УДК 004

А. Олійник, магістр гр. КІ-21М-1,4,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ CAN-МЕРЕЖІ НА ОСНОВІ ТЕХНОЛОГІЇ CSDN

У статті розроблено програмне забезпечення, яке призначено для системи CAN-мережі на основі технології CSDN. Метою розробки є дослідження та програмна реалізація системи CAN-мережі на основі технології CSDN. Об'єктом дослідження є процес CAN-мережі на основі технології CSDN. Предметом дослідження є методи CAN-мережі на основі технології CSDN. Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи CAN-мережі на основі технології CSDN. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, CAN-мережі, CSDN

Постановка проблеми. Новий етап, що наступив у розвитку обміну інформацією, який характеризується інтенсивним впровадженням сучасних інформаційних технологій, широким поширенням локальних, корпоративних і глобальних мереж, створює нові можливості і якість інформаційного обміну.

Корпоративні інформаційні системи (CAN) стають сьогодні одним з головних інструментів управління бізнесом, найважливішим засобом виробництва сучасного підприємства, вони використовуються в банківських, фінансової сферах, у сфері державного управління. CAN містить у собі інфраструктуру й інформаційні сервіси. Інфраструктура CAN (мережі, сервери, робочі станції, додатки) є географічно розподілені, її структурна одиниця – сегмент CAN (СГ CAN).

Однак застосування інформаційних технологій немислимо без підвищеної уваги до питань інформаційної (комп'ютерної) безпеки через наявність погроз захищеності інформації.

Для сучасного етапу розвитку теорії й, особливо, практики забезпечення захисту інформації (ЗІ) характерна парадоксальна ситуація: з одного боку, посилене увага до безпеки інформаційних об'єктів, істотне підвищення вимог по ЗІ, прийняття міжнародних стандартів в області інформаційної безпеки (ІБ), постійно зростаючі витрати на забезпечення захисту, з іншого боку – настільки ж неухильно зростаючий збиток, заподіюваний власникам і власникам інформаційних ресурсів, про що свідчать публікуємі регулярно дані про збиток світовій економіці від комп'ютерних атак.

Очевидно, що сучасні підходи до організації ЗІ не повною мірою забезпечують виконання вимог по захисту інформації. Основні недоліки СЗІ визначаються сформованими твердими принципами побудови архітектури й застосуванням в основному оборонної стратегії захисту від відомих погроз. Критична ситуація в сфері ІБ збільшується у зв'язку з використанням глобальної мережі для зовнішніх і внутрішніх електронних транзакцій підприємства й появою невідомих раніше типів деструктивних інформаційних впливів.

Тому для успішного використання сучасних інформаційних технологій необхідно ефективно управляти не тільки мережею, але й СЗІ, при цьому на рівні СГ CAN автономно повинна працювати система, що реалізує управління складом подій інформаційної безпеки, планування модульного состава СЗІ й аудит. Оскільки об'єкт управління – СЗІ є досить

складною організаційно-технічною системою, що функціонує в умовах невизначеності, суперечливості й неповноти знань про стан інформаційного середовища, управління такою системою повинне бути засноване на застосуванні системного аналізу, методів теорії прийняття рішень і необхідної інтелектуальної підтримки.

Разом з тим в області розробки методів і систем захисту інформації в цей час практично відсутні дослідження, спрямовані на забезпечення автоматизованої підтримки управління ЗІ для рішення проблеми забезпечення необхідного рівня захищеності інформації протягом усього періоду функціонування СЗІ.

Одним з варіантів рішення даної проблеми, розглянутим у магістерській роботі, є використання методів інтелектуальної підтримки управління ЗІ в сегменті корпоративної інформаційної системи, що у свою чергу, вимагає розробки на основі принципів системного аналізу й загальнонаукових підходів методологічних основ управління захистом інформації, що відповідають моделей, методів, алгоритмів і програмного забезпечення.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи CAN-мережі на основі технології CSDN.

Мета й завдання дослідження. роботи є дослідження та програмна реалізація системи CAN-мережі на основі технології CSDN.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем CAN-мережі на основі технології CSDN.
- Дослідження системи CAN-мережі на основі технології CSDN.
- Програмна реалізація системи CAN-мережі на основі технології CSDN.

Об'єктом дослідження є процес CAN-мережі на основі технології CSDN.

Предметом дослідження є методи CAN-мережі на основі технології CSDN.

Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Опис архітектури Cisco Self-Defending Network

Частково завдяки діяльності Cisco, що представляє стратегію мережі, яка самозахищається Cisco (Self-Defending Network) (CSDN), багато хто починає усвідомлювати необхідність інтегрованих засобів мережного захисту.

Механізми забезпечення мережної безпеки еволюціонували від незалежно використовуваних «точкових» продуктів, таких як міжмережні екрани або засоби виявлення вторгнень, в область інтегрованих і цілісних рішень. Cisco Systems є провідною компанією по розробці технології, що дозволяє зробити мережі, що самозахищаються, реальністю.

Ідея рішення досить просте: призначення IT-інфраструктури полягає в створенні систем, що надають можливість виявлення порушень безпеки й захисту від несанкціонованого доступу з одночасним наданям оперативного доступу легальним користувачам. Проста відмова в доступі вже не є підходящою реакцією на атаку – сучасні мережі повинні реагувати на атаки, зберігаючи свою доступність, надійність і працездатність. У багатьох відносинах, метою забезпечення безпеки стає підвищення ступеня відказостійкості мереж. Замість того, щоб ставати жертвами, мережі повинні стати здатними «поглинати» атаки й зберігати працездатність, подібно імунній системі людини, що дозволяє організму функціонувати при наявності в ньому вірусів і бактеріальних інфекцій.

Розвиток ситуації в сфері безпеки

За останні три роки технології забезпечення безпеки змінилися більше, ніж за все попереднє десятиліття. Обсяг і темп цих змін ускладнили покладену на IT-Фахівців завдання підтримки належного рівня захищеності. Перед тим, як продовжити розповідь про Cisco SDN, необхідно одержати поданя про суть цих змін:

– Захист периметра мережі. Мабуть, найбільш істотним фактором, що вплинув на зміну підходу до забезпечення безпеки мереж, стала зміна самої сутності мережі. Після того, як корпорації стали консолідувати центри обробки даних, використовувати конверговані внутрішні мережі й активно використовувати мережу Інтернет, уже не можна забезпечити безпеку мережі тільки за рахунок організації захисту її периметра. Середовище, що раніше вважалося ізольованим і контрольованим, тепер є напіввідчиненим за рахунок, наприклад, мереж "екстранет", підключень пунктів роздрібного продажу, надомних працівників та ін. Розширення корпоративної мережі, таким чином, приводить до необхідності взаємодії через ненадійні проміжні мережі й неконтрольовані середовища. Пристрої, що підключаються до корпоративної мережі через ці проміжні мережі, найчастіше не відповідають вимогам корпоративних політик безпеки. Пристрої, їм відповідні, часто використовуються для доступу до інших неконтрольованих мереж до з'єднання з корпоративною мережею. У результаті, пристрої, підключені до зовнішніх мереж, можуть стати «перевалочним пунктом» для атак і пов'язаних з ними несанкціонованих дій.

– Бездротові мережі й мережі мобільного зв'язку. Прив'язані до поняття периметра захисту бездротові мережі й мережі мобільного зв'язку підприємств тепер забезпечують підтримку ноутбуків, кишенькових комп'ютерів (PDA) і мобільних телефонів, які підключені до декількох мереж. Ці пристрої з декількома мережними інтерфейсами підтримують можливість установлення однорангових бездротових з'єднань для роботи в мережі "точка-точка". Крім того, пакети можуть ефективно передаватися між пристроями на прикладному рівні. У результаті поняття границь мережі стає усе більше розмитим і для забезпечення безпеки компаніям необхідно мати можливість управління такими мобільними пристроями.

– Електронна комерція, мережі "екстранет" і проведення ділових операцій у глобальній мережі. Поява загальних прикладних інтерфейсів на основі протоколів передачі повідомлень, таких як XML і SOAP, зробило благотворний вплив на електронну комерцію й продуктивність роботи підприємств. Але, як і в більшості випадків появи нових технологій, їхня поява привела до виникнення зовсім нових уразливістей і джерел атак, з якими доводиться боротися. Дані, які раніше передавалися за допомогою множини мережних протоколів і проходили фільтрацію на міжмережних екранах, тепер передаються за допомогою декількох або всього одного транспортного протоколу (наприклад, HTTP з використанням порту 80 TCP). У результаті, більша частина даних, що раніше містилася в заголовках пакетів, тепер розташовується в тілі пакетів. Це істотно полегшує зловмисникові завдання обходу класичної системи захисту мережі. Більше того, для забезпечення конфіденційності й цілісності корпоративних даних всі частіше використовується шифрування трафіка прикладного рівня за допомогою протоколів SSL/TLS і HTTPS. При цьому виникає побічний ефект, пов'язаний з ускладненням контролю доступу на границі мережі через неможливість перевірки пакетів у зашифрованих потоках даних.

– Віруси, Інтернет-хробаки й швидкість їхнього поширення. Кількість і різноманіття вірусів, що з'явилися за останні три роки, і Інтернет-хробаків саме по собі є застрашливим. Дивовижний вплив цих Інтернет-хробаків і вірусів на мережі підприємств і їхня продуктивність було обумовлено наявністю двох факторів: короткого проміжку часу між виявленням уразливості й появою атаки з її використанням, а також швидкості, з якою більшість атак поширювалося по мережі. При цьому число порушень роботи мереж досягало неприпустимого рівня, а для усунення наслідків доводилося йти на незаплановані витрати людських, тимчасових і матеріальних ресурсів.

– Дотримання встановлених норм. Факти, що одержали широкий розголос, порушень і неправомірні дії усередині корпорацій підштовхнули керуючі органи багатьох галузей до створення норм по регулюванню ризиків відносно корпоративної інформації. У США ці норми, найбільш відомими з яких є закон Сарбейнса-Окслі, закон Гремма-Ліча-Блілі й закон про дотримання конфіденційності інформації про охорону здоров'я й особистих даних пацієнтів (HIPAA), привели до корінних змін способів організації корпоративних мереж, серверів, баз даних і хостів. Аналогічна тенденція спостерігається й в Україні.

Хоча багато організацій думають, що дотримання норм забезпечує більш надійний захист їхньої інфраструктури, дане думка найчастіше є помилковим. Сам процес проходження встановленим нормам може привести до виникнення нових уразливістей. Наприклад, Інтернет-хробаки й віруси можуть більш ефективно поширюватися в мережі, що підтримує наскрізні VPN-з'єднання, у зв'язку з тим, що минаючі по них потоки даних є невидимими для проміжних вузлів. Такі потоки даних можуть переносити Інтернет-хробаків на критично важливі корпоративні сервери за допомогою надійно зашифрованих пакетів. Крім того, що на виявлення такої атаки йде багато часу, наскрізні VPN-з'єднання ускладнюють процес усунення її наслідків.

Принципи побудови сучасних безпечних мереж

Корпорації не можуть нескінченно додержуватися напрямків в області безпеки, що змініються. В ідеалі, удосконалювання системи безпеки повинне впливати на існуючу інфраструктуру маршрутизації й комутації, методи розмежування й контролю доступу й суміжних організаційних структур, що забезпечують підтримку цих систем. У цьому розділі ми опишемо основні елементи мережі, що самозахищається, **Cisco Self-Defending Network**:

– Присутність. Фундаментальним поняттям захищеної системи є поняття контрольних точок, що ми визначимо як присутність. Подібно імунній системі людини, що заснована на розосереджені по всьому тілу людини й виконуючі функції виявлення інфекції й виконання відповідних дій клітки, мережа покладається на наявність певних можливостей в окремих вузлів. До таких можливостей відносяться класичні методи ідентифікації, контролю доступу, перевірки даних і захисту взаємодії, а також нові можливості аналізу дій клієнтів файлообмінних мереж, web-сервісів, голосових сервісів і сервісів передачі динамічного контенту по мобільних мережах.

– Контекст. При вході користувача в систему мережа запитує й одержує доступ до набору реквізитів доступу користувача й хоста, що представляють собою кінцеву сутність. Повноваження можуть змінюватися із часом залежно від дій підключеного до мережі хоста. Сукупність цих даних і являє собою контекст. На відміну від існуючих систем мережної безпеки, у яких велика увага приділяється тільки перевірці повноважень користувача при вході в мережу, мережа, що самозахищається Cisco Self-Defending Network ухвалює рішення щодо наданя або скасування повноважень на основі змін поводження й відповідного йому контексту за увесь час з'єднання користувача з мережею. Наприклад, якщо мережа виявляє, що хост заражено вірусом (при цьому користувач може мати всі повноваження на доступ), вона ізолює цей хост у карантинний сегмент мережі. Оскільки дані можуть бути підмінені, у процесі забезпечення безпеки системи може знадобитися одержання контексту від інших систем для точного й своєчасного визначення прав хоста й привілеїв у конкретний момент часу.

– Взаємозв'язок. Взаємозв'язки між окремими пристроями дозволяють обмінюватися контекстом і створювати «систему». Традиційно, взаємозв'язки між пристроями мережі встановлювалися за допомогою протоколів маршрутизації, такими як протокол BGP. Для того щоб протистояти найсучаснішим видам погроз і несанкціонованих дій, тепер необхідно розширювати ці взаємозв'язки по всьому маршруті від джерела до одержувача мережного трафіка. Крім того, через зростаюче число мобільних пристроїв, взаємозв'язки вийшли за межі границь, які донедавна розглядалися як зовнішні границі мереж у традиційному розумінні. Привілеї, які пристрій одержує при доступі до мережі й характер їхньої зміни в процесі сеансу роботи визначаються на основі контексту цього пристрою і його взаємозв'язків у мережі.

– Довіра. Безпека системи визначається безпекою вступної у неї інформації; система функціонує набагато ефективніше, якщо в ній присутні довірчі відносини. Раніше ступінь довіри визначалася головним чином на основі ідентифікації пристрою або користувача. Результати останніх досліджень показали, що в концепцію захищених систем повинні бути включені поняття стану й місця розташування пристрою.

По багатьом параметрам дії, виконувані користувачами або пристроями в мережі, можна зрівняти з управлінням автомобілем. Подібно тому, як людина дістає водійські права, що дозволяють йому управляти певним класом транспортних засобів, користувачі повинні мати деяку ідентифікаційну інформацію для входу в мережу. Крім того, у кожного автомобіля є ідентифікаційний номер, що повинен бути зареєстрований у місцевих органах управління – мережі й кінцеві вузли незабаром будуть мати цифрові сертифікати, створювані під час випуску й потребуючі виконання певного типу реєстрації при використанні в рамках компанії. Але оскільки пристроям не завжди вдається вчасно надавати ідентифікаційні дані, мережі, що самозахищаються Cisco Self-Defending Network використовує передові методи непрямої довіри й максимальних зусиль для автентифікації й авторизації сутностей. Мережа, що самозахищається, Cisco Self-Defending Network повинна як мінімум уміти запитувати ідентифікаційні дані кожного пристрою й користувача, виконувати аналіз стану пристрою й установлювати місце розташування пристрою в мережі. Технологія, що дозволяє реалізувати ці можливості, буде повсюдно поширена й задіяна за допомогою чітко певних стандартних форматів повідомлень і протоколів, таких як протокол 802.1x і протокол автентифікації EAP.

Саме по собі кожне із цих понять не дуже примітно. Але вони здобувають силу при об'єднанні в мережі, що самозахищається, Cisco Self-Defending Network. У частині, що залишилася, даного огляду описуються деякі способи використання цих понять у рамках мережі, що самозахищається Cisco Self-Defending Network.

Елементи й побудова мережі

Оскільки одночасна перебудова всіх підсистем без порушення цілісності IT-сервисів може виявитися складним завданням, більшість споживачів не зможе впровадити всі компоненти стратегії Cisco SDN одночасно. Крім того, деякі споживачі можуть баритися з передачею функцій контролю безпеки автоматизованій системі доти, поки вони не переконаються в надійності роботи рішення. Стратегія мережі, що самозахищається, Cisco Self-Defending Network дозволяє таким компаніям здійснювати поступовий перехід до Cisco SDN за рахунок наданя продуктів, які можуть використовуватися незалежно друг від друга. Таким чином, має сенс розглянути наступні основні етапи проектування мережі, що самозахищається, Cisco Self-Defending Network.

Захист кінцевих вузлів. Віруси й Інтернет-хробаки, що заражають кінцеві вузли, часто приводять і до побічного ефекту – перевантаженню мережі, що є наслідком їхнього швидкого поширення.

Cisco пропонує засіб запобігання вторгнень на кінцеві вузли Cisco Security Agent, що дозволяє вирішити обидві проблеми. Використовувані в Cisco Security Agent передові методи захисту на основі аналізу поводження дозволяють виявляти віруси й Інтернет-хробаки, а також запобігати їхнє проникнення на кінцеві системи й поширення по мережі. Фактично, Cisco Security Agent є першою лінією оборони для запобігання поширення вірусів і Інтернет-хробаків.

Другим очевидним аргументом на користь застосування Cisco Security Agent є те, що він використовується на кінцевих вузлах і дозволяє створити ланцюг відповідної реакції між кінцевим вузлом і мережею. У результаті виходить мережа, здатна швидко адаптуватися до виникаючих погроз.

Контроль доступу. Однією з найбільш важливих можливостей мережі, що самозахищається, Cisco Self-Defending Network є механізм контролю доступу до мережі Cisco Network Admission Control (NAC).

NAC дозволяє вирішити, який рівень доступу варто надати кінцевому вузлу, виходячи з відповідності стану вузла політиці безпеки компанії, обумовленого шляхом аналізу стану безпеки операційної системи й установлених додатків. На додаток до функцій контролю й розмежування доступу NAC надає IT-адміністраторам можливість автоматичного перекладу в карантин і лікування кінцевих вузлів, що не пройшли перевірку відповідності. Перевірка відповідності є ефективною другою лінією оборони для запобігання поширення вірусів і

Інтернет-хробаків. NAC можна також розглядати як інструментальний засіб аналізу уразливістей і управління установкою «латок» на вимогу.

Відмінною рисою NAC є наданя як клієнтського, так і адміністративного інтерфейсу AAA, що дозволяють споживачам додатково встановлювати продукти великої кількості розроблювачів засобів захисту.

У цей час більше 250 лідируючих на ринку розроблювачів інтенсивно впроваджують або вже впровадили у свої продукти механізми NAC.

Важливо надати можливість використання NAC у системах малих і середніх підприємств. Для цього Cisco кілька років назад придбала корпорацію Perfigo, областю діяльності якої є розробка комплексних рішень контролю доступу до мережі. Основними функціями рішень є аналіз політик кінцевих вузлів, перевірка відповідності стану вузлів установленим вимогам і забезпечення працездатності засобів контролю й розмежування доступу. Тепер у рамках ініціативи Network Admission Control компанія Cisco пропонує рішення за назвою Cisco NAC Appliance (Cisco Clean Access).

Обмеження області зараження. Посилені політики доступу не є панацеєю й не усувають необхідність моніторингу пристроїв після їхнього входу в мережу. Кваліфіковані зловмисники в стані обійти практично будь-яку перевірку прав доступу, а мережі не можуть постійно покладатися на заражений елемент або довіряти йому. Пристрої, що пройшли перевірку відповідності, також можуть бути інфіковані за допомогою різноманітних джерел зараження після входу в мережу – наприклад, зараження з USB-накопичувача.

Мережа, що самозахищається Cisco Self-Defending Network спроектована для виконання перевірок безпеки не тільки під час одержання вузлом доступу до мережі, але й протягом усього сеансу з'єднання. Крім того, мережа, що самозахищається Cisco Self-Defending Network може покладатися на інші елементи мережі, включаючи кінцеві вузли для визначення компрометації інших вузлів, за аналогією з тим, як поліція контролює рівень злочинності шляхом аналізу дзвінків на номер 911. Cisco розглядає засоби обмеження області зараження як третю лінію оборони для запобігання поширення вірусів і Інтернет-хробаків.

На жаль, протоколи автентифікації, що існують, не розроблялися для роботи після початкового обміну інформацією. Таким чином, мережа, що самозахищається Cisco Self-Defending Network повинна забезпечувати нові способи обміну інформацією про стан пристроїв (контекст), а також способи оцінки вірогідності цієї інформації на основі як непрямого, так і прямої довіри. Наприклад, адміністратор повинен мати можливість створювати правило, відповідно до якого повідомлення, отримане від кінцевого вузла із установленим агентом Cisco Security Agent, заслуговує більшої довіри, чим повідомлення, що прийшло від незахищеного кінцевого вузла. У результаті компанія Cisco почала розробку нових механізмів кореляційного аналізу й відповідної реакції на основі непрямих атрибутів.

Інтелектуальні засоби кореляційного аналізу й реагування на інциденти

Для забезпечення ефективної роботи методів відповідної реакції, швидкої оцінки впливу, вибору конкретної дії й визначення найкращого засобу захисту необхідно, щоб мережа, що самозахищається, Cisco Self-Defending Network надавала сервіси кореляційного аналізу подій у сфері безпеки в режимі реального часу.

Для рішення цього завдання компанія Cisco придбала компанію Protego Networks, що розробила сімейство продуктів MARS, що надають методи зв'язування відповідної реакції від різних мережних пристроїв (міжмережні екрани, системи виявлення вторгнень, маршрутизатори, комутатори й хости) з контекстом, одержуваним у результаті вивчення топології мережі на рівні 2 і 3. Це дозволяє групі реакції на порушення в сфері безпеки швидко визначити місце появи атак у мережі.

Інтегровані системи виявлення вторгнень і механізми виявлення аномалій. Проектування ефективних систем виявлення мережних вторгнень (NIDS) завжди було важливим напрямком в області постійно, що ведуться досліджень, і розробок Cisco. Одним з

перших нововведень Cisco у цій області було впровадження NIDS у маршрутизатори й комутатори.

Але для того щоб система NIDS мала повну функціональність, її необхідно перетворити в систему запобігання вторгнень (IPS) з убудованими можливостями фільтрації трафіка, що дозволяє відкидати непотрібні пакети за допомогою підсистем, що набудовуються тонко, класифікації трафіка.

На жаль, більшість NIDS видають занадто багато помилкових спрацьовувань і не можуть надійно виконувати завдання запобігання атак при установці системи на проміжному пристрої. Почасти проблема полягає в необхідності збору й обробки великого обсягу інформації (контексту) протягом досить короткого проміжку часу.

Особливо це, до речі, стосується додатків, які дуже чутливі до затримок передачі (наприклад, IP-телефонія). Для рішення цього завдання Cisco розробляє кілька методів, що забезпечують високоякісну й ефективну обробку й класифікацію контрольованого трафіка.

Багато легальних дій можуть бути помилково сприйняті мережею як аномальні; головним чином, це стосується мереж зі значним числом змінних факторів.

У результаті компанія Cisco стала випливати консервативному поетапному підходу до виявлення аномалій, починаючи з Cisco Security Agent, оскільки було встановлено, що операційні системи моделювати простіше, ніж мережні середовища. Після цього компанією Cisco була придбана ефективна система запобігання вторгнень Riverhead, що характеризується низьким числом помилкових спрацьовувань за рахунок чіткого поділу дій, спрямованих на проведення атак типу «відмова в обслуговуванні», і іншої мережної активності.

Безпека додатків і захист від шкідливих програм (Anti-X). За останні кілька років з'явилися нові мережні додатки, що забезпечують захист від нових видів погроз, включаючи віруси, Інтернет-хробаків, спам, шпигунські програми, зловмисне використання web-сервісів і засобів IP-телефонії, а також несанкціоноване використання клієнтів файлообмінних мереж, – захист від яких не забезпечувалася повною мірою класичними міжмережними екранами й продуктами NIDS.

З метою захисту від цих погроз фахівцями Cisco були розроблені сервіси захисту нового покоління, що виконують перевірку заголовків пакетів і їхнього вмісту. Це дозволяє забезпечити ретельну перевірку трафіка в критично важливих точках мережі й обробляти зловмисний трафік до влучення в корпоративну мережу.

Об'єднання цих сервісів у багатофункціональні платформи дозволяє розширити можливості розроблювачів, а також знизити сукупну вартість володіння для споживача. Крім того, інтеграція цих механізмів дозволить розширити можливості мережі, що самозахищається, Cisco Self-Defending Network по контролі додатків.

Якщо в додатках використовується наскрізне шифрування, мережа, що самозахищається Cisco Self-Defending Network може збирати інформацію з кінцевих вузлів, компенсуючи втрати, пов'язані з неможливістю контролю даних на границі мережі.

Структурна схема мережі, що самозахищається, Cisco Self-Defending Network наведена на рисунку 1.

Розробка структурної схеми

Ґрунтуючись на принципах системного аналізу, що являє собою теорію й практику поліпшуючого втручання в проблемну ситуацію, пропонується варіант декомпозиції проблеми дозволу наявних протиріч в області забезпечення безпеки інформації.

На підставі системного підходу видно, що модель проблемної ситуації в області захисту інформації містить сукупність трьох взаємодіючих систем:

– проблемоутримуючої СЗІ,

– проблемодозволяючої керуючої системи, що розробляється для того, щоб проблема зникла або ослабнула, що оточує;

– істотного середовища, з якої взаємодіє СЗІ, під якою розуміється безліч потенційна можливих погроз інформаційної безпеки.

Вимога постійно наростаючої деталізації приводить до побудови моделі состава проблемоутримуючої системи, моделі об'єкта захисту й моделі погроз.

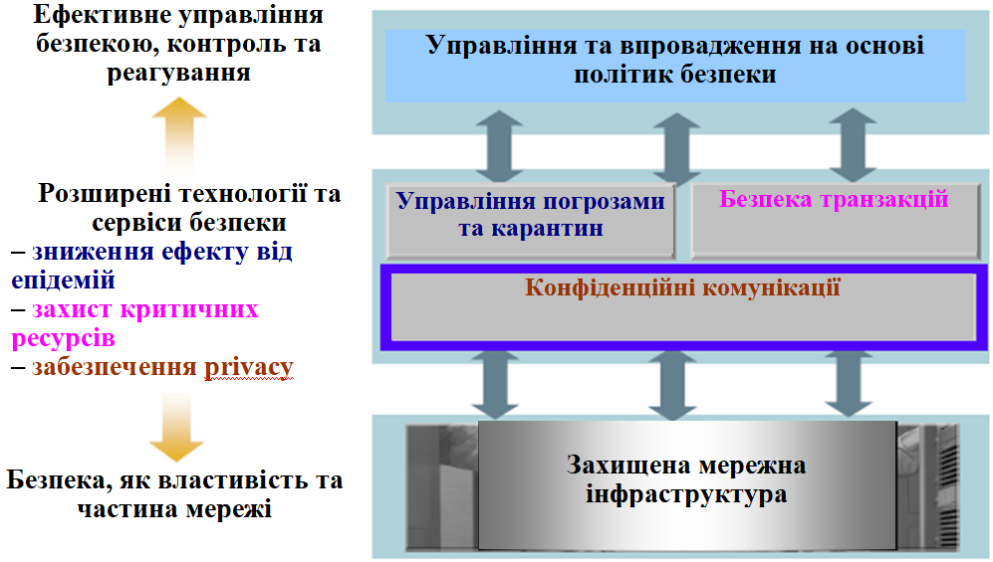

Рисунок 1 – Структурна схема мережі, що самозахищається, Cisco Self-Defending Network

Відзначається, що основною проблемою при побудові керуючої системи є розробка моделі погроз, що зв'язано зі специфічністю взаємодії об'єкта управління – СЗІ з навколишнім середовищем. У зв'язку із цим пропонується концепція побудови моделі погроз безпеки інформації, що базується на розроблювальній класифікаційній схемі навмисних цілеспрямованих погроз інформаційному середовищу корпоративної інформаційної системи. Показано доцільність побудови сукупності моделей:

– функціональної, на основі опису послідовності дій зловмисника (порушника) за допомогою дерев погроз;

– просторової графової, систематизованих у форматі інтегральної структурної моделі каналів несанкціонованого доступу, витоку й деструктивних впливів, що дозволяє провести всебічний аналіз реальних погроз, підвищити адекватність моделі погроз для конкретного об'єкта захисту.

На основі аналізу принципів управління в умовах невизначеності пропонується узагальнена архітектура системи управління захистом інформації в сегменті корпоративної інформаційної системи. Проаналізуємо основні функції управління, обґрунтовується доцільність варіанта побудови системи, що включає дві функціональні підсистеми:

– підсистему організаційно-технічного управління;

– і підсистему оперативного управління в реальному масштабі часу.

Відповідно до вимоги кількісної оцінки характеристик систем, висунутим системотехнікою, у якості керованої змінної введемо показник – рівень захищеності, необхідна значення якого залежить від максимального рівня критичності оброблюваної в даний період часу інформації.

У контурі організаційно-технічного управління створюються механізми управління захистом інформації при зміні інфраструктури, бізнес-додатків, планів обробки інформації й відповідних їм вимог до рівня захищеності інформації. Контур включає: систему інтелектуальної підтримки прийняття рішень на вибір стратегії захисту, систему оцінки рівня захищеності (ризику), що управляє вплив реалізується співробітниками відділу інформаційної безпеки. Командна інформація формується в ході планування – цілеспрямованого вибору раціонального комплексу засобів захисту.

У контурі оперативного управління формується оперативна командна інформація, що доводить до об'єкта управління адміністратором безпеки або автоматично за допомогою засобів реалізації керуючих впливів на убудовані в засоби захисту керуючі модулі.

У системі управління, що має таку архітектурну побудову, ефективні рішення вибираються й приймаються як на основі відомостей про технічні характеристики засобів захисту, так і на основі аналізу контрольованого простору.

Структурна схема системи управління захистом інформації в сегменті корпоративної інформаційної системи показана на рисунку 2.

На основі аналізу можливостей удосконалювання управління захистом інформації за рахунок застосування нових методів рішення завдань управління й скорочення тривалості циклу управління розробляється функціональна модель системи управління в стандарті IDEF0, що дозволяє наочно й ефективно відобразити механізм управління загрозами, виявити процеси, для реалізації яких необхідна розробка автоматизованої системи інтелектуальної підтримки управління.

Рисунок 2 – Структурна схема системи управління захистом інформації в сегменті корпоративної інформаційної системи

У структурній схемі застосовуються наступні скорочення:

- АБ – адміністратор безпеки;
- ОІБ – співробітники відділу інформаційної безпеки;
- Обу (СЗІ) – об'єкт управління;
- ГПБ, ЛПБ – глобальна, локальні політики безпеки;
- НСДУВ – несанкціонований доступ, витік, деструктивний вплив;
- ЗЗ – засоби захисту;
- $\eta_{тр}$ – необхідне значення рівня захищеності.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів CAN-мережі на основі технології CSDN. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем CAN-мережі на основі технології CSDN. Досліджена система CAN-мережі на основі технології CSDN. На основі отриманих результатів досліджень створена програмна реалізація системи CAN-мережі на основі технології CSDN. Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання CAN-мережі на основі технології CSDN. Проведено аналіз предметної

галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. https://doi.org/10.1007/s42979-021-00739-w (Scopus).
2. Smirnov O., Kovalenko O., Kovalenko A., Kavun S. «Quantitative Risk Assessment Method Development in the Context of the SDLC-model». 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 203-208, doi: 10.1109/PICST54195.2021.9772143 (Scopus).
3. Smirnov O., Neskorodieva T., Fedorov E., Rymar P. «Neural Network Modeling Method of Transformations Data of Audit Production with Returnable Waste». CEUR Workshop Proceedings Volume 3101, 2021, Pages 192-207. (Scopus).
4. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». CEUR Workshop Proceedings Volume 2805, 2020, Pages 44-58. (Scopus).
5. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256. (Scopus).
6. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114. (Scopus).
7. Smirnov O.A., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346. (Scopus).
8. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». CEUR Workshop Proceedings Volume 2654, 2020, Pages 122-131. (Scopus).
9. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14. (Scopus).
10. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». Lecture Notes in Networks and Systems, vol 152. Springer, Cham. 2021, pp 66-84. (Scopus).
11. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587. (Scopus).
12. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
13. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011.
14. Смирнов С.А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы / А.К. Дидык, С.А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко С.Г., 2016. – 566 с.
15. Смирнов С. А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, А. В. Коваленко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2014. – Вип. 9(125). – 105-110.
16. Смирнов С. А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2014. – Вип. 4 (41). – С. 48-52.
17. Смирнов С. А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2014. – № 4(17). – С. 90-95.
18. Смирнов С. А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2015. –Вип. 1(126). – С. 150-153.

19. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.
20. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.
21. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2015. –№ 3(20). – С. 134-141.
22. Смирнов С. А. Комплекс gert-моделей технологии облачной антивирусной защиты телекоммуникационной системы / А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Безпека інформації: наук. - практ. журн. – К.: НАУ, 2015. – Т. 21, № 3. – С. 251-262.

УДК 004

А.Пилипенко, магістр гр. КН-21М-1,4,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ BIG DATA НАУКОВИХ ДОСЛІДЖЕНЬ

У роботі розроблено програмне забезпечення, яке призначено для системи big data наукових досліджень. Метою розробки є дослідження та програмна реалізація системи big data наукових досліджень. Об’єктом дослідження є процес big data наукових досліджень. Предметом дослідження є методи big data наукових досліджень. Методи дослідження базуються на методах big data, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи big data наукових досліджень. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп’ютерні науки, big data, наукові дослідження

Постановка проблеми.

Великі дані (big data) обіцяють революціонізувати виробництво знань у науці та за її межами, забезпечивши нові, високоефективні способи планування, проведення, поширення та оцінки досліджень. Останні кілька десятиліть стали свідками створення нових способів виробництва, зберігання та аналізу даних, кульмінацією яких стала поява галузі даних, яка об’єднує обчислювальні, алгоритмічні, статистичні та математичні методи для екстраполяції знань із великих даних. У той же час рух *відкритих даних,* що виник на основі таких політичних тенденцій, як поштовх до відкритого уряду та відкритої науки, заохочував обмін і взаємозв’язок різнорідних дослідницьких даних через великі цифрові інфраструктури. Наявність величезних обсягів даних у машиночитаних форматах створює стимул для створення ефективних процедур збору, організації, візуалізації та моделювання цих даних. Ці інфраструктури, у свою чергу, служать платформами для розвитку штучного інтелекту з метою підвищення надійності, швидкості та прозорості процесів створення знань. Дослідники з усіх дисциплін бачать, що нова здатність зв’язувати та перехресно посилатися на дані з різних джерел покращує точність і прогностичну силу наукових висновків і допомагає визначити майбутні напрямки дослідження, таким чином, зрештою, забезпечуючи нову відправну точку для емпіричного дослідження. Як свідчить зростання цільового фінансування, навчальних програм і місць публікацій, великі дані широко розглядаються як започаткування нового способу проведення досліджень і кидання виклику існуючому розумінню того, що вважається науковим знанням.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи big data наукових досліджень.