КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (12), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.12.3650
УДК 338.47

Якименко Юрій Михайлович
к.військ.н. доцент, доцент кафедри управління
інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID ID: 0000-0002-6848-852X
yakum14@ukr.net

Мужанова Тетяна Михайлівна
к.держ. упр., доцент, доцент кафедри управління
інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID ID: 0000-0002-7435-0287
muzanovat@gmail.com

Легомінова Світлана Володимірівна
д.екон.н., професор, завідувач кафедри управління
інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID ID: 0000-0002-4433-5123
chiarasvitlana77@gmail.com

СИСТЕМНИЙ АНАЛІЗ ТЕХНІЧНИХ СИСТЕМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ ВІД КОМПАНІЇ FIREEYE

Анотація. Розглянуті питання, які пов'язані з інформаційною безпекою підприємства. Інформаційна безпека являє собою набір інструментів і методів, використовуваних для захисту цифрової та аналогової інформації. Показано призначення системи управління інформаційною безпекою і роль технічних засобів захисту інформації від інформаційних загроз підприємству. Використаний методичний підхід системного аналізу щодо забезпечення інформаційної безпеки підприємства. Для створення та ефективної експлуатації системи забезпечення інформаційної безпеки необхідно завжди використовувати вже напрацьовані практики (стандарти, методології) побудови подібних системи забезпечення інформаційної безпеки та реалізовувати їх до систем управління (менеджменту) інформаційною безпекою. Оскільки сучасні системи забезпечення інформаційної безпеки підприємства, як досить складні організаційно-технічні системи, функціонують в умовах невизначеності стану зовнішнього і внутрішнього інформаційного середовища, управління такими системами мають грунтуватися тільки на результатах застосування системного аналізу. Відзначено необхідність переосмислення підходів і методів системного аналізу до створення та розвитку сучасних інформаційних технологій. Питання забезпечення інформаційної безпеки повинні розглядатися як складові елементи при створенні сучасних систем забезпечення інформаційної безпеки - із моменту проектування, на всіх стадіях функціонування і підтримки. Світові кампанії - вендори комп'ютерних систем приділяють значну увагу у напрямку підвищення їх можливостей по захисту інформації завдяки розробки і поліпшенню саме технічних засобів, в яких значне місце наділяється своєчасному виявленню загроз, їх аналізу і недопущенню негативних впливів на зниження інформаційної безпеки підприємств. Одним із провідних світових виробників ІТ є компанія FireEye, лідер у галузі постачання своїх технічних рішень. Зроблений аналіз технічних рішень компанії FireEye, яка є однієї з провідних світових ІТ-виробників в галузі інформаційної безпеки. Запропоновано до реалізації інноваційні рішення від компанії FireEye на підприємствах України в цілях підвищення ефективності виявлення інформаційних сучасних загроз і захисту інформації.

Ключові слова: інформаційна безпека, інформаційні технології, система управління інформаційною безпекою підприємства, системний аналіз, технічні засоби, компанія.

ВСТУП

Інформаційна безпека являє собою набір інструментів і методів, використовуваних для захисту цифрової та аналогової інформації. Вона охоплює широкий спектр інформаційних технологій, які активно проникають в життя, стаючи необхідною умовою успішного функціонування все більшого числа підприємств. Забезпечення інформаційної безпеки в бізнесі слід розглядати як невід'ємний елемент процесу управління підприємством.

Щоб зберегти бізнес, розвиватися і бути конкурентоспроможним підприємством, необхідно створювати ефективну систему управління інформаційною безпекою (СУІБ). Оскільки сучасні системи забезпечення інформаційної безпеки підприємства, як досить складні організаційно-технічні системи, функціонують в умовах невизначеності стану зовнішнього і внутрішнього інформаційного середовища, управління такими системами мають ґрунтуватися тільки на результатах застосуванні системного аналізу.

Головною метою будь-якої системи забезпечення інформаційної безпеки, в тому числі і СУІБ, є створення умов функціонування підприємства, запобігання загроз його безпеки, захист законних інтересів підприємства від протиправних посягань, недопущення розголошення, втрати, витоку, спотворення і знищення конфіденційної інформації та забезпечення в межах виробничої діяльності всіх підрозділів підприємства. Управління інформаційною безпекою в СУІБ – це, насамперед, процеси управління: персоналом, засобами захисту інформації, ризиками, інцидентами, безперервністю бізнесу, ресурсами з метою забезпечення інформаційної безпеки підприємства. Проблема автоматизації процесів управління забезпеченням інформаційної безпеки підприємств в час масової цифровізації суспільства вирішується на практиці по різному. Для створення та ефективної експлуатації систем забезпечення інформаційної безпеки необхідно завжди використовувати вже напрацьовані практики (стандарти, методології) побудови подібних системи та реалізовувати їх до систем управління інформаційною безпекою.

Технічні засоби СУІБ включають в себе різні апаратні засоби захисту інформації - фільтри, міжмережеві екрани, регулярне тестування систем безпеки, оновлення програм. Але в цілому це не збільшує рівень інформаційної безпеки підприємства через недостатню інтеграцію між ними. В той же час компанії - вендори комп'ютерних систем приділяють значну увагу у напрямку підвищення їх можливостей по захисту інформації завдяки розробці і поліпшенню саме технічних засобів, в яких значне місце наділяється своєчасному виявленню загроз, їх аналізу і недопущенню негативних впливів на зниження інформаційної безпеки підприємств. На внутрішньому ринку України пропонуються компаніями сучасні системи забезпечення інформаційної безпеки для впровадження на підприємствах. Лідируючі позиції у сфері поставок своїх технічних рішень займає одна з провідних світових виробників інформаційних технологій (IT) компанія FireEye.

Постановка проблеми. Реалізація підходів системного аналізу технічних систем забезпечення інформаційної безпеки включає комплекс взаємопов'язаних заходів (спеціальних, технічних, програмних, організаційних заходів), які завжди спрямовані на захист інформації. Головною метою будь-якої системи забезпечення інформаційної безпеки є створення умов нормального функціонування підприємства, запобігання негативним проявам від всіх видів загроз інформації. Незважаючи на постійне вдосконалення інформаційних технологій (IT) і інструментів захисту інформації на підприємствах не завжди забезпечується їх достатній рівень інформаційної безпеки.

Тому проблеми забезпечення інформаційної безпеки підприємства, особливо в умовах збільшення і появи нових внутрішніх та зовнішних загроз, виходять на перший план, потребують пошуку, аналізу і впровадженню ефективних систем захисту інформації, спрямованих на їх вирішення.

Актуальним є аналіз можливостей сучасних систем забезпечення інформаційної безпеки від IT-виробників, на прикладі компанії FireEye - по виявленню інформаційних загроз і захисту інформації підприємств.

Аналіз останніх досліджень і публікацій. Проблеми створення системи інформаційної безпеки на підприємствах намагалися вирішити у своїх наукових пошуках В.В. Андріанова, А.А. Гладких, Ю.А. Гатчина, Є.В. Климов, А.І. Моїсеєва, В.А. Ромака [1].

Визначенням інформаційної безпеки, механізмів забезпечення інформаційної безпеки України аналізували також такі вчені: О.Д. Довгань, В.А. Лужецький, О.О. Тихомиров, В.В. Марков. Зазначені автори аналізують поняття «інформаційна безпека», класифікацію інформаційної безпеки, водночас не розкривають підходи системного аналізу щодо системи інформаційної безпеки в публічному управлінні.

Маркіна І.А., Дячков Д.Н. в своїх роботах [2] уточнили визначення поняття інформаційної безпеки підприємства і на основі сформованої цілі, завдання, принципів побудови та видів загроз запропонували методичний підхід (послідовність) до створення систем інформаційної безпеки і системи менеджменту інформаційної безпеки промислових підприємств у вигляді моделі інформаційного протиборства з факторами внутрішнього та зовнішнього середовищ.

Данілова Е.І. в роботі [3] запропонувала методологію системного підходу щодо управління економічною безпекою підприємства. Так безпека підприємства досягається завдяки безпеці реалізації функцій підприємства, які формуються при умові безпечності використання ресурсів, реалізації бізнес-процесів, функціонування структур та впливу середовища. При цьому в основу системного підходу покладена ідентифікація всіх функцій підприємства і ресурсів, необхідних для їх виконання.

Чмир Я.І. у статті [4] відзначає, що, на сьогодні інформаційна безпека відіграє одну з ключових ролей у забезпеченні життєво важливих інтересів країни та суспільства, яке обумовлено швидким розвитком сучасних інформаційно-телекомунікаційних технологій, засобів зв'язку й інформатизаціїі. Основними проблемами забезпечення інформаційної безпеки залишаються: відсутність дієвих механізмів забезпечення інформаційної безпеки; відсутність інституцій, які комплексно забезпечуватимуть систему інформаційної безпеки в управлінні безпекою підприємства.

Панченко В.А. в роботі [5] визначив поняття інформаційної безпеки підприємства і виявів основні цілі, завдання, принципи побудови та види загроз. На основі проведеного аналізу сучасних підходів до визначення сутності інформаційної безпеки, на основі узагальнення теоретичних положень та досвіду функціонування організацій запропоновано систему інформаційної безпеки підприємства. Використання розробленого підходу в практиці господарювання промислових підприємств допоможе підвищити ефективність розробки, впровадження та використання системи інформаційної безпеки.

Аналіз літератури з проблематики дає підстави зазначити, що поняття «інформаційна безпека» розглядається з різних ракурсів. Наведено деякі з них визначення інформаційної безпеки як стану захищеності підприємств в умовах забезпечення збереження якісної інформації - від реальних або потенційних до неї загроз з боку інформаційно-комунікаційного середовища.

Проте поза увагою вчених залишилися організаційні та технічні аспекти управління забезпеченням інформаційної безпеки підприємств, пов'язаних з аналізом і впровадженням в них сучасних інформаційних технологій та систем управління у сфері безпеки , що вимагає проведення додаткових досліджень в цих питаннях.

Мета статті. Узагальнення дослідження вчених у галузі забезпечення інформаційної безпеки, використання методів і підходів системного аналізу щодо технічних систем забезпечення інформаційної безпеки підприємств від компанії FireEye та пропозиції до впровадження отриманих результатів.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Інформаційна безпека захисту цифрової та аналогової інформації являє собою набір інструментів і методів, що охоплює широкий спектр IT, включаючи в першу чергу мережеву інфраструктуру, аудит і тестування. В той же час IT активно проникають в бізнес, стаючи необхідною умовою успішного функціонування все більшого числа промислових підприємств. Зростання масштабів бізнесу відбувається з ефективним використанням IT в таких сферах як матеріально-технічне забезпечення, логістика, планування, оперативне управління, контроль якості продукції, маркетинг. При цьому надійне забезпечення інформаційної безпеки бізнесу є неодмінною умовою переходу на модель стійкого розвитку не тільки окремого підприємства, але й національної економіки в цілому. Неспроможність підприємств протидіяти цифровим загрозам може призвести до втрати довіри їх клієнтів, погіршення фінансового становища та створити умови для виникнення ризику втрати конкурентоспроможності на ринку, а регуляторні органи, у свою чергу, можуть накласти санкції на бізнес за нехтування інформаційною безпекою. Тому забезпечення інформаційної безпеки слід розглядати як невід'ємний елемент процесу управління підприємством [6], [7].

Умовою успішного функціонування бізнесу, його розвитку та конкурентоспроможності являється ефективна СУІБ. І це питання не може бути другорядним при виникненні прямих інформаційних загроз сучасним інформаційним системам підприємств. Інформаційна безпека досягається за допомогою виконання відповідного набору засобів управління, сформованого в ході керованих процесів менеджменту ризику і інших обраних через СУІБ, включаючи політики, процедури, організаційні структури, програмне та технічне забезпечення, для захисту інформаційних активів підприємств.

Оскільки сучасні системи забезпечення інформаційної безпеки, як досить складні організаційно-технічні системи, функціонують в умовах невизначеності стану зовнішнього і внутрішнього інформаційного середовища, управління такими системами мають ґрунтуватися тільки на результатах застосування системного аналізу [5], [8]. Системний аналіз в англомовній літературі використовують частіше як синонім системного підходу. Реалізація системного підходу включає комплекс взаємопов'язаних заходів при використанні спеціальних технічних і організаційних засобів, нормативно-правових актів. Системний підхід дозволяє визначити забезпечення інформаційної безпеки як складний, комплексний вид діяльності, що висуває особливі вимоги до його структурної характеристики. Головною метою будь-якої системи забезпечення інформаційної безпеки є створення умов функціонування підприємства, запобігання загроз його безпеки, захист законних інтересів підприємства від протиправних посягань, недопущення розголошення, втрати, витоку, спотворення і знищення конфіденційної інформації. Саме фахівці з системного аналізу проектують, створюють й експлуатують комп'ютерні системи управління та проектування динамічних процесів в технічних і

технологічних об’єктах, здійснюють аналіз бізнес-процесів з погляду їхньої подальшої автоматизації, розробляють технічні завдання та специфікації, тестують програмне забезпечення, формують аналітичні звіти. В наш час виникає необхідність переосмислення підходів і методів системного аналізу до створення та розвитку сучасних ІТ, а питання забезпечення інформаційної безпеки повинні розглядатися як складові елементи при створенні сучасних систем забезпечення інформаційної безпеки із моменту проектування, на всіх стадіях виробництва і підтримки [7], [9].

СУІБ можна розглядати умовно як сучасну систему забезпечення безпеки інформаційних ресурсів будь-якого підприємства. В той же час вона є частиною загальної системи управління, яка ґрунтується на системному підході, що враховує всі події інформаційної безпеки у бізнес-діяльності, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки. Тому забезпечення інформаційної безпеки повинно бути представлене як безперервний і динамічний процес, основний зміст якого становить управління безпекою в загальній системі управління, а управління інформаційною безпекою в СУІБ - це також є процеси управління: персоналом, засобами захисту інформації, ризиками, інцидентами, безперервністю бізнесу, ресурсами з метою забезпечення інформаційної безпеки [8].

Масове застосування комп'ютерних систем на підприємствах, які дозволили вирішити завдання автоматизації управлінських процесів, пов'язаних з обробкою постійного збільшення наростаючих обсягів інформації, зробило ці процеси надзвичайно вразливими по відношенню до агресивних (випадкових або навмисних) впливів і приводить в залежність рівня їх безпеки від використання сучасних ІТ. Проблема автоматизації процесів управління забезпеченням інформаційної безпеки підприємств в час масової цифровізації суспільства вирішується на практиці по різному [7].

Для створення та ефективної експлуатації системи забезпечення інформаційної безпеки необхідно завжди використовувати вже напрацьовані практики (стандарти, методології) побудови подібних систем забезпечення інформаційної безпеки та реалізовувати їх у створенні систем управління (менеджменту) інформаційною безпекою. Так, міжнародні (ISO:27001) і національні (ДСТУ:27001) стандарти [10] , як нормативні документи у галузі інформаційної безпеки, пропонують вимоги для використання при побудові та експлуатації СУІБ. В стандартах ISO:27002 та ДСТУ:27002 [11] містяться кращі практики, які являють собою усереднений або уніфікований опис підходів, прийомів і рекомендацій щодо створення, розвитку та підтримки СУІБ підприємств.

До основних організаційних заходів в СУІБ, які забезпечують достатній рівень інформаційної безпеки будь-якого підприємства, відносяться:

- організація використання технічних засобів збору, обробки, накопичення і зберігання конфіденційної інформації;
- організація роботи з аналізу внутрішніх і зовнішніх (гібридних) загроз конфіденційної інформації та вироблення заходів щодо забезпечення її захисту [12].

На практиці технічні засоби включають в себе різні апаратні засоби захисту інформації - фільтри, міжмережеві екрани на апаратуру, регулярного тестування систем безпеки, оновлення програм і т.п. Але в цілому це не збільшує рівень безпеки в організації через погану інтеграцію між ними на підприємстві. Саме ефективне використання новітніх досягнень в області ІТ, програмних засобів підтримки та підготовки даних для прийняття рішень, з дотриманням правил щодо забезпечення комп'ютерної та інформаційної безпеки дозволить підвищити ефективність роботи СУІБ

в напрямку аналізу даних і в реальному часі для виявлення та пріоритизації загроз, виявлення аномальної поведінки користувачів, а також реагування на тактики, методи і процедури різних зловмисників.

Група компаній БАКОТЕК (ВАКОТЕСН®) - міжнародна група компаній, яка займає лідируючі позиції в сфері поставок рішень провідних світових IT-виробників і є офіційним дистриб'ютором компанії FireEye в Україні, розробила і пропонує спеціалізовані платформи і рішення з безпеки, засновані на базі віртуальних машин , які забезпечують захист інформації підприємств і державних установ від кібератак нового покоління [13]. Захист інформації повинно здійснюватися цілодобово і цілорічно та охоплювати весь її життєвий цикл - від створення до знищення або від надходження до втрати актуальності. Треба теж враховувати, що сучасні атаки легко обходять традиційні системи захисту інформації (NG Firewall, IPS \ IDS, антівіруси і шлюзи безпеки), бо вони не мають на них сигнатур. Спеціалізовані платформи, наприклад FireEye, усувають цей недолік і забезпечують захист від гібридних загроз на різних етапах їх життєвого циклу - в режимі реального часу без використання сигнатур [14]. Основні послуги від компанії FireEye: тестування на проникнення і безпека додатків, попереднє виявлення та запобігання загрозам та зловмисному програмному забезпеченню, збереження журналу та відповідність вимогам, управління вразливістю, оцінка ризиків, моніторинг безпеки в хмарі, управління інцидентами тощо. Продукція від компанії - це рішення для керованої інформаційної безпеки по дотриманню вимог щодо захисту від загроз і управління ризиками в кібербезпеці.

Компанія FireEye пропонує передові засоби протидії сучасним, вузьконаправленим і професійно організованим атакам, в тому числі ще невідомим («нульового дня»), які практично не визначаються традиційними засобами у відмінності з антивірусами, брандмауерами і ін. Таким чином, її продукція здатна доповнити будь-яку існуючу систему захисту підприємства і підняти її на якісно новий рівень.

Сталася переорієнтація компанії в підході до забезпечення інформаційної безпеки підприємств, коли сьогодні керівникам необхідно дбати не про надійність захисту інформації, а перемикати увагу на готовність до атак - їх виявлення та припинення, а також і детальному аналізу. Тому захист, запропонований FireEye, грунтується не тільки на передових технологіях, але також на глибокому аналізі зібраної інформації (завдяки якому фахівці компанії зуміли виявити 14 з останніх 19 атак нульового дня), а також великий досвід у протидії найвитонченішим атакам. Компанія обслуговує 4400 клієнтів у 61 країнах світу і забезпечує інформаційну безпеку від глобальних загроз, здійснюючи приблизно 250 мільярдів кіберподій [15].

В Україні є досвід спільної співпраці FireEye з Національною поліцією в проведенні криміналістичного огляду та дослідження уражених серверів і робочих станцій вірусами від кібератак. Фахівці компанії FireEye постійно приймають участь в вивченні та аналізі даних телеметрії спеціального мережевого обладнання для розвідки та аналітики, з метою попередження різних сучасних атак.

Технічні засоби IT у вигляді платформ безпеки від компанії FireEye легко інтегруються в мережеву інфраструктуру підприємств і на сьогоднішній день дозволяють забезпечити співробітників інформаційної безпеки надійними інструментами для виявлення загроз, аналізу та розслідування інцидентів в найкоротші терміни в порівнянні з традиційними підходами. Технічні засоби IT можна також розцінювати як засоби інформаційно-аналітичної роботи аналітика інформаційної безпеки будь-якого підприємства (фірми) при функціонуванні СУІБ [16].

ISSN 2663 - 4023

Платформи безпеки FireEye включають в себе основні програмні продукти: **FireEye AX, FireEye FX, FireEye NX, FireEye EX** [17]**.** Всі ці продукти входять в централізоване управління системою безпеки FireEye CM [18], яка дозволяє об'єднати управління, звітність та поширення інформації про загрози (рис.1).

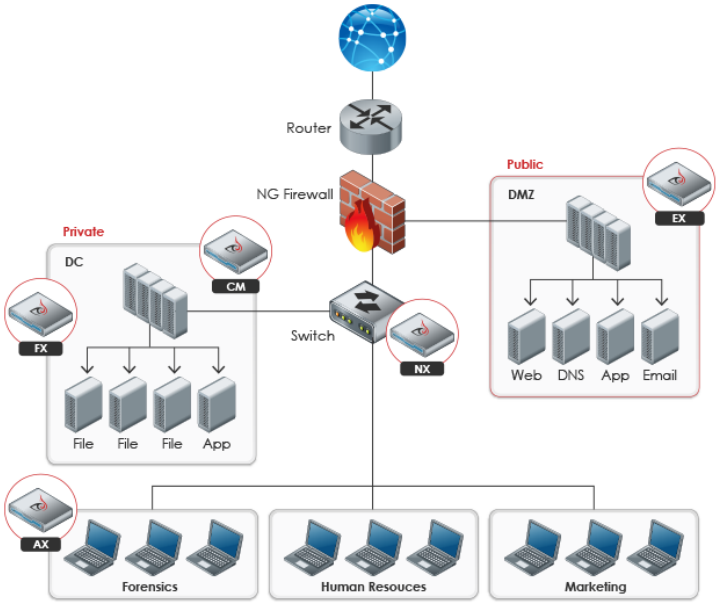

Рис.1. Схема зв'язків основних програмних продуктів платформ безпеки FireEye [17].

FireEye AX - це платформа для повноцінного детального аналізу загроз нового покоління і розслідування взаємозв'язку змішаних атак [19]. FireEye AX дає аналітикам безпеки контроль над потужним налаштуванням тестового середовища, де абсолютно безпечно можна досліджувати вплив загроз нового покоління (Zero-Day і APT), які вбудовані у файли різного формату, вкладення поштових повідомлень або web об'єкти. Коли аналітикам безпеки необхідне захищене середовище для тестування, відтворення, характеризації та документування APT (Advanced Persistent Threat) шкідливих активностей, FireEye AX дозволяє просто завантажити підозрілий файл на платформу, де він буде обстежений за допомогою технології MVX (FireEye Multi-Vector Virtual Execution), яка в той час є ядром платформи FireEye для проведення динамічного аналізу просунутих загроз в режимі реального часу [20]. Всі підозрілі об'єкти (поштові вкладення, завантаження, скрипти) запускаються в контрольованому віртуальному середовищі з метою виявлення їх нестандартної поведінки і інших ознак шкідливого коду (щоб уникнути затримок трафіку такі операції можуть бути асинхронними). На відміну від інших аналогічних підходів, в разі FireEye використовуються повноцінні віртуальні машини, що дозволяє отримати максимально реалістичне уявлення про досліджуваний код. У процесі аналізу PDF файлів, Web-об'єктів, і шкідливих URL, платформа AX надає детальний звіт, який дозволяє отримати всеосяжний огляд атаки, від початкового експлоїта і установки шкідливої програми, до місця призначення і подальших спроб її завантаження.

FireEye FX – це платформа для захисту від загроз нового покоління, які знаходяться в файлової системі, тематичних атак, що поширюються через файли різного формату [21]. Вона аналізує вміст мережевих файлових сховищ з метою виявлення і

подальшого карантину загроз, які могли бути занесені вручну, за допомогою Web або поштою, тим самим перешкоджаючи їх подальшому поширенню. FireEye FX перешкоджає поширенню просунутих загроз, які пропускають традиційні засоби інформаційної безпеки, такі як NG Firewall, IPS, антивіруси і шлюзи. Просунуті спрямовані атаки використовують складне шкідливе програмне забезпечення і APT-тактики, які не тільки проникають крізь захист, а й поширюються по всій мережі встановлюючи довгостроковий плацдарм для атак. FireEye FX аналізує загальні папки використовуючи технологію MVX , яка виявляє zero-day шкідливий код, вбудований в найбільш популярні формати файлів. Пристрій FireEye FX може здійснювати рекурсивне сканування за розкладом або за запитом. У процесі сканування виявляються і відправляються в карантин всі шкідливі об'єкти, які знаходяться в доступних для мережі загальних папках.

FireEye NX і **FireEye EX** [17] входять до системи для захисту інтернет трафіку.

FireEye NX - це платформа для рішення по боротьбі з загрозами нового покоління, які надходять по Web.

FireEye NX зупиняє Web атаки з якими не справляються традиційні Firewall, NG Firewall, IPS, антивіруси і Web шлюзи. NX захищає від Zero-Day експлойтів і спроб шкідливого ПЗ встановити зворотний зв'язок або передати вкрадені дані.

FireEye EX - це платформа для захисту організації від загроз нового покоління, які надходять по електронній пошті - спрямований фішинг поштових атак, які обходять традиційні репутаційні та антиспам технології. Атаки спрямованого фішингу використовують методи соціальної інженерії для створення правдоподібних повідомлень, які змушують користувача перейти за посиланням або відкрити вкладення, що надалі дає можливість кіберзлочинцю отримати контроль над системою.

FireEye HX – це платформа для рішення, яке дозволяє швидко і точно приймати рішення щодо події безпеки на робочій станції [22]. FireEye HX дозволяє об'єднати активності на події, які виробляються на рівні мережі і на рівні робочіх станцій, що дозволяє скоротити часові витрати на відновлення в зв'язку з інцидентом безпеки. FireEye HX забезпечує захист віддалених робочіх станцій, дозволяє приймати ефективні рішення з аналізу загроз, скорочує час на виявлення і розслідування інциденту і інтегрується з іншими платформами FireEye. FireEye HX використовує «індикатори ризику» (IOC) отримані з інших платформ FireEye (NX, EX, FX, AX) для оперативного підтвердження того, що кінцева станція була схильна до атаки. У процесі постійного моніторингу всіх робочих станцій, FireEye HX дозволяє корелювати повідомлення з мережевих пристроїв з подіями на робочіх станціях. Після того, як інцидент на робочій станції підтверджений, FireEye HX може негайно заблокувати скомпрометовану машину і не дозволити зловмиснику продовжити атаку. У той же час ця робоча станція буде доступна для розслідування.

Можливості FireEye HX:

1. Моніторинг та підтвердження загроз:

- підтвердження загроз виявлених мережевими пристроями шляхом кореляції їх з подіями на робочих станціях
- моніторинг всіх хостів на предмет загроз виявлених на периметрі або ідентифікованих іншими платформами безпеки
- забезпечує безперервний захист інформації за межами корпоративної мережі.

2. Блокування загроз:

- блокування зламаних робочіх станцій для негайного переривання атаки

- блокування всіх мережевих комунікацій на рівні робочої станції перед проведенням ґрунтовного аналізу загрози
- забезпечення доступу до системи для розслідування інциденту безпеки з можливістю гарантувати нормальну роботу робочої станції з довіреними IP адресами.

FireEye Endpoint - це платформа для унікального комплексного рішення по захисту кінцевих точок [23]. Завдяки інтегрованому інструменту FireEye Threat Intelligence, проактивний і адаптивний захист здійснюється безпосередньо на пристрої, де встановлений агент. Це забезпечує високу ефективність реагування і на загрози, і захисту від атак. Захист кінцевих точок FireEye включає в себе найактуальнішу інформацію про загрози. Її надають фахівці FireEye, які більше 200 000 годин на рік досліджують кібератаки по всьому світу. Ця інформація доповнює роботу системи FireEye Threat Intelligence, яка дозволяє аналізувати загрози в режимі реального часу. Версія FireEye Endpoint 4.0 доступна з 28 вересня 2017 року і може працювати в хмарі, on-premise, віртуальній або гібридної інфраструктурі.

Ключові переваги FireEye Endpoint:

- постійне і швидке оновлення інформації про актуальні загрози від системи FireEye Threat Intelligence;
- вбудований механізм виявлення і запобігання запуску шкідливих програм, який швидко зупиняє відомі загрози;
- розширені можливості виявлення / запобігання загрозам за допомогою постоянного аналізу;
- детальний аналіз загроз і їх проявів.

З метою підвищення ефективності і надання оперативних рішень по захисту від загроз безпеки, які еволюціонують, відбулося об'єднання зусиль компаній **FireEye** і **F5 Networks** в сфері протидії передовим кібератакам [24]. Ці рішення дозволяють поліпшити роботу служб безпеки підприємств, підвищити продуктивність додатків і серверів та можливість клієнтам і співробітникам користуватися будь-якими додатками з різних пристроїв (рис.2). Одночасно з підвищенням продуктивності, високої доступності та масштабованості додатків, клієнти отримують комплексний захист як додатків, так і внутрішньої мережі. Всі рішення вендора легко інтегруються в будь-яку інфраструктуру: локальну, хмарну або гібридну.

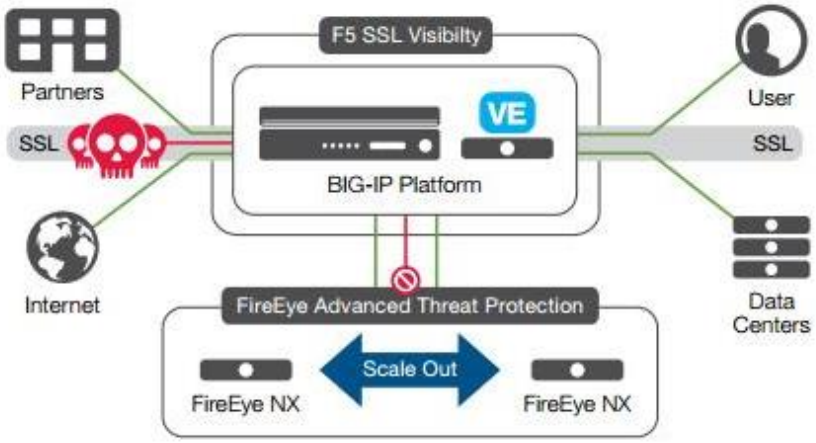

Рис.2. Схема об'єднання платформ компаній FireEye і F5 Networks по комплексному захисту від загроз [24].

ISSN 2663 - 4023

Можливості компаній FireEye і F5 Networks з комплексного вирішення захисту від загроз:

- Захист спільних папок від просунутих загроз - платформа працює в режимі активного карантину (захисту) або в режимі аналізу (моніторинг).
- Підтримка безлічі типів файлів - використовуючи технологію MVX, FireEye FX виявляє і блокує просунуті спрямовані атаки, які вбудовані в найбільш популярні типи файлів (PDF, MS Office, vCards, ZIP / RAR / TNEF і т.д) і мультимедіа контент (QuickTime, MP3 , Real Player, JPG, PNG, etc.).
- Можливість застосовувати захист в різних ситуаціях - здійснює вибіркове сканування файлів, жорстких дисків, довірених і не довірених файлових доменів і забезпечує захист бекапів.
- Інтеграція з FireEye NX, EX і AX платформами – завдяки такому об'єднанню шкідливий контент, виявлений за допомогою FireEye FX може бути перенаправлений на іншу платформу FireEye для миттєвого реагування на загрозу.

Компанія FireEye постійно наділяє увагу розвитку продуктів **FireEye Security** [25].У зв'язку з висновком про те, що одних технологій для боротьби з кіберзагрозами недостатньо, компанія впроваджує використання унікального інноваційного циклу, що поєднує технології з досвідом, щоб постійно покращувати рішення зі швидкістю і витонченістю, яка не має аналогів в галузі інформаційної безпеки.

Платформа безпеки Helix (Helix Security Platform)- застосовує аналіз загроз, автоматизацію і управління справами до рішень FireEye та стороннім розробникам на єдиній платформі операцій по забезпеченню безпеки .

Endpoint Security- забезпечує комплексний захист кінцевих точок, захищаючи користувачів від поширених загроз, виявляючи складні атаки і розширюючи можливості реагування.

Виявлення за запитом (Detection On Demand) - платформа служби виявлення загроз, що надається у вигляді API для інтеграції в робочий процес SOC, аналітику SIEM, в репозиторії даних або веб-додатки клієнтів.

Рішення хмарної безпеки (Cloudvisory Security Solution) - платформа для інтелектуального управління станом безпеки в декількох хмарах і захисту робочих навантажень.

Безпека електронної пошти (Email Security) - платформа для виявлення кібератак на основі електронної пошти та блокування найнебезпечніших загроз, включаючи шкідливі вкладення, фішингові сайти і атаки з підміною особи.

Мережева безпека та криміналістика (Network Security and Forensics) – платформа, яка забезпечує видимість мережі та захист від найскладніших і руйнівних кібератак у світі.

Екосистема FireEye Affinity Partner, як допомога в розробці більш надійної системи безпеки, а також - у створенні і підтримці надійної програми безпеки за допомогою додаткових послуг, прямого аналізу складних проблем і інноваційних рішень з безпеки.

Використовуючи потужне поєднання технологій, можливостей і досвіду, компанія FireEye удосконалює свої технічні розробки в напрямку в підвищення ефективності захисту інформації від сучасних інформаційних загроз, оперативно знаходить і блокує складні атаки, з якими не завжди справляються традиційні інструменти безпеки. Компанія надає кращі в сфері безпеки послуги з оцінки загроз, керованого виявлення подій і реагування на інциденти, їх оцінці і перетворенню даних для прийняття якісного

та оперативного рішення з управління інформаційною безпекою підприємства, які можуть ефективно використані в функціонуванні СУІБ підприємства.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведене дослідження системного аналізу технічних систем забезпечення інформаційної безпеки підприємств від компанії FireEye дозволяє зробити висновки:

1. Неспроможність підприємств протидіяти цифровим загрозам може призвести до втрати довіри їх клієнтів, погіршення фінансового становища та ризик втрати конкурентоспроможності на ринку, що знижує загальний рівень інформаційної безпеки. Тому забезпечення інформаційної безпеки слід розглядати як невід'ємний елемент процесу управління підприємством.

2. Ефективна СУІБ являється гарантом успішності підприємства, його безпечного функціонування. СУІБ можна розглядати умовно як сучасну систему забезпечення безпеки інформаційних ресурсів будь-якого підприємства.

3. Оскільки сучасні системи забезпечення інформаційної безпеки, як досить складні організаційно-технічні системи, управління такими системами мають ґрунтуватися тільки на результатах застосування системного аналізу.

Системний підхід дозволяє визначити забезпечення інформаційної безпеки як складний, комплексний вид діяльності.

4. Масове застосування комп'ютерних систем на підприємствах, які дозволили вирішити завдання автоматизації управлінських процесів, пов'язаних з обробкою постійного збільшення наростаючих обсягів інформації, зробило ці процеси надзвичайно вразливими по відношенню до агресивних (випадкових або навмисних) впливів і приводить в залежність рівня їх безпеки від використання сучасних інформаційних технологій.

5. Для створення та ефективної експлуатації системи забезпечення інформаційної безпеки необхідно завжди використовувати вже напрацьовані практики (стандарти, методології) побудови подібних системи та реалізовувати їх у створенні систем управління інформаційною безпекою.

6. До основних організаційних заходів забезпечення достатнього рівня інформаційної безпеки будь-якого підприємства відносяться: організація використання технічних засобів збору, обробки, накопичення і зберігання конфіденційної інформації і організація роботи з аналізу внутрішніх і зовнішніх (гібридних) загроз конфіденційної інформації та вироблення заходів щодо забезпечення її захисту.

7. Компанії - вендори комп'ютерних систем приділяють значну увагу у напрямку підвищення своїх можливостей по захисту інформації завдяки розробки і поліпшенню саме технічних засобів, в яких значне місце наділяється своєчасному виявленню загроз, їх аналізу і недопущенню негативних впливів. Ефективне використання новітніх досягнень в області IT дозволить також підвищити ефективність роботи СУІБ в напрямку аналізу даних і в реальному часі для виявлення та пріоритизації загроз, виявлення аномальної поведінки користувачів, а також реагування на тактики, методи і процедури різних зловмисників.

8. Компанія FireEye, як одна з провідних світових IT-виробників, розробила і пропонує спеціалізовані платформи і рішення з безпеки, засновані на базі віртуальних машин , які забезпечують ефективний захист інформації підприємств від кібератак нового покоління.

Платформи безпеки FireEye включають в себе основні програмні продукти: FireEye AX, FireEye FX, FireEye NX, FireEye EX. FireEye AX - це платформа для повноцінного детального аналізу загроз нового покоління і розслідування взаємозв'язку змішаних атак. FireEye FX – це платформа для захисту від загроз нового покоління, які знаходяться в файлової системі, та тематичних атак, що поширюються через файли різного формату. FireEye NX і FireEye EX входять до системи для захисту інтернет трафіку від загроз нового покоління. FireEye HX – це платформа для захисту віддалених робочих станцій, дозволяє приймати ефективні рішення з аналізу загроз, скорочує час на виявлення і розслідування інциденту завдяки постійному моніторингу всіх робочих станцій і інтегрується з іншими платформами FireEye-NX, EX, FX, AX.

9. FireEye Endpoint - це платформа для унікального комплексного рішення по захисту кінцевих точок, має найактуальнішу оновлену інформацію про загрози і їх аналіз в режимі реального часу; може працювати в хмарі, віртуальній або гібридній інфраструктурі.

10. З метою підвищення ефективності і надання оперативних рішень по захисту від загроз безпеки здійснено об'єднання зусиль компаній FireEye і F5 Networks в сфері протидії передовим кібератакам, що дозволило поліпшити роботу служб безпеки підприємства, підвищити продуктивність додатків і серверів та можливість користуватися будь-якими додатками з різних пристроїв для отримання комплексного захисту інформації і внутрішньої мережі, легко інтегрується з іншими платформами FireEye - NX, EX, AX і в будь-яку з інфраструктур: локальну, хмарну або гібридну.

11. Компанія FireEye активно впроваджує використання унікального інноваційного циклу в своєму розвитку, що поєднує технології з досвідом, щоб постійно покращувати рішення зі швидкістю і витонченістю, яка не має аналогів в галузі інформаційної безпеки. Компанія своїми рішеннями в IT зі своїми можливостями по захисту інформації представляє значний інтерес і її продукція може бути запропонована до реалізації на підприємствах України в цілях підвищення ефективності процесів і рівня забезпечення інформаційної безпеки підприємств.

У перспективі подальших досліджень передбачається проаналізувати методичні підходи і досвід використання технічних засобів IT як інструментів інформаційно-аналітичної роботи аналітика інформаційної безпеки на підприємстві.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Легомінова, С. В. (2015). Теоретичні засади інформаційної безпеки підприємства. *Економіка. Менеджмент. Бізнес*, *3* (13), 87-92.
2. Маркіна, І., Дячков, Д. (2016). Основи формування системи менеджменту інформаційної безпеки підприємства. *Проблеми і перспективи розвитку підприємництва*, *3*(1), 80–88.
3. Данілова, Е. І. (2020). *Концепція системного підходу до управління економічною безпекою підприємства: Монографія*. Європейська наукова платформа. https://ojs.ukrlogos.in.ua/index.php/monograph/article/view/danilova.kontseptsiia-2020/1859.
4. Чмир, Я. І. (2018). Проблеми забезпечення інформаційної безпеки в системі публічного управління. *Аспекти публічного правління*, *6*(9). 2018. 442-ArticleText-597-l-10-20181029.pdf.
5. Панченко, В.А. (2020). Управління інформаційною безпекою держави та підприємств: правові та організаційні аспекти. *Актуальні проблеми правознавства*, *1*(21), 103-109. http://dspace.wunu.edu.ua/bitstream/316497/38493/1/%D0%9F%D0%B0%D0%BD%D1%87%D0%B5%D0%BD%D0%BA%D0%BE.pdf.
6. Системи забезпечення інформаційної безпеки. https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review.

7. Коваленко, Ю.О. (2010). Забезпечення інформаційної безпеки на підприємстві. *Економіка промисловості*, 3, 123-129. http://dspace.nbuv.gov.ua/bitstream/handle/123456789/24811/st_51_18.pdf?sequence=1.
8. Якименко, Ю. М. (2021). Системний аналіз методологічних підходів до управління підприємством у сфері інформаційних технологій. ДУТ. http://www.dut.edu.ua/uploads/n_9074_59003267.pdf.
9. Yakymenko, Y. M., & Muzhanova, T. M. (2020). Analysis of the state of use of methodical approaches to assessing the enterprise's economic security level. *Economy. Management. Business*, *31*(1), 64-69. https://doi.org/10.31673/2415-8089.2020.016469
10. *Інформаційні технології. Методи захисту. системи управління інформаційною безпекою. вимоги.* (ДСТУ ISO/IEC 27001:2015). (б. д.).
11. *Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.* (ДСТУ ISO/IEC 27002). (б. д.).
12. Системи забезпечення інформаційної безпеки. Огляд. https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review.
13. Компания FireEye Inc. Продукты и решения. https://bakotech.ua/vendor/fireeye/.
14. FireEye: новый подход к кибербезопасности. https://ko.com.ua/fireeye_novyj_podhod_k_kiberbezopasnosti_107098.
15. Top 10 Penetration Testing Companies. https://uk.myservername.com/top-10-penetration-testing-companies#14_FireEye
16. Якименко, Ю.М. (2020). Використання спеціалізованих платформ і рішень з безпеки інформації в системному аналізі інформаційної безпеки організацій. ДУТ, 5-8. http://www.dut.edu.ua/uploads/n_9126_88033533.pdf.
17. Компания FireEye Inc. Продукты и решения. https://bakotech.ua/vendor/fireeye/.
18. FireEye CM – система централізованого управління. https://bakotech.ua/product/138/
19. FireEye AX – детальный анализ угроз нового поколения. https://bakotech.ua/product/137/.
20. Multi-Vector Virtual Execution (MVX). http://bakotech.ua/uploads/ckeditor/files/FireEye_MVX.pdf.
21. FireEye FX – защита от угроз нового поколения находящихся в файловой системе. https://bakotech.ua/product/136/.
22. FireEye HX – защита рабочих станций от современных киберугроз. https://bakotech.ua/product/200/.
23. FireEye представляет комплексную защиту конечных точек следующего поколения (FireEye Endpoint). https://bakotech.ua/news/fireeye-predstavlyaet-kompleksnuyu-zashchitu-konechnih-tochek-sleduyushchego-pok/.
24. F5 Networks и FireEye объявили о партнерстве в области решений комплексной безопасности. https://bakotech.ua/news/f5-networks-i-fireeye-obyavili-o-partnerstvo-v-oblasti-resheniy-kompleksnoy-bezo/.
25. FireEye Security Products. The FireEye Innovation Cycle. https://www.fireeye.com/products.html.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (12), 2021
ISSN 2663 - 4023

Yakymenko Yuriy Mykhailovych
Ph.D. Associate Professor, Associate Professor of Management
information and cyber security
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0002-6848-852X
yakum14@ukr.net

Muzhanova Tetyana Mykhailivna
к.держ. Manager, Associate Professor, Associate Professor of Management
information and cyber security
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0002-7435-0287
muzanovat@gmail.com

Lehominova Svitlana Volodymyrivna
Doctor of Economics, Professor, Head of the Department of Management
information and cyber security
State University of Telecommunications, Kyiv, Ukraine
ORCID ID: 0000-0002-4433-5123
chiarasvitlana77@gmail.com

SYSTEM ANALYSIS OF TECHNICAL SYSTEMS FOR ENSURING INFORMATION SECURITY OF FIREEYE ENTERPRISES

Abstract. Issues related to information security of the enterprise are considered. Information security is a set of tools and methods used to protect digital and analog information. The purpose of the information security management system and the role of technical means of information protection from information threats to the enterprise are shown. The methodical approach of the system analysis concerning maintenance of information security of the enterprise is used. To create and effectively operate an information security system, it is always necessary to use already established practices (standards, methodologies) to build such information security systems and implement them in information security management systems. Since modern systems of information security of the enterprise, as a rather complex organizational and technical systems, operate in conditions of uncertainty of the external and internal information environment, the management of such systems should be based only on the results of system analysis. The need to rethink the approaches and methods of systems analysis to the creation and development of modern information technologies is noted. Issues of information security should be considered as components in the creation of modern information security systems - from the moment of design, at all stages of operation and support. Global campaigns - vendors of computer systems pay considerable attention to increase their capacity to protect information through the development and improvement of technical means, in which a significant place is given to timely detection of threats, their analysis and prevention of negative impacts on reducing information security. One of the world's leading IT manufacturers is FireEye, a leader in the supply of its technical solutions. An analysis of technical solutions of FireEye, which is one of the world's leading IT manufacturers in the field of information security. Innovative solutions from the FireEye company at the enterprises of Ukraine for the purpose of increase of efficiency of detection of information modern threats and protection of the information are offered for realization.

Key words: information security, information technologies, enterprise information security management system, system analysis, technical means, company.

REFERENCES

1. Lehominova, S. V. (2015). Teoretychni zasady informatsiinoi bezpeky pidpryiemstva. Ekonomika. Menedzhment. Biznes, 3 (13), 87-92.

2. Markina, I., Diachkov, D. (2016). Osnovy formuvannia systemy menedzhmentu informatsiinoi bezpeky pidpryiemstva. Problemy i perspektyvy rozvytku pidpryiemnytstva, 3(1), 80–88.
3. Danilova, E. I. (2020). Kontseptsiia systemnoho pidkhodu do upravlinnia ekonomichnoiu bezpekoiu pidpryiemstva: Monohrafiia. Yevropeiska naukova platforma. https://ojs.ukrlogos.in.ua/index.php/monograph/article/view/danilova.kontseptsiia-2020/1859.
4. Chmyr, Ya. I. (2018). Problemy zabezpechennia informatsiinoi bezpeky v systemi publichnoho upravlinnia. Aspekty publichnoho pravlinnia, 6(9). 2018. 442-ArticleText-597-l-10-20181029.pdf.
5. Panchenko, V.A. (2020). Upravlinnia informatsiinoiu bezpekoiu derzhavy ta pidpryiemstv: pravovi ta orhanizatsiini aspekty. Aktualni problemy pravoznavstva, 1(21), 103-109. http://dspace.wunu.edu.ua/bitstream/316497/38493/1/%D0%9F%D0%B0%D0%BD%D1%87%D0%B5%D0%BD%D0%BA%D0%BE.pdf.
6. Systemy zabezpechennia informatsiinoi bezpeky. https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review.
7. Kovalenko, Yu.O. (2010). Zabezpechennia informatsiinoi bezpeky na pidpryiemstvi. Ekonomika promyslovosti, 3, 123-129. http://dspace.nbuv.gov.ua/bitstream/handle/123456789/24811/st_51_18.pdf?sequence=1.
8. Iakymenko, Yu. M. (2021). Systemnyi analiz metodolohichnykh pidkhodiv do upravlinnia pidpryiemstvom u sferi informatsiinykh tekhnolohii. DUT. http://www.dut.edu.ua/uploads/n_9074_59003267.pdf.
9. Yakymenko, Y. M., & Muzhanova, T. M. (2020). Analysis of the state of use of methodical approaches to assessing the enterprises economic security level. Economy. Management. Business, 31(1), 64-69. https://doi.org/10.31673/2415-8089.2020.016469
10. Informatsiini tekhnolohii. Metody zakhystu. systemy upravlinnia informatsiinoiu bezpekoiu. vymohy. (DSTU ISO/IEC 27001:2015). (b. d.).
11. Informatsiini tekhnolohii. Metody zakhystu. Zvid praktyk shchodo zakhodiv informatsiinoi bezpeky. (DSTU ISO/IEC 27002). (b. d.).
12. Systemy zabezpechennia informatsiinoi bezpeky. Ohliad. https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review.
13. Kompanyia FireEye Inc. Produktы y reshenyia. https://bakotech.ua/vendor/fireeye/.
14. FireEye: novыi podkhod k kyberbezopasnosty. https://ko.com.ua/fireeye_novyj_podhod_k_kiberbezopasnosti_107098.
15. Top 10 Penetration Testing Companies. https://uk.myservername.com/top-10-penetration-testing-companies#14_FireEye
16. Iakymenko, Yu.M. (2020). Vykorystannia spetsializovanykh platform i rishen z bezpeky informatsii v systemnomu analizi informatsiinoi bezpeky orhanizatsii. DUT, 5-8. http://www.dut.edu.ua/uploads/n_9126_88033533.pdf.
17. Kompanyia FireEye Inc. Produktы y reshenyia. https://bakotech.ua/vendor/fireeye/.
18. FireEye CM – systema tsentralizovanoho upravlinnia. https://bakotech.ua/product/138/
19. FireEye AX – detalnыi analyz uhroz novoho pokolenyia. https://bakotech.ua/product/137/.
20. Multi-Vector Virtual Execution (MVX). http://bakotech.ua/uploads/ckeditor/files/FireEye_MVX.pdf.
21. FireEye FX – zashchyta ot uhroz novoho pokolenyia nakhodiashchykhsia v failovoi systeme. https://bakotech.ua/product/136/.
22. FireEye HX – zashchyta rabochykh stantsyi ot sovremennыkh kyberuhroz. https://bakotech.ua/product/200/.
23. FireEye predstavliaet kompleksnuiu zashchytu konechnыkh tochek sleduiushcheho pokolenyia (FireEye Endpoint). https://bakotech.ua/news/fireeye-predstavlyaet-kompleksnuyu-zashchitu-konechnih-tochek-sleduyushchego-pok/.
24. F5 Networks y FireEye obъiavyly o partnerstve v oblasty reshenyi kompleksnoi bezopasnosty. https://bakotech.ua/news/f5-networks-i-fireeye-obyavili-o-partnerstvo-v-oblasti-resheniy-kompleksnoy-bezo/.
25. FireEye Security Products. The FireEye Innovation Cycle. https://www.fireeye.com/products.html..