УДК 004.056.53
DOI: 10.31673/2409-7292.2019.014852

А.М. Зідан, А.М. Котенко
https://orcid.org/0000-0002-4793-3305

АНАЛІЗ НЕДОЛІКІВ СИСТЕМ АВТОМАТИЗОВАНОГО ЗАХИСТУ ІНФОРМАЦІЇ ПІДПРИЄМСТВА ВІДНОСНО ІНСАЙДЕРСЬКИХ АТАК ТА МЕТОДИ ВДОСКОНАЛЕННЯ ЗАХИСТУ

В статті розглянуто та проведений аналіз методів автоматизованого захисту інформації підприємства. Визначені недоліки систем автоматизованого захисту та запропоновані методи вдосконалення захисту.

Ключові слова: захист інформації, загроза, інсайдер, атака, система захисту

На сьогоднішній день інформаційні технології використовуються для втручання в діяльність як підприємств так режимних об'єктів інформації. Загалом основним напрямком дій зловмисників у кіберпросторі є блокування серверів та ресурсів за допомогою DDoS – атак та комп'ютерних атак, метою яких є:

1. Виведення з ладу комунікаційних мереж та систем зв'язку за допомогою вірусів.
2. Блокування веб-сайтів за допомогою спамів.
3. Розміщення повідомлень дискретизаційного спрямування на офіційних веб-сайтах державних установ та комерційних організацій.
4. Викрадення даних.

Тому комерційні підприємства все частіше розпочинають свою діяльність із атестації об'єктів інформації, що є необхідним для розуміння рівня надійності системи автоматизованого захисту інформації підприємства. За поняття захищеності систем автоматизованого захисту інформації ми приймаємо рівень механізмів захисту відносно ризиків відповідно існуючим загрозам. Є велика кількість загроз системам автоматизованого захисту, якими можуть скористатись інсайдери. Відповідно є декілька факторів. Що визначають рівень автоматизованого захисту:

1. Кожен можливий шлях загрози інформації має бути перекритий відповідним механізмом захисту;
2. Стійкість механізмів захисту, що характеризується рівнем супротиву можливим реалізаціям загроз;
3. Розмір втрат, що можуть спричинити можливі реалізації загроз.

Також наступними характеристиками систем автоматизованого захисту є:

1. *Ефективність автоматизованої системи захисту інформації* – це рівень відповідності результатів автоматизованого захисту необхідній меті;
2. *Показник ефективності автоматизованої системи захисту інформації* – це характеристика для оцінки автоматизованої системи захисту;
3. *Норми ефективності автоматизованої системи захисту інформації* – це значення показників ефективності автоматизованої системи захисту інформації, визначені нормативними документами;
4. *Категорії інформації, що захищається* – визначення градації важливості інформації, що захищається;
5. *Контроль стану автоматизованої системи захисту* – це перевірка відповідності організації та ефективності автоматизованої системи захисту інформації встановленим вимогам та нормам;
6. *Метод контролю стану ефективності автоматизованої системи захисту* – це порядок та правила застосування принципів та засобів автоматизованого захисту;
7. *Засоби контролю автоматизованої системи захисту* – це технічний або програмний засіб для контролю ефективності автоматизованої системи захисту інформації;

8. *Контроль ефективності автоматизованої системи захисту інформації* – це перевірка відповідності ефективності автоматизованої системи захисту інформації існуючим вимогам та нормам ефективності захисту інформації;
9. *Контроль проведення автоматизованого захисту інформації* – це перевірка відповідності стану організації проведення автоматизованого захисту інформації, наявності та змісту документів вимогам правових, організаційно – розпорядних та нормативних документів із захисту інформації;
10. *Організаційний контроль ефективності автоматизованого захисту інформації* – це перевірка повноти та необхідності заходів автоматизованої системи захисту вимогам нормативних документів із захисту інформації;
11. *Технічний контроль ефективності автоматизованого захисту інформації* – це контроль ефективності автоматизованої системи захисту інформації, що реалізується шляхом застосування засобів контролю.

Для визначення рівня захищеності систем автоматичного захисту інформації необхідно застосувати наступні методи:

1. Вивчення вхідних даних автоматичної системи захисту інформації;
2. Оцінка ризиків від можливої реалізації загроз системи автоматизованого захисту інформації.
3. Аналіз технологій безпеки організаційного рівня, політики безпеки підприємства, забезпечення режиму інформаційної безпеки та оцінки їх відповідності вимогам існуючим нормативним документам.
4. Аналіз конфігураційних файлів маршрутизаторів, проксісерверів, що виконують роботу із взаємодії, поштових та DNS серверів та інших критичних елементів мережевої інфраструктури.
5. Сканування зовнішніх мережевих адрес ліній зв’язку з мережі інтернет.
6. Сканування ліній зв’язку.
7. Аналіз конфігурації серверів та робочих станцій ліній зв’язку за допомогою спеціалізованих програмних агентів.

Під час реалізації вищезазначеного аналізу використовуються як активні, так і пасивні методи тестування системи автоматизованого захисту.

Активне тестування системи автоматичного захисту інформації – це імітація дій потенційного зловмисника під час атаки системи захисту.

Пасивне тестування системи автоматизованого захисту інформації – це аналіз конфігурації операційної системи та додатків за стандартами з використанням списків перевірки. Тестування виконується за використання програмних засобів або власноруч.

Для проведення аналізу необхідно мати наступні дані:

1. Повна назва об’єкту інформації та призначення.
2. Характер діяльності (науково – технічна, економічна, політична, виробнича, фінансова, військова) та рівень секретності інформації.
3. Організаційна структура об’єкта інформації.
4. Склад приміщень технічного комплексу об’єкта інформації, в яких виконується обробка інформації.
5. Особливості розташування об’єкта інформації, враховуючи межі контрольованої зони.
6. Структура використовуваного на об’єкті інформації програмного забезпечення для обробки інформації, що захищається.
7. Протоколи обміну інформацією, що захищається.
8. Загальна схема функціонування об’єкта інформації, що захищається (протоколи та режими обробки інформації).
9. Зв’язки та характер взаємодії з іншими об’єктами.

10. Склад та структура функціонування системи захисту інформації на об’єкті.
11. Перелік технічних та програмних засобів захисту й контролю на об’єкті інформації із відповідними сертифікатами та приписами до експлуатації.
12. Відомості про розробників системи автоматизованого захисту інформації.
13. Наявність служби безпеки на об’єкті інформації та служби адміністрування (автоматизованої системи, мережі, баз даних).
14. Наявніть та основні характеристики фізичного захисту об’єкта інформації.
15. Наявність та готовність проектної та експлуатаційної документації на об’єкті інформації.

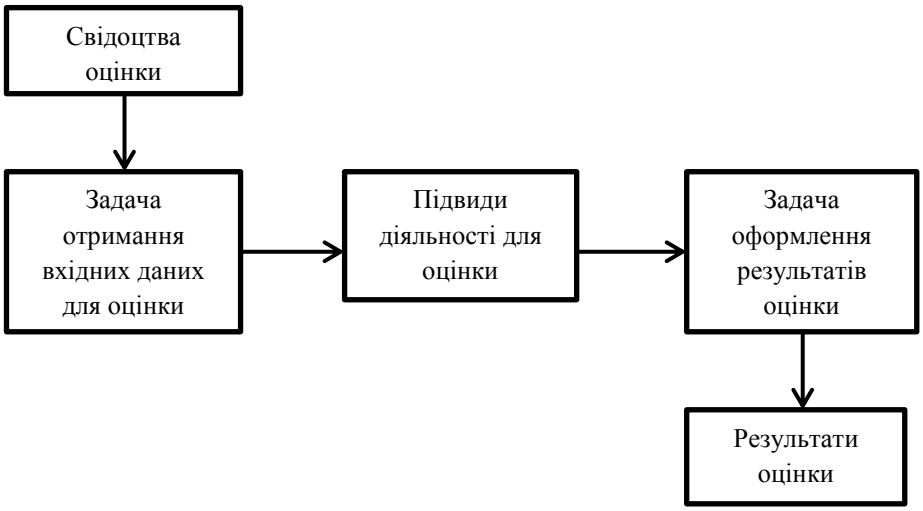

Рис. 1. Модель оцінки системи автоматизованого захисту об’єкта інформації.

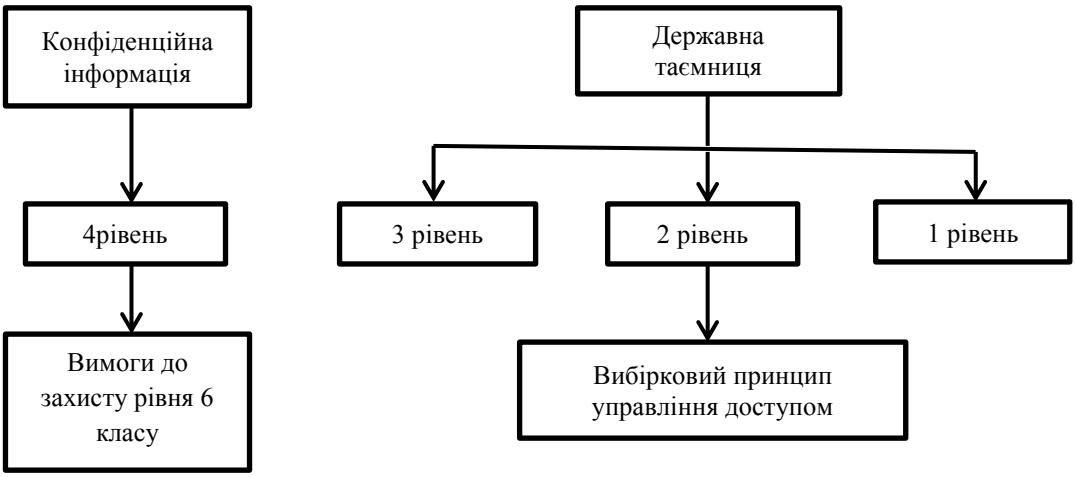

Рис. 2. Співвідношення ступеню конфіденційності інформації та рівня контролю доступом.

Також необхідно враховувати об’єкти захищеності інформації. Вони можуть бути наступними:

1. Автоматизовані системи – повинна знаходитися тільки на контрольованій території.
2. Засоби обчислюваної техніки.
3. Виділені приміщення.

4. Засоби захисту інформації.

Об'єктами захисту інформації можуть бути як комплекси, так і окремі засоби автоматизації, телекомунікаційні та інформаційні системи.

Найбільш поширеною загрозою роботі пристроїв під'єднаних до мережі Інтернет є різноманітність видів шкідливого програмного забезпечення. Можна пригадати атаки вірусів – шифрувальників WannaCry, Petya, Locky, BadRabbit тощо. Зазначені атаки призвели до великих фінансових втрат, незважаючи на існуючі системи автоматичного захисту інформації підприємств. Антивірусні програми, що працюють за процедурою перегляду великої кількості різновидів вірусів взагалі не змогли їх виявити та знешкодити.

Світовими компаніями із кіберзахисту запропоновано антивірусну систему next – generation antiviruses (NGAV) ROMAD Endpoint Defense

Переваги: використання багатоступеневої перевірки системних викликів.

Складається з:

1. *Multi – tier filtering system* – система, що відповідає за фільтрування системних вкликів.
2. *Malware Genome database* – система, що реалізує біоінформатичні алгоритми пошуку поведінкових «ДНК» шкідливого програмного забезпечення.

Траси системних викликів структуруються в так звані «фрейми», що підлягають опису в форматі ROMAD. В свою чергу детектор агрегує фрейми відповідно процесів операційної системи. Кожна генетична секвенція складається з одного і більше фреймів. Сукупність генетичних фреймів утворюють Malware Genome. Таким чином, опис шкідливого програмного забезпечення через Malware Genome не має схильностідо поліморфізму, що властиво класичним антивірусним системам. Наведений підхід до системи автоматизованого захисту дозволяє значно підвищити рівень системи захисту.

В теперішній час комерційні підприємства для оптимізації бізнес – процесів використовують CRM та ERP системи (веб - додатки) для обробки даних. Звичайно, це дає свої переваги, але має величезну вразливість цих систем. В цьому випадку необхідно розглянути застосування спеціалізованих систем захисту веб – додатків. Одним з яскравих прикладів таких систем є *Web Application Firewall* (WAF) – підвищення захисту досягається тим, що спочатку HTTP – трафік від користувачів до веб – додатку потрапляє на WAF, а потім проходить перевірка на наявність елементів атаки. Для реалізації виявлення атак використовуються наступні методи:

1. Сигнатурний аналіз.
2. Репутаційні списки.
3. Автоматичне навчання.
4. Поведінковий аналіз.
5. Ручна настройка правил.
6. Використання модулів динамічного аналізу вразливостей додатків, віртуального патчінга виявлених вразливостей, управління автентифікацією користувачів, комунікації з іншими системами захисту.

Неможна недооцінювати загрозу для інформації веб – додатків з боку інсайдерів. Співробітники, що мають доступ до даних для виконання службових обов'язків, адміністратори з прямим доступом до сервера баз даних повинні перевірятися та контролюватися. В цьому випадку ефективним є моніторинг звернень до баз даних. Для контролю локальних та мережевих підключень до баз даних використовуються агенти, що встановлюються безпосередньо на сервери баз даних. Недоліком є складність визначення користувача, що зробив запит, так як всі запити трафіку до серверу йдуть від імені

облікового запису. Для персоналізації співробітника передбачена з WAF, що аналізує трафік до сервера додатків чи передача копії трафіку до системи захисту баз даних.

Таким чином методи розмежування інформації та максимальний моніторинг, контроль доступу до інформації є основними задачами системи автоматизованого захисту.

Список літератури:

1. McAfee Labs Threat Report / [Електронний ресурс] / Режим доступу: https://www.mcafee.com/ru/resources/reports/rp-quarterly-threats-sept-2017.pdf
2. Digital Immunity Stay Productive, Stay Secure. / [Електронний ресурс]. – Режим доступу : https://www.digitalimmunity.com/wp-content/uploads/2018/04/EMA-NGES-2017-RR.pdf
3. WAF очима хакерів.URL: https://habr.com/ru/company/dsec/blog/340144/
4. SECURITYLAB. Чим захищають сайти, або Навіщо потрібен WAF? URL: https://www.securitylab.ru/analytics/475861.php
5. BISA. Впровадження і настройка web application firewall URL: https://bis-expert.ru/blog/1984/49145
6. Золотарев В.В., Федорова Н.А. Анализ защищенности автоматизированных систем. Учебное пособие – Красноярск, 2007 – 93с.
7. Яремчук Ю. Є. Комплексні системи захисту інформації : навчальний посібник / Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. – Вінниця : ВНТУ, 2017. – 120 с.
8. Комплексна_система_захисту_інформації. Електронний ресурс. URL: https://uk.wikipedia.org/wiki/