УДК 004.056.55, 003.26

*П.М. Павленко, д.т.н., проф., Е.І. Самборський*
*(Національний авіаційний університет, Україна)*

**Моделі обробки подій безпеки для управління захистом комп'ютерних систем**

*Розглянуто існуючі загрози комп'ютерним системам, проаналізовані існуючі способи їх захисту та запропоновано підхід щодо розробки моделей обробки масивів безпеки цих структур в інтегрованих SIEM - системах.*

Системний аналіз особливостей функціонування сучасних комп'ютерних систем (КС) свідчить про те, що найголовнішим аспектом для підвищення ефективності їх застосування (за рахунок ліквідації можливих загроз) є необхідність реалізації процесу управління подіями безпеки в цих складних, великих, розосереджених організаційних інформаційних структурах [1-2].

Для створення ефективних моделей та методів обробки і оптимального управління подіями безпеки КС (ПБКС) у промислово розвинених країнах світу проводиться велика кількість різноманітних досліджень та розробок. Створена значна кількість відповідних систем захисту КС. Разом з тим, кожна з цих систем збирає різноманітні дані про події безпеки в своїх форматах. Це є певною проблемою, а саме: необхідність уніфікації та агрегації масивів даних ПБКС із використанням єдиних підходів до опису тих чи інших полів із подальшою інтеграцією і масовим використанням [3-4].

Таким чином, необхідні подальші дослідження по створенню нових методів аналізу, оцінки і управління ПБКС та удосконалення існуючих, з метою підвищення ефективності систем захисту КС. Так відомо, що сучасні КС можуть піддаватися різноманітним типам загроз. Найбільш поширеними серед них є віруси, хакерські атаки, шпигунство (несанкціоноване використання програмного забезпечення) та фішинг. Кожна загроза має свої особливості, які необхідно всебічно розглядати при оцінці подій безпеки та небезпечних станів КС.

Враховуючи, що кожна з перерахованих загроз має свої специфічні, лише їй притаманні, особливості, які необхідно враховувати для оцінки небезпечних станів комп'ютерної системи, проведена класифікація та опис відомих систем захисту від розглянутих загроз. При цьому акцентована увага на сильні та слабкі сторони найбільш поширених систем та моделей, які в них реалізовані у вигляді інформаційних технологій.

Виділено три групи систем, а саме: на основі правил; на основі аномалій; на основі кореляції.

Результати їх аналізу, особливості підходів до створення моделей функціонування цих структур та приклади реалізації у відомих системах, які зараз широко використовуються для захисту інформаційних масивів в КС , а також переваги та недоліки, що їм притаманні, представлені в наступній таблиці.

*Таблиця*

Результати аналізу систем захисту КС

| Види системи | Особливості створення моделі системи та специфіка функціонування | Приклади систем захисту |
|---|---|---|
| На основі правил | Використовують заздалегідь визначені правила, які ґрунтуються на експертних оцінках атак і формуються експертами з безпеки КС. Ці моделі відносно прості в реалізації та високоточні. Але вони можуть генерувати велику кількість помилкових спрацьовувань, а також не спроможні ефективно оцінити невідомі експертам події безпеки КС та ефективно і своєчасно адаптуватися до їх варіацій. | Snort<br>Suricata<br>Iptables<br>Cisco ASA<br>McAfee<br>Norton<br>Mod Security<br>F5 BIG-IP<br>Mimecast<br>Proofpoint |
| На основі аномалій | Використовують алгоритми машинного навчання. Це дозволяє ідентифікувати шаблони в подіях безпеки та визначати і оцінювати відхилення від цих шаблонів, як потенційно шкідливе для ефективної роботи КС. Такі моделі - ефективні у виявленні та оцінці нових типів атак. Але вони можуть генерувати помилкові спрацьовування, тому що не завжди можливо забезпечити необхідну кількість вхідних даних для оперативного машинного навчання. | AISec<br>ADAMS<br>NIDPS<br>ADAMS-N<br>OSSEC<br>AIDE<br>Tripwire<br>AIDE<br>Exabeam<br>Rapid7<br>InsightIDR |
| На основі кореляції | Використовують статистичні методи для аналізу подій безпеки та визначення зв'язків між ними. Вони-ефективні для виявлення складних атак, які є багатоетапними та багатокомпонентними. Специфіка цих моделей полягає в тому, що вони потребують інтенсифікації роботи обчислювальних засобів та вимагають ресурсозатратної обробки даних. | Bro<br>SELKS<br>Splunk<br>IBM QRadar<br>Splunk<br>IBM QRadar<br>RSA NetWitness<br>McAfee<br>Enterprise<br>Security Manager<br>HP ArcSight |

Наразі для захисту КС створюються і використовуються також деякі гібридні системи (ГС). Розробники цих засобів намагалися таким чином подолати обмеження однієї системи захисту КС, поєднуючи сильні сторони інших. Реалізовані в ГС функціональні моделі дозволяють поєднати низку розглянутих вище систем, а саме систем на основі правил, на основі аномалій і на основі кореляції. Як показує досвід експлуатації КС, такий підхід дозволяє частково покращити продуктивність роботи КС за рахунок незначного

підвищення ефективності оцінки можливих атак та управління подіями безпеки цих інформаційних засобів.

Прикладами відомих гібридних систем є такі, як, наприклад HIDS, Snort, Suricata Fortinet, FortiGate, брандмауер нового покоління Check Point, McAfee Endpoint Security, Symantec Endpoint Protection, Cisco Advanced Malware Protection, FireEye Advanced Threat Protection Platform, SIEM та інші.

Серед вказаних ГС слід особливо відмітити групу систем гібридного керування інформацією та подіями безпеки – Security Information and Event Management (SIEM). Системи цієї групи використовують розглянуті раніше моделі, а саме: моделі побудовані на основі правил, аномалій і кореляції. Прикладом ГС SIEM може бути симбіоз таких структур, як RSA Security Analytics і LogRhythm. Такий підхід частково компенсує недоліки деяких не гібридних систем.

Разом з тим, активізація воєнних і терористичних дій та інтенсивне зростання кібертерорістичної діяльності в світі призводить до все активнішої модернізації і розробки нові методів і засобів формування загроз КС. Тому, з метою протидії, необхідно розробляти нові моделі, методи і на їх основі створювати і використовувати нові інформаційні технології захисту КС. Основною гіпотезою розробки э використання системно – синергетичного моделювання даних МПБС. Саме такий підхід використовується при розробці інтегрованої синергетичної системи управління подіями безпеки КС.

В основу їх функціонування покладено нові моделі та методи обробки масивів подій безпеки КС. При цьому, об’єднані відомі технології обробки інформаційних масивів із використання комбінування таких способів, як:

- лінійного способу, який передбачає послідовне оброблення кожного елементу масиву;
- багатопотокового способу, який одночасно обробляє декілька елементів масиву;
- рекурсивного способу, який враховує затримку при обробленні кожного елементу масиву, а також оптимізацію за рахунок одночасної (паралельної) обробки декількох операцій;
- радіального способу, в якому реалізується відносно рівномірне оброблення всіх елементів масиву;

У процесі обробки даних масивів БПКС враховано можливість інтеграції розглянутих способів та використано, з метою подальшої їх синергетизації, наступні моделі обробки масивів даних КС:

- MapReduce - це модель, використання якої передбачено для обробки великих об'ємів даних на віддалених вузлах мережі КС;
- Stream processing - це модель, яка використовується для обробки в реальному часі даних, що постійно надходять у вигляді потоку інформації;
- In-memory processing - це модель, яка використовується для обробки даних, записаних у пам'ять КС, для суттєвого підвищення швидкості обробки;
- Batch processing - це модель, яка використовується для обробки великих об'ємів даних в одному пакеті;
- Distributed processing - це модель, яка використовується для обробки великих об'ємів даних на декількох різних вузлах комп’ютерної мережі.

Аналіз можливостей цих моделей показав, що при гармонічному поєднання їх функціональних елементів можливо створити ефективні засоби обробки масивів ПБКС.

Таким чином, для розробки методів та інструментальних засобів ефективної протидії загрозам КС необхідно було провести дослідження та глибокий аналіз існуючих способів та моделей обробки ПБКС. Це дозволяє врахувати накопичений досвід розробників, врахувати всі існуючі переваги того чи іншого способу чи моделі і, що є головним - врахувати сучасні потреби і виклики. Аналіз досвіду використання існуючих систем захисту, функціонування яких ґрунтується на розглянутих вище моделях, свідчить про неможливість досягти бажаної оцінки подіями безпеки та реалізації ефективного управління ними в сучасних КС. Для подолання цієї ситуації авторами використовується синергетичний підхід, який дозволяє функціонально об'єднати переваги моделей, які побудовані на основі правил, аномалій або кореляції. Використання такого системно - синергетичного моделювання покладено в основу створюваного методу обробки подій безпеки і оптимального управління масивами ПБКС та розроблення інтегрованої систему захисту КС, в яких оптимізована обробка даних масивів ПБКС.

**Список літератури**

1. Bishop M. Computer Security: art and science. ISBN 0-201-44099-7. 2020. 1084 p.

2. Міжнародний стандарт ISO/IEC 27037:2012 «Інформаційні технології. Методи забезпечення безпеки. Настанови щодо ідентифікації, збору, придбання і збереження цифрових даних» [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/catalogue_detail?csnumber=4438.

3. Drew Robb, Top SIEM Products [Електронний ресурс]. – Режим доступу: https://www.esecurityplanet.com/products/top-siem-products.htm

4. Abhishek Sharma, Senior Technical Marketing Engineer at Securonix The Anatomy of a Modern SIEM: https://www.securonix.com/the-anatomy/