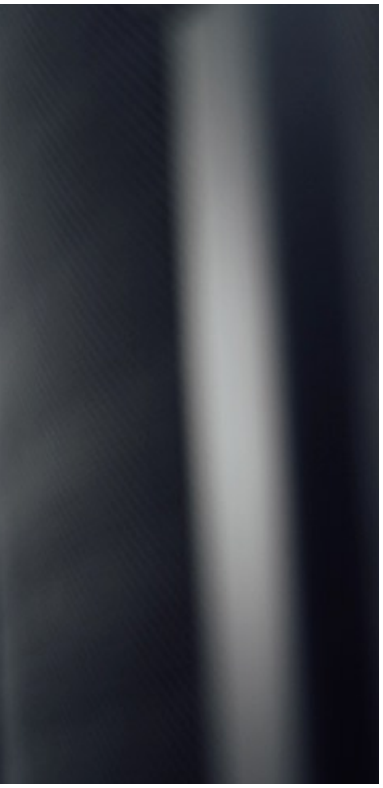
БЕЗПЕКА

Надійний центр обробки даних має кілька рівнів забезпечення безпеки IT-інфраструктури та даних.

Фізична безпека та контроль доступу забезпечується за допомогою цілого ряду взаємопов'язаних систем, в число яких входять: датчики руху, магнітні замки (відкриваються смарт-картами), броньовані двері, сигналізація. На об'єкті діє суворий пропускний режим, шлюзова система доступу, фізична охорона території і центральний пульт безпеки.

Також на об'єкті розгорнута потужна система відеоспостереження на базі IP-відеокамер Cisco з вбудованими функціями відеоаналітики. Це дозволяє контролювати всі дії, які відбуваються в ЦОД.


фото: http://transexpo.ua/

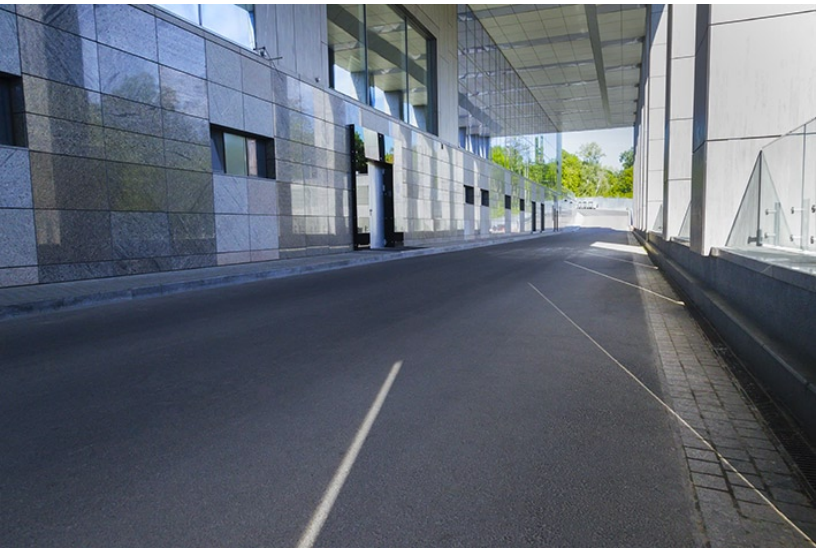


ГЕОГРАФІЧНЕ ПОЛОЖЕННЯ

Фізичне розташування визначає наскільки дата-центр захищений від зовнішніх загроз і незалежний від сторонніх організацій.

«Парковий» розміщується у власному приміщенні в центрі Києва, в його радіусі немає житлових будинків або промислової інфраструктури. Приміщення автономно, на його збереження і безпеку не впливають зовнішні чинники, а центральне розташування забезпечує зручну транспортну логістику.

«Парковий» – це один з найбільших центрів обробки даних в Україні, який розміщується в центрі столиці.



ЦОД входить до числа найкращих експертів у сфері безпеки інформаційних ресурсів України, що підтверджено міжнародним сертифікатом ISO / IEC27001 та атестатом відповідності системам технічного захисту інформації ДСС331.

Нещодавно «Парковий» в черговий раз підтвердив високий ступінь надійності, ставши технологічним партнером Національного центру кібербезпеки України.

У дата-центрі розташовані 17 машинних залів, які захищені відповідно до стандарту TIER III. 13 з них забезпечують найвищий рівень безпеки та конфіденційності, так звані, екрановані зали. Вони особливо актуальні для фінансових і державних установ.

«ПАРКОВИЙ» ПРОПОНУЄ 2 ВИДИ СПІВПРАЦІ:

1. Розміщення серверного обладнання в машинних залах – colocation. Клієнт отримує надійне сховище, цілодобову підтримку фахівців, швидкість і продуктивність.
2. Використання хмарних послуг. Сучасна платформа дозволяє гнучко адаптувати рішення під завдання клієнта. IT-фахівці організують міграцію, розгортання, адміністрування.

КІБЕРБЕЗПЕКА – ЦЕ НЕ ПРОСТО СЛОВА

ОЛЕГ ГАЙДУК

перший заступник голови
ГС КіберКовчег

керівник компанії
Трайбекс
(оператор української захищеної операційної системи Січ)

https://cyberark.org.ua
https://traybex.com
https://sich.help
https://oleg.carrd.co

Сучасний світ все більше інтегрується із віртуальним і цьому є декілька по-справжньому серйозних причин. Перше – це глобальні перетворення економіки провідних країн, які призвели до появи Інформаційного Суспільства та Економіки 4.0. Друге – розвиток технологій, що все ширше відкриває двері у віртуальність. І останнє – світова пандемія вірусу, яка карантинами розділила людей і країни, спонукаючи до віддаленої роботи, спілкування за допомогою віртуальних площадок та месенджерів, переміщуючи всю можливу ділову активність до віртуального світу.

Як медаль, яка має дві сторони, разом із позитивним розвитком інформаційних технологій, бурхливо розвивається їхній темний бік. Сьогодні він являє собою весь спектр криміналу – від дрібного шахрайства до крадіжок величезних сум та впливу на вибори. Приголомшлива особливість його у тому, що люди до останнього не розуміють, що саме відбувається і як цьому завадити. Брутальна аналогія – сліпий безхатько, сидячий на перехресті вулиць великого міста просто не бачить, як кривдник краде гроші з його кашкета, що лежить поруч на землі. Часто ми так само не в змозі відчути, як з нашої картки або віртуального гаманця зникають гроші. І злодій у цьому випадку може бути поруч – в сусідньому будинку, а може бути і на іншому боці землі. Як побачити небезпеку, завадити крадіжкам, позбутися відчуття безпорадності?

На відміну від фізичної сліпоти, у віртуальному світі можна навчитися бачити і не дати себе ошукати. Щодня з'являються тисячі нових засобів, налаштованих проти кримінального світу – розробники і власники програмного забезпечення намагаються швидко реагувати на виклики в цій гонці озброєнь. Оновлення безпеки, усунення помилок у коді, ліквідація вразливостей – ось чому є сенс особисто для себе налаштувати смартфон та комп'ютер на автоматичні якнайшвидші оновлення операційних систем, додатків і програм. Так, інколи оновлення змушують поморочитися,- адже витрачається час, треба згадати і ввести паролі, поновити звичні налаштування, але це точно краще, ніж пустити до себе шахрая.

Відомий вислів **«Щоби спіймати злодія, треба мислити як злодій»** працює і тут. У звичайному світі перед тим, як піти на злочин, професійні крадії намагаються вивчити жертву. Коли їм відомо, що саме можна вкрасти, особливості поведінки, час виходу і повернення, чи є сигналізація і яка саме, які встановлені замки, хто і коли лишається вдома і т. д. і т. п., вони намагаються здійснити злочин. Так само і кіберзлочинці вивчають вас та ваш бізнес з віртуального боку. Але на додачу до звичайного, у віртуальному світі ласими об'єктами крадіжок стають логіни і паролі до аккаунтів, приватні фото, контакти, транзакції, номери рахунків, бази клієнтів тощо. Часто можна почути: **«Мені не важлива приватність, я не роблю нічого протизаконного»**. Нажаль, ці люди не усвідомлюють, що саме через порушення приватності здійснюється основна маса віртуальних злочинів.

Сучасні оператори пропонують вам додати другий крок до вашої ідентифікації. На цьому другому етапі проводиться подвійна перевірка того, чи це справді ви ввійшли в систему. Це може бути смарт-картка, сканер відбитків пальців на смартфоні, кардрідер або, як у більшості випадків, смс, повідомлення в месенджері або телефонний дзвінок. Вмикайте двох факторну автентифікацію всюди, де це можливо.

Чим далі, тим більше сучасні кіберзагрози приймають різну форму і надсилаються різними способами. Однак електронна пошта все ще є одним із улюблених засобів кіберзлочинців. Приватне та ділове спілкування по електронній пошті виглядає особистим, але це не так: кожен може надіслати вам електронний лист – і ви маєте бути до цього готові. Атаки електронною поштою зазвичай намагаються змусити вас зробити щось, чого не слід робити. Наприклад, пропонується натиснути на посилання, відкрити документ або переказати гроші. І у них є щось спільне: вони просять вас негайно зреагувати. Щоб ви не стали занадто багато думати, це завжди терміново.
Зловмисники хочуть, щоб ви відвідали підроблений веб-сайт, де будуть викрадені ваші дані для входу, або відкрили чи завантажили вкладений файл – тоді комп'ютер буде заражено шкідливим програмним забезпеченням.
Типові методи такої маніпуляції: заманлива пропозиція; загроза; або лист від контакту, який здається надійним.
Якщо таке сталося і ви відкрили лист або завантажили файл, не треба панікувати. Видаліть файл і лист, запустіть антивірус, змініть паролі і зверніться до свого відділу IT та кібербезпеки.

Витоки даних з великих інтернет-компаній лишають мільйони імен користувачів та паролів в руках кіберзлочинців. Тому важливо, щоб ви використовували інший пароль для кожного облікового запису. «Qwerty», «123456» або «password» є одними з найбільш часто використовуваних паролів. Це особливо полегшує роботу хакерів, оскільки за допомогою автоматичних програм вони можуть перевірити тисячі записів зі словників у зв'язку з комбінацією чисел за секунди. Отже, прості паролі - одна з найбільших прогалин безпеки в мережі після витоку даних. Поєднання надійних і різних паролів для різних аккаунтів, разом із двох факторною автентифікацію становить просту, але дуже важливу ланку кібербезпеки кожного.

Фахівці з кібербезпеки **громадської спілки Кібер-Ковчег** складають команду досвідчених професіоналів і на практиці переймаються питаннями кібербезпеки, інтеграцією і адаптацією відповідного програмного забезпечення в Україні.
Крім цього, ними була розроблена і розповсюджується українська **захищена операційна система «Січ»**, яка дозволяє своїм користувачам надійно позбутися багатьох загроз та кіберризиків.

На фото зліва направо:
Роман ШИРШОВ, Денис ШВЕЦЬ, Еллі ЄЛІЗАР'ЄВА, Олена СУНІЧУК, Дмитро ВОЙТИШИН, Олександр ЛОГВИНЕНКО

МІЖНАРОДНИЙ УНІВЕРСИТЕТ КІБЕРБЕЗПЕКИ: ВІДПОВІДІ НА ВИКЛИКИ

МИКОЛА ХУДИНЦЕВ

член ГО
«Міжнародний університет кібербезпеки»

icu-ng.org
info@icu-ng.org
mykola.khudyntsev@icu-ng.org

На початку 2019 року невелика група однодумців вирішила створити нову громадську організацію з претензійною назвою «Міжнародний університет кібербезпеки» (МУК). Усі вони на той час встигли попрацювати в IT та кібербезпеці, у державному секторі і в приватних компаніях. Хтось з них мав досвід наукової роботи та викладання у вишах, хтось служив у міліції або працював у Держспецзв'язку. Головний сенс створення полягав у власному досвіді та переконанні: кібербезпека – така сфера, де треба постійно рухатися, випробовувати або навіть створювати нові інструменти, спілкуватися з однодумцями і опонентами та головне – працювати по 20 годин на добу.

Але був й інший досвід і розуміння: у державному органі або установі дуже велика кількість умовностей і обмежень, які заважають досягти результат з оптимальною швидкістю та виваженістю; комерційна компанія має заробляти гроші, а не утримувати волонтерів; нові форми потрібні, але за умов, коли або держава, або бізнес підтримуватиме ці нові форми фінансово.

Який вихід? Очевидний! Неприбуткова організація – об'єктивно єдина прозора можливість цивілізованого уникнення корупції у взаємовідносинах між державним чиновником і бізнесменом. Як це зробити? За рахунок прозорості процесів та критичної важливості та необхідності співпрацювати. Корупція – це не гроші, корупція – це нелегітимна, непрозора, незаслужена винагорода. Отже винагороду треба унормувати, заслужити та оподаткувати.

Засновник ГО «Міжнародний університет кібербезпеки» **Роман Боярчук** (праворуч) та генеральний директор **Євген Владіміров**

Чи потрібна організація взаємодії між державою та бізнесом в сфері кібербезпеки? Очевидно, що так. Більш того, взаємодіяти потрібно як-то кажуть і пересічним громадянам, і інститутам громадянського суспільства. Тобто усім. Тому що безпека (йдеться про «кібер», або взагалі про безпеку) з процесу перетворюється на стан, коли усі учасники цього процесу спільно працюють для досягнення стану. Якщо хтось або відверто «сачкує», або «робить вигляд» (неважливо, це держава, комерсант або людина), загальна безпека, безпека для усіх і для кожного – недосяжна мета.

Чому громадська організація?

Формат громадської неприбуткової організації потрібен саме для результативного уникнення звинувачень у корупції в адресу державного службовця. Інакше – тільки замовлення товару чи послуги, тільки за гроші, з дотримання бюджетної дисципліни, на відкритому тендері. Зрозуміло, що конфлікт інтересів може виникати де завгодно, але для такого формату подолати його простіше і зручніше.

Що відрізняє від інших?

За останні роки громадських організацій, благодійний фондів, спілок та асоціацій в Україні створили можливо більше, ніж у решті світу.
Навіщо була створена ще одна? По-перше, до організації увійшли відразу три колишніх керівника державних структур, які не просто не пасли задніх у питаннях кібербезпеки (до речі – це екс-керівники Державного центру кіберзахисту та Галузевого центру цифровізації та кібербезпеки Мінінфраструктури, один з яких до того ж заслу-

Під час проведення «круглого столу» з міжвідомчою робочою групою з кібербезпеки критичної інфраструктури енергетичного сектору України (м.Одеса, вересень 2020):
Євген Владіміров (генеральний директор ГО «Міжнародний університет кібербезпеки»), **Вікторія Гнатовська** (голова робочої групи, в.о. генерального директора Директорату формування енерго- та ресурсоефективної політики Міністерства енергетики України), **Валерій Кулик-Куличенко** (заступник голови робочої групи, начальник Управління цифрової політики та безпеки Міністерства енергетики України)

жив на Державну премію в галузі науки і техніки саме за цим профілем).

По-друге, засновники та члени організації накопили унікальний досвід і простої участі, і безпосереднього керівництва у десятках проєктах з кіберзахисту і кібербезпеки аж до національного рівня. При чому з повним «зануренням» і в нормативні, і в організаційні, і в технічні, і навіть (і нажаль) у політичні супутні процеси.

По-третє, і, мабуть, це найважливіше – наша країна, наша держава, наше суспільство, наші люди потребують цих спільних зусиль – бо сфера кібербезпеки дуже складна, багатофакторна, динамічна і має не просто велике, а визначальне значення для гідного та комфортного життя у цифровому, інформаційному, небезпечному XXI столітті.

Що вдалося зробити?

Міжнародний університет кібербезпеки за минулі півтора роки пройшов шлях становлення. Його партнерами (з якими укладені і підписані меморандуми про співробітництво та взаємодію і, що важливіше, триває конкретна робота) стали Державна служба спеціального зв'язку та захисту інформації, Служба безпеки, Міністерство внутрішніх справ, Міністерство енергетики, Державна фіскальна служба, Державне агентство «Укркосмос». Представники організації прийняли участь у підготовці низки нормативних документів – від відомчих та галузевих концепцій розвитку у сферах IT та кібербезпеки до проєкту Закону про критичну інфраструктура та її захист.

Організували декілька конференцій та круглих столів, з них останній – разом з Міністерством енергетики України, у якому прийняли участь більше півсотні ключових державних експертів країни у сфері кібербезпеки.

Взяли участь (але поки не перемогли) у проєктах Агентства з міжнародного розвитку USAID та Національного фонду досліджень. Створили науково-навчальний центр та наукову експертну раду, які мають запрацювати разом з іншими небайдужими до проблем безпеки у кіберпросторі однодумцями. Долучились до участі у Місяці кібербезпеки, організованому Торгово-промисловою палатою України разом з основними суб'єктами забезпечення кібербезпеки країни.

Які плани?

Не збавляти темпу. Продовжувати усі розпочаті напрями роботи. Додати до них щонайменше три великих ініціативних проєкта: подання внесків у глобальні індекси кібербезпеки та мережевої спроможності, розробка методики та впровадження оригінального індексу стану кібербезпеки для національних суб'єктів, організація процесу практичного страхування від ризиків у кіберпросторі в Україні. Сподіваємося на продовження розмови.

Під час проведення «круглого столу» з міжвідомчою робочою групою з кібербезпеки критичної інфраструктури енергетичного сектору України (м.Одеса, вересень 2020)

Розвиток людського потенціалу у безпечному кіберпросторі

СПРИЯННЯ ФОРМУВАННЮ
ТА РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ
У СФЕРІ **КІБЕРБЕЗПЕКИ**

СПРИЯННЯ ПІДВИЩЕННЮ РІВНЯ ОБІЗНАНОСТІ,
ЕФЕКТИВНІЙ ВЗАЄМОДІЇ ТА КООРДИНАЦІЇ
У СФЕРІ **КІБЕРБЕЗПЕКИ**

ОРГАНІЗАЦІЯ НАУКОВО-ДОСЛІДНИЦЬКОЇ РОБОТИ
У СФЕРІ **КІБЕРБЕЗПЕКИ**

МІЖНАРОДНИЙ УНІВЕРСИТЕТ КІБЕРБЕЗПЕКИ

INTERNATIONAL CYBERSECURITY UNIVERSITY

Телефон: **+38 067 657 00 11** E-mail: **info@icu-ng.org**

Директор Київської МАН **Ірина Поліщук** та **Вікторія Клименко**, випускниця Київської МАН, переможниця всеукраїнських конкурсів науково-технічної творчості молоді, студентка 3-го курсу Київського університету ім. Бориса Гринченка

ІРИНА ПОЛІЩУК

директор

Київської Малої академії наук

+38 **044 451 73 75**

man-kiev@ukr.net
https://kman.org.ua/ua/

НАШІ ДІТИ. МАЙБУТНІЙ ФОРПОСТ КІБЕРЗАХИСТУ

Наші діти вже у 3-4-річному віці «юзають» планшети, смартфони, знаходять у мережі інтернет «свої» мультики та ігри. Тож молодшає вік користувачів, а разом з тим, зростає рівень потенційних загроз та нашої вразливості щодо доступності приватної інформації

Єдиним дієвим механізмом запобігання кіберзагроз є формування окремою культури кібербезпеки. Ми маємо змалку вчити наших дітей азам безпеки щодо використання паролів, налаштування телефонів та комп`ютерів, застосування

Учні Київської малої академії наук

запобіжних заходів під час користування домашнім інтернетом чи вільним WI-FI. Це не менш важливо, ніж навчити дитину переходити дорогу на зелений сигнал світлофору. І це вже завдання освітянської сфери – надати дитині максимальний обсяг знань та можливості для набуття необхідних компетенцій.

Кібербезпека – достатньо новий напрямок в IT. Але ця спеціальність у вишах стає все більш популярною. Київська МАН завжди залишає на хвилі сучасних трендів, адже справжня наука завжди на передовій у вирішенні глобальних проблем.

Кілька років тому ми відкрили нове наукове відділення – відділення «Безпеки та оборони», в якому одне з провідних місць належить секції кібербезпеки. На цей навчальний рік у секції плануються нові форми заходів, вже створено дистанційний навчальний курс і 2 жовтня стартував 4-тижневий онлайн марафон з кібербезпеки. У рамках проведення Місячника кібербезпеки, ініціатором якого є за традицією **Торгово-промислова палата України** та **Комітет з електронних комунікацій ТПП України**, 29 жовтня 2020 року буде проведено Digital Classroom з інформаційної безпеки – відкритий урок для учнів і вчителів (тренер із учнями працюватиме очно, одночасно буде трансляція для всієї України). Модератором заходу традиційно стане Антоніна Букач, Google for Education, Certified Trainer.

Наша ціль – залучити наших дітей, підростаюче покоління до вирішення актуальних проблем кіберзахисту.

Кібербезпека – не просто назва, а реальні проблеми і ситуації, з якими ми всі вже стикаємось кожного дня. І це безмежний простір для дослідницьких пошуків наших вихованців. У дослідженнях та навчанні учням Академії допомагають студенти ФТІ КПІ 125 спеціальності Кібербезпека, які стають їх менторами і помічниками, допомагають створювати реальні й цікаві проєкти.

Найкращі роботи наших вихованців будуть представлені на 3-му етапі Всеукраїнського конкурсі-захисті науково-дослідницьких робіт учнів – членів МАН. Цьогоріч, оскільки діють обмеження, що пов'язані із пандемією COVID-19, захід відбудеться дистанційно у режимі он-лайн. Запрошую всіх, особливо представників вищих навчальних заходів, подивитися цей захід. Я впевнена, що кожен з вас побачить на ньому своїх майбутніх студентів, якими у майбутньому пишатимуться ваші кафедри та інститути.

Зараз у структурі Київської МАН функціонує 15 наукових відділень, в яких працює 70 наукових секцій. Щорічно Київська МАН залучає до 9 -10 тисяч учнів до наукових досліджень у різноманітних галузях науки. І в цьому нам допомагають наші партнери – наукові інститути і заклади вищої освіти. На їх базах наші вихованці мають можливість експериментувати, набувати вмінь та навичок винахідницької роботи. Ми формуємо покоління новаторів і ми відкриті до партнерства із усіма зацікавленими сторонами.

Багато наших випускників просувають українську науку, займають високі посади у державних установах, творять сучасну історію України. Київська мала академія наук – це традиції у вихованні переможців. Щороку сотні наших учнів стають переможцями всеукраїнських і міжнародних конкурсів. Ці діти – це майбутнє нашої науки та майбутній форпост кібербезпеки нашої держави!

ВОЛОДИМИР БЕЗРУЧЕНКО

заступник директора, кандидат фізико-математичних наук, доцент, старший науковий співробітник

ТОВ «Київська енергетична агенція»

Електронний освітній проект **«E-schools»** успішно впроваджується в освітніх закладах України в межах виконання державної програми **«Нова українська школа»** та схвалений до використання МОН України.

Електронні журнали і щоденники використовують практично у всіх розвинених країнах світу. Їх впровадження передбачено **Концепцією розвитку електронного урядування в Україні** *(розпорядження КМ України від 20 вересня 2017 р. № 649-р).*

«МИ НАВЧАЄМО ПРИЙОМАМ РОБОТИ НА ПЛАТФОРМІ E SCHOOLS.INFO ЗА СХВАЛЕНОЮ МОН УКРАЇНИ ПРОГРАМОЮ «ЕЛЕКТРОННЕ ОСВІТНЄ СЕРЕДОВИЩЕ ЗАКЛАДУ ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ» (ПРОТОКОЛ № 4 ВІД 18.06.2018 Р.) СПІЛЬНО З РЕГІОНАЛЬНИМИ ЗАКЛАДАМИ ПІСЛЯДИПЛОМНОЇ ПЕДАГОГІЧНОЇ ОСВІТИ»

СЕРГІЙ НЕДІЛЬКО

директор

Український державний центр національно-патріотичного виховання, краєзнавства і туризму учнівської молоді

«МЕТОЮ СТВОРЕННЯ І ДІЯЛЬНОСТІ ЦЕНТРУ Є ЦЕНТРАЛІЗАЦІЯ ПРОЦЕСУ НАЦІОНАЛЬНО-ПАТРІОТИЧНОГО ВИХОВАННЯ В СИСТЕМІ ОСВІТИ ДЛЯ ФОРМУВАННЯ У ДІТЕЙ ТА МОЛОДІ НАЦІОНАЛЬНОЇ САМОСВІДОМОСТІ ТА САМОІДЕНТИФІКАЦІЇ, АКТИВНОЇ ГРОМАДЯНСЬКОЇ ПОЗИЦІЇ

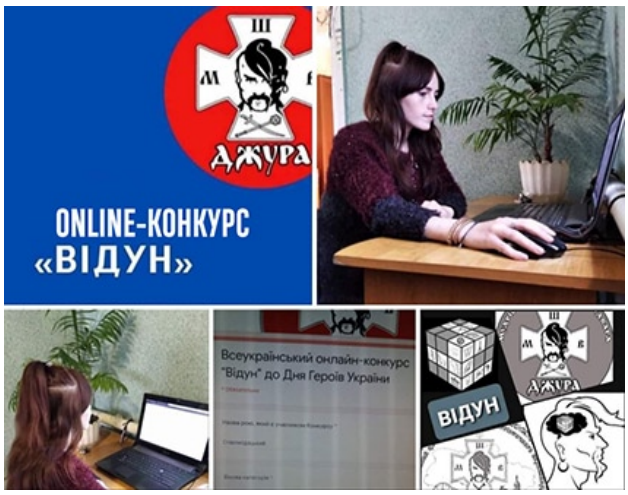
ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ У НАЦІОНАЛЬНО-ПАТРІОТИЧНОМУ ВИХОВАННІ

+38 **044 531 19 98**
center.patriot.ua@gmail.com
http://ukrjuntur.org.ua/

+38 **063 170 77 21**
e.schools.info@gmail.com
https://e-schools.info/

З початку введення карантину Український державний центр національно-патріотичного виховання, краєзнавства і туризму учнівської молоді більшість заходів проводить у онлайн-форматі з використанням різних платформ. Це стосується, насамперед, заходів, пов'язаних з проведенням Всеукраїнської дитячо-юнацької військово-патріотичної гри «Сокіл» («Джура») (далі – «Джура»).

«Джура» – важлива складова щодо формування ціннісних орієнтирів, громадянської самосвідомості та готовності щодо захисту незалежності та територіальної цілісності України на прикладах героїчної боротьби українського народу за самовизначення і творення власної держави.



«Джура» – це не просто гра, **«Джура»** – це системна форма національно-патріотичного виховання дітей та молоді, що спрямована на становлення громадянина України, патріота своєї країни.

Скажете, до чого тут інформаційні технології? А куди ж тепер без них? Навіть у звичайних квестах не обійтися без системи орієнтування, бодай мінімальних управлінських рішень, а тут значно відповідальніші завдання і цілі, і треба вміти застосовувати сучасні інформаційні засоби, системи управління.

У співпраці з Всеукраїнським освітнім проектом **E-SCHOOLS** (портал **https://e-schools.info/**), Українським державним центром національно-патріотичного виховання, краєзнавства і туризму учнівської молоді запропоновані шляхи використання платформи **E-SCHOOLS** при проведенні Всеукраїнської дитячо-юнацької військово-патріотичної гри **«Джура»**.

Спочатку коротко про платформу **E-SCHOOLS**. На порталі **https://e-schools.info/** заклад освіти (загальної середньої, дошкільної, позашкільної), зареєструвавшись, може створити власний сайт із потужним функціоналом:

- кожен учасник освітнього процесу має на ньому персональну сторінку, так само окремі сторінки створюються і для кожного класу;
- є можливість розмістити на сайті файловий архів з навчально-методичними матеріалами та фотогалерею;
- на платформі функціонують різноманітні інструменти для підтримання комунікацій між усіма учасниками освітнього процесу;
- працюють сервіси електронних щоденників і журналів, засоби моніторингу та аналітики та багато іншого.

Зазначимо, що для закладів освіти всі ці можливості надаються БЕЗКОШТОВНО!

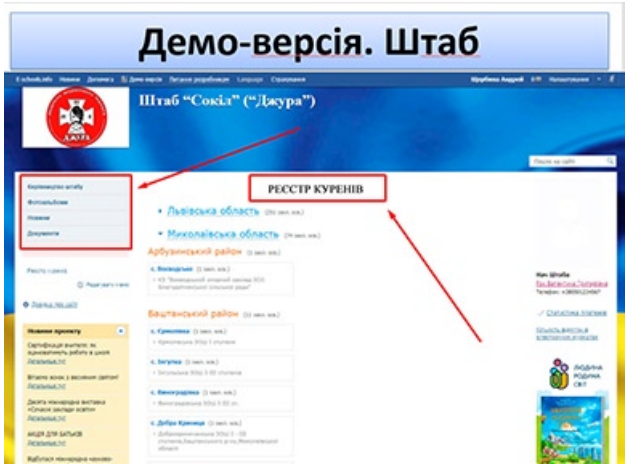
Платформа чудово підходить для створення інформаційної мережі будь-якої розгалуженої організації.

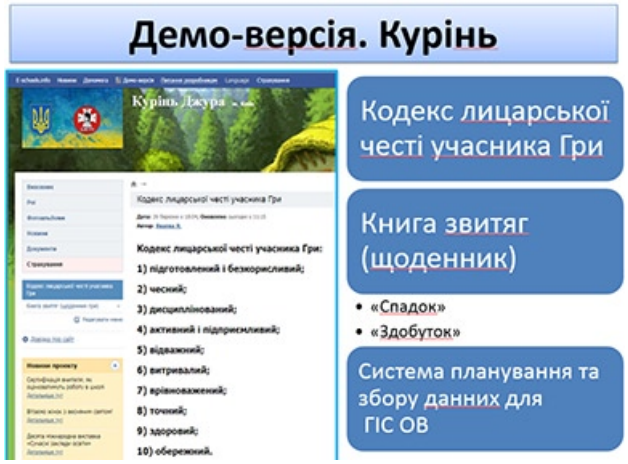
Постановою **КМ України від 17 жовтня 2018 р. № 845 «Деякі питання дитячо-юнацького військово-патріотичного виховання»** передбачено висвітлення в Інтернеті матеріалів, пов'язаних з діяльністю штабів та куренів **Всеукраїнської дитячо-юнацької військово-патріотичної гри «Джура»**.

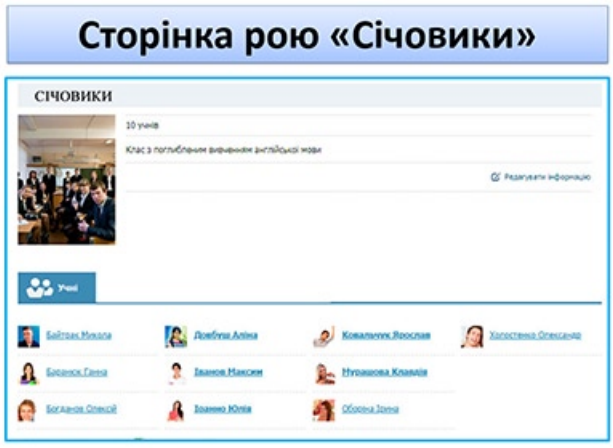
Освітній проект **E-schools** спільно з **Українським державним центром національно-патріотичного виховання, краєзнавства і туризму учнівської молоді** започатковує експеримент щодо розміщення на порталі **https://e-schools.info/** сайтів штабів та куренів гри **«Джура»**.

Наразі Українським державним центром національно-патріотичного виховання, краєзнавства і туризму учнівської молоді розробляються демо-версії штабів та куренів гри, після чого на порталі будуть доступні кнопки для перегляду цих демо-версій та підключення штабів та куренів.

Наприклад, так можуть виглядати демо-версії головних сторінок сайтів штабів та куренів гри, створених на порталі **e-schools.info**:







На сайті куреню є можливість розмістити персональну сторінку виховника та сторінки всіх роїв, що входять до куріння, а також персональні сторінки учасників гри.

За допомогою сервісу «Новини» платформи **https://e-schools.info/** є можливість оперативно опубліковувати фотоальбоми та новини роїв та куренів, що забезпечує виконання пункту 17 Положення про **Всеукраїнську дитячо-юнацьку військово-патріотичну гру «Джура»**.

Учасники мають змогу відправляти повідомлення виховнику та один одному. Наявність персонального сайту для куреню, а також окремої сторінки для кожного рою, без сумніву, зробить гру більш цікавою, а учасників гри – більш згуртованими.

Для впровадженні платформи **https://e-schools.info/** при проведенні **Всеукраїнської дитячо-юнацької військово-патріотичної гри «Джура»** пропонуються використовувати дистанційне навчання для представників штабів гри.

Серед подальших планів – проведення всеукраїнських конкурсів з краєзнавства і туризму на платформі **https://e-schools.info/**, впровадження елементів кіберспорту при проведенні **Всеукраїнської дитячо-юнацької військово-патріотичної гри «Джура»**, використання геоінформаційних технологій, навчання учасників гри основам кібергігієни.

ЖУРНАЛ
КИЇВСЬКОЇ
ТОРГОВО-
ПРОМИСЛОВОЇ
ПАЛАТИ

the CHAMBER rev!ew

#Зроби крок до нас

і ти вже в наших кращих виданнях

KYIV
CHAMBER
OF COMMERCE
AND INDUSTRY

kiev-chamber.org.ua

КІБЕРБЕЗПЕКА – НАШ АЛГОРИТМ

БОГДАН ЖОВТОБРЮХ

директор компанії
«Алгорітм-Х»

+380 67 431 02 02

zb@algorytmx.com.ua
https://algorytmx.com.ua

Товариство з обмеженою відповідальністю «Алгорітм-Х» (саме через «і») працює на ринку кібербезпеки більше трьох років, – родповідає нам Богдан ЖОВТОБРЮХ, директор компанії.

– Цікава історія нашої назви. Спочатку засновник придумав, як він вважав, досить нетривіальну назву «Алгоритм». Але під час реєстрації швидко з'ясувалося, що «алгоритмів» хоч греблю гати, тому державний реєстратор запропонував щось додати до назви – до болі знайома історія, коли на якомусь сайті старий звичний логін виявляється зайнятим і нам пропонується додати до нього літери або цифри. Тоді, пригадавши відомого «Містера-Ікс», наш засновник додав до назви літеру «Х».
Але не тут-то було – підприємство з такою назвою вже існувало. Шкода було шукати іншу ідею для назви, тому було вирішено змінити ще одну літеру – так з'явився на світ **«Алгорітм-Х»**.

До речі, термін **«алгоритм Х»** означає одну досить цікаву річ – алгоритм на ім'я відомого американського вченого в галузі інформатики Дональда Кнута, автора всесвітньо відомого «Мистецтва програмування» та видавницьких систем TEX та Metapoint. Сам алгоритм Х пов'язаний з розв'язком задачі про точне покриття (двомірна інтерпретація лежить в основі ідеї комп'ютерної гри Tetris).
Ось така орфографічно-математична суміш.

За три роки поступового, поступального та послідовного розвитку товариством «Алгорітм-Х» реалізовано та взято участь більш, ніж у 50 різних проєктах – від малих до великих – від високорентабельних до волонтерських – від простих до побудови складних систем із закритою тематикою.

Спільно з **Державним центром кіберзахисту Державної служби спеціального зв'язку та захисту інформації України** та **Інститутом телекомунікацій і глобального інформаційного простору Національної академії наук України** ТОВ «Алгорітм-Х» веде ініціативну науково-технічну роботу «Розробка окремих структурних елементів захищеної мобільної мультисервісної інфраструктури» (код державної реєстрації 0119U102716). Товариство активно співпрацює з **Київською торгово-промисловою палатою** та її віце-президентом **Володимиром Коляденко**, з Міжнародним університетом

кібербезпеки та його генеральним директором Євгеном Владіміровим, є розробником двох стандартів організації України – методик первісної перевірки та оцінки стану захищеності інформаційно-телекомунікаціних систем суб'єктів господарювання.

Директором компанії **Богданом Жовтобрюхом** в Міністерстві розвитку економіки, торгівлі та сільського господарства України вперше була зареєстрована авторська методика на послуги з керування автоматизованою системою захищеного доступу до мережі Інтернет.

Якщо вам потрібна консультація або впровадження оптимальних рішень з безпеки або захисту систем чи інформаційних ресурсів, будемо завжди раді вам допомогти.
Ми маємо реальний досвід з:

- проведення оцінки стану захищеності та тестування інформаційних ресурсів;
- розробки проєктів модернізації інформаційно-телекомунікаційних систем;
- надання послуг IT-аутсорсингу (обслуговування усіх або частини функціоналу IT-систем);
- розробки і постачання спеціалізованого аналітичного програмного забезпечення;
- постачання IT-та безпекових рішень відомих світових виробників (з представництвами яких укладені партнерські договори);
- надання послуг у галузі криптографічного та технічного захисту інформації.

АлгорІтм-Х

НАДІЙНИЙ ПАРТНЕР
ДЛЯ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ
ТА ЗАПОБІГАННЯ КРИТИЧНИХ СИТУАЦІЙ
В ІНФОРМАЦІЙНІЙ СИСТЕМІ

КІБЕРБЕЗПЕКА
НАШ АЛГОРИТМ

Algorytm-X

ALGORYTM-X | **Cybersecurity**

тел. +38 (044) **221 74 82** · e-mail: **info@algorytmx.com.ua**

ЯК ШУКАТИ КЛІЄНТІВ В КАРАНТИН

ukraine
CIS Events Group
your new marketing wave

Перенесіть свої маркетингові активності в віртуальний простір: утримайте і наростіть клієнтську базу, проінформуйте потенційних споживачів, дізнайтеся її побажання і збережіть зв'язок з аудиторією.

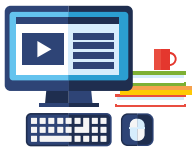
КОНФЕРЕНЦІЇ В ОНЛАЙН-ФОРМАТІ

Це унікальна можливість для вас запропонувати, а для учасників Форуму поспілкуватися зі спікерами та фахівцями, які в інших умовах не змогли б цього зробити через свою зайнятість або територіальну віддаленість. Знайомі Форуми BIT/BIS тепер ще доступніші для відвідування!

ВЕБІНАРИ І ОНЛАЙН НАВЧАННЯ

Ми готові допомогти вам з проведенням маркетингових і навчальних сесій онлайн. Наші співробітники зберуть цільову аудиторію для вебінарів, допоможуть з їх проведенням (від налаштування до безпосереднього асистування). Також ми готові допомогти в розгортанні і створенні навчальних курсів для вас на онлайн-платформах: підготовка програми, збір аудиторії, проведення занять і оцінка результатів.

ЛІДОГЕНЕРАЦІЯ



Напрацьовуйте клієнтську базу за рахунок цільових розсилань по потенційно цільовій аудиторії, корисної технічної та аналітичної інформації, збирайте аналітику потреб клієнтів за допомогою опитувань, призначайте і проводьте віртуальні зустрічі з нашою допомогою. Ми допомагаємо вам побудувати працюючу воронку лідогенерації за рахунок аналізу інтересу заданої ЦА до контенту заданого профілю.

online.ciseventsgroup.com