Міністерство освіти і науки України
Державний університет «Одеська політехніка»

Навчально-науковий інститут штучного інтелекту та роботехніки
Кафедра комп’ютерних систем

Кунаков Олексій Андрійович,
студент групи УК-162

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Дослідження ефективності моделей захисту інформації.

Спеціальність:
123 - Комп'ютерна інженерія

Спеціалізація, освітня програма:
Спеціалізовані комп’ютерні системи

Керівник:
Ступень Павло В’ячеславович,
доцент

Одеса – 2021

ЗМІСТ

ВСТУП

Останнім часом бездротові (Wi-Fi) мережі отримали величезне розповсюдження. Сьогодні бездротові мережі можуть бути використані як у офісах, хот-спотах, так і в домашніх умовах. Їхнє використання може бути зумовлене одним із наступних чинників: необхідність забезпечення мобільності користувачів, необхідність підключення великої кількості користувачів у майбутньому; неможливість використання дротової мережі. Також безпровідною мережею передаються важлива особиста і комерційна інформація, проводяться банківські транзакції – кількість людей які бажають заволодіти подібною інформацією також збільшується. Відповідно, дослідження щодо підвищення ефективності захисту інформації в комп’ютерних мережах є актуальним.

Серед багатьох літературних джерел, що стосуються криптографії та захисту мереж, виділимо найважливіші. В монографії [1] розглянуто основні поняття сучасної криптографії, в монографії [2] – загальні принципи криптографії та особливості захисту комп'ютерних мереж. До основних функцій, які мають виконувати засоби захисту інформації, зараховують конфіденційність, аутентифікацію, цілісність, доступність, керування доступом. Конфіденційність – це гарантія можливості користування інформацією наперед визначеним суб’єктам та гарантія неможливості доступу до цієї інформації зловмисникам. В монографії [3-4] розглянуто протоколи шифрування.

Мета роботи - дослідити можливості злому Wi-Fi мережі та можливості застосування комплексного рішення для захисту від несанкціонованого доступу.

Основні результати дослідження

У бездротових мереж є багато переваг перед провідними мережами, але є й недоліки. І однією з найважливіших вад – це досить низьких рівень безпеки. Існують різні причини, що спонукають хакерів займатися атаками. Одна з

причин: заради цікавості. Такі люди займаються зламуванням задля розваги та самоствердження. Вони можуть навіть зробити послугу суспільству, публічно сповістити про виявлені небезпечні місця мереж, що примусить звернути увагу на існуючі проблеми.

Інша причина атак криється в застосуванні чужої мережі, тобто в крадіжці інтернет-трафіку.

Третя, найважливіша причина – це викрадення конфіденційної інформації. Ці зловмисники є найнебезпечнішими. Стандартні заходи безпеки можуть лише затримати такого супротивника на декілька годин. Якщо безпеці мережі 802.11 не приділити належної уваги, то атака неминуче виявиться успішною.

Відповідно для забезпечення безпечної роботи даної мережі треба розуміти основні принципи безпеки заложенні в даній технології.

РОЗДІЛ 1. ПРИНЦИПИ БЕЗПЕКИ ІНФОРМАЦІЇ

1.1. Поняття безпеки інформації

Безпека бездротової мережі спеціально створена для того, щоб неавторизовані користувачі не могли отримати доступ до вашої бездротової мережі і вкрасти конфіденційну інформацію. Тип бездротового безпеки, яку використовує окремий користувач, визначається його бездротовим протоколом. Сьогодні багато будинків і компанії працюють і покладаються на бездротові мережі.[1] Wi-Fi неймовірно ефективний для підтримки користувачів підключеними до інтернету 24 години на добу кожен день тижня. Вищезазначене перевага в поєднанні з тим, що він поставляється без перешкод, робить бездротову мережу ще більш привабливою. Однак є й інша сторона, оскільки сигнали Wi-Fi можуть транслюватися за межами будинку або компанії.

Це означає, що Wi-Fi вразливий для хакерів; збільшуючи легкий доступ людей в сусідніх будинках або навіть людей на сусідній парковці. Ось тут-то і виникає важливість забезпечення надійної бездротової безпеки. Ви можете задатися питанням, що представляє собою небезпеку, якщо вона взагалі існує, для інших людей, що мають доступ до вашого Wi-Fi. Ну, є ряд небезпек для вразливою бездротової мережі. Наприклад, хакери зможуть отримати доступ до особистої інформації, вкрасти вашу особистість і використовувати її проти вас. Були випадки, коли люди потрапляли до в'язниці за злочин, який вони не скоювали через інтернет. Коли інші люди зможуть отримати доступ до вашого Wi-Fi, швидше за все, ваш щомісячний рахунок різко зросте. [2]Крім того, інші люди, які використовують ваше Wi-Fi з'єднання без вашого дозволу, значно знизять швидкість доступу в Інтернет. В сучасну цифрову епоху, коли Інтернет є місцем, де живуть недобросовісні люди, безпеку Wi-Fi не може бути занижена.

Неважко захистити ваш Wi-Fi. У цій статті ми розповімо вам, як ефективно захистити мережу Wi-Fi і захистити себе і всіх інших користувачів у вашому будинку або офісі від злому. Перший крок - розглянути тип безпеки вашого Wi-Fi.[3]

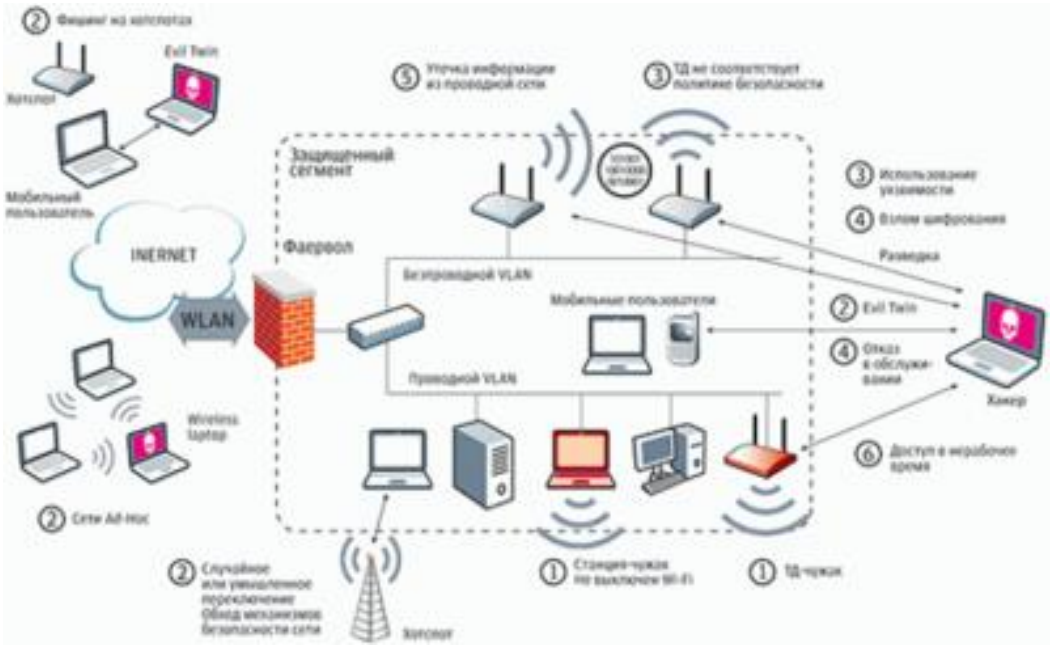


Рисунок 1.1 – Загрози в мережах Wi-Fi

Якого типу безпеки має ваш WiFi? Перший крок до того, як убезпечити мережі Wi-Fi від неавторизованих користувачів, - перевірити тип безпеки, який використовується вашої Wi-Fi. Примітно, що існує як мінімум чотири бездротових протоколу, які включають в себе: Wired Equivalent Privacy (WEP) Захищений доступ Wi-Fi (WPA) Захищений доступ Wi-Fi 2 (WPA 2) Захищений доступ Wi-Fi 3 (WPA 3) Перш ніж ми зможемо детально вивчити згадані вище бездротові протоколи, важливо навчитися визначати тип використовуваної бездротової безпеки. [4]

Пам'ятайте, що тип вашої бездротової мережі буде WEP, WPA, WPA2 або WPA3.Нижче наведено відомості перевірці типу використовуваної бездротової безпеки: Зайдіть в налаштування підключення Wi-Fi на вашому телефоні У

списку доступних мереж знайдіть свою конкретну бездротову мережу.[5] Однак більш простий спосіб перевірки на шифрування - використовувалася програма, відомого як NetSpot, яке вважається кращим в галузі. Після того, як ви визначили тип безпеки вашого Wi-Fi, ви повинні переконатися, що він використовує ефективний бездротової протокол.

Що таке бездротові протоколи безпеки? Бездротові протоколи призначені для захисту бездротових мереж, які використовуються в будинках і будівлях інших типів, від хакерів і неавторизованих користувачів. Як згадувалося раніше, існує чотири протоколи безпеки бездротової мережі, кожен з яких відрізняється за силою і можливостями. Бездротові протоколи також шифрують особисті дані, що передаються по радіохвилях.[6] Це, в свою чергу, захищає ваші особисті дані від хакерів і ненавмисно захищає вас. Нижче докладно розглядається тип бездротових протоколів, про які повинен знати кожен: Wired Equivalent Privacy (WEP): це перший протокол безпеки бездротового зв'язку, коли-небудь розроблений. Незважаючи на те, що він був розроблений в 1997 році, він все ще використовується сьогодні.[7] Незважаючи на це, він вважається найбільш уразливим і найменш безпечним протоколом безпеки бездротової мережі. Захищений доступ Wi-Fi (WPA): цей бездротової протокол безпеки передує WEP. [8]

Отже, він призначений для усунення недоліків, виявлених в протоколі WEP. Зокрема, для шифрування використовується протокол інтеграції тимчасового ключа (TKIP) і попередній ключ (PSK). Захищений доступ Wi-Fi 2 (WPA 2): WPA 2, наступник WPA, володіє розширеними функціями і можливостями шифрування.[9] Наприклад, WPA 2 використовує протокол коду аутентифікації ланцюжка повідомлень (CCMP) шифрувального режиму лічильника замість (TKIP). Відомо, що ця функція заміни ефективна при шифруванні даних.

Отже, WPA 2 вважається кращим протоколом безпеки бездротової мережі. Захищений доступ Wi-Fi 3 (WPA 3): це недавній бездротової протокол. Він поліпшений з точки зору можливостей шифрування і захисту хакерів від приватних і загальнодоступних мереж. З огляду на вищенаведену інформацію, було б краще переконатися, що ваш бездротової протокол є WPA 2 або WPA 3. [10]Якщо це не так, ви можете легко змінити свій протокол Wi-Fi на WPA 2. Ніколи не використовуйте WEP для шифрування вашого бездротова мережа, так як вона дуже слабка і неефективна в кращому випадку. Тепер, з огляду на все вищесказане, нижче наведені кращі поради з безпеки WiFi. Перевірка шахрайських точок доступу Wi-Fi. Шахрайські точки доступу представляють серйозну загрозу безпеці, оскільки вони забезпечують доступ для хакерів.[11] Кращий спосіб - провести опитування сайтів Wi-Fi у вашому будинку або в будівлі компанії. Краще додаток для цього - додаток NetSpot.

Ця програма не тільки виявляє шахрайські точки доступу, а й ефективно позбавляється від них. Посилення шифрування Wi-Fi: щоб посилити шифрування Wi-Fi, вам необхідно ідентифікувати бездротової протокол, як ми бачили вище. Використання NetSpot допоможе визначити ваш тип шифрування. Безпечний пароль WPA 2: Змініть пароль WPA 2 на щось непомітне. Щоб переконатися, що ваш пароль надійний, використовуйте різні символи і цифри. Приховати ім'я мережі. Ідентифікатор вашого набору служб або SSID часто налаштований на передачу імені вашої бездротової мережі. Це збільшує вашу вразливість. Ви можете легко переключитися на «прихований», що ускладнить для кого-небудь підключення до нього, якщо вони не знають тоді назва вашої бездротової мережі.

Наступною моделлю оцінки функціональної безпеки є GERT-модель.

Дана модель описана не так явно, як МНК. Тому для її розуміння слід визначити комплекс понять.

Для того, щоб краще зрозуміти, які саме властивості ми будемо оцінювати, розглянемо структуру і взаємозв'язок атрибутів надійності, ІБ і ФБ.

Почнемо з визначення надійності.Надійність - це властивість об'єкта зберігати в часі у встановлених межах значення всіх параметрів, що характеризують здатність виконувати необхідні функції в заданих режимах і умовах застосування, технічного обслуговування, зберігання і транспортування.Це можна продемонструвати у вигляді простої схеми.Для системи задається термін служби, і граничні значення параметрів.Поки параметри знаходяться в заданих межах, система працездатна і навпаки, якщо параметри вийшли за значення меж, то відбулася відмова (Малюнок 1.2).

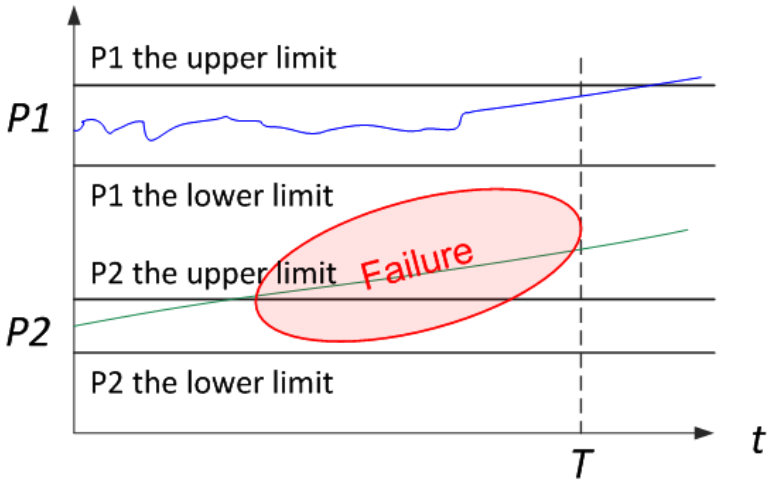


Рисунок 1.2 – Графічна інтерпретація визначення надійності

Про співвідношення властивостей dependability та reliability слід сказати окремо, оскільки в області стандартизації цієї властивості західна і радянська наука свого часу пішли кілька різними шляхами.Коректний переклад терміна надійність - це dependability, оскільки і надійність, і dependability розглядаються, як комплексні властивості.Reliability - це правильний переклад для терміна безвідмовність, яка є важливою, але все ж тільки однією зі складових надійності.Безвідмовністю називається властивість об'єкта безупинно зберігати

працездатний стан протягом деякого часу або напрацювання, тобтобезвідмовність можна узагальнювати з надійністю тільки для необслуговуваних систем.

Крім безвідмовності, складовими властивостями надійності є ремонтопридатність (Maintainability), довговічність (Durability) і збереженість (Storability). Готовність (availability) є комбінацією безвідмовності і ремонтопридатності.

Підкреслимо, що ми розглядаємо саме випадкові відмови апаратних засобів, до яких може бути застосований математичний апарат теорії ймовірностей.Теорія надійності дає практичну картину світу, в якій можна будувати надійні системи з не цілком надійних компонентів (як правило, методами резервування і діагностування).По-іншому йде справа з систематичними відмовами, які, очевидно, не можуть бути описані в рамках теорії надійності.Саме такі відмови складають найбільшу проблему, оскільки вони непередбачувані.У 1980-90-і роки були спроби застосувати імовірнісні моделі для оцінювання надійності програмного забезпечення, помилок оператора, а потім і показників ІБ.До теперішнього моменту цей шлях не дав практичних результатів.

Ще одним підходом до аналізу атрибутів надійності є так званий RAMS підхід, який розшифровується, як Reliability (безвідмовність), Availability (готовність), Maintainability (ремонтопридатність), andSafety (безпека).Іноді до цієї четвірки атрибутів додається ще і Integrity, інтегрованість або повнота, бо саме так це слово перекладається в російськомовній версії МЕК 61508. Найбільш простими визначеннями для цих властивостей є:

- Готовність - це придатність до правильної експлуатації;
- Безвідмовність - це безперервність правильного обслуговування;
- Ремонтопридатність - це здатність піддаватися модифікаціям і ремонту.

- Безпека - це відсутність катастрофічних наслідків для користувача та навколишнього середовища;

- Інтегрованість - це відсутність неналежних системних змін.

Security (ІБ) являє собою сукупність атрибутів конфіденційності, інтегрованості і готовності (так звана тріада CIA).Готовність або доступність розглядається для авторизованих дій щодо доступу до інформації, а інтегрованість розглядається для коректної роботи з даними, що виключає їх неавторизоване зміна.Конфіденційність є додатковим, в порівнянні з надійністю, атрибутом, який означає відсутність несанкціонованого розкриття інформації.Таким чином, найпростіша модель, що описує dependability (тобто надійність) і security (тобто інформаційну безпеку) представлена всього шістьма атрибутами (Малюнок 1.3).

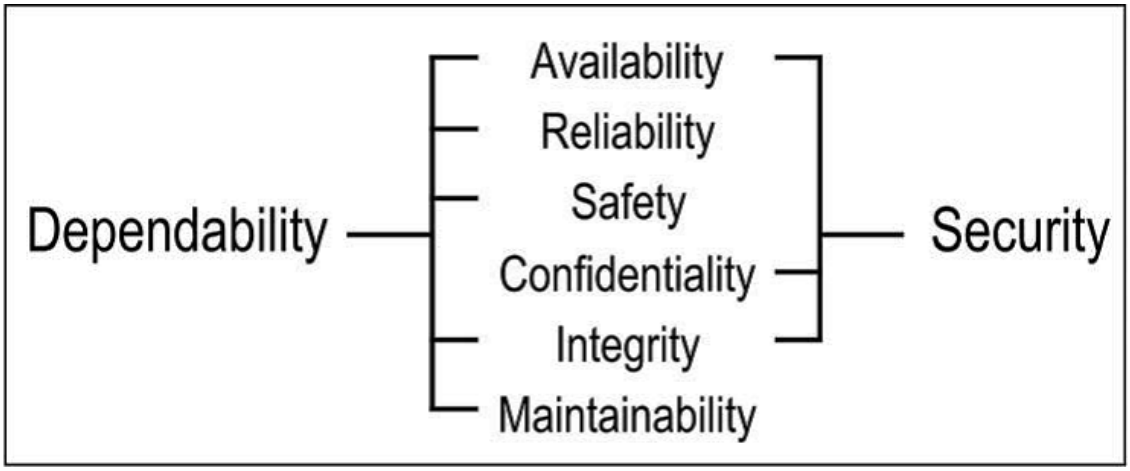


Рисунок 1.3 – Атрибути RAMS & CIA

Тепер зробимо ще одну ітерацію і спробуємо уявити всі відомі нам атрибути у вигляді однієї діаграми (Малюнок 1.4).

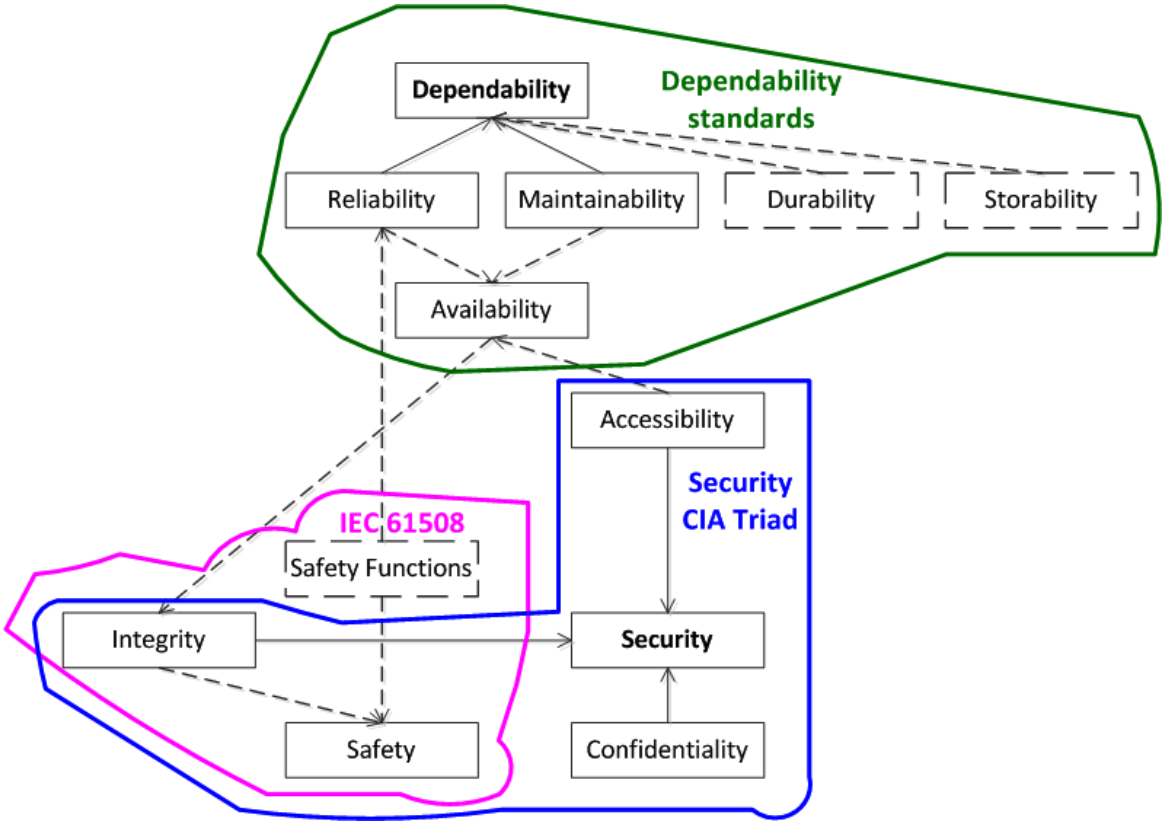


Рисунок 1.4 – Узагальнена таксономія атрибутів надійності, інформаційної та функціональної безпеки

Звичайними лініями відзначені атрибути та зв'язку, відповідні тільки що розглянутої моделі з шести атрибутів.Пунктиром додані додаткові атрибути.Одна з груп атрибутів відноситься до складових надійності (dependability).ФБ (Safety), згідно з МЕК 61508, включає safetyfunctions&integrity, причому, через функції безпеки ФБ пов'язана з безвідмовністю, готовністю і надійністю, а інтегрованість виконання функцій забезпечує цілий ряд властивостей, в тому числі, ІБ.Таким чином, між атрибутами надійності, ІБ і ФБ існують взаємний вплив і певні зв'язки, які ми будемо враховувати при кількісному оцінюванні.

Аналіз ризиків і показники функціональної безпеки

Тепер звернемося до показників безпеки. Базовим поняттям і показником ФБ є ризик, що представляє собою комбінацію ймовірності небажаного події та її наслідків.

Оцінювання ризиків буває кількісним і якісним, при якісному оперують такими категоріями, як «високий», «середній», «низький» і т.д.

Якщо небажана подія і збиток від нього зафіксовані, то ризик стає чисельно дорівнює ймовірності P (t) виникнення фіксованого шкоди.Наприклад, ризик аварії атомної електростанції з викидом радіоактивних речовин в атмосферу на сьогоднішній день встановлюється не більше, ніж 10^{-7} 1 / рік.

Широке поширення для оцінювання та управління ризиками отримав так званий принцип ALARA (ALARP) (aslowasreasonablyapplicable / practicable) - підхід до управління ризиком, який має на увазі його максимально можливе зниження, що досягається за рахунок реальних (обмежених) ресурсів (Малюнок 1.5).

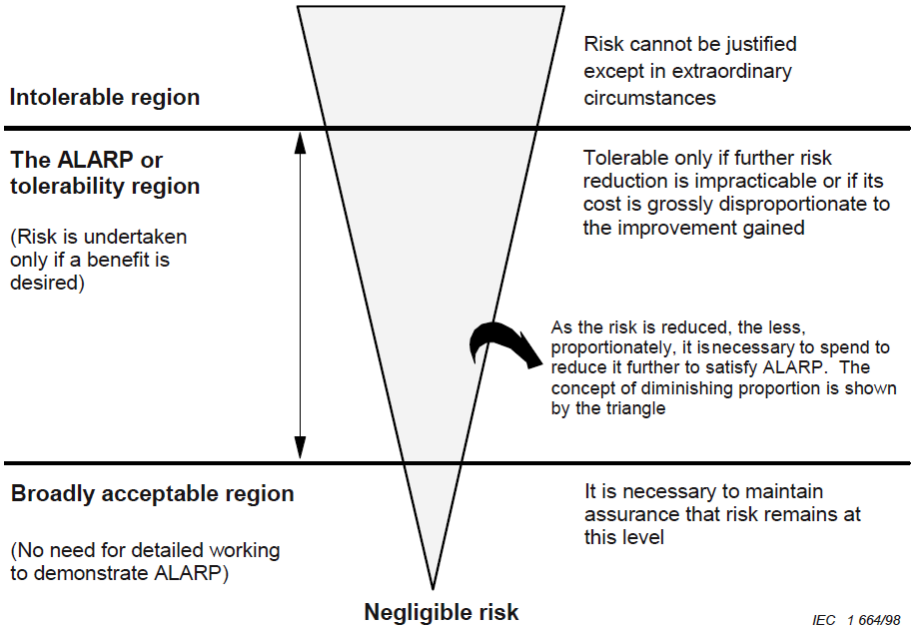


Рисунок 1.5 – Зниження ризику на основі методу ALARP (aslowasreasonablypracticable), IEC 61508-5

Зручною моделлю є граф ризиків (Малюнок 1.6).Приклад узятий із стандарту з безпеки промислового обладнання (EN ISO 13849-1 Safetyofmachinery - Safety-relatedpartsofcontrolsystems - Part 1: Generalprinciplesfordesign).Крім ймовірності і наслідків подій врахована ще можливість уникнення небезпек і шкоди.Ці три категорії мають високе і низьке значення, в результаті отримуємо шість комбінацій, кожна з яких відповідає тому або іншому PerformanceLevel (PL), від a до e, який є аналогом SafetyIntegrityLevel (SIL).

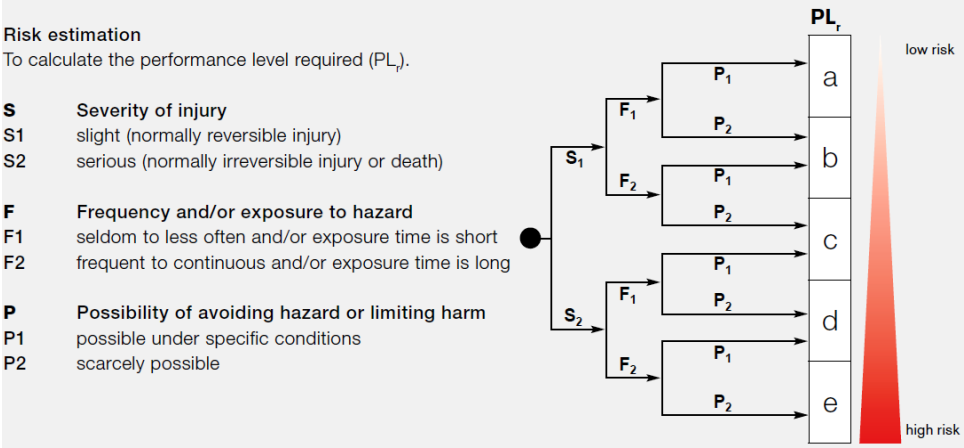


Рисунок 1.6 – Граф ризиків, EN ISO 13849-1

Такий якісний підхід до оцінювання ризиків, тепер розглянемо, як в МЕК 61508 нормуються кількісні значення показників безпеки.Якщо розглядати системи управління, то подіями, пов'язаними з ризиком, є відмови функцій безпеки, тому логічно, що в якості показників безпеки обрані ймовірності відмов для функцій безпеки.

Повернемося до базових понять теорії надійності.Теорія надійності є прикладною областю теорії ймовірностей, де в якості випадкової величини розглядається час до відмови системи.

Одним з найважливіших показників є ймовірність безвідмовної роботи, під якою розуміється ймовірність того, що відмова не відбудеться за встановлений час MTTF, зване напрацюванням до відмови: P (t) = P {MTTF> t}.Як і будь-яка ймовірність, ймовірність безвідмовної роботи приймає значення від 1 до 0, причому одиниці вона дорівнює в початковий момент часу, а нулю дорівнює при часу прагне до нескінченності.

Ймовірністю відмови називається ймовірність того, що відмова відбудеться за встановлений час T, тобтоймовірність відмови доповнює ймовірність безвідмовної роботи до одиниці (відмова або станеться, чи ні, тобто маємо повну групу подій): F (t) = 1 - P (t).

Інтенсивність відмов - умовна щільність розподілу (тобто похідна по часу) напрацювання до відмови за умови, що відмова не стався, має розмірність 1 / год:

(T) = f (t) / P (t) = - [1 / P (t)] • [dP (t) / dt] = - [1 / (1 - F (t)] • [dF (t / dt].

При статистичній оцінці інтенсивність відмов визначається як відношення кількості відмовили однотипних виробів до тривалості інтервалу часу, на якому ці відмови спостерігалися (наприклад, якщо за 1000 годин відмовило 10 виробів, то= 10/1000 = 0,01 1 / год).

Важливим припущенням теорії надійності є застосування так званого експоненціального розподілу часу до відмови, коли інтенсивність відмов вважається постійної в часі.

Напрацювання до відмови MTTF обчислюється як певний інтеграл в межах від нуля до нескінченності для ймовірності безвідмовної роботи за часом:

$$MTTF = \exp \int_0^\infty t \cdot f(t) \mathrm{d}t = \int_0^\infty P(t) \mathrm{d}t$$

Іноді MTTF трактується як середнє або гарантований час роботи системи, але це не так, оскільки ймовірність безвідмовної роботи в момент часу MTTF дорівнює 1 / e, що приблизно дорівнює 0,37. Це означає, що для одиничного

пристрою ймовірність того, що пристрій залишиться в працездатним по закінченню MTTF становить всього лише 0,37. Для групи однотипних пристроїв це означає, що тільки 37% з них залишиться працездатним по закінченню MTTF.

Коефіцієнт готовності (availability) - це ймовірність того, що об'єкт виявиться в працездатному стані в довільний момент часу, крім запланованих періодів, протягом яких застосування об'єкта за призначенням не передбачається. Розраховується коефіцієнт готовності, як відносини напрацювання до відмови від суми напрацювання до відмови (MTTF) і середнього часу відновлення після відмови (MTTR):

$$A = MTTF / (MTTF + MTTR).$$

Для розуміння співвідношення між надійністю і безпекою звернемося до класифікації відмов, розглянутої в МЕК 61508 (Малюнок 1.7). Відмови можуть бути небезпечні і безпечні, а також діагностуються і недіагностіруемие.В рамках надійності розглядаються всі види відмов.З точки зору безпеки нас цікавлять тільки небезпечні відмови, причому важливо, щоб такі відмови були діагностуються, і при їх виявленні система могла перейти в безпечний стан.

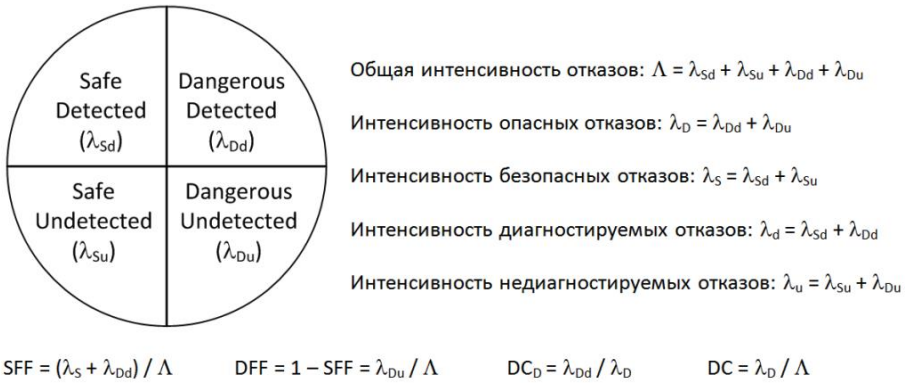


Рисунок 1.7 – Класифікація відмов і показники безпеки згідно IEC 61508

МЕК 61508 говорить про наступних показниках безпеки.

По-перше, це так звана стійкість до апаратних відмов (HardwareFaultTolerance, HFT). Це дуже простий показник, який говорить про те, скільки може статися апаратних відмов в системі до виходу її з ладу.По суті, це еквівалентно кількості додаткових резервних каналів.Тобто, якщо система нерезервованої, то будь-яка відмова виводить її з ладу, HFT = 0. Якщо в система два резервних каналу, то один з них є додатковим, надмірною.Після одиничного відмови система залишиться працездатне, тобтоHFT = 1, і т.д.

По друге, повинна бути визначена частка безпечних відмов (SafeFailureFraction, SFF). У термінах МЕК 61508 це відношення інтенсивності безпечних і небезпечних діагностованих відмов до сумарної інтенсивності відмов (див. Малюнок 2.6). Виходить, що в термінах МЕК 61508 враховуються, в першу чергу небезпечні недіагностіруемие відмови, а небезпечні діагностуються відмови в частці безпечних відмов відносяться до безпечних.

Відповідно, може бути визначена частка небезпечних відмов (DangerousFailureFraction, DFF), яка доповнює частку безпечних відмов до одиниці і розраховується, як відношення інтенсивності небезпечних недіагностіруемих відмов до сумарної інтенсивності відмов (див. Малюнок 2.6).

Діагностичне покриття (DiagnosticCoverage, DC $_{D)}$ в МЕК 61508 визначається тільки виходячи з інтенсивності небезпечних відмов, це відношення інтенсивності небезпечних діагностованих відмов до інтенсивності небезпечних відмов (див. Малюнок 1.7).

У технічній діагностиці більш звичним є підхід, коли діагностичне покриття (DC) визначається, як відношення інтенсивності діагностованих відмов до сумарної інтенсивності відмов (див. Малюнок 2.6). Однак, МЕК 61508 декларує діагностичне покриття, виходячи з частки зменшення ймовірності небезпечних відмов за рахунок вбудованого діагностування.

Виходячи з отриманого значення частки безпечних відмов (SafeFailureFraction) може бути визначено максимально досяжний рівень повноти безпеки SIL, в залежності від резервованої або нерезервованої конфігурації (Малюнок 2.8).

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Рисунок 1.8 – Максимально досяжний рівень SIL, виходячи з показників SafeFailureFraction (SFF) і HardwareFaultTolerance (HFT), IEC 61508-2

Наприклад, для частки безпечних відмов 90% -99% для нерезервованої конфігурації (HFT = 0) може бути досягнутий максимальний рівень повноти безпеки SIL2. У дубльованої системі (HFT = 1) може бути досягнутий SIL3, а в троірованной - SIL4 (HFT = 2).Зазвичай такий підхід застосовують розробники ПЛК та іншого обладнання для керуючих систем безпеки. Стійкість до випадкових відмов апаратних засобів відповідає рівню SIL2 для нерезервованої конфігурації і рівню SIL3 для дубльованої конфігурації. Однак, слід пам'ятати, що при цьому стійкість до систематичних відмов, обумовлена реалізацією процесів життєвого циклу також повинна відповідати рівню SIL3.

Ще однією градацією, встановленої в МЕК 61508, є поділ обладнання на типи A і B (Type A &Type B). До типу A відносяться найбільш прості, переважно механічні та електричні компоненти.Всі програмовані електронні компоненти відносяться до типу B.

Крім розглянутих вимог, існують ще вимоги до чисельним значенням показників безпеки.

З базових визначень МЕК 61508 згадаємо, що існує три режими роботи обладнання: з низькою частотою запитів (lowdemandmode), в якому частота запитів на виконання функції безпеки не перевищує одного в рік, з високою частотою запитів (highdemandmode), в якому частота запитів на виконання функції безпеки перевищує один на рік, і безперервний режим (continuousmode). Виявляється, що МЕК 61508 рекомендує різні показники надійності для цих режимів.

Для систем, що працюють з низькою частотою запитів, як цільового показника повинна бути визначена середня ймовірність небезпечного відмови виконання функції безпеки за запитом (Малюнок 2.8). Для рівняповноти безпеки SIL1 цей показник не повинен перевищувати 0,1.3 підвищенням SIL кожен раз ймовірність небезпечного відмови повинна зменшуватися в 10 разів.Таким чином, для рівня повноти безпеки SIL4 ймовірність небезпечного відмови повинна складати від 10^{-5} до 10^{-4}.

Якщо провести паралель з вже розглянутими нами показниками, то цей показник еквівалентний коефіцієнту неготовність, тобтодоповненню коефіцієнта готовності до одиниці.

Safety integrity level (SIL)	**Average probability of a dangerous failure on demand of the safety function (PFD_{avg})**
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Рисунок 1.9 – Залежність рівня SIL від значення середньої ймовірності небезпечного відмови виконання функції безпеки за запитом (режим з низькою частотою запитів), IEC 61508-1

Для систем, що працюють з високою частотою запитів або в безперервному режимі, визначається середня частота (або інтенсивність) небезпечних відмов функції безпеки (Малюнок 1.10).Для рівняповноти безпеки SIL1 цей показник не повинен перевищувати 10^{-5} 1 / год, що еквівалентно одному відмови в 11,4 років.З підвищенням SIL кожен раз інтенсивність небезпечного відмови повинна зменшуватися в 10 разів.Для рівняповноти безпеки SIL4 інтенсивність небезпечного відмови повинна складати від 10^{-9} до 10^{-8} 1 / год, тобто, не частіше, ніж один відмову в 11 400 років.Звичайно, для одиничної системи це звучить дещо абсурдно, але, якщо врахувати, що в світі експлуатуються тисячі однотипних систем, то навіть з такою низькою інтенсивністю відмов небезпечні відмови є цілком вірогідними, що ми спостерігаємо в дійсності.

1.2.Огляд існуючих стандартів безпеки інформації

SIEM - об'єднання двох визначень, значущих область застосування програмного забезпечення: SEM - управління подіями безпеки і SIM - управління інформаційною безпекою. SIEM системи забезпечують аналіз подій безпеки, що виходять з додатків і мережевих пристроїв в реальному часі. SIEM складається з додатків, приладів, послуг, а так само використовується для журналирования даних. [1]

Подібні системи допоможуть вирішити такі завдання:

- Консолідація та зберігання журналів подій від різних джерел - мережевих пристроїв, журналів ОС, додатків і СЗІ.

- Надання інструментів для аналізу подій і розбору інцидентів.
- Кореляція і обробка за правилами.
- Автоматичні сповіщення і інцидент-менеджмент.
- При наявності сканера вразливостей, система частково допоможе оцінити ризики. [2]

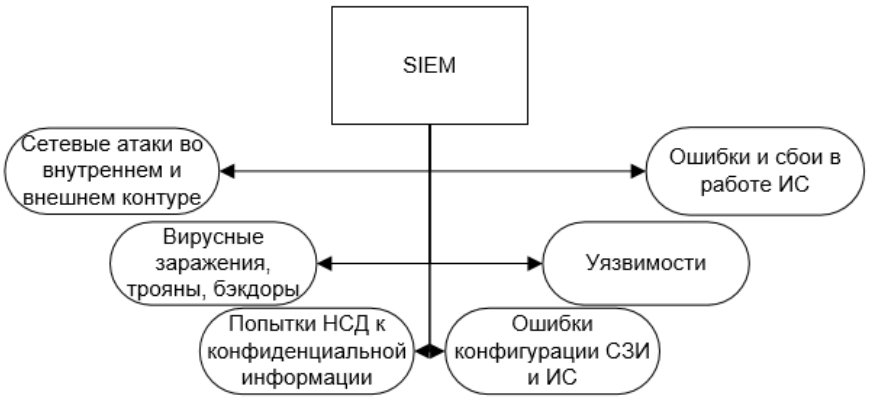


Рис. 1.10

Системи збору і кореляції подій універсальні за рахунок своєї логіки, але для того, щоб домогтися від них очікуваного результату, необхідні корисні джерела і правила кореляції подій. Будь-яка подія (наприклад, з DLP системи) може бути подано на вхід системи і використано.

Найчастіше подібні системи складаються з декількох компонентів:

– Агенти, що встановлюються на контрольовану систему і відправляють дані на сервер

– Корелятори на агентах, є модулями для розуміння конкретного журналу подій

– Сервери-корелятори, виробляють попередню акумуляцію подій від безлічі інспектованих джерел

– Сервер-коррелятор, що відповідає за збір інформації з корреляторов і агентів, і обробку за заданими правилами і алгоритмами

– Сервер БД і сховища, який відповідає за зберігання журналів подій [3]

Дані про події збираються від джерел за допомогою агентів, або віддалено. У разі віддаленого збору подій виникає навантаження на мережу і джерело подій, тому що деякі системи не дозволяють передати тільки ті події, які ще не були передані, і передають весь журнал подій, що складається їх великої кількості інформації.

SIEM здатний корелювати:

– Загрозу, описану правилами.

– Загрозу на базі загального шаблону.

– Аномалію в разі відключення бази накопиченої статистики.

– Відхилення від принципу «все, що не дозволено - заборонено».

– Причинно - наслідковий зв'язок, якщо використовуються окремі алгоритми (CBR, GBR, statistical, Bayesian). [4]

SIEM системи автоматично об'єднують і узгодять собою події ІБ, отримані від різний захисних пристроїв, дозволяючи аналітикам зосередитися на більш складних критичних завданнях. На даний момент не існує універсальних систем виявлення і запобігання вторгнень. Так як всі захисні рішення мають свої слабкості і переваги, а все що захищаються ресурси і інформаційні системи вкрай різноманітні. Системи виявлення вторгнень можна комбінувати і цим самим підвищувати працездатність системи безпеки в цілому, але в силу свого різноманітності системи виявлення можуть видавати різну вихідну інформації в плані рівня тривожності, так як він пов'язаний з рівнем конфіденційності інформації, що захищається.

Вторгнення відбувається тоді, коли зловмисник намагається потрапити в захищається систему або неправильно використовувати її. Термін «неправильно використовувати» може тлумачитися по-різному і відноситься до багатьох дій, починаючи з розкриття конфіденційної інформації і закінчуючи банальною

розсилкою спаму. Наприклад, більшість тривожних подій, що генеруються системами контролю доступу до ресурсів на серверах і комп'ютерах персоналу, не відображають безпосередньо атаки. Вони описують дії користувача, який працює з захищеними ресурсами, тому при аналізі ситуації ми повинні враховувати контекст, в якому з'явилися тривожні події. Розглянемо деякі з них:

– Подія «це наслідок неправильного введення паролю» дуже часто виникає у всіх системах, тому має ігноруватися, однак якщо воно багаторазово відбувалося в неробочий час компанії, має бути створено попередження високого рівня.

– Якщо дивна поведінка, користувача виявлено на одному сервері, то це може і швидше за все, є помилковою аномалією і може бути проігноровано. Однак якщо ж це відбувається на декількох серверах, то хтось явно досліджує мережу (наприклад, перегляд портів)

– У деяких комп'ютерних системах подія класу «не вдалося увійти в систему» може відбуватися багато разів в день, в той час як в інших середовищах таких подій не повинно бути взагалі.

Вище були описані деякі події, які є найменшою частиною даних про виявлення вторгнення. Події, обов'язково потрібно запротоколювати. Після, ці дані будуть брати участь в трьох стадіях протидії вторгненням:

– виявлення

– реакція

– Запобігання [5]

Система кореляції отримує інформацію на всіх цих стадіях і об'єднує її з раніше заданими алгоритмами. Це робить процес виявлення керованим і постачає необхідними відомостями для майбутнього запобігання і відповідної реакції. Варто відзначити, що кореляція подій на великому підприємстві - трудомістке завдання по обробці великих обсягів даних. Для таких випадків створюються

автоматизовані системи, які допоможуть об'єднати велику кількість інформації, позбутися від надлишку даних, знайти потрібні події і діяти, спираючись на зібраний матеріал. Кожна така задача може бути виконана системою збору та кореляції подій інформаційної безпеки.

На основі даних кореляції, виробленої під час появи події, може бути заборонений доступ до атакованому пристрою, таким чином, збиток від вторгнення буде знижений. Без централізованого управління системою і механізмами кореляції, практично неможливо визначити вид атаки, оцінити адекватність системи захисту і вжити заходів в реальному часі. Найбільш ефективною, система буде в тому випадку, коли системи виявлення вторгнення, міжмережеві екрани, системи мережевого захисту і системи безпеки додатків будуть працювати разом і спільними діями будуть зменшувати ризик виникнення, проведення і реалізації загроз. Такі рішення здійснюють функції:

- Отримує інформацію від одного або декількох джерел
- Обробляє повідомлення, грунтуючись на їх характеристиках
- Обробляє повідомлення, грунтуючись на правилах їх кореляції
- Зберігає повідомлення в реляційної базі даних

Побудова ланцюжка проходження подій.

Кореляція досить корисна при виявленні порушень режиму безпеки, так як ці інциденти являють собою ряд подій, що відбуваються в різних "сенсорних" точках мережі. Даний процес характеризується взаємозв'язками "багато до одного" (тобто майже всі події від величезного числа сенсорів говорять про одне нападі). У порівнянні з мережевим керуванням, в якому, зазвичай, використовуються відносини виключення подій (потрібні - непотрібні) або взаємозв'язку "один до одного", управління захистом інформації набагато складніше. Проникнення зазвичай залишає сліди в різних точках мережі і в різній тимчасовій послідовності. Знаходячи ці всі сліди, фахівці, що займаються

інформаційною безпекою, зуміють знайти і з високим ступенем надійності запобігти нападу.

Тому, слідуючи людській логіці, потрібно так само вчинити і в разі створення SEM-системи. Після того як всі дані будуть отримані і оброблені в єдиній БД, потрібно розібратися, як і в якій черговості дані події з'являються, щоб з їхсукупностізмоделюватиодиночну подію вторгнення.

Механізм прийняття рішень

Наступним етапом у створенні SIEM системи є побудова механізму прийняття рішень. На цьому кроці адміністратор ІБ вже має уявлення, як виглядає схема проходження атаки, яких видів і в який час з'являються події, він має шаблони різних ситуацій. Тепер, спираючись на накопичену інформацію, треба впровадити в систему шаблони прищепив прийняття рішень. Наприклад: якщо ви отримали кілька повідомлень типу «доступ до внутрішніх адресами» від маршрутизатора, що виходить у зовнішній контур, а пізніше з'явилося повідомлення типу «заборонений порт» від МЕ, то потрібно чекати повідомлень «атака, типу сканування портів» від СОВ.

На цьому етапі виробляється рішення, яке пов'язує набір помічених дій з певним інцидентом, а так само присвоює йому класифікацію, щодо методів нападу Проблемами при допущенні помилок на даному етапі можуть бути:

– Падіння продуктивності системи

– Ризик обходу умов моніторингу

– Упущення в описі можливих ситуацій Падіння продуктивності системи

Першою небезпекою, що виникає при неналежному підході до реалізації механізму прийняття рішень, є зниження продуктивності. Включення будь-якого правила може викликати спад швидкодії системи. Не будемо забувати, що в системах, побудованих на сигнатурному підході, кожен, хто входить елемент

порівнюється з шаблонами, тому потрібно відповідально підходити до процесу створення бази шаблонів. При збільшенні входять даних або кількості правил, швидкість роботи програми знаходиться під загрозою.

Ризик обходу умов моніторингу.

Друга важлива проблема в кореляції подій: Комп'ютери поки не можуть оцінювати вірогідність схожості тих чи інших подій з їх збереженими шаблонами.

Упущення в описі можливих ситуацій

Ясна річ, що служба безпеки повинна описати стільки правил, скільки необхідно, але кількість подій в мережі величезна, а кількість атак постійно зростає. Щоб знизилася не ймовірність таких помилок потрібно використовувати як мікро, так і макро кореляцію. Спільне використання цих технологій допоможе швидше виявити збійні ділянки ланцюгів проходження подій, некоректні правила і шаблони. Оптимальним варіантом є поєднання подій з різних джерел, наприклад: оцінка роботи кадру в мережі проводиться з урахуванням інформації, що надійшла з СКУД, тобто з урахуванням того, чи проходив він через КПП. Такі схеми набагато більш стійкі до помилок, ніж ті, які зіставляють меншу кількість подій від схожих джерел, наприклад: ME і IDS. Стадія реакції на вторгнення управління системоюзахистуздійснюється людьми, а, отже, схильне до помилок.

Автоматичний запуск програм, які повинні відповісти на виявлений напад (наприклад, заблокувати доступ до інформаційного ресурсу або відправити повідомлення про виявлення самому порушнику і т.п.) - найбільш активна реакція на виявлені атаки. Деякі системи можуть сприяти з мобільними телефонами та іншими засобами зв'язку, вміють подавати світловий і звуковий сигнал. Сучасні SIEM системи мають цими можливостями, але експериментувати потрібно дуже обережно, тільки переконавшись, що дії систем під контролем.

1.3. Постановка задачі

Вихідні дані для FMECA можуть бути отримані в результаті застосування таких методів, як структурні схеми надійності, аналіз дерева відмов і марковский аналіз.[2]

Моделей оцінки функціональної безпеки є близько десятка, однак, свою увагу зосередимо на двох: МНК та GERT-моделі. Згідно дослідження [6] саме ці дві моделі показали найменшу похибку оцінювання.

Розглянемо першу модель оцінки функціональної безпеки, МНК.

Під моделлю лінійної регресії будемо розуміти модель виду:

$$y = b_0 + b_1 x_1 + \cdots + b_k x_k + e,$$

де y - пояснюється ряд, $x_1, \ldots, x_k$ - пояснюють ряди, e - вектор помилок моделі, $b_0, b_1, \ldots, b_k$ - коефіцієнти моделі.

Для кожного коефіцієнта на панелі «ідентифікувати рівняння» обчислюється ряд статистик: стандартна помилка,t-Статистика,ймовірність значущості коефіцієнта. Остання є найбільш універсальною і показує, з якою ймовірністю видалення з моделі фактора, яке відповідає даному коефіцієнту, чи не виявиться значущим.

Відкриваємо панель і дивимося на останній рядок, адже він - саме той, хто відразу ж скаже нам про значущість коефіцієнтів.

Идентифицированное уравнение

Y = 276.1227 + 0.0097*X1 - 0.0152*X2 - 0.0000*X3

Коэффициент	Значение	Стандартная ошибка	t-статистика	Вероятность
константа	276.122716507	15.554266742	17.752216873	0.000000000
при X1 ({Data!Pax[t]})	0.009678849	0.000582394	16.619085776	0.000000000
при X2 ({Data!Mail[t]})	-0.015185883	0.004991216	-3.042521598	0.003172816
при X3 ({Data!Cargo[t]})	-0.000030856	0.000102065	-0.302317344	0.763194762

Факторів з великою ймовірністю незначущості в моделі бути не повинно.

Идентифицированное уравнение

Y = 276.6017 + 0.0097*X1 - 0.0158*X2

Коэффициент	Значение	Стандартная ошибка	t-статистика	Вероятность
константа	276.601740948	15.386319920	17.977121390	0.000000000
при X1 ({Data!Pax[t]})	0.009661595	0.000576330	16.763989663	0.000000000
при X2 ({Data!Mail[t]})	-0.015825170	0.004495700	-3.520068261	0.000711179

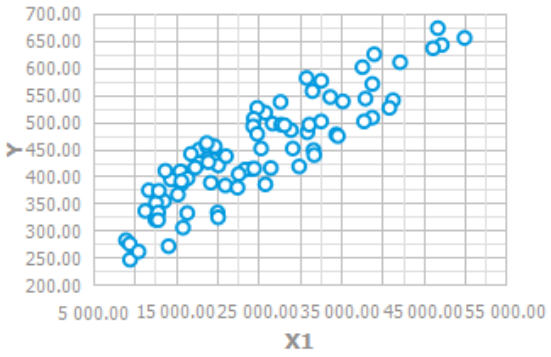
При виключенні останнього фактора коефіцієнти моделі практично не змінилися.

Панель «Кореляція чинників» містить матрицю кореляції між усіма змінними моделі, а також будує хмара спостережень для виділеної пари значень.

Корреляция факторов

	Y	X1	X2
Y	1.0000	0.8879	0.4235
X1	0.8879	1.0000	0.6244
X2	0.4235	0.6244	1.0000

Умеренная взаимосвязь
Сильная взаимосвязь
X1 - {Data!Pax[t]}
X2 - {Data!Mail[t]}



Коефіцієнт кореляції показує силу лінійної залежності між двома змінними. Він змінюється від -1 до 1. Близькість до -1 каже про негативну лінійної залежності, близькість до 1 - про позитивну.

Хмара спостережень дозволяє візуально визначити, чи схожа залежність однієї змінної від іншої на лінійну.

Якщо серед чинників зустрічаються сильно корелюють між собою, виключіть один з них. При бажанні замість моделі звичайної лінійної регресії ви можете побудувати модель з інструментальними змінними, включивши в список інструментальних виключені з-за кореляції чинники.

Висновок до першого розділу

Підіб'ємо підсумки і представимо перелік перевірених характеристик у вигляді таблиці:

	Линейная регрессия (оценка МНК)	Линейная регрессия (метод инструментальных переменных)	Модель бинарного выбора	Нелинейная регрессия
Проверка значимости каждого фактора	t-статистика и её вероятность	t-статистика и её вероятность	z-статистика и её вероятность	t-статистика и её вероятность
Проверка корреляции факторов	матрица корреляции	матрица корреляции	матрица корреляции	-
Проверка критериев качества	R2, Adj R2	R2, Adj R2	McFadden R2	R2, Adj R2
Проверка значимости всех факторов	F-статистика и её вероятность	F-статистика и её вероятность, J-статистика и её вероятность	LR-статистика и её вероятность	F-статистика и её вероятность
Сопоставление сравнительных критериев	SSR, LogL	SSR, LogL	LogL	SSR
	AIC, SC, HQ	AIC, SC, HQ	AIC, SC, HQ	AIC, SC, HQ
Анализ остатков	DW	DW	DW	DW

2. МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

2.1. Вразливості інформації

2.1.1.Прямі загрози або способи злому

Основні норми функціональної безпеки створюваних електричних, електронних та електронних програмованих пристроїв та систем наведені у стандартах МЕК 61508 та МЕК 61511. Особливістю цих стандартів є ризик-орієнтований підхід. Залежно від шкоди, яка може бути завдана техногенними об’єктами (до яких відносяться БСМ) життю або здоров’ю людини чи зовнішньому середовищу, встановлюються відповідні рівні ризику (рис. 3.1). Для зменшення рівня ризику передбачено комплекс заходів, які регламентовано стандартами МЕК 61508 та МЕК 61511.

Сімейство стандартів МЕК 61508 містить сім частин (рис. 3.2). Як випливає з рис. 2, перша частина стандартів МЕК 61508 охоплює загальні вимоги до систем, які відповідають за безпеку системи. Друга частина охоплює пов'язані з безпекою вимоги до електричних, електронних та електронних програмованих систем. Третя частина визначає вимоги до ПЗ. Четверта частина містить основні терміни та визначення, які стосуються функціональної безпеки. П'ята частина включає приклади методів визначення рівнів повноти безпеки (safety integrity level – SIL). Шоста частина є настановою застосування методів, які викладені в другій та третій частинах. В сьомій частині наведено огляд і приклади технічних і організаційних заходів, спрямованих на забезпечення функціональної безпеки створюваного виробу (у нашому випадку БСМ).

Слід зазначити, що всі системні функції, які регламентовано цими стандартами, підтримуються БСМ.

БСМ – це багаторівневі розподілені мережі, побудовані за принципами самоорганізації, з великою кількістю сенсорів та виконавчих механізмів, які об’єднані радіоканалом (рис. 3.1) [2]. На основі БСМ реалізуються проекти, які виконані за технологією Інтернету речей, тобто об’єктів, які взаємодіють один з одним без участі людини. Широке впровадження технології Інтернету речей у

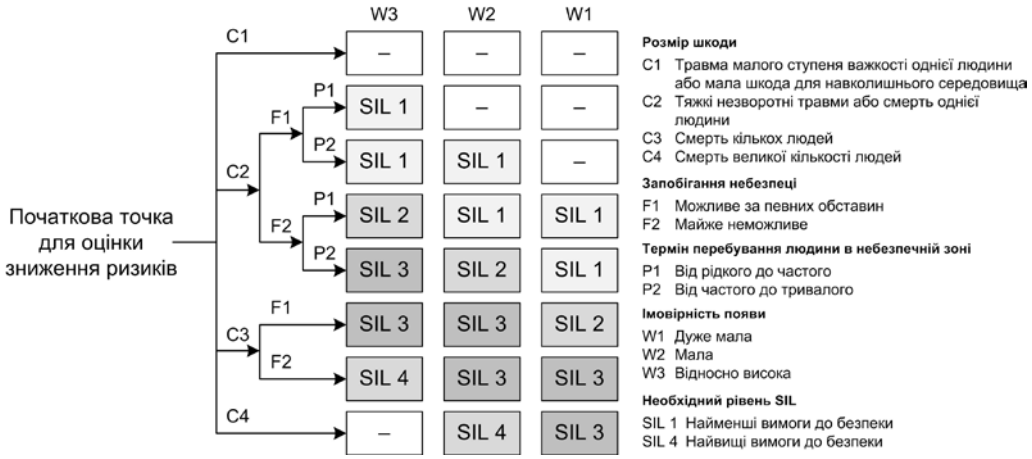


Рисунок 2.1 – Діаграма рівнів ризиків для оцінки функціональної безпеки

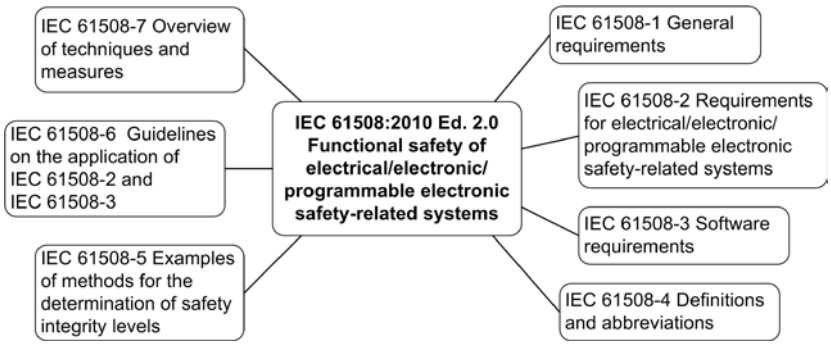


Рисунок 2.2 – Перелік міжнародних стандартів з функціональної безпеки сімейства МЕК 61508

Глобальні міжнародні проекти протягом останніх трьох років [3] свідчить про появу нового класу, так званих, кібер-фізичних об'єктів. У цих об’єктах засоби забезпечення надійності, функціональної та інформаційної безпеки повинні бути об’єднані у єдину систему. Зв'язок атрибутів, що відповідають за

надійність, функціональну та інформаційну безпеку, показано на діаграмі (Рис.2.4) [4].

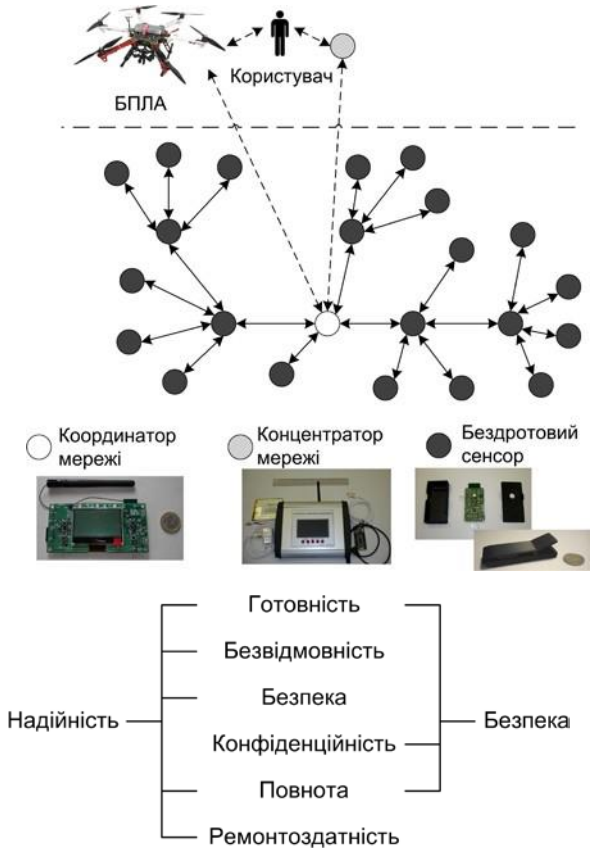


Рисунок 2.4 – Стандарт МЕК 61508 визначає чотири рівня повноти безпеки SIL – це рівні SIL 1, SIL 2, SIL 3

Базовим показником функціональної безпеки є ризик. Ризики за міжнародними стандартами можна оцінювати якісно або кількісно. Методи оцінки ризиків або оцінки рівнів повноти безпеки (SIL) наведені в стандарті МЕК 61508-5. Відповідно до цього стандарту функціональна безпека є ознакою систем, для яких відмова функції безпеки може привести до суттєвих втрат для людей та/або зовнішнього середовища. Властивість системи забезпечувати функцію безпеки визначається рівнем повноти безпеки SIL. Як випливає з SIL 4. Найвищим рівнем безпеки є рівень SIL 4, найменшим – рівень SIL 1. Для того,

щоб присвоїти створюваному виробу відповідний рівень безпеки SIL, використовують методи розрахунку, наведені в стандартах МЕК 61508 та МЕК 61511.

Якщо необхідний рівень безпеки SIL визначено, то здійснюють вибір засобів, які дозволяють забезпечити необхідну функцію безпеки у цілому.

Стандарт МЕК 61508 регламентує три режими роботи системи, яка підтримує функцію безпеки: з низькою частотою запитів (low demand mode), тобто частота запитів на здійснення функції безпеки у цьому режимі не перевищує одного на рік; з високою частотою запитів (high demand mode), тобто частота запитів на здійснення функції безпеки є більшою, ніж раз на рік; безперервний режим (continuous mode). Залежність рівня SIL від значення середньої імовірності небезпечної відмови у разі здійснення системою функції безпеки на запит для режиму з низькою частотою запитів (Average of the safety function – PFD_{AVG}) наведена у табл. 3.1. Одиницею виміру функції безпеки системи в режимі з високою частотою запитів є значення середньої інтенсивності небезпечних відмов функції безпеки (Average frequency of dangerous failure of the safety function [h^{-1}] – PFH). Залежність рівня SIL від цього параметра наведена у табл. 3.1.

Таблиця 2.1 – Залежність рівня SIL від значення PFD_{AVG} і PFH

Рівень SIL	Значення PFD_{AVG}	Значення PFH[h^{-1}]
4	від 10^{-5} до 10^{-4}	від 10^{-9} до 10^{-8} (одна відмова за 11 400 років)
3	від 10^{-4} до 10^{-3}	від 10^{-8} до 10^{-7} (одна відмова за 1 140 років)
2	від 10^{-3} до 10^{-2}	від 10^{-7} до 10^{-6} (одна відмова за 114 років)
1	від 10^{-2} до 10^{-1}	від 10^{-6} до 10^{-5} (одна відмова за 11,4 років)

Звичайно, забезпечувати рівень безпеки SIL 4 для однієї конкретної БСМ немає сенсу, але враховуючи те, що в світі працюють тисячі однотипних мереж,

то навіть при такій низькій частоті відмов, які відповідають рівню безпеки SIL 4, небезпечні відмови є досить імовірними подіями.

Слід зазначити, що рівень безпеки SIL є функцією всієї БСМ, тому треба враховувати середню частоту небезпечних відмов усіх елементів мережі.

Розраховувати рівень SIL функції безпеки можна за методикою, яку викладено у стандарті МЕК 61508. У цьому стандарті запропоновано такі показники, як імовірності відмов для оцінки функції безпеки. Спочатку визначають долю небезпечних відмов (Dangerous Failure Fraction – DFF), яка доповнює долю безпечних відмов до одиниці та обчислюється як відношення інтенсивності небезпечних недіагностованих відмов до сумарної інтенсивності відмов. Діагностичне покриття (Diagnostic Coverage – DC) відповідно до МЕК 61508 розраховують на основі визначення інтенсивності небезпечних відмов. Діагностичне покриття є відношенням інтенсивності небезпечних діагностованих відмов до інтенсивності небезпечних відмов. Звідси випливає, що діагностичне покриття свідчить про долю зменшення імовірності тільки небезпечних відмов за рахунок вбудованих, наприклад, у БСМ засобів діагностики.

Виходячи з розрахункового значення долі безпечних відмов (Safe Failure Fraction – SFF), визначають максимальний рівень безпеки SIL як для резервованих, так і нерезервованих конфігурацій БСМ. Приклад розрахованих таким чином рівнів SIL наведено у табл. 2.

Як випливає з табл. 3.2, для долі безпечних відмов 90–99 % (БСМ нерезервована, тобто HFT = 0) максимальний рівень безпеки не перевищує SIL 2. Якщо елементи БСМ дубльовані (HFT = 1), то рівень безпеки для елементів складає SIL 3. Для тройованих елементів мережі (HFT = 2) рівень безпеки елементів сягає значення SIL 4. Для розрахунку рівня безпеки усієї БСМ недостатньо враховувати PFD_{AVG} окремих компонентів. Для цього треба

визначити сумарне значення PFD_{AVG}, після чого сумарне значення PFD_{AVG} треба порівняти з допустимою загальною імовірністю відмов відповідного рівня SIL. Відзначимо, що рівень безпеки SIL можна підвищити за рахунок додаткового резервування надійних елементів БСМ або вбудованими засобами діагностики.

Таблиця 2.2 – Максимальний рівень SIL в залежності від значення SFF та показника апаратної відмовостійкості (Hardware Fault Tolerance – HFT)

Доля безпечних відмов на елемент БСМ, або SFF	Допустима кількість апаратних відмов БСМ або HFT		
	0	1	2
>60 %	—	SIL 1	SIL 2
від 60 % до 90 %	SIL 2	SIL 2	SIL 3
від 90 % до 99 %	SIL 2	SIL 3	SIL 4
≥99 %	SIL 3	SIL 4	SIL 4

Приклад розрахунку загального показника PFD для БСМ показано на Рис.5. Як свідчить цей приклад, для мережі, яка містить 100 сенсорів, один координатор та один концентратор, середня імовірність небезпечної відмови $PFD_{AVG} = 4.46 \cdot 10^{-1}$, що нижче рівня безпеки SIL 1. З цього випливає, що для підвищення рівня безпеки SIL БСМ необхідно, перш за все, дублювати сенсори, які вносять найбільший вклад у долю небезпечних відмов або обладнати елементи мережі вбудованими засобами діагностики.

Рисунок 2.5 – Розрахунок значень функції безпеки PFD елементів БСМ у складі сенсора, координатора та концентратора

У БСМ однаково важливо застосовувати методи, спрямовані на забезпечення як функціональної безпеки, так й інформаційної безпеки. Треба відзначити, що в стандартах сімейства МЕК 61508 практично не йде мова про інформаційну безпеку, відсутні підходи до її забезпечення.

Високі вимоги як до інформаційної безпеки, так і безпеки в цілому бездротових сенсорних мереж у першу чергу зумовлені тим, що бездротові технології та бездротові сенсорні мережі все глибше та ширше проникають у виробничі процеси багатьох галузей промисловості та повсякденне життя пересічних громадян. Відповідно до [5] ризики, які супроводжують впровадження та застосування системи інформаційної безпеки телекомунікаційної системи, можна визначити як імовірність загрози безпеці та реалізація цієї загрози.

Забезпечення інформаційної безпеки бездротових мереж – досить складне завдання і на даний час не існує чітких та беззаперечних рекомендацій щодо побудови системи гарантування безпеки.

Більшість загроз інформаційній безпеці БСМ мають більш складний характер ніж подібні загрози дротовим комп'ютерним мережам, оскільки бездротові мережі набагато складніше захистити із-за загальнодоступного середовища передавання даних та широкосмугового характеру бездротових з'єднань. Забезпечення безпеки в бездротових сенсорних мережах є складною та комплексною задачею через цілий ряд причин.

1. Масштабованість БСМ, тобто мережа може складатися як з кількох вузлів, так і з кількох тисяч. Відповідно алгоритми та механізми гарантування інформаційної безпеки повинні також масштабуватися до обсягів мережі.

2. Змінна топологія бездротової мережі, що супроводжується додаванням нових вузлів або видаленням існуючих. Це вимагає використання складних алгоритмів маршрутизації та механізмів підтримання цілісності мережі.

3. Уразливість бездротових каналів, оскільки передавання даних здійснюється в загальнодоступному середовищі. Доступ до бездротового каналу можна отримати значно легше, ніж до дротових мереж передавання даних.

4. Уразливість вузлів мережі, оскільки вузли можуть переміщатися обслуговуючим персоналом або в інший спосіб, та не існує можливості завжди гарантувати фізичний захист будь-якого вузла мережі. Це робить імовірним фізичний доступ до незахищеного вузла мережі.

5. Обмежені енергетичні та обчислювальні можливості вузла, що зумовлює ситуацію, коли на рівні вузла майже неможливо реалізувати надійні механізми та алгоритми безпеки, оскільки вони є досить ресурсота енергозатратними.

6. Системні помилки в роботі вузла і мережі, зокрема, втрати пакетів даних при передаванні, відсутність зв'язку з центральним вузлом, вихід з ладу вузла або розрядження батареї. Оскільки такі помилки можуть виникати в мережі часто, то навмисні дії, які маскують під системні збої, досить важко виявити.

Аналізуючи вище наведене, можна зробити висновок, що заходи по забезпеченню інформаційної безпеки бездротової сенсорної мережі (Рис.6) можна розділити на основні та другорядні [6]. До основних слід віднести гарантування конфіденційності, цілісності мережі, аутентифікації та доступності даних. Другорядними є гарантування самоорганізації мережі, часової синхронізації та актуальності даних.

Конфіденційність, зазвичай, в основному і визначає рівень безпеки бездротової мережі. Мережа з високим рівнем конфіденційності захищає дані, що передаються по мережі, та закриває до них доступ для потенційних загроз. Конфіденційність досягається застосуванням механізмів контролю доступу, шифруванням тощо.

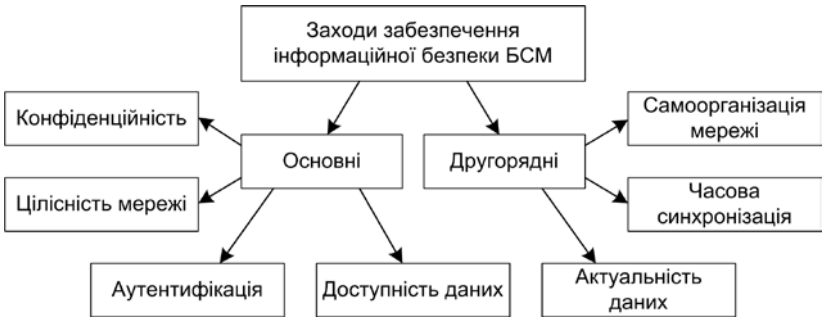


Рисунок 2.6 – Заходи по забезпеченню інформаційної безпеки БСМ

Аутентифікацію даних в бездротовій мережі реалізовують з метою підтвердження автентичності даних, що передаються, через застосування механізмів ідентифікації їх походження або, іншими словами, джерела передавання даних. Через механізм аутентифікації можна підтвердити справжність джерела та приймача даних, що реалізується, зазвичай, через обмін таємними ключами.

Механізми цілісності даних необхідні для гарантування того, що дані, які передаються через бездротовий канал, не будуть замінені чи модифіковані під час транспортування від одного вузла до іншого. Цей механізм, зазвичай, дозволяє виявити пошкоджене повідомлення або фальшиві дані, які були вбудовані в автентичне повідомлення або передані скомпрометованим вузлом.

Доступність даних передбачає, що бездротова сенсорна мережа виконує одну з основних своїх функцій, передавання даних між вузлами. Зумовити загрозу доступності даних можна виведенням з ладу центрального вузла мережі.

При відсутності можливості передавати дані виникає питання в доцільності мережі.

Актуальність даних дозволяє гарантувати, що передаються дані, які є актуальними на даний момент. Це дозволяє уникнути пересилання застарілих даних або повторного пересилання даних, що може зумовити конфлікти в мережі.

Механізми самоорганізації дозволяють вузлу мережі бути функціонально гнучким та незалежним з метою самовідновлення свого місця в топології мережі при різних умовах довкілля або при виникненні різних ситуацій. Реалізувати цей механізм з дотриманням усіх вимог інформаційної безпеки досить складно.

Алгоритми часової синхронізації необхідні для встановлення загальної шкали часу для усіх вузлів мережі з метою синхронізації вбудованих механізмів.

Аналізуючи заходи забезпечення інформаційної безпеки бездротових сенсорних мереж, можна чітко розділити атаки мереж (Рис.3.7) на пасивні та активні.

При пасивних атаках відсутні втручання в процес маршрутизації, а виконується лише моніторинг мережі та прослуховування трафіку для отримання інформації про топологію мережі, розташування вузлів, взаємодію між вузлами тощо. Пасивний моніторинг мережі дозволяє отримати інформацію про інтенсивність обміну в мережі. Якщо з певним вузлом ведеться інтенсивний обмін даними, то це може свідчити про важливість вузла, а отже він може стати ціллю атаки. Зазвичай від пасивних атак дуже важко захиститися, а виявити їх у багатьох випадках неможливо. При цьому виді атак не порушується цілісність мережі та доступність даних, зате страждає конфіденційність.

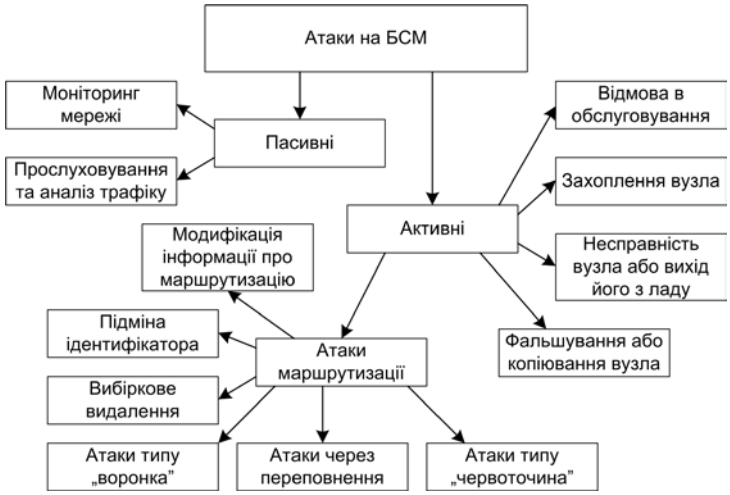


Рисунок 2.7 – Види атак

Активні атаки передбачають втручання в роботу протоколів маршрутизації через зміну полів повідомлень керування, інформації про маршрутизацію або, одним з найпоширеніших способів, спричиненням відмови в обслуговуванні. Найчастіше зустрічаються активні атаки на мережевому рівні, а саме атаки маршрутизації:

1) підміна ідентифікатора, коли скомпрометований вузол може використовувати кілька псевдо ідентифікаторів та видавати себе за декілька вузлів. Такі атаки, зазвичай, використовують для порушення механізмів маршрутизації, агрегації даних, розподіленого зберігання даних тощо. Чим більш рівноправних вузлів у мережі, тим більше мережа є схильною до такого типу атаки;

2) вибіркове видалення, яке полягає у тому, що скомпрометований вузол може вибірково видаляти певні пакети. Це призводить до порушення цілісності мережі та доступності даних;

3) модифікація інформації про маршрутизацію. Найбільш схильні до такої атаки мережі з певною децентралізацією, де прості вузли можуть виконувати функції маршрутизації та, відповідно, змінювати дані маршрутизації.

Як наслідок такої атаки може відбуватися збільшення часу на передавання маршруту ізза спотворених даних про маршрут, закільцювання маршруту тощо;

4) атаки типу "воронка", коли скомпрометований вузол починає концентрувати на собі весь трафік мережі. В цьому разі скомпрометований вузол слухає запити на маршрути та відповідає, що знає короткий маршрут до центрального вузла. Через деякий час такому вузлу вдається сконцентрувати на собі велику частину трафіку мережі, що дозволяє йому модифікувати пакети даних;

5) атака через переповнення, яка являє собою широкосмугову атаку та націлена на спрямування у БСМ великої кількості непотрібних повідомлень. Така атака є ресурсозатратною для атакованої мережі, що спричинює зниження пропускної здатності, зменшення енергетичних та обчислювальних ресурсів тощо;

6) атаки типу "червоточина" передбачають, що в мережі є два або більше скомпрометованих вузлів. При цьому між такими вузлами створюється маршрут для передавання перехоплених пакетів, які стають недоступними для атакованої системи [7]. Така атака впливає на мережу загалом через передавання фальшивих пакетів, які спричиняють спотворення маршрутних таблиць сусідніх вузлів.

Іншим типом активної атаки є відмова в обслуговуванні. Така атака може бути результатом ненавмисного виходу з ладу будь-якого вузла мережі або результатом навмисних дій. Атака направлена на швидку трату всіх ресурсів скомпрометованого вузла шляхом розсилання непотрібних пакетів даних. При цьому користувачі мережі не можуть у повній мірі використовувати ресурси мережі із-за значної завантаженості [8]. Атаки такого типу направлені на руйнування мережі, розірвання бездротових каналів, створення подій у мережі, які унеможливлюють виконання мережею закладених у неї функцій тощо.

До активних атак відносять захоплення вузла, що може зумовити розкриття важливої інформації, наприклад, криптографічних ключів. При успішній атаці цього типу може бути скомпрометовано цілу бездротову сенсорну мережу [9].

2.2. Протоколи захисту інформації

Пристрої стандарту 802.11 зв’язуються один з одним, використовуючи в якості передавача даних сигнали, що передаються в діапазоні радіочастот. Дані передаються по радіо відправником, які вважають, що приймач також працює в обраному радіодіапазоні. Недоліком такого механізму є те, що будь-яка інша станція, що використовує цей діапазон, теж здатна прийняти ці дані.

Якщо не використовувати який-небудь механізм захисту, будь-яка станція стандарту 802.11 зможе обробити дані, послані по бездротовій локальній мережі, якщо тільки її приймач працює в тому ж радіодіапазоні. Для забезпечення хоча б мінімального рівня безпеки необхідні наступні компоненти.

- Засоби для ухвалення рішення щодо того, хто або що може використовувати бездротову LAN. Ця вимога задовольняється за рахунок механізму аутентіфікації, що забезпечує контроль доступу до LAN.
- Засоби захисту інформації, переданої через безпровідне середовище.

Ця вимога задовольняється за рахунок використання алгоритмів шифрування.

На рис. 2.11. показано, що захист в бездротових мережах забезпечується як за рахунок аутентифікації, так і завдяки шифруванню. Жоден з названих механізмів окремо не здатний забезпечити захист бездротової мережі.

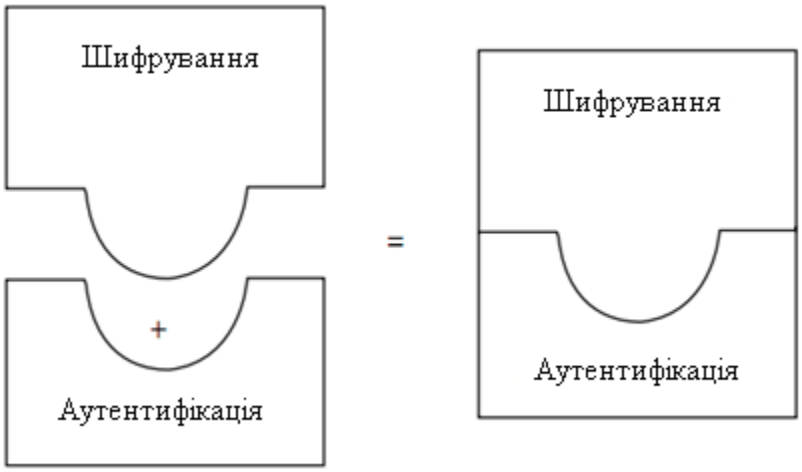


Рисунок 2.11 – Захист в бездротових мережах забезпечується за рахунок аутентифікації і шифрування

Також існують головні та допоміжні методи захисту представлені на рисунку 2.12.

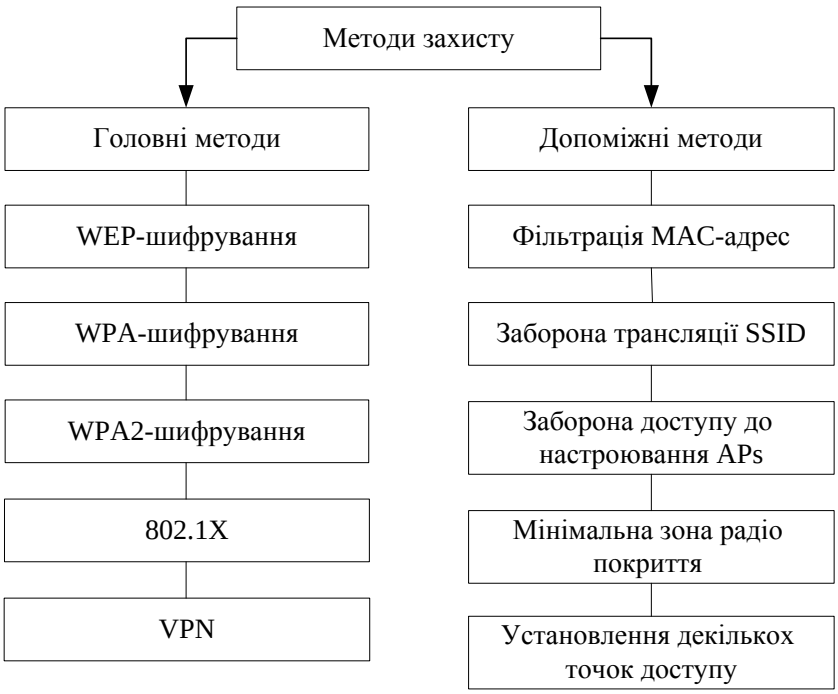


Рисунок 2.12 – Класифікація методів захисту бездротових локальних мереж

Розглянемо кожен з методів більш детально:

1. Основні методи захисту

WEP (Wired Equivalence Privacy) – це протокол шифрування, що базується на алгоритмі RC4. Алгоритм використовує ключі довжиною 64, 128, 256 та 512 біт. Чим більше біт використовується для зберігання ключа, тим більше можливих комбінацій ключів, а відповідно більша стійкість мережі до злому.

Але довжина ключа тільки сповільнить дію хакера на деякий час, а не зупинить його. Частина ключа WEP є статичною (40 біт у випадку 64-бітного шифрування), а інша частина (24 біт) – динамічна (вектор ініціалізації), тобто вона змінюється в процесі роботи мережі. Головною уразливістю WEP протоколу є те, що вектори ініціалізації повторюються через деякий проміжок часу.

Отже, для досягнення мінімального рівня безпеки ключі необхідно періодично змінювати. Якщо для бездротової мережі, що складається з точки доступу та трьох клієнтів, це не буде складати великої проблеми, то для корпоративних мереж із сотнями бездротових користувачів дане рішення не підходить. Більше того, для забезпечення достатнього рівня безпеки при використанні WEP-шифрування потрібна зміна 64-бітного ключа раз у пів години, а 128-бітного – раз у годину (в реальності ключі часто вводять один раз і назавжди).

WPA (Wi–Fi Protected Access) – протокол, в основі якого покладено підмножину стандарту IEEE 802.11i. В WPA використовується декілька засобів й алгоритмів для вдосконалення методів керування ключем та шифрування.

Якщо в WEP протоколі ключ, що використовується для шифрування даних, вводиться ручним способом та використовується до тих пір, поки не буде змінений, то в WPA ключ вводиться один раз, але використовується не для шифрування даних, а для генерації справжніх ключів для шифрування даних. WPA періодично змінює ключ. Отже, навіть якщо зловмиснику пощастить, і він відгадає ключ шифрування, то зможе ним користуватися лише до того часу, доки

бездротова точка доступу та клієнт автоматично не змінять його. Ключ шифрування в бездротових точках доступу змінюється доволі часто: раз на 1-2 години.

У стандарті WPA передбачено використання захисних протоколів 802.1x, EAS, TKIP і RADIUS. Конфіденційність та цільність даних забезпечуються за допомогою протоколу TKIP (Temporal Key Integrity Protocol), який на відміну від протоколу WEP використовує інший механізм генерації ключів, щоправда він теж заснований на алгоритмі RC4. Якщо в WEP довжина вектору ініціалізації дорівнює 24 бітам, то в протоколі TKIP використовується 48 біт. Крім того, вектор ініціалізації відбирається не випадково (псевдо-випадково) як раніше, а послідовно, до того ж пакети, що прийшли з невірним номером, відкидаються геть. Це виключає можливість здійснення reply-атаки. У протоколі TKIP новий ключ формується для кожного нового пакету, для цього використовується криптографічний контроль суми MIC (Message Integrity Code), призначеного для контролю цілісності пакетів та виявлення підробки у бездротових мережах, що перешкоджають зловмиснику змінювати зміст пакетів.

У системі передбачено два режими роботи: PSK (Pre-Shared Key) та Enterprise (корпоративний). Pre-Shared легко розгорнути, простий у використанні та налаштуванні, використовується для користувачів малого та домашнього офісу. Система Enterprise більш надійна завдяки серверу ідентифікації, що використовується для середніх та великих підприємств.

WPA2-шифрування – це система шифрування, заснована на остаточній редакції стандарту IEEE 802.11i. Алгоритм шифрування побудовано на блочному шифрі стандарту AES (Advanced Encryption Standard). Захисний протокол, що його використовує, отримав назву Counter-Mode CBC MAC Protocol (CCMP). Основна різниця між протоколами CCMP і TKIP знаходиться на рівні шифрування, дешифрування переданих даних: TKIP використовує чотири тимчасових ключі

шифрування, а AES – три. Механізм керування ключами в обох випадках однаковий.

Недоліком системи можна вважати те, що через велике навантаження алгоритму на центральний процесор бездротового клієнтського обладнання для переведення мережі на новий стандарт необхідно нове обладнання, що підтримує алгоритм шифрування AES. Вважається, що цей алгоритм, так само як WPA, при правильному налаштуванні майже неможливо зламати.

802.1X – це стандарт безпеки, що включає декілька протоколів. Почнемо з протоколу EAP (Extensible Authentication Protocol). Протокол розширеної ідентифікації.

У документі RFC 2284 протокол EAP описано наступним чином: “Розширений протокол ідентифікації (EAP) – це загальний протокол для підтвердження автентичності протоколу PPP, який підтримує кілька механізмів ідентифікації. EAP не обирає певний механізм ідентифікації на етапі керування каналом, а відкладає вибір до етапу ідентифікації. Це дозволяє ідентифікатору запитати більше інформації ще до вибору певного механізму. Це також відкриває можливість для застосування підтримуючого серверу, який реалізує різні механізми, тоді як ідентифікатор на рівні PPP просто пропускає через себе всі необхідні для ідентифікації повідомлення”.

Серед плюсів протоколу EAP можна зазначити наступне: підтримка різних методів ідентифікації без необхідності фіксувати який-небудь механізм на етапі керування каналом, пристрій може працювати як агент, що переадресує запити RADIUS-серверу, тобто обладнання буде тільки стежити за результатами ідентифікації та відстежувати наслідки вдалих або невдалих ідентифікацій.

Поряд з цим, у даного протоколу є декілька мінусів: він не підтримує динамічний розподіл ключів; уразливий до атаки «людина посередині» з використанням фальшивої точки доступу та до атаки на сервер ідентифікації:

зловмисник може підслухати запит та зашифровану відповідь, після чого провести атаку з невідомим відкритим або зашифрованим текстом.

RADIUS (Remote Authentication Dial-In User Server). Широко використовується в багатьох мережах. Його можна визначити як протокол безпеки, в якому для ідентифікації віддалених користувачів використовується модель клієнт-сервер. Він реалізується у вигляді серії запитів та відповідей, які клієнт передає від сервера доступу до мережі (Network Access Server - NAS) кінцевому користувачу. Протокол RADIUS був розроблений у відповідь на необхідність мати який-небудь метод ідентифікації, авторизації та обліку дій користувачів, яким необхідний доступ до різних обчислюваних ресурсів.

2. Серед допоміжних методів слід виділити наступні

Фільтрація MAC-адреси. MAC-адреса (Media Access Control - керування доступом до носія) – це унікальний ідентифікатор обладнання, що надає виробник. Фільтрація MAC-адреси міститься у розширенні доступу до мережі тільки визначених користувачів. Це створює зловмиснику додаткову заваду, але не зупиняє його. Крім того необхідність своєчасно поновляти список MAC-адрес важко здійсненна для великих мереж.

Заборона широкомовної трансляції ідентифікатора SSID. SSID – ідентифікатор мережі, знання якого є необхідною умовою для підключення. SSID може широко транслюватися в ефір або бути «прихованим» – у такому випадку клієнту прийдеться прописати ідентифікатор у налаштуваннях свого підключення. Більшість обладнання дозволяє його приховати, так що при скануванні мережі цього не буде видно. Крім того, необхідно змінити SSID, встановлений з початку. Звісно, це не надто серйозна перешкода, але вона є необхідною для елементарних заходів обережності.

Заборона доступу до налаштувань точки доступу або роутера через бездротову мережу. Активувавши цю функцію можна заборонити доступ до

налаштувань точки доступу через Wi-Fi мережу, але це не захистить від перехоплення трафіку або від проникнення до мережі.

Мінімально припустима зона радіо покриття. В ідеалі вона не повинна виходити за межі контрольованої території. При необхідності можна встановити параболічні відбивачі, що перешкоджають розповсюдженню сигналу в небажаних напрямках.

Встановлення декількох точок доступу в бездротовій мережі не тільки створює резервну смугу пропускання на випадок виходу з ладу однієї з точок, але й підвищує стійкість мережі до деяких видів атак.

2.3. Моделі захисту інформації

Активною загрозою бездротовій мережі є також несправність будь-якого вузла або вихід його з ладу. Несправний вузол може генерувати некоректні дані, що може зумовити порушення цілісності мережі. При виході з ладу вузла з функціями маршрутизації може бути порушена маршрутизація мережі.

До активних атак, крім того, слід віднести фальшування або копіювання вузла. Впровадження в мережу фальшивого вузла дозволяє такому вузлу розсилати некоректні дані, що може призвести, в певних випадках, до руйнування цілої мережі через розсилання зловмисного коду. При атаці копіюванням у мережу впроваджується завчасно підготовлений вузол, який використовує ідентифікатор існуючого в мережі вузла. Далі конфігураційні дані, які зібрані вузлом-копією, використовуються для маніпулювання сусідніми вузлами, що може призвести до захоплення керування цілим сегментом бездротової сенсорної мережі.

Для протидії атакам використовуються механізми забезпечення інформаційної безпеки. Зазвичай, такі механізми призначені для ідентифікації, попередження та відновлення БСМ після атак різного типу. В залежності від рівня використання механізми забезпечення безпеки можна розділити на механізми високого та низького рівня.

До механізмів забезпечення безпеки низького рівня можна віднести такі:

1) керування ключами та використання центрів довіри. Оскільки вузли БСМ обмежені в обчислювальних та енергетичних ресурсах, то застосування шифрування асиметричними ключами недоцільне і нераціональне у БСМ. Краще використовувати симетричне шифрування. Механізми встановлення та керування ключами мають бути придатними та масштабованими для використання в мережах, які складаються з сотень або тисяч вузлів. Деякі принципи побудови БСМ передбачають, що вузли мають встановлювати ключі з сусідніми вузлами;

2) захищена маршрутизація. Як відомо, маршрутизація є основним процесом, без якого неможлива комунікація між вузлами взагалі. Але сучасні протоколи маршрутизації при своїй, часто надмірній складності, містять багато вразливостей інформаційній безпеці мережі в цілому. Найпростіші атаки передбачають включення неправдивих маршрутних даних в БСМ, що може порушити канали передавання даних як між певними вузлами, так і у межах цілої мережі. Застосування нових методів аутентифікації та захищених протоколів маршрутизації дозволить захиститися від подібних атак;

3) секретність та аутентифікація. БСМ гостро потребують захисту від прослуховування, вбудування та модифікування пакетів даних. Криптографія є стандартним механізмом захисту. Для певних типів БСМ виникають проблеми при застосуванні криптографії. Наприклад, для бездротових мереж з рівноправними вузлами криптографія дає високий рівень захисту, але потребує

встановлення ключів між всіма вузлами мережі та є несумісною з широкосмуговим розсиланням повідомлень. Застосування криптографії на канальному рівні дозволяє легко встановлювати ключі та підтримує широкосмугове розсилання, але проміжні вузли зможуть перехоплювати та змінювати повідомлення;

4) захист від захоплення вузла. Така атака є досить серйозною проблемою, оскільки вузли не завжди знаходяться у недоступних для фізичного впливу місцях. З викраденого вузла можна отримати криптографічну інформацію, перепрограмувати вузол або замінити викрадений вузол фальшивим вузлом з зловмисною програмою. Найбільш простими методами захисту від подібних атак є застосування захищених від злому корпусів, удосконалених алгоритмічних рішень або техніки хешування.

5) стійкість до відмов в обслуговуванні. Причинами відмов в обслуговуванні можуть бути неполадки апаратних ресурсів, помилки прикладних програм, параметри довкілля або сукупність вказаних факторів. Причиною, наприклад, може бути потужний сигнал, яким намагалися заглушити всі комунікаційні канали та вивести БСМ з ладу. Протидією може бути використання механізму розширеного спектру, який дозволяє штучно розширити діапазон частот.

До механізмів забезпечення безпеки високого рівня можна віднести такі:

1) захищене агрегування даних. Зазвичай, дані, які збираються з вузлів, агрегуються на рівні базових станцій, які мають бути надійно захищені за допомогою захищених протоколів маршрутизації та надійних схем аутентифікації;

2) захищене керування групою. Кожний вузол має обмежені комунікаційні можливості, енергетичні та обчислювальні ресурси. Але певні функції, такі як агрегування та аналіз мережевих даних, можуть здійснюватися

групою вузлів. Отже, необхідні захищені протоколи для керування групами вузлів БСМ, які виконують спільні функції. Такі протоколи повинні дозволяти приймати нові вузли у функціональні групи та підтримувати захищену комунікацію між вузламичленами такої групи;

3) ідентифікація вторгнень. БСМ схильні до різних вторгнень. Тому необхідна наявність механізмів ідентифікації вторгнень, які б проводили моніторинг стану мережі, ідентифікували можливі спроби проникнення та повідомляли користувача про такі спроби. При захисті від таких атак корисним буде використання захищених груп вузлів.

Узагальнене представлення загроз та відповідних рішень наведено у табл. 2.3.

Таблиця 2.3 – Узагальнене представлення загроз і рішень

	Загроза	Вразливість	Рішення
1	Пасивний моніторинг мережі	Конфіденційність	Криптографія, шифрування
2	Прослуховування та ана ліз трафіку	Конфіденційність	Криптографія, шифрування
3	Атаки маршрутизації	Цілісність мережі, маршрутизація, доступність даних	Захищена маршрутизація, аутентифікація, керування ключами, центр довіри
3.1	Підміна ідентифікатора	Механізми маршрутизації, агрегація даних	Захищена маршрутизація, захищене агрегування даних
3.2	Вибіркове видалення	Цілісність мережі, доступність даних	Захищена маршрутизація
3.3	Модифікація інформації про маршрутизацію	Таблиці маршрутизації	Захищена маршрутизація

3.4	Атаки типу "воронка"	Маршрутизація, цілісність мережі	Захищена маршрутизація
3.5	Атака через переповнення	Пропускна здатність каналів мережі, енергетичні та обчислювальні ресурси	Захищена маршрутизація
3.6	Атаки типу "червоточина"	Цілісність мережі, таблиці маршрутизації	Захищена маршрутизація
4	Відмова в обслуговуванні	Цілісність мережі, енергетичні та обчислювальні ресурси	Стійкість до відмов в обслуговуванні, зокрема механізм розширеного спектру
5	Захоплення вузла	Цілісність мережі, криптографічні ключі, конфіденційна інформація	Ідентифікація вторгнень
6	Несправність вузла або вихід його ладу	Цілісність мережі	Альтернативні маршрути, вбудована діагностика
7	Фальшування або копіювання вузла	Цілісність мережі, конфіденційна інформація	Ідентифікація вторгнень

Висновки до другого розділу

Моделей оцінки функціональної безпеки є близько десятка, однак, свою увагу зосередимо на двох: МНК та GERT-моделі. Згідно дослідження [6] саме ці дві моделі показали найменшу похибку оцінювання.

Крім критеріїв, що дозволяють говорити про якість моделі самої по собі, існує ряд характеристик, що дозволяють порівнювати моделі один з одним (за умови, що ми пояснюємо один і той же ряд на одному і тому ж періоді).

Більшість моделей регресії зводяться до задачі мінімізації суми квадратів залишків (sumofsquaredresiduals,SSR). Таким чином, порівнюючи моделі за цим

показником, можна визначити, яка з моделей краще пояснила досліджуваний ряд. Такий моделі буде відповідати найменше значення суми квадратів залишків.

Ще однією моделлю оцінки функціональної безпеки є GERT-модель.

Базовим поняттям і показником ФБ є ризик, що представляє собою комбінацію ймовірності небажаного події та її наслідків.

Оцінювання ризиків буває кількісним і якісним, при якісному оперують такими категоріями, як «високий», «середній», «низький» і т.д.

Якщо розглядати системи управління, то подіями, пов'язаними з ризиком, є відмови функцій безпеки, тому логічно, що в якості показників безпеки обрані ймовірності відмов для функцій безпеки.

3. ЗАХИСТ ІНФОРМАЦІЇ НА БАЗІ МОДЕЛЕЙ БЕЗПЕКИ

3.1. Небезпека інформації

У загальному вигляді інтегрована модель загроз включає в себе [19]:

- компонент, що описує комплексний рівень;
- компонент, що описує сценарний рівень;
- компонент, що описує дії порушника.

Компонент моделі загроз об'єкта захисту, що представляє комплексний рівень, служить для параметризації процесу формування сценаріїв і обліку моделі порушника, і в загальному вигляді включає в себе: Мн - модель порушника; $Pur^{KУ} = \{pur_i^{KУ}\}_{i=1}^{K_{KУ}} \subset Pur$ - безліч цілей комплексного рівня, Pur - безліч цілей дій порушників, де $K_{KУ} \le \|Pur^{KУ}\|$ - число цілей, $O = \{o_i\}_{i=1}^{K_O}$ - безліч об'єктів на даному об'єкті захисту, КО - число аналізованих об'єктів; ГКУ - безліч функцій даного компонента.

$$Pur^{KУ} = O \times Pur \times \langle T_H, V_H \rangle, \qquad (3.1)$$

де Тн - тип порушника; Vн - вид порушника.

Компонент моделі загроз об'єкта захисту, що представляє сценарний рівень, служить для формування безлічі різних сценаріїв (послідовності дій порушника) з урахуванням мети, яка повинна бути досягнута порушником, і в загальному вигляді включає в себе безліч реалізованих в ньому функцій. Основна функція формує безліч сценаріїв, виконання яких дозволяє досягти цілей комплексного рівня:

$$Pur^{KУ} \times A \to S, \qquad (3.2)$$

де $S = \{S_k\}_{k=1}^{N_S}$ - безліч сценаріїв реалізації загроз; NS - число сценаріїв.

Сценарій Sk формується методом повного перебору всіх дій порушника

подцелей мети PurКУ.

Сценарії реалізації загроз об'єкту захисту можуть бути представлені байесовськими мережами довіри (БСД) [15]:

$$BN_{O3} = \langle A, Tab_{O3} \rangle, \quad (3.3)$$

де $A = \{a_i\}_{i=1}^{N_A}$ - безліч дій порушників; NA - число всіх дій порушників; TabОЗ - безліч таблиць умовних ймовірностей кожної дії-нащадка аі з батьківськими діями parents (ai).

Такий підхід дозволяє з більшою точністю визначати ймовірність реалізації загрози за допомогою того чи іншого сценарію. Вузлами БСД в цьому випадку будуть атакуючі дії порушників. Таблиці умовних ймовірностей описуються наступним чином:

$$Tab_{O3} = \{P(A_1 | parents(A_1)), ..., P(A_n | parents(A_n))\}. \quad (3.4)$$

Коли дія Аі не має батька, тобто з цього дії порушник починає реалізацію загрози, використовується безумовна ймовірність Р (Аі).

Компонент моделі загроз об'єкта захисту, що представляє дії порушника, в загальному вигляді включає в себе: $A = \{a_i\}_{i=1}^{N_A}$ - безліч дій порушників, NA - число всіх дій порушників; FУДН - безліч функцій даного компонента.

Кожна дія порушника представлено в наступному вигляді:

$$a_i = \langle aid_i, pur_i, T_{ra}, Y_{\max i}, P_i^E, RE_i \rangle \forall i \in N_A, i \le N_A, \quad (3.5)$$

де aidi - ідентифікатор дії порушника;

$pur_i \in Pur$ - мета, що досягається виконанням дії порушника;

Tra - час, необхідний порушнику для успішної реалізації дії;

Ymaxi- ймовірний збиток, що наноситься СНП при реалізації дії

порушника; $P_i^{Б}$ - безумовна ймовірність виконання порушником даного дії; $RE_i = \{re_i\}_{i=1}^{N_{re}}$ - безліч рекомендацій з виявлення, затримки і реагування на дану дію силами КСЗІ;

Nre - число рекомендацій, відомих системі.

При аналізі уразливості об'єкта захисту необхідно проводити відбір серед отриманих сценаріїв, одним з можливих методів відбору може бути модифікований спосіб «відсіву» сценаріїв реалізації загроз за величиною ризику. Імовірність реалізації загрози (P (B)) обчислюється за формулою повної ймовірності події. Це дає більш точні значення показників ймовірності реалізації загрози за певним сценарієм. Сумарний збиток (Y) від реалізації сценарію можна визначити як суму збитків всіх дій з даного сценарію. Тоді, з урахуванням виразу $R = YP$, Ризик від реалізації сценарію обчислюється за формулою:

$$R = YP(B) \qquad (3.6)$$

Для відсіву сценаріїв розрахований ризик R порівнюється с прийнятним ризиком Rпр.

На основі проведеного аналізу функцій і завдань, що стоять перед КСЗІ, розроблена загальна функціональна модель КСЗІ (рис.21), якавідображає безперервний процес забезпечення безпеки об'єкта захисту в вигляді послідовності взаємопов'язаних функцій.

За допомогою різних засобів виявлення проводиться моніторинг загроз, які не можуть бути усунені превентивними заходами захисту. За допомогою знань про загрози, потенційних порушників і основних вразливих місцях об'єкта захисту, накопичених в сховище даних, відбувається виявлення поточних загроз.

Вони аналізуються і оцінюються на основі моделей сценаріїв розвитку атак. На основі отриманих даних і за допомогою моделей протидії атакам організовуються, а потім і реалізуються заходи щодо нейтралізації виявлених

загроз засобами протидії.

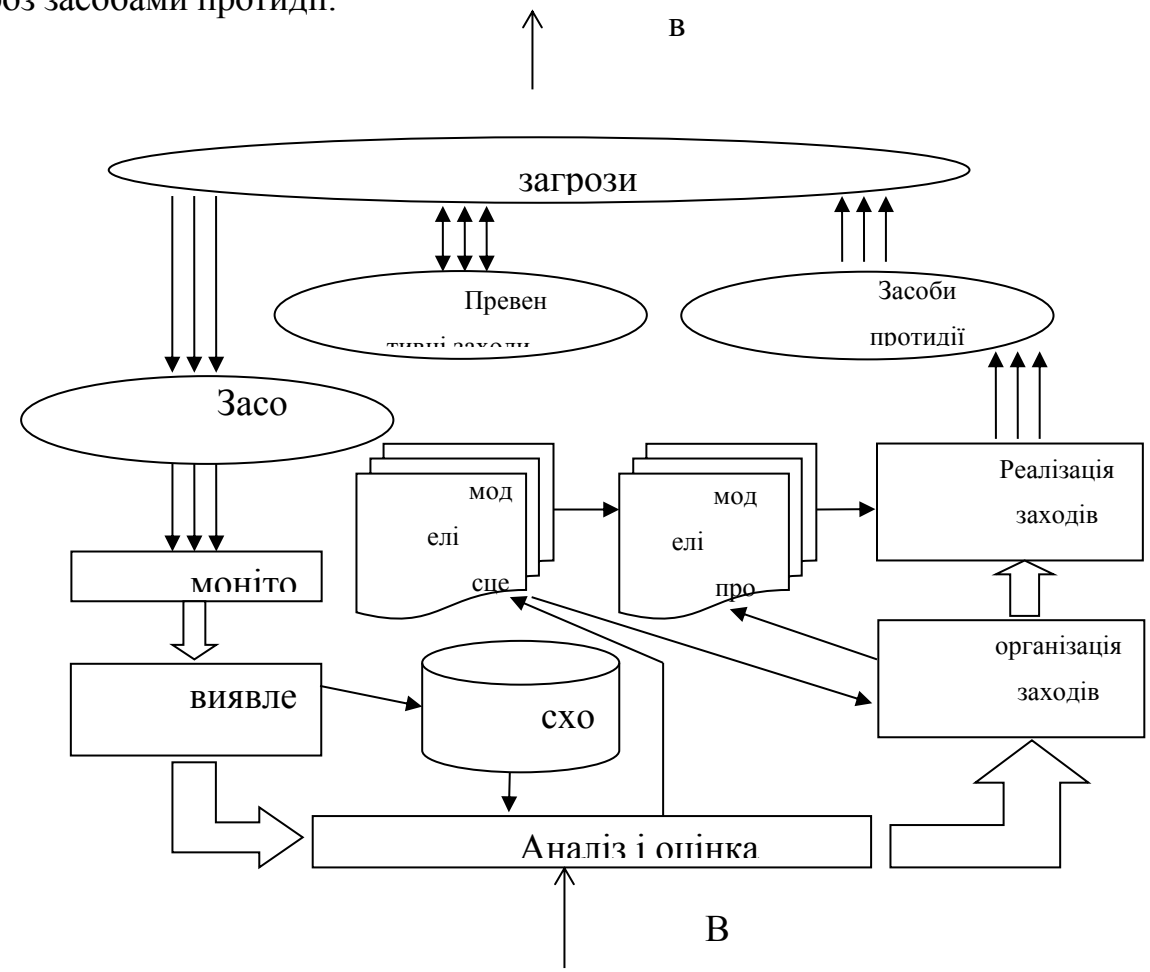


Рисунок 3.3 – Модель КСЗІ

У загальному вигляді модель КСЗІ включає в себе компоненти, які описують підсистеми виявлення, бар'єрів, прийняття рішень і реагування, а також безліч функцій моделі КСЗІ.

3.2. Методи захисту інформації

Для кожного розглянутого інструмента оцінюється як можливість проведення аналізу трафіку в реальному часі, так і відкладений аналіз попередньо

збережених мережевих трас. Тестування на трафіку в реальному часі істотно залежить від самого трафіку. У той же час, для порівняння результатів розглянутих інструментів необхідно забезпечити однаковий трафік на мережевому інтерфейсі. Для цього використовується програма Colasoft Packet Player [1], що дозволяє «відтворити» на заданому мережевому інтерфейсі вміст попередньо збереженої траси. Більш того, Packet Player дозволяє витримувати відповідні трасі тимчасові інтервали між відправкою мережевих пакетів на інтерфейс. Таким чином, можна отримати об'єктивні порівняльні результати роботи інструментів при аналізі трафіку в реальному часі. Що стосується тестування на збережених мережевих трасах, то для всіх інструментів використовується один і той же набір трас.

Для кожного інструменту проводиться ряд випробувань, що дозволяють оцінити його можливості:

відновлення потоків і виділення зв'язків між ними

розпізнавання протоколів (на тестовому наборі трас Wireshark Trace Files [2])

Результати тестування представлені в порівняльних таблицях. Крім того, оцінюються можливості навігації за результатами аналізу трафіку.

Метод адаптеру

Технологія дозволяє користувачеві переглядати і зберігати весь трафік, що проходить по мережі в режимі реального часу. Крім того, в рамках ОС Windows існує можливість (за допомогою спеціального адаптера) перехоплення і аналізу трафіку бездротових мереж Wi-Fi (802.11 WLAN).

На Рис.3.8 представлена архітектура інструменту. Вона складається з двох компонентів:

1. бібліотека, за допомогою якої здійснюється перехоплення мережевого трафіку (WinPcap для ОС Windows, libpcap для ОС Linux);

2. прикладна програма, що надає функції розбору протоколів і графічний інтерфейс для візуалізації результатів аналізу і взаємодії з системою.

За допомогою WinPcap (libpcap) здійснюється взаємодія з драйвером мережевого інтерфейсу. Безпосередня взаємодія з драйвером дозволяє перехоплювати і впроваджувати мережеві пакети, а також застосовувати різні критерії фільтрації. Бібліотека libwiretap використовується для роботи (читання / запис даних) з мережевими трасами різних форматів (у тому числі pcap). Компонент Dumpcap здійснює запис перехоплених мережевих пакетів в файл, а також передає їх на обробку. Бібліотека libwireshark відповідає за розбір і подальший аналіз мережевих пакетів, а також за візуалізацію результатів.

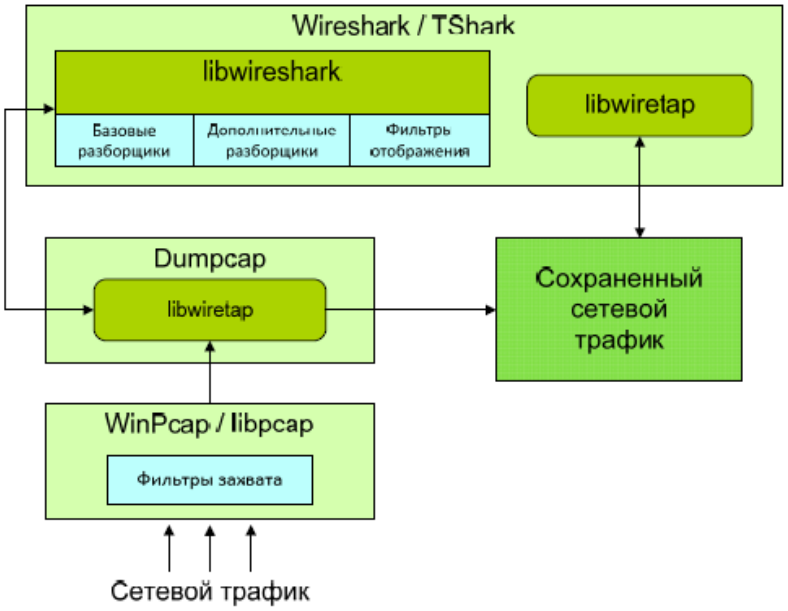


Рисунок 3.8 – Архітектура Wireshark

Особливу увагу необхідно приділити механізму зв'язування розбирачів (функцій розбору). Wireshark надає три сценарії взаємодії:

прямий виклик (безпосередній виклик розбирача)

зворотний виклик (викликається визначається значенням деякого ключового поля, отриманим при розборі більш низькорівневогоо протоколу; наприклад, значення поля «Порт» в заголовку TCP пакету)

евристична прив'язка (викликається разборщик визначається шляхом пошуку патернів в уже згадуваному буфері).

Wireshark надає можливість для підключення додаткових (в тому числі самостійно розроблених) модулів розбору трафіку.

Основні переваги інструменту:

1. Підтримка великої кількості мережевих протоколів (в тому числі протоколів IP-телефонії);

2. Підтримка різних форматів мережевих трас;

3. Можливість розширення (можливість створення і підключення додаткових модулів розбору);

4. Детальна система фільтрації мережевих пакетів;

5. Можливість відновлення потоків TCP;

Недоліки:

1. Відновлений потік не розглядається інструментом як єдиний буфер пам'яті, внаслідок чого його подальша обробка неможлива;

2. Код модулів розбору містить функції, що відповідають за візуалізацію результатів (логіка розбору перемішується з логікою відображення в графічному інтерфейсі);

3. Відсутня можливість виконання деякого дії в разі виявлення сигнатур в трафіку.

Wireshark підтримує аналіз тунелювання трафіку, однак надається компонента відображення результатів є вкрай незручною. Справа в тому, що кожен з послідовно застосовуваних до мережевого пакету розбирачів

перезаписує інформацію в головному вікні. У той же час при аналізі тунелю необхідна візуалізація результатів всіх розбирачів.

Наведені недоліки не дозволяють застосовувати Wireshark для аналізу даних, переданих за допомогою багаторівневого тунелю, а також ефективної роботи з відновленими потоками.

Метод сигнатур

Інструмент Bro Network Security Monitor [5] (далі Bro) дозволяє аналізувати трафік в реальному часі і виконувати певні дії в разі виявлення в ньому заданих сигнатур.

З точки зору архітектури можна виділити два компоненти:

1. генератор подій (здійснює аналіз трафіку, одержуваного за допомогою libpcap, і генерує події);

2. обробники подій (власну мову створення скриптів дозволяє видавати попередження, вести логування, а також запускати сторонні додатки в разі настання певних подій; таким чином, може бути сформульована деяка політика безпеки).

Архітектура системи Bro схематично представлена на Рис.2.3. Інструмент підтримує аналіз трафіку в режимі реального часу, а також відкладений аналіз мережевих трас (у форматі pcap).

Разом з системою поставляється велика кількість скриптів (повний список наведено тут [6]). Мова скриптів підтримує фіксований набір типів і атрибутів ([7]), серед яких відзначимо тип event (подія). Кожному події (повний список наведено тут [8]) можна поставити у відповідність обробник (один або кілька) в разі настання події буде викликаний відповідний обробник. Якщо до одного й того ж події «прив'язане» кілька обробників, необхідно задати атрибут пріоритетності, що визначає порядок виклику цих обробників. Події генеруються ядром системи Bro. Додавання нового типу події на увазі зміни ядра.

Одним з найбільш важливих подій з точки зору аналізу є подія signature_math. Воно генерується в разі виявлення деякого патерну в розглядуваної мережевому пакеті.

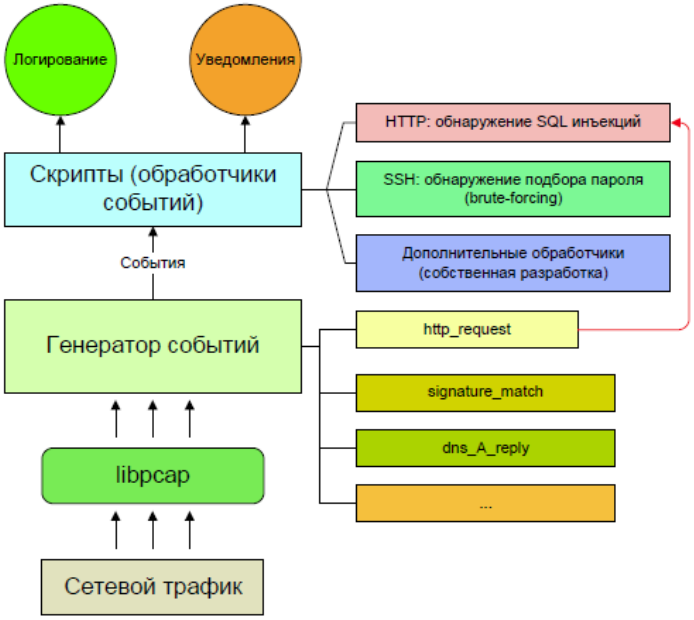


Рисунок 3.9 – Сигнатури в Bro

За допомогою сигнатури здійснюється пошук регулярного виразу (/.*root/)во всіх пакетах протоколу TCP, відправлених на порт 80. Кожна сигнатура має набір атрибутів. Існує два типи атрибутів: conditions (умови) і actions (дії). Умови є критерії збігу, а дії визначають операції, вироблені в разі збігу. Умови можуть застосовуватися як до заголовків пакетів, так і до їх корисного навантаження. Існує можливість встановлення залежностей між сигнатурами, яка фактично поширює механізм сигнатурного пошуку на послідовності пакетів. В системі визначені два дії:

генерація події signature_match;

запуск розбору протоколу наступного рівня.

Таким чином, разборщики зв'язуються за допомогою механізму подій. Крім того, в системі Bro реалізована система динамічного розпізнавання протоколів на

основі сигнатурного пошуку. Підтримуються протоколи ftp, http, bittorrent, ssh, ssl, pop3, smtp, ayiya. Як приклад можна привести сигнатуру для протоколу HTTP.

```
signature dpd_http_client
{
ip-proto == tcp
payload / ^ [[: space:]] * (GET | HEAD | POST) [[: space:]] * / tcp-state originator
}
```

Сигнатура для протоколу HTTP в Bro.

Інструмент підтримує аналіз тунелів. У той же час, автоматичне відновлення стека протоколів тунелю відсутня. Інформація про відновлених тунелях зберігається в текстовому лог файлі.

Метод сигнатурного пошуку

Аналіз здійснюється шляхом пошуку зазначених в файлі конфігурації патернів в мережевих пакетах (сигнатурний пошук).

У разі успіху виконуються певні аналітиком дії. Архітектура Snort представлена на Рис.3.10.

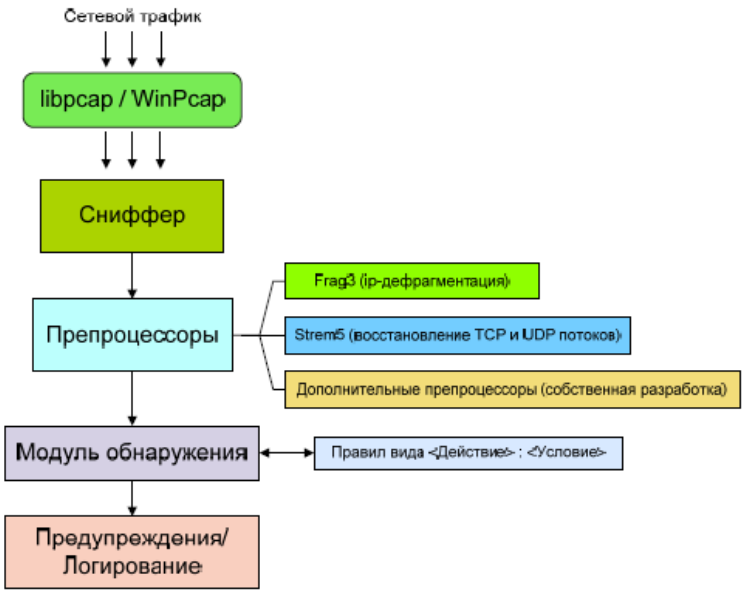


Рисунок 3.10 – Архітектура Snort

Можна виділити два головних компонента набір препроцесорів і модуль виявлення. Фактично препроцесори займаються розбором мережевих протоколів (аналіз пакетів, відновлення потоків). Snort надає близько двадцяти базових препроцесорів (в тому числі Frag3 модуль ip-дефрагментації, Stream5 модуль відновлення TCP і UDP потоків).

Аналітик може створювати додаткові препроцесори і додавати їх в систему. Кожен препроцесор має власний набір параметрів (параметри використовуваних препроцесорів повинні бути описані в файлі конфігурації snort.conf). Базові препроцесори докладно описані на сайті розробника [10]. Завдання модуля виявлення полягає в тому, щоб виконувати певні дії в разі виявлення заданих аналітиком патернів в розібраних пакетах і відновлених потоках.

Основу модуля складають правила. Кожне правило складається з заголовка і набору опцій. Тема містить дію, протокол, до якого застосовується це правило, ip-адреса і порт джерела, ip-адреса і порт приймача. Одна з опцій є патерн, в разі виявлення якого буде зроблено дію, вказане в заголовку.

У Snort реалізована підтримка тунелювання (GRE, IP in Ip, PPTP). У той же час, інструмент не може декодувати більш одного рівня інкапсуляції. Після закінчення роботи інструменту (як в режимі читання раніше збереженого pcap-файлу, так і в online-режимі) виводиться статистика проведеного аналізу (окремо для кожного препроцесора).

3.3. Наявні інструменти захисту інформації

Сучасні технології виявлення атак

Під виявленням атак розуміють процес оцінки подій ІС та її інформаційних потоків, який реалізується за допомогою аналізу журналів реєстрації операційних

систем (ОС) і додатків або мережевого трафіку. Реалізація більшості мережевих атак здійснюються в три етапи.

Перший, підготовчий, етап полягає в пошуку передумов для здійснення тієї чи іншої атаки. На даному етапі шукають вразливості, використання яких робить можливим в принципі реалізацію атаки, яка і складає другий етап. На третьому етапі атака завершується. При цьому перший і третій етапи самі по собі можуть бути атаками. Наприклад, пошук порушником вразливостей за допомогою сканерів безпеки вже вважається атакою.

Технології виявлення атак постійно розвиваються і удосконалюються, і ця область постійно залучає нових виробників і розробників. Незважаючи на брак теоретичних основ технології виявлення атак, існують досить ефективні методи, що використовують на сьогодні.

Існує кілька способів класифікації систем виявлення атак, кожен з яких заснований на різних характеристиках. Тип слід визначати, виходячи з таких характеристик:

- Спосіб контролю за системою. За способами контролю за системою поділяються на network-based, host-based і application- based.
- Спосіб аналізу. Це частина системи визначення проникнення, яка аналізує події, отримані з джерела інформації, і приймає рішення, чи відбувається проникнення. Способами аналізу є виявлення зловживань (misuse detection) та виявлення аномалій (anomaly detection).
- Затримка в часі між отриманням інформації з джерела та її аналізом і прийняттям рішення. Залежно від затримки в часі, системи виявлення атак діляться на interval-based (або пакетний режим) і real-time.

Більшість комерційних систем виявлення атак є real-time network-based системами.

Виявлення атак вимагає виконання однієї з двох умов: або знання всіх можливих атак та їх модифікацій, чи розуміння очікуваної поведінки контрольованого об’єкта системи. Всі існуючі технології виявлення мережевих атак можна розділити на два типи: методи на основі сигнатур (зразків і правил); методи на основі аномалій.

Зазвичай в СВА намагаються поєднувати обидві технології, щоб усунути недоліки, властиві кожній окремо. Перевага “аномальних” систем - виявлення невідомих або нових видів атак, які можуть “обійти” СВА. Реєстрація такого роду подій тягне за собою їх аналіз адміністратором, створення для них шаблону і внесення останнього до бази даних СВА. Системи, засновані на методі аномалій, вважаються досить перспективними, але ще розвиваються і перебувають у стадії дослідження.

Особливістю технології виявлення атак на основі сигнатур є процес опису атаки у вигляді шаблону або сигнатури і пошуку даного шаблону в контрольованому просторі (наприклад, мережевому трафіку або журналі реєстрації). Така СВА може виявити всі відомі атаки, але вона мало пристосована для виявлення нових, ще невідомих, атак.

При розробці СВА, заснованих на цьому підході, виникають дві основні проблеми. Перша полягає у створенні механізму опису сигнатур, тобто мови опису атак, а друга проблема виражається в наступному: як записати атаку, щоб зафіксувати всі можливі її модифікації? Схема технології виявлення атак на основі сигнатур показана на рис. 1.1.

Переваги:

- Детектори зловживань ефективно визначають атаки і дуже рідко створюють помилкові повідомлення;

– Детектори зловживань швидко й надійно діагностують використання конкретного інструментального засобу або технології атаки. Це дає змогу адміністратору скоригувати заходи для забезпечення безпеки;
– Швидкість аналізу.

Недоліки:

– Оскільки детектори зловживань виявляють лише відомі їм атаки, слід постійно оновлювати їхні бази даних для отримання сигнатур нових атак;
– Більшість детекторів зловживань розроблено так, що вони використовують лише певні сигнатури, а це не дає виявити мо- жливі варіанти атак;

Технологія виявлення атак на основі аномалій побудована на припущенні, що аномальна поведінка суб'єкта ІС (системи, програми, користувача), тобто, як правило, атака або яка-небудь ворожа дія часто проявляється як відхилення від нормальної поведінки. Зазвичай системи виявлення аномальної активності використовують як джерело даних журнали реєстрації і поточна діяльність користувача, хоча існують приклади системи виявлення аномалій в мережевому трафіку.

Традиційне використання цієї технології полягає не в чіткому виявленні атак, а у визначенні підозрілої активності, що відрізняється від нормальної. Основна проблема методу полягає в тому, щоб визначити критерій нормальної активності. Необхідно також встановити допустимі відхилення від нормального трафіку, які ще не вважатимуться атакою.

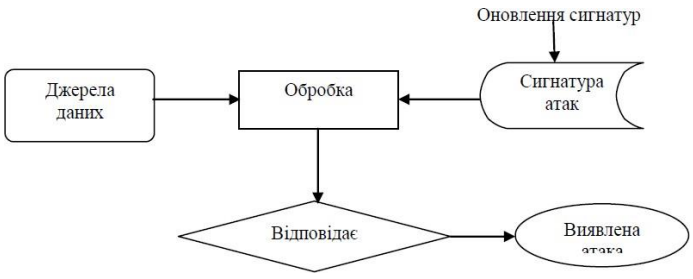


Рис.1.1 – Схема виявлення атак на основі сигнатур

При використанні даної технології виявлення атак можливі два варіанти неправильного виявлення атаки:

- виявлення дії, яка не є атакою, і віднесення його до класу атак;
- пропуск атаки, яка не підпадає під сигнатури атак. Цей випадок більш небезпечний, ніж помилкове віднесення дозволеного дії до класу атак. Підкатегорією такого методу є аналіз на основі профілів, коли нормальна поведінка визначається для окремих суб'єктів (користувачів / систем).

Іноді елементи такого аналізу зустрічаються і в інших методах, скажімо, в розшифровці протоколу, коли виявлений елемент, що не належить наперед визначеному протоколу або порушує правила використання протоколів.

Схема типової системи виявлення аномалій показана на рис. 1.2.

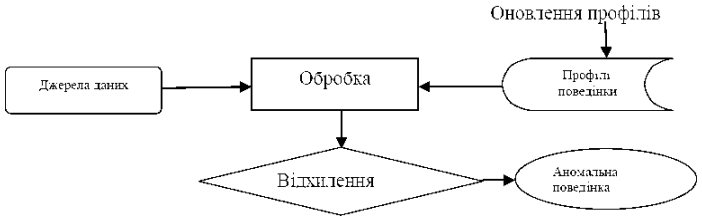


Рис. 1.2 – Схема системи виявлення аномальної поведінки

Прикладами аномальної поведінки є велика кількість з'єднаньза короткий проміжок часу, високі завантаження центрального процесора і коефіцієнт мережевого навантаження або використання периферійних пристроїв, які зазвичай не використовуються.

Якщо описати профіль нормальної поведінки суб'єкта, то будь-яке відхилення від нього можна охарактеризувати як аномальна поведінка.

Переваги:

- СВА, що виявляють аномалії, фіксуючи несподівану поведінку системи, отримують можливість визначати симптоми атак, не маючи відомостей про їхні конкретні деталі;
- Детектори аномалій збирають інформацію, якою в подальшому можуть скористатися детектори зловживань для визначення сигнатур.

Недоліки:

- Під час виявлення аномалій, як правило, створюється велика кількість помилкових сигналів про атаки у разі непередбачуваної поведінки користувачів і мережної активності;
- Цей метод часто потребує певного етапу навчання системи, під час якого визначаються характеристики нормальної поведінки. Якість проведення цього навчання суттєво впливає на подальшу ефективність СВА;
- Не можна реалізувати опис атаки за елементами. Повідомляється те, що відбувається щось підозріле;
- Дана технологія значно залежить від середовища функціонування як визначального фактор анормальної поведінки;
- Відносно низька швидкість аналізу;
- Трудомістке завдання побудови профілів суб’єктів ІС.

Для забезпечення інформаційної безпеки як окремих підприємств, так і держави в цілому важливим є питання оцінки ризиків, які виникають в процесі діяльності підприємств. Для оцінки ризиків інформаційної безпеки використовуються різні методики і стандарти управління інформаційними ризиками.

Аналіз ризиків інформаційної безпеки є методом виявлення вразливостей і загроз, оцінки можливого їх впливу, що дозволяє вибирати адекватні захисні заходи для тих систем і процесів, у яких вони необхідні. Методики аналізу інформаційних ризиків дають змогу забезпечити ефективний і актуальний захист

інформаційного простору підприємств і можливість вчасно реагувати на загрози інформаційній безпеці.

Кожен засіб захисту адресовано конкретній загрозі в системі. Більше того, кожен засіб захисту має слабкі та сильні сторони. Тільки комбінуючи їх, можна захиститися від максимально великого спектру атак.

Firewall'и є механізмами створення бар'єру, заступаючи вхід деяких типів мережевого трафіку і дозволяючи інші види трафіку. Створення такого бар'єру відбувається на основі політики firewall'a. Системи виявлення атак служать механізмами моніторингу, спостереження активності та прийняття рішень про те, чи є спостережувані події підозрілими. Вони можуть виявити атакуючих, які обійшли firewall, і видати звіт про це адміністратору, який, у свою чергу, зробить кроки щодо запобігання атаки.

Системи виявлення атак стають необхідним доповненням інфраструктури безпеки в кожній організації. Технології виявлення проникнень не роблять систему абсолютно безпечною. Проте практична користь від систем виявлення атак існує, і не маленька, що доведено експертним методом оцінювання у таблиці 2.2.

Таблиця 1.

Характеристика	**Сигнатурні мето-** **Методианомалій**
М ножина них	виявле- ми вида	обмежується жливостями налаштування і ме- тодами анал
Ймовірність середня ску атаки	пропу-	ізуСВА
Ймовірність низька кового	помил- дуже	исока
спрацьовування Вимоги до	обчислю-	

Порівняння методів СВА

Швидкість реакції

Важливим елементом в системах виявлення атак є швидкість реакції,що відбувається через певні проміжки часу, тобто пакетно. Швидкість реакції вказує на час, що минув між подіями, які були виявлені монітором, аналізом цих подій і реакцією на них.

У системах, реакція яких відбувається через певні проміжки часу, інформаційний потік від точок моніторингу до інструментів аналізу не є безперервним. У результаті інформація обробляється способом, аналогічним комунікаційним схемами "зберегти і перенаправляти". Багато ранніх host-based систем виявлення атак вико- ристовують дану схему хронометражу, тому що вони залежать від записів аудиту в ОС. Засновані на інтервалі системи не виконують ніяких дій, які є результатом аналізу подій.

Real-Time (безперервні) системи виявлення атак обробляють безперервний потік інформації від джерел. Найчастіше це є домінуючою схемою в network-based системах, які отримують інформацію з потоку мережевого трафіку. Термін "реальний час"використовується в тому ж сенсі, що і в системах управління процесом. Це означає, що визначення проникнення, що виконується системами виявлення атак в "реальному часі призводить до результатів досить швидко, що дозволяє виконувати певні дії в автоматичному режимі.

Таблиця 3.2. Імовірності подолання загроз різними засобами захисту

Вид атакуючої дії	Засіб захисту Між-	VPN	СВА	Анти-
	мережевий екран	шлюз		вірус
Троянські програми				0,96
Віруси				0,92
DoS-атаки	0,81	0,98	0,98	
DDoS-атаки	0,62	0,79	0,97	

Макровіруси				0,6
IP Spoofing	0,69	0,96	0,95	
DNS Spoofing			0,92	
WEB Spoofing			0,54	
Захоплення мережевих підключень	0,51	0,97	0,93	
Різні види сканування мережі	0,59		0,89	
Порушення конфіденційності даних		0,95		
Автоматичний підбір паролів	0,75		0,91	
Атаки на протоколи			0,79	
Неавторизоване використання прав	0,32		0,91	
Неконтрольоване використання ресурсів	0,53	0,61	0,81	0,64
Неавторизоване використання АС	0,62	0,73	0,79	0,67
Прослуховування мережі		0,92		
Шпигунське ПЗ			0,54	0,97

Вибір СВА повинен ґрунтуватись на вимогах, що висуваються до системи захисту інформації в кожному конкретному випадку. Проведене дослідження та порівняльний аналіз сучасних систем виявлення атак та запобігання вторгненням показав, що при вдосконаленні існуючих та проектуванні нових систем необхідно враховувати визначені властивості, зважаючи на особливості реалізації та функціонування інформаційної системи, які підлягають захисту.

Загальну структуру процесів системи відображає контекстна діаграма, яка забражена на рисунку 3.1. Вона показує вхідні та вихідні дані системи, яка проектується, засоби і методи здійснення аналізу та користувачів системою.

Вхідними даними для додатку є вхідні дані користувача, на виході отримуємо зашифровані та захищені дані користувача. Методи які використовуються – консоль для вибору захищеного протоколу з’єднання, генерування ключів доступу і зихист каналів з’єднання (HTTPS) (рис. 2.1)

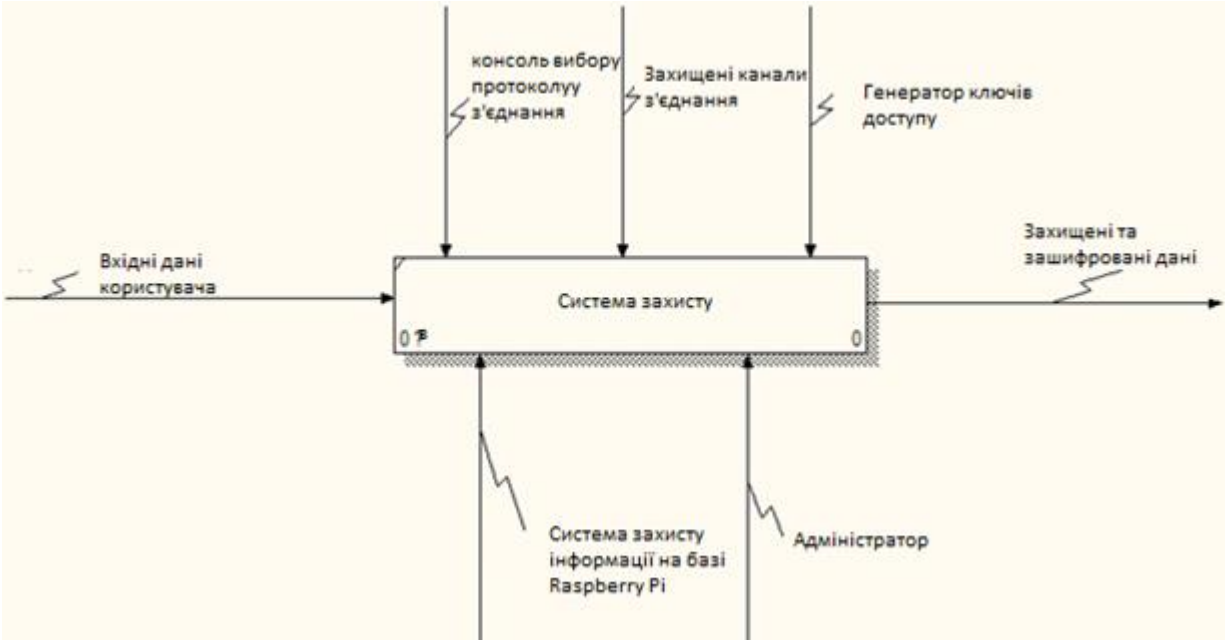


Рисунок 3.1. Контекстна діаграма

Декомпозиція 1-ого рівня

Для деталізації контекстної діаграми використовують діаграму декомпозиції першого рівня, розбиваючи її на певну кількість підпроцесів.

У даному випадку, для поетапної демонстрації кожного кроку використання системи, діаграму композиції розбито умовно на 2 підпроцеси:

процес вибору протоколу передачі даних та надання користувачу ключа доступу на 12 годин, що представлено на рис. 3.2.

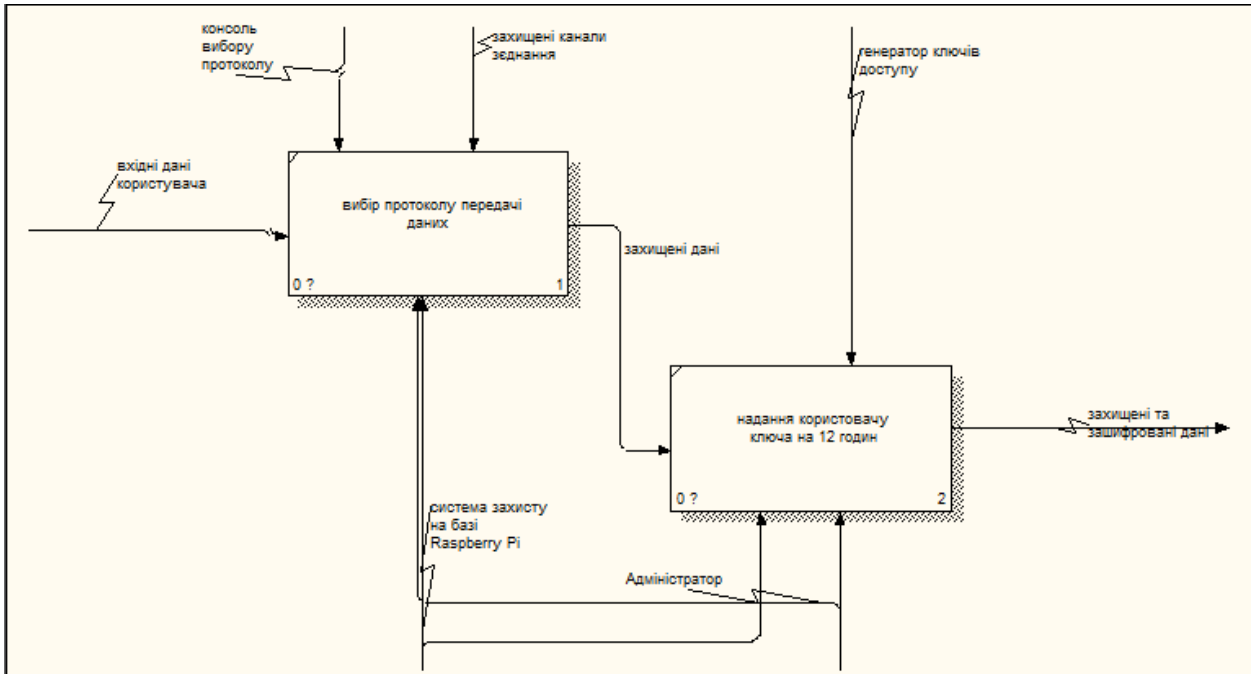


Рисунок 3.2. Декомпозиція першого рівня

Діаграма дерева вузлів

Створення діаграми дерева вузлів необхідне для відображення ієрархії процесів у системі. Усі процеси та підпроцеси візуалізовано та зображено на рисунку 3.3.

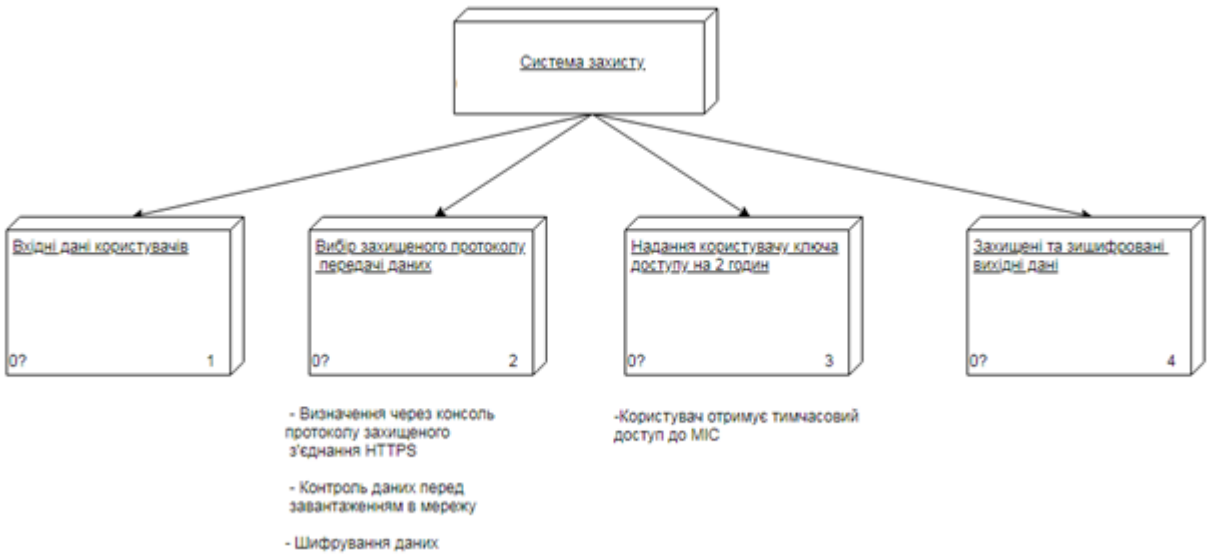


Рисунок 3.3. Діаграма дерева вузлів

Use CASE діаграма

Use Case діаграма описує усі процеси, які відбуваються під час виконання алгоритму, з точки зору користувачів. Учасниками виконання програми є адміністратор системи захисту персональних даних.

Окремі варіанти використання на діаграмі позначені еліпсами, адміністратор - фігуркою людини.

На діаграмі (рис. 3.4) зображено можливі варіанти використання програмного продукту:

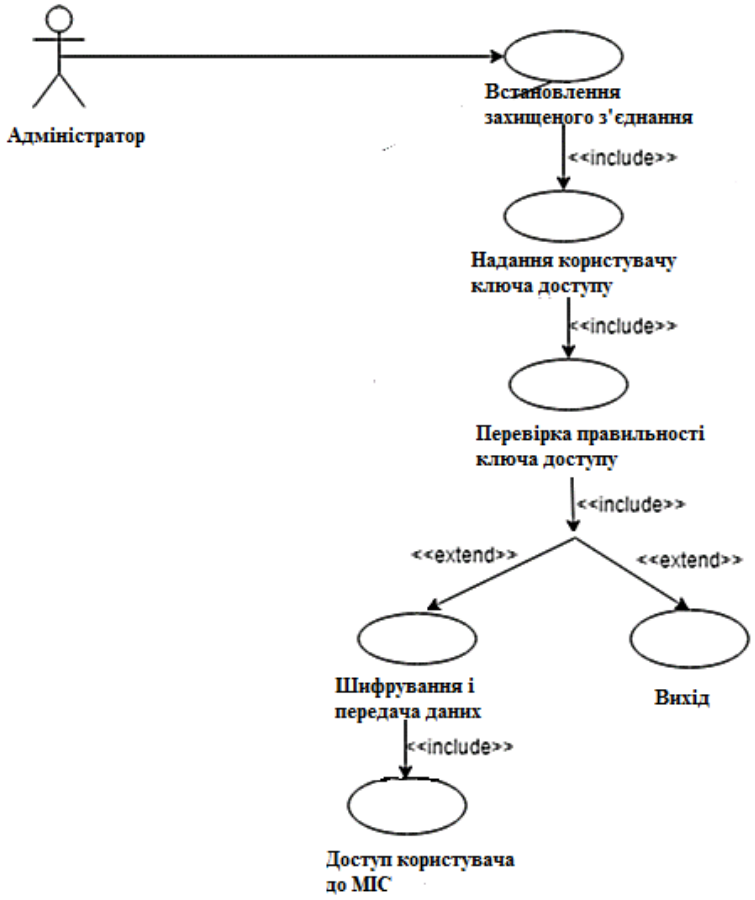


Рисунок 3.4. Діаграма варіантів

Діаграма діяльності

Діаграма діяльності є відображення алгоритму процесу роботи, що представлений на рис. 3.5.

Дана діаграма діяльностіпобудованаяк орієнтований граф, у якому вершини – це процеси, а ребра – це міжпроцесові переходи.

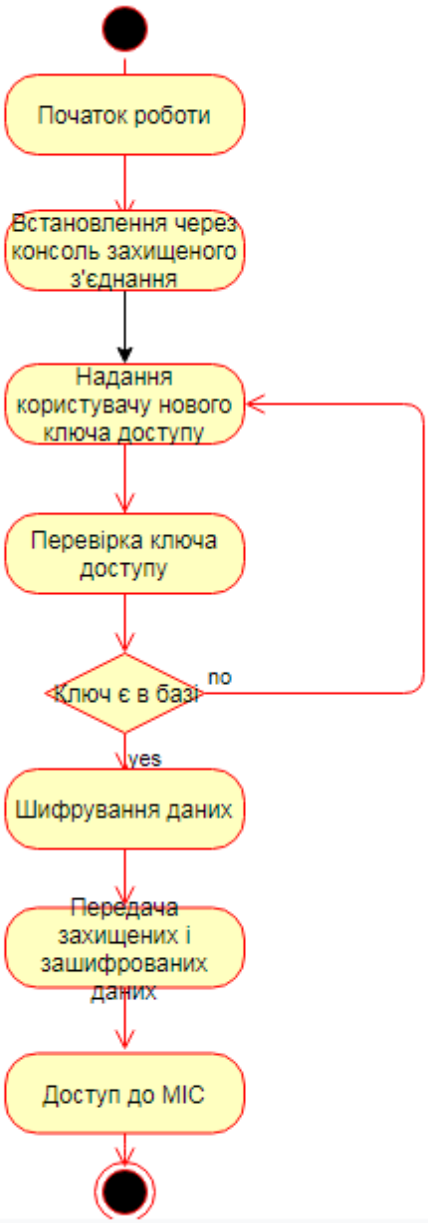


Рисунок 3.5. Діаграма діяльності

Діаграма станів

Для моделювання циклу ПЗ є необхідною діаграма станів. Вона описує процес зміни станів об’єктів у часі.

Діаграму станів зображена на рис. 3.6, та показує життєвий цикл користувача який планує увійти у медичну інформаційну систему.

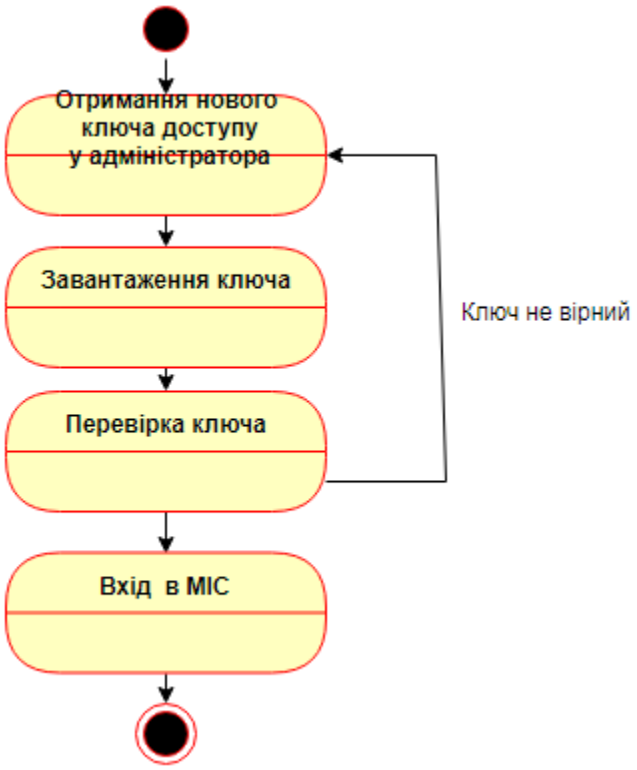


Рисунок 3.6. Діаграма станів

Загальний алгоритм роботи

На рисунку 3.7 наведено загальну схему алгоритму роботи системи захисту персональних даних за допомогою мікросервісів портативних систем управління.

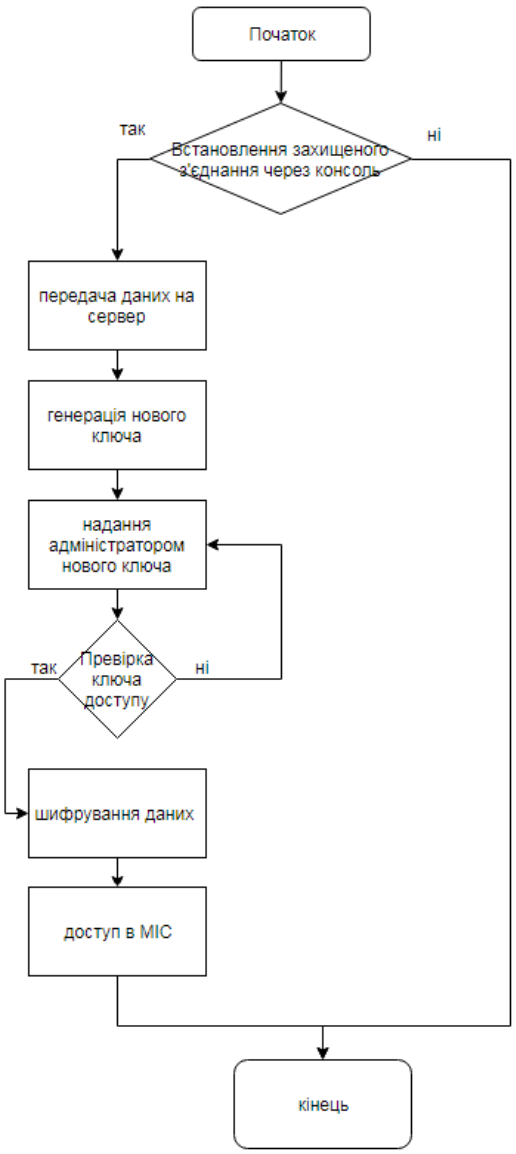


Рисунок 3.7. Схема загального алгоритму роботи

Для більш простого і ефективного збору інформації про події безпеки в складі HP ArcSight ESM і HP ArcSight Logger можуть використовуватися програмні комплекси HP ArcSight Connectors. Необхідно відзначити, що HP ArcSight Connectors також можуть поставлятися у вигляді програмно-апаратних комплексів (HP ArcSight Connector Appliance).

Рішення HP ArcSight Security Intelligence включають в себе наступні продукти:

HP ArcSight Logger - забезпечує збір і фільтрацію подій;

HP ArcSight Threat Response - забезпечує миттєву реакцію на інциденти за допомогою аналізу інформації від HP ArcSight ESM, обчислення географії проблеми і прийняття відповідних дій;

HP ArcSight Configuration Management - дозволяє настроїти мережеве обладнання та налаштування безпеки;

HP ArcSight Fraud Detection - унікальне рішення для виявлення та запобігання шахрайству в області інтернет-банкінгу і банківських (пластикових) карт.

Використання системи моніторингу на основі HP ArcSight допомагає автоматизувати процесреакціїнаподії, пов'язані з порушенням політикбезпеки. Такожзастосуваннясистеммоніторингу підвищує ефективність вже встановлених засобів захисту інформації. [6]

Сьогодні рішення від HP популярні в усьому світі серед фінансових організацій, державних структур і операторів зв'язку.

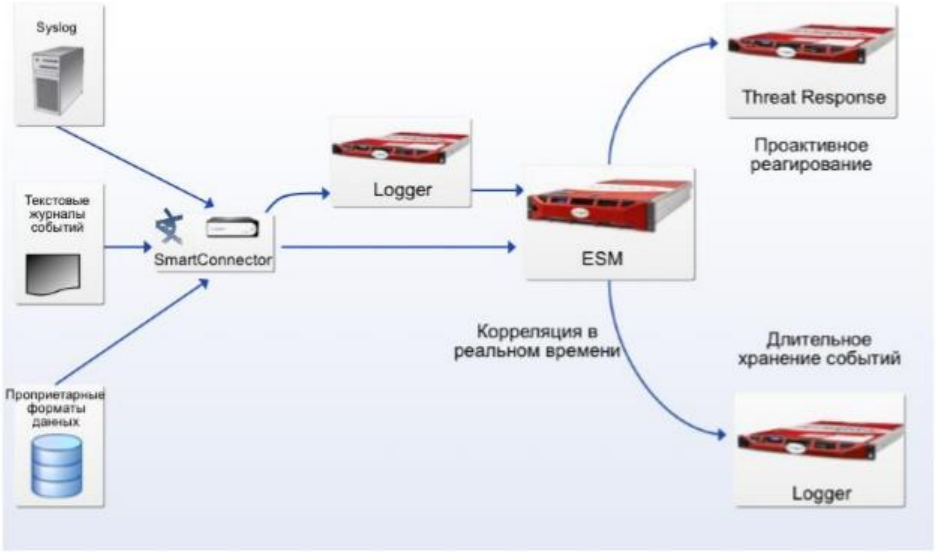


Рис.3.2. Архітектура HP Arcsight

HP Arcsight складається з наступних компонентів:

– ArcSight Manager - основний серверний компонент, «ядро» системи, що забезпечує кореляцію подій і їх обробку;

– ArcSight DB - база даних (на основі СУБД Oracle 11g), призначена для зберігання інформації;

– ArcSight Console - консоль для управління і роботою з системою, що представляє собою додаток, яке встановлюється на клієнтське робоче місце адміністратора або користувача системи;

– ArcSight Web - серверний компонент web-консолі для моніторингу та отримання звітності. Для доступу до інформації використовується будь-який сучасний web-браузер;

– ArcSightSmartConnectors-компоненти системи, забезпечують збір подійз джерел, їхпопередню фільтрацію і агрегацію,атакож передачу подій в ArcSight Manager. [7]

MAX PATROL 8

MaxPatrol 8 дозволяє отримувати оцінку стану захищеності всієї системи, а так само окремих підрозділів, додатків і вузлів. Механіка системних перевірок, контролю відповідності стандартам і тестування на проникнення, в купе з можливістю аналізу різних операційних систем, систем баз даних і веб-додатків, дають можливість забезпечувати постійний аудит безпеки на всіх рівнях інформаційної системи.

Ключові можливості

Ядром SIEM системи MaxPatrol 8 є професійний сканер вразливостей XSpider. Існуючі в ньому механізми контролю були доповнені за рахунок додавання компонентів системних перевірок і аналізу безпеки без даних. Поєднання в одному комплексі функцій системних і мережевих сканерів, а так само засобів оцінки стану захищеності систем управління баз даних та веб-

додатків, дозволяють отримувати максимально реальну картину захищеності системи.

При наявності доступу до механізмів віддаленого управління вузлом модуль сканування може використовувати їх для глибокої перевірки безпеки операційної системи і додатків. Даний метод дозволяє з мінімальним використанням ресурсів отримати комплексну оцінку захищеності, а також провести аналіз параметрів, недоступних в режимі тесту на проникнення.

База знань включає в себе системні перевірки для більшості поширених операційних систем лінійок Windows, Linux iUnix, а також спеціалізованого обладнання, такого як маршрутизатори і комутатори Cisco IOS, міжмережеві екрани Cisco PIX і Cisco ASA.

В відміну від класичних системних сканерів, MaxPatrol 8 не вимагає розгортання програмних модулів на вузлах, що спрощує експлуатацію і знижує сукупну вартість володіння. Всі перевірки проводяться віддалено з використанням вбудованих механізмів віддаленого адміністрування. За підтримки вузлом декількох протоколів (наприклад, Telnet і SSH) MaxPatrol 8 вибирає найбільш безпечний з них, що забезпечує захист чутливих даних при передачі по мережі.

Архітектура MaxPatrol:

– Безпека

– Захист даних

При передачі та зберіганні використовуються криптографічні методи захисту, що забезпечують конфіденційність і цілісність важливої інформації, такої як паролі користувачів, привілеї на доступ і т. Д. Передбачена можливість використання сертифікованих реалізацій вітчизняних криптографічних алгоритмів.

Захист трафіку забезпечується за допомогою цифрових сертифікатів і протоколу SSL / TLS, що є індустріальним стандартом, щозабезпечуєвисоку сумісність і захист даних.

Гнучка система розмежування прав доступу дає можливість здійснювати моніторинг інформаційної безпеки на різнихрівнях ієрархії (наприклад, на рівні адміністраторів, менеджерів по ІТ та ІБ підрозділу, Директора з ІБ Компанії). Для кожного з користувачів системи можна задати список завдань, які він може виконувати в системі, а також дозволу на операції над конкретними об'єктами системи. Так, адміністратору Web-серверів можуть бути делеговані права на зміну профілю сканування, запуск і перегляд результатів завдання по оцінці захищеності керованих їм серверів, але заборонено змінювати список сканованих вузлів. У той же час розробник Web-додатків матиме можливість лише переглядати звіти за результатами сканування.

Дозволи можуть призначатися на рівні MaxPatrol 8 Server або MaxPatrol 8 Consolidator. Такий підхід дозволяє адаптувати систему розмежування доступу практично під будь-яку ієрархію управління системою ІБ. [8]

Security Capsule

SIEM ссістема реєстрації подій безпеки ПАКАБ «Security Capsule »сертифікована ФСТЕК Росії для захисту конфіденційної інформації, включаючи ІСПДн. Сертифікат ФСТЕК Росії №2705 від 7 вересня 2012 року.

ПАКАБ SIEM «Security Capsule» призначений для реєстрації подій інформаційної безпеки і виконує наступні функції: реєстрація та облік подій інформаційної безпеки (ІБ) в інформаційно-обчислювальних системах і мережах, розмежування доступу користувачів до інформаційних ресурсів SIEM, контроль доступу SIEM, контроль цілісності файлів SIEM , кореляцію подій ІБ, реакцію на події ІБ.

На основі аналізу інформації, отриманої за допомогою SIEM «Security Capsule», адміністратор безпеки вживає заходів щодо забезпечення безпеки об'єктів інформаційно-обчислювальних систем і мереж.

Реєстрація подій інформаційної безпеки реалізується шляхом ведення журналів реєстрації подій інформаційної безпеки:

доступ користувача до додатка і завершення роботи;

дозволені та недозволені дії користувачів по доступу до інформаційних ресурсів;

повідомлення, одержувані від мережевих пристроїв;

дії операторів на клієнтських робочих станціях такі як: встановлення доступу до робочої станції за допомогою USB-ключа eToken; звернення до зовнішніх USB-пристроїв, звернення до файлів на зовнішніх пристроях.

Склад модулів програми, у вигляді розроблених конекторів може встановлюватися і надаватися опціонально.

За погодженням із замовником перелік конекторів може бути розширений під конкретні потреби Замовника.

Перелік розроблених конекторів, що дозволяють накопичувати такі дані про події інформаційної безпеки:

- дані від мережевих пристроїв, що використовують протокол syslog
- дані в журналах СУБД,
- дані в системному журналі ОС сімейств Windows, Linux;
- дані при застосуванні знімних носіїв інформації типу eToken, USB, LPT, COM. IEEE 1394, ZlocK, Device Lock;
- дані, отримані від СЗІ від НСД, наприклад
- дані, отримані від антивірусних засобів,
- дані, отримані з Active Direcory;
- дані реєстру ОС Windows;

– дані, отримані від IDM систем (Identity Management)

– дані, отримані від DLP систем (Data Leak Prevention)

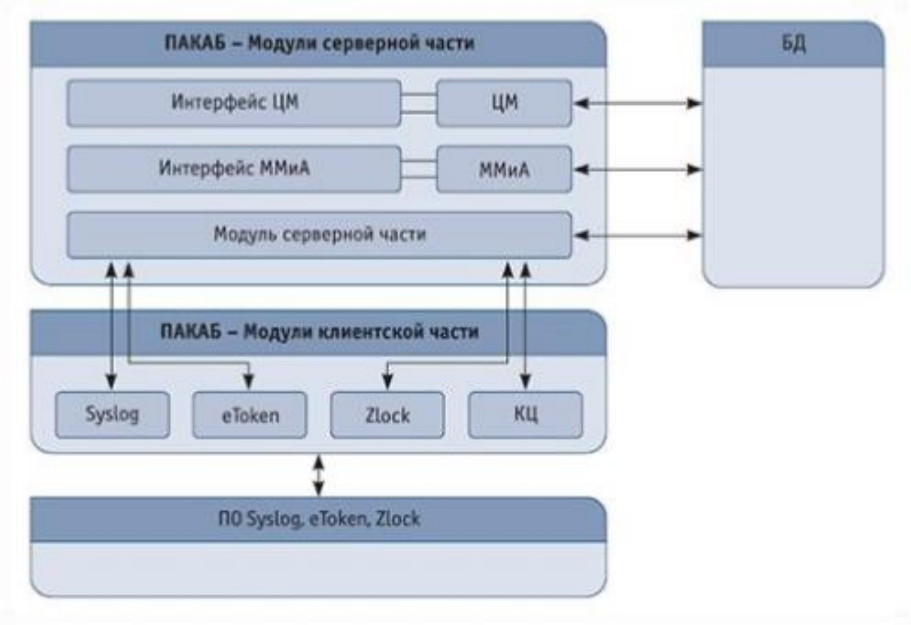


Рис. 3.3. Архітектура

ПАКАБ «Security Capsule» ґрунтується на клієнт-серверній технології для розподілених неоднорідних ІС, СПД, ЛВС і системи захисту конфіденційної інформації.

ПАКАБ «Security Capsule» має модульну архітектуру, що включає в себе:

– модульсерверної частини;

– модуль моніторингу і адміністрування;

– центральний модуль;

– клієнтські модулі;

– коннектори;

– модуль формування звітів. [9]

Таблиця 1. Порівняння SIEM систем

	Security Capsule	HP ArcSight	MaxPatrol SIEM

сертифікат щодо захисту конфіденційної інформації, включаючи ІСПДн	сертифікат від 07.09.2012 (На серійне виробництво) інспекційний контроль	Тільки у 5-й версії ESM. сертифікат від 06.05.2014 (200 примірників)	сертифікат від 31.12.2013
сертифікат відповідності за рівнем контролю відсутності НДВ	Так	немає	Так
Принцип роботи	Syslog, Eventlog, SNMP, SQL, власний протокол	збір і наступний аналіз логів (в тому числі по Syslog і з мережевих пристроїв)	За допомогою протоколу віддаленого доступу відбувається підключення до системі, аутентифікація, авторизація, збір логів ElasticSearch,
СУБД	MySQL	Своя розробка CORR-E,Red HatEnterprise	MongoDB, MS,SQL
платформа	OS Windows, OS Windows server, OS RedHat з версії 4.8, RedHat Enterprise Linux 6.X	Linux, версії 6.4 і 6.5, SUSE 11 SP3 (64 розрядна, Windows Server 2012	ОС Windows XP \ 7 \ 8, ОС Windows Server \ 2008 рік \ 2010 рік \ 2 012
Мова інтерфейсу	російська	російська або англійська	російська або англійська
Звіти	Так	Так	Так
Лог-Менеджмент	Так	Так	Так
Інцідент-менеджмент	Так	Так	да
оповіщення про інциденти	Так	Так	Так
можливість установки на сервер	Так	Так	Так

програмно апаратнареалізація	Так	Так	Так
облік вразливостей ресурсів	Так	Так	Так
управління сховищем даних	Так	Так	Так
збір логів	Так	Так	Так
кореляція	Так	Так	Так
управління інцидентами	Так	Так	Так
Захист інформації про події безпеки	Так	Так	Так

На рисунку 3.1 зображено статистику веб-додатків за високою та середньою ступінню ризику вразливості, що була проведена міжнародною компанією, що спеціалізується на розробці програмного забезпечення у сфері інформаційної безпеки Positive Technologies.[11]Високий ступінь позначений червоним кольором, середній ризик позначений жовтим кольором.

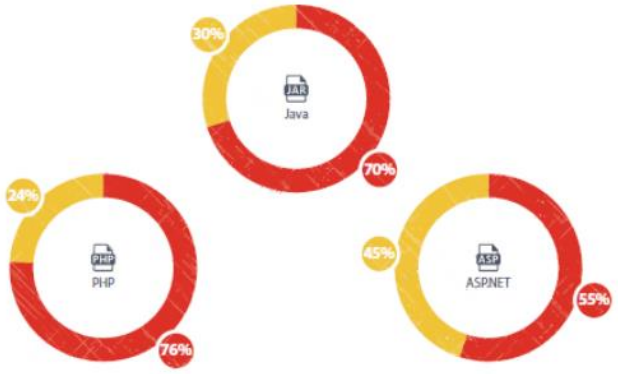


Рисунок 3.1 - Статистика веб-додатків за ступенями ризику вразливості

Як видно в рисунку 1.2, платформа має найменшу частку веб-додатків за високим ризиком вразливості.

Якщо розглянути тенденцію щодо частки сайтів, а саме – їх схильності до різних атак та врахувати мову програмування, на якій цей додаток створено – побачимо наступне (див табл.1.1). [28]

Таблиця 3.1 – Показники схильності сайтів до атак за критерієм «мова програмування»

PHP	Частка сайтів, %	Java	Частка сайтів, %	ASP.NET	Частка сайтів, %
Cross Site Scripting	90	Cross Site Scripting	80	Cross Site Scripting	73
Credential/Session Prediction	86	Fingerprinting	60	Brute Force	73
Brute Force	81	Brute Force	45	Fingerprinting	55
Information Leakage	67	Credential/Session Prediction	45	Cross Site Request Forgery	55
SQL Injection	62	Server Misconfiguration	35	Credential/Session Prediction	45
Fingerprinting	43	Information Leakage	30	Information Leakage	45

Загальномовне середовище виконання CLR і платформа .NET Framework надають багато корисних класів і служб, які дозволяють розробникам легко створювати безпечний код, а адміністраторам – налаштовувати доступ до захищених ресурсів. Крім того, середовище виконання і платформа .NET надають корисні класи і служби, що дозволяють використовувати шифрування і безпеку на основі ролей, що і буде реалізовано в захищеному веб-додатку. Систему безпеки в .NET можна представити у вигляді декількох функціональних блоків (рисунок 4.2).

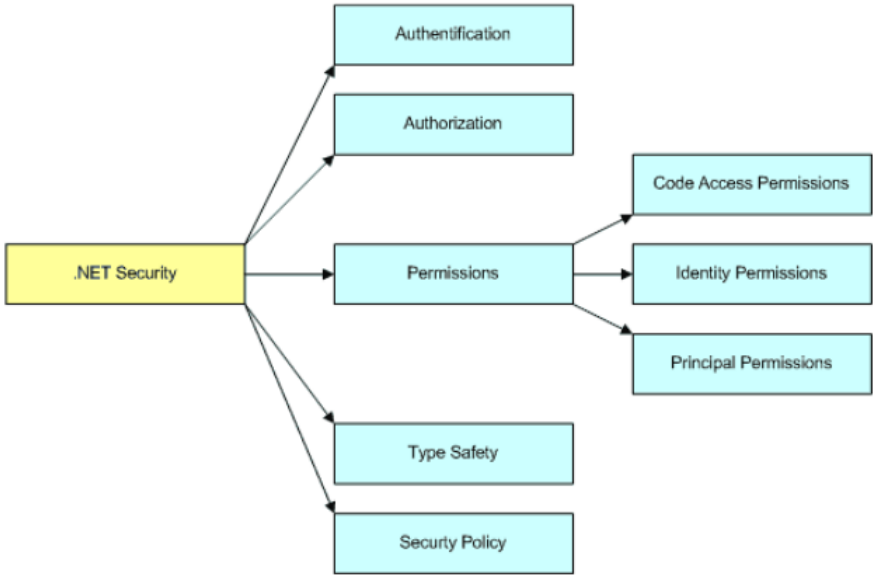


Рисунок 3.2 – Система безпеки

Робота і управління цими службами доступні як адміністраторам, так і прикладним програмістам. В .NET Framework визначено чотири групи політик безпеки (Policy Level): Enterprise, Machine, User і Application Domain. Кожен з рівнів містить свій набір правил, на основі яких визначається які права можна надати коду.[2]

Рівень Enterprise поширюється на кожен комп'ютер в домен і зазвичай управляється адміністраторами домену. За замовчуванням на цьому рівні всім надаються повні права.

Рівень Machine поширює свою дію на весь комп'ютер і може адмініструватися локальним адміністратором або адміністратором домену. За замовчуванням саме на цьому рівні визначається більшість налаштувань безпеки.

Рівень Personal використовується для управління настройками безпеки поточного користувача. За замовчуванням, як і на рівні Enterprise, всім надаються повні права.

Рівень AppDomain –спеціальний рівень. Особливість даного рівня в тому, що будь-які налаштування можна змінити лише програмно.

Безпека веб-додатків ASP.NET полягає в тому, що дана платформа в поєднанні зі службами Microsoft Internet Information Services (IIS) може виконувати перевірку автентичності облікових даних користувача, наприклад імен і паролів, використовуючи будь-який з перерахованих нижче методів перевірки автентичності.

1) Windows: стандартна, шифрована або вбудована перевірка справжності Windows (NTLM або Kerberos).

2) Перевірка справжності в формах, в яких розробник створює сторінку входу і управляє перевіркою достовірності в додатку.

3) Перевірка справжності за допомогою сертифікатів клієнта.

У власному веб-додатку ведення та обліку наукових заходів (конференцій) буде застосовано другий метод перевірки автентичності. ASP.NET контролює доступ доінформації на веб-сайті шляхом порівняння облікових даних, які пройшли перевірку автентичності, або їх сумісність з дозволами файлової системи NTFS або з XML-файлом, в якому перераховані авторизовані користувачі, авторизовані ролі (групи) або авторизовані команди HTTP.

Веб-додатки є одними з найбільш уразливих систем на сьогоднішній день. Чим більше критично важливих і конфіденційних даних зберігає програмне забезпечення, тим важливіше стає проведення контролю його безпеки.

Забезпечення високої доступності додатків, якісних серверних рішень і захист конфіденційних даних забезпечується розробкою надійних і безпечних програмних рішень. Застосування методів захисту веб-додатків від можливих атак полягає в запобіганні потенційних вразливостей. Для власного веб-додатку особливу увагу слід приділити запобіганню XSS-атакам, CSRF-атакамта SQL-ін’єкціям. [8] Оскільки дані види атак є найнебезпечнішими, якщо за критерій брати сферу приналежності веб-додатку (Інформаційні технології).

3.4. Підбір найбільш ефективного набору засобів захисту інформації

Пристрої стандарту 802.11 зв’язуються один з одним, використовуючи в якості передавача даних сигнали, що передаються в діапазоні радіочастот. Дані передаються по радіо відправником, які вважають, що приймач також працює в обраному радіодіапазоні. Недоліком такого механізму є те, що будь-яка інша станція, що використовує цей діапазон, теж здатна прийняти ці дані.

Якщо не використовувати який-небудь механізм захисту, будь-яка станція стандарту 802.11 зможе обробити дані, послані по бездротовій локальній мережі, якщо тільки її приймач працює в тому ж радіодіапазоні. Для забезпечення хоча б мінімального рівня безпеки необхідні наступні компоненти.

- Засоби для ухвалення рішення щодо того, хто або що може використовувати бездротову LAN. Ця вимога задовольняється за рахунок механізму аутентіфікації, що забезпечує контроль доступу до LAN.
- Засоби захисту інформації, переданої через безпровідне середовище.

Ця вимога задовольняється за рахунок використання алгоритмів шифрування.

На рис. 3.11. показано, що захист в бездротових мережах забезпечується як за рахунок аутентифікації, так і завдяки шифруванню. Жоден з названих механізмів окремо не здатний забезпечити захист бездротової мережі.

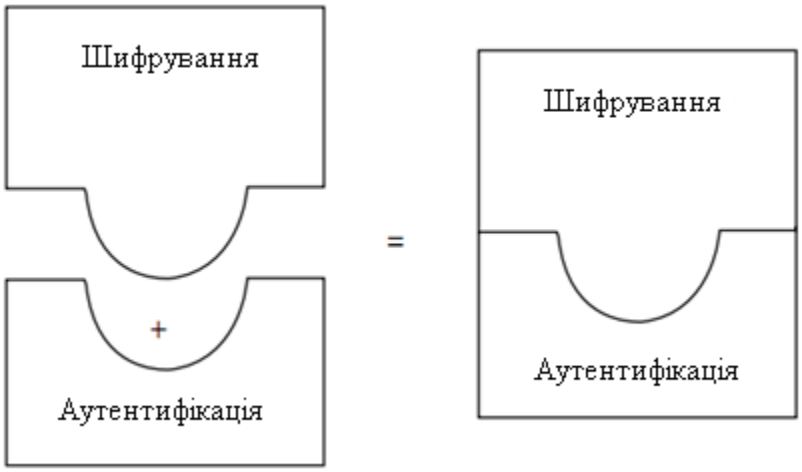


Рисунок 3.11 – Захист в бездротових мережах забезпечується за рахунок аутентифікації і шифрування

Також існують головні та допоміжні методи захисту представлені на рисунку 3.12.

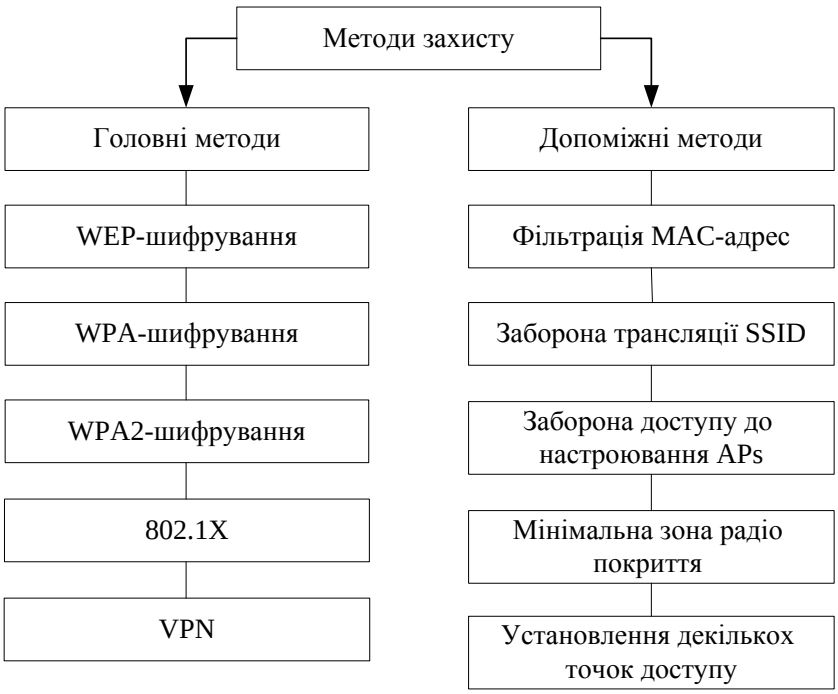


Рисунок 3.12 – Класифікація методів захисту бездротових локальних мереж

Розглянемо кожен з методів більш детально:

3. Основні методи захисту

WEP (Wired Equivalence Privacy) – це протокол шифрування, що базується на алгоритмі RC4. Алгоритм використовує ключі довжиною 64, 128, 256 та 512 біт. Чим більше біт використовується для зберігання ключа, тим більше можливих комбінацій ключів, а відповідно більша стійкість мережі до злому.

Але довжина ключа тільки сповільнить дію хакера на деякий час, а не зупинить його. Частина ключа WEP є статичною (40 біт у випадку 64-бітного шифрування), а інша частина (24 біт) – динамічна (вектор ініціалізації), тобто вона змінюється в процесі роботи мережі. Головною уразливістю WEP протоколу є те, що вектори ініціалізації повторюються через деякий проміжок часу.

Отже, для досягнення мінімального рівня безпеки ключі необхідно періодично змінювати. Якщо для бездротової мережі, що складається з точки доступу та трьох клієнтів, це не буде складати великої проблеми, то для корпоративних мереж із сотнями бездротових користувачів дане рішення не підходить. Більше того, для забезпечення достатнього рівня безпеки при використанні WEP-шифрування потрібна зміна 64-бітного ключа раз у пів години, а 128-бітного – раз у годину (в реальності ключі часто вводять один раз і назавжди).

WPA (Wi–Fi Protected Access) – протокол, в основі якого покладено підмножину стандарту IEEE 802.11i. В WPA використовується декілька засобів й алгоритмів для вдосконалення методів керування ключем та шифрування.

Якщо в WEP протоколі ключ, що використовується для шифрування даних, вводиться ручним способом та використовується до тих пір, поки не буде змінений, то в WPA ключ вводиться один раз, але використовується не для шифрування даних, а для генерації справжніх ключів для шифрування даних. WPA періодично змінює ключ. Отже, навіть якщо зловмиснику пощастить, і він відгадає ключ шифрування, то зможе ним користуватися лише до того часу, доки

бездротова точка доступу та клієнт автоматично не змінять його. Ключ шифрування в бездротових точках доступу змінюється доволі часто: раз на 1-2 години.

У стандарті WPA передбачено використання захисних протоколів 802.1x, EAS, TKIP і RADIUS. Конфіденційність та цільність даних забезпечуються за допомогою протоколу TKIP (Temporal Key Integrity Protocol), який на відміну від протоколу WEP використовує інший механізм генерації ключів, щоправда він теж заснований на алгоритмі RC4. Якщо в WEP довжина вектору ініціалізації дорівнює 24 бітам, то в протоколі TKIP використовується 48 біт. Крім того, вектор ініціалізації відбирається не випадково (псевдо-випадково) як раніше, а послідовно, до того ж пакети, що прийшли з невірним номером, відкидаються геть. Це виключає можливість здійснення reply-атаки. У протоколі TKIP новий ключ формується для кожного нового пакету, для цього використовується криптографічний контроль суми MIC (Message Integrity Code), призначеного для контролю цілісності пакетів та виявлення підробки у бездротових мережах, що перешкоджають зловмиснику змінювати зміст пакетів.

У системі передбачено два режими роботи: PSK (Pre-Shared Key) та Enterprise (корпоративний). Pre-Shared легко розгорнути, простий у використанні та налаштуванні, використовується для користувачів малого та домашнього офісу. Система Enterprise більш надійна завдяки серверу ідентифікації, що використовується для середніх та великих підприємств.

WPA2-шифрування – це система шифрування, заснована на остаточній редакції стандарту IEEE 802.11i. Алгоритм шифрування побудовано на блочному шифрі стандарту AES (Advanced Encryption Standard). Захисний протокол, що його використовує, отримав назву Counter-Mode CBC MAC Protocol (CCMP). Основна різниця між протоколами CCMP і TKIP знаходиться на рівні шифрування, дешифрування переданих даних: TKIP використовує чотири тимчасових ключі

шифрування, а AES – три. Механізм керування ключами в обох випадках однаковий.

Недоліком системи можна вважати те, що через велике навантаження алгоритму на центральний процесор бездротового клієнтського обладнання для переведення мережі на новий стандарт необхідно нове обладнання, що підтримує алгоритм шифрування AES. Вважається, що цей алгоритм, так само як WPA, при правильному налаштуванні майже неможливо зламати.

802.1X – це стандарт безпеки, що включає декілька протоколів. Почнемо з протоколу EAP (Extensible Authentication Protocol). Протокол розширеної ідентифікації.

У документі RFC 2284 протокол EAP описано наступним чином: “Розширений протокол ідентифікації (EAP) – це загальний протокол для підтвердження автентичності протоколу PPP, який підтримує кілька механізмів ідентифікації. EAP не обирає певний механізм ідентифікації на етапі керування каналом, а відкладає вибір до етапу ідентифікації. Це дозволяє ідентифікатору запитати більше інформації ще до вибору певного механізму. Це також відкриває можливість для застосування підтримуючого серверу, який реалізує різні механізми, тоді як ідентифікатор на рівні PPP просто пропускає через себе всі необхідні для ідентифікації повідомлення”.

Серед плюсів протоколу EAP можна зазначити наступне: підтримка різних методів ідентифікації без необхідності фіксувати який-небудь механізм на етапі керування каналом, пристрій може працювати як агент, що переадресує запити RADIUS-серверу, тобто обладнання буде тільки стежити за результатами ідентифікації та відстежувати наслідки вдалих або невдалих ідентифікацій.

Поряд з цим, у даного протоколу є декілька мінусів: він не підтримує динамічний розподіл ключів; уразливий до атаки «людина посередині» з використанням фальшивої точки доступу та до атаки на сервер ідентифікації:

зловмисник може підслухати запит та зашифровану відповідь, після чого провести атаку з невідомим відкритим або зашифрованим текстом.

RADIUS (Remote Authentication Dial-In User Server). Широко використовується в багатьох мережах. Його можна визначити як протокол безпеки, в якому для ідентифікації віддалених користувачів використовується модель клієнт-сервер. Він реалізується у вигляді серії запитів та відповідей, які клієнт передає від сервера доступу до мережі (Network Access Server - NAS) кінцевому користувачу. Протокол RADIUS був розроблений у відповідь на необхідність мати який-небудь метод ідентифікації, авторизації та обліку дій користувачів, яким необхідний доступ до різних обчислюваних ресурсів.

4. Серед допоміжних методів слід виділити наступні

Фільтрація MAC-адреси. MAC-адреса (Media Access Control - керування доступом до носія) – це унікальний ідентифікатор обладнання, що надає виробник. Фільтрація MAC-адреси міститься у розширенні доступу до мережі тільки визначених користувачів. Це створює зловмиснику додаткову заваду, але не зупиняє його. Крім того необхідність своєчасно поновляти список MAC-адрес важко здійсненна для великих мереж.

Заборона широкомовної трансляції ідентифікатора SSID. SSID – ідентифікатор мережі, знання якого є необхідною умовою для підключення. SSID може широко транслюватися в ефір або бути «прихованим» – у такому випадку клієнту прийдеться прописати ідентифікатор у налаштуваннях свого підключення. Більшість обладнання дозволяє його приховати, так що при скануванні мережі цього не буде видно. Крім того, необхідно змінити SSID, встановлений з початку. Звісно, це не надто серйозна перешкода, але вона є необхідною для елементарних заходів обережності.

Заборона доступу до налаштувань точки доступу або роутера через бездротову мережу. Активувавши цю функцію можна заборонити доступ до

налаштувань точки доступу через Wi-Fi мережу, але це не захистить від перехоплення трафіку або від проникнення до мережі.

Мінімально припустима зона радіо покриття. В ідеалі вона не повинна виходити за межі контрольованої території. При необхідності можна встановити параболічні відбивачі, що перешкоджають розповсюдженню сигналу в небажаних напрямках.

Встановлення декількох точок доступу в бездротовій мережі не тільки створює резервну смугу пропускання на випадок виходу з ладу однієї з точок, але й підвищує стійкість мережі до деяких видів атак.

Висновки до третього розідлу

Отже розглянувши усі доступні на сьогоднішній день методи захисту, можна виділити головні: WEP, WPA, WPA2, 802.1X. Який саме метод вибрати залежить від мети, яку переслідує ко¬ристувач, та від існуючого обладнання. WPA2 та 802.1X - більш нові методи захисту, вони по¬требують потужного обладнання для крипто¬графічних обчислень. Якщо пристрої спромож¬ні підтримувати ці методи, то краще вибрати саме їх. Якщо ні, то можна зупинити свій вибір на WPA, якщо і цей стандарт обладнанням не підтримується, то хоча б на WEP.

ВИСНОВКИ

Бездротові сенсорні мережі – основа технології Інтернету речей. Широке застосування технології Інтернету речей неможливе без забезпечення функціональної та інформаційної безпеки бездротових сенсорних мереж.

Основні вимоги до функціональної безпеки бездротових сенсорних мереж регламентовані сімейством міжнародних стандартів МЕК 61508 та МЕК 61511. Головна особливість цих нормативних документів – ризик-орієнтований підхід.

Нормативні документи, спрямовані на регламентацію вимог до інформаційної безпеки, поки що не розроблені, що стримує розвиток технології Інтернету речей та її впровадження у різні сфери людської діяльності.

Проаналізовані підходи до забезпечення інформаційної безпеки бездротових сенсорних мереж. Проаналізовано види атак на бездротові сенсорні мережі, наслідки дії цих атак і основані методи та засоби боротьби з загрозами та наслідками цих атак.

Отже розглянувши усі доступні на сьогоднішній день методи захисту, можна виділити головні: WEP, WPA, WPA2, 802.1X. Який саме метод вибрати залежить від мети, яку переслідує ко¬ристувач, та від існуючого обладнання. WPA2 та 802.1X - більш нові методи захисту, вони по¬требують потужного обладнання для крипто¬графічних обчислень. Якщо пристрої спромож¬ні підтримувати ці методи, то краще вибрати саме їх. Якщо ні, то можна зупинити свій вибір на WPA, якщо і цей стандарт обладнанням не підтримується, то хоча б на WEP.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Digital, Social and Mobile in 2015 report indicates [Електронний ресурс] –Режим доступу до ресурсу: http://wearesocial.com/sg/special-reports/digital-social-mobile-2015

2. Веб-фреймворки и с чем их едят [Електронний ресурс] –Режим доступу до ресурсу: http://iwsm.ru/blog/show/veb-freymvorki-i-s-chem-ih-edyat.

3. Фреймворки в веб-разработке [Електронний ресурс] –Режим доступу до ресурсу: : https://web-creator.ru/articles/about_frameworks.

4. Результаты тестирования шести ведущих фреймворков на производительность [Електронний ресурс] –Режим доступу до ресурсу: http://www.alrond.com/ru/2007/jan/25/rezultaty-testirovanija-6-frameworks/.

5. Адаптивные CSS-фреймворки, сетки, классы видимости [Електронний ресурс] –Режим доступу до ресурсу: http://klondike-studio.ru/blog/responsive-css-framework/.

6. Обзор CSS-фреймворков [Електронний ресурс] –Режим доступу до ресурсу: http://iantonov.me/page/obzor-css-frejmvorkov.

7. Використання PHP фреймворків в розробці сайту [Електронний ресурс] –Режим доступу до ресурсу: http://ukrbukva.net/page,5,39718-Ispol-zovanie-PHP-freiymvorkov-v-razrabotke-saiyta.html.

8. Сравнение каркасов веб-приложений [Електронний ресурс] –Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Сравнение_каркасов_веб-приложений.

9. Обзоры Web-фреймворков [Електронний ресурс] –Режим доступу до ресурсу: https://praktikatech.wordpress.com/category/обзоры-web-фреймворков/

10. Полное руководство по Yii [Електронний ресурс] –Режим доступу до ресурсу: http://www.yiiframework.com/doc/guide/1.1/ru/index.

11. Каркас веб-приложений [Електронний ресурс] –Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Каркас_веб-приложений.

12. Что такое фреймворк? [Електронний ресурс] –Режим доступу до ресурсу: http://www.dbhelp.ru/what-is-framework/page/.

13. Десять причин избегать тяжеловесных фреймворков, а также лишних зависимостей в проекте [Електронний ресурс] –Режим доступу до ресурсу: http://eax.me/avoid-frameworks/.

14. 5 самых популярных фреймворков 2014года [Електронний ресурс] –Режим доступу до ресурсу: http://lpgenerator.ru/blog/2016/03/10/5-samyh-populyarnyh-frejmvorkov-2014-goda/.

15. What is a Web Framework? [Електронний ресурс] –Режим доступу до ресурсу: https://jeffknupp.com/blog/2014/03/03/what-is-a-web-framework/.

16. Популярные frontend и backend фреймворки [Електронний ресурс] –Режим доступу до ресурсу: http://web-diz.com.ua/poleznosti/populyarnye-frontend-i-backend-freymvorki/.

17. О фреймворках [Електронний ресурс] –Режим доступу до ресурсу: http://web-elive.com/stati/raznoe/o-frejmvorkax/.

18. Веллинг Л. Разработка веб-приложений с помощью PHP и MySQL / Л. Веллинг, Л. Томсон. –Москва: Вильямс, 2010. –848 с.

19. Шлосснейгл Д. Профессиональное программирование на PHP / Джордж Шлосснейгл.–Москва: Вильямс,2006. –624 с.

20. Кузнецов М. В. PHP 5 на примерах / М. В. Кузнецов, И. В. Симдянов, С.

21. 103В. Голышев.–Санкт-Петербург: БХВ-Петербург., 2005. –576 с.

22. Кухарчик А. С. PHP: обучение на примерах / А.С.Кухарчик.–Минск: Новое знание, 2004. –240 с

23. Аткинсон Л. PHP 5. Библиотека профессионала / Л. Аткинсон, З. Сураски.–Москва: Вильямс, 2006. –944 с.

24. Мазуркевич А. М. PHP: Настольная книга программиста / А. М. Мазуркевич, Д. С. Еловой.–Минск: Новое знание, 2004. –480 с.

25. Суэринг С. PHP и MySQL. Библия программиста / С. Суэринг, Д. Парк, Т. Конверс.–Москва: Вильямс, 2010. –912 с.

26. Дронов В. А. PHP 5/6, MySQL 5/6 и Dreamweaver CS4. Разработка интерактивных Web-сайтов / Владимир Александрович Дронов.–Санкт-Петербург: БХВ-Петербург., 2009. –544

27. AUMA – функциональная безопасность – SIL. https:www.auma/ru/reshenija/service- conditirus functional-safety-sil/.

28. Palagin O.V., Romanov V.O., Galelyka I.B., Voronenko O.V., Brayko Yu.O., Imamutdino- va R.G. Wireless sensor network for precision farming and environmental protection. Informa- tion theories and applications. 2017. Vol. 24, N 1. P. 19–34.

29. Функциональная безопасность часть 5 из 6. Жизненный цикл информационной и функциональной безопасности. https://habrahabr.ru/post/322428/

30. Функциональная безопасность часть 6 из 6. Оценивание показателей функциональной безопасности и надежности. https://habrahabr.ru/post/323776

31. ITU-T Recommendation E.408. Telecommunication Network Security Requirement, 2004.

32. Walters J.P., Liang Z., Shi W., Chaudhary V. Wireless Sensor Network Security: A Survey. Security in Distributed, Grid and Pervasive Computing. Yang Xiao (Eds), 2006.

33. Hu Y., Perrig C., Johnson D.B. Packet leashes: a defense against wormhole attacks in wireless networks. Twenty-Second Annual Joint Conference of

the IEEE Computer and Communica- tions Societies, Vol. 3. 3 April 2003. P. 1976–1986.

34. Blackert W.J., Gregg D.M., Castner A.K., Kyle E.M., Hom R.L., Jokerst R.M. Analyzing inte- raction between distributed denial of service attacks and mitigation technologies. Proc. DARPA Information Survivability Conference and Exposition. Vol. 1. 24 April 2003. P. 26–36.

35. Pathan A.S.K., Hyung-Woo Lee, Choong Seon Hong. Security in wireless sensor networks: issues and challenges. Advanced Communication technology (ICACT). 2006.