МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ПАВЛЮК РОСТИСЛАВ МИХАЙЛОВИЧ

Допускається до захисту:
Завідувач кафедри
інформаційних технологій,
к.т.н., доцент
_____Т. В.Нескородєва
«__» _____20__р.

ПРОГНОЗУВАННЯ ВТРУЧАННЯ У РОБОТУ ІКС НА ОСНОВІ АНАЛІЗУ "ЖУРНАЛУ ПОДІЙ"

Спеціальність 125 Кібербезпеки

Кваліфікаційна (бакалаврська) робота

Керівник
Крижановський В.Г., професор кафедри
інформаційних технологій
д-р.т.н., професор

_____
(підпис)

Оцінка: _____ / _____ / _____
(бали за шкалою ЄКТС/за національною шкалою)

Голова ЕК: _____
(підпис)

Вінниця 2021

АННОТАЦІЯ

Павлюк Р.М. Прогнозування втручання у роботу ІКС на основі аналізу "Журналу подій» Спеціальність 125 Кібербезпека, Освітня програма «Кібербезпека». Донецький національний університет імені Василя Стуса, Вінниця, 2021.

У кваліфікаційній роботі визначено сутність поняття інформаційно-комунікаційних систем, надано характеристику інформаційним ресурсам ІКС, з’ясовано особливості та призначення «Журналу подій», проаналізовано особливості роботи журналу подій, встановлено особливості очищення «Журналу подій» в ІКС та обґрунтовано важливість використання «Журналу подій» на сучасному етапі.

Ключові слова: журнал подій, інформаційно-комунікаційні системи, інформаційні ресурси, журнал безпеки, методи реалізації.

Табл. 2. Рис. 9. Бібліограф. 22

ANNOTATION

Pavliuk R.M. Forecasting of interference in the work of ICS based on the analysis of the "Journal of Events" Specialty 125 Cybersecurity, Educational program "Cybersecurity". Vasyl Stus Donetsk National University, Vinnytsia, 2021.

The qualification work defines the essence of the concept of information and communication systems, provided a description of the information resources of the ICS, clarified the features and purpose of the "Event Log", analyzed the features of the event log, established the features of cleaning the "Event Log" in the ICS and substantiated the importance of using the "Event Log" at the present stage.

Keywords: event log, information and communication systems, information resources, security log, implementation methods.

Table. 2. Fig. 9. Bibliographer. 22

ЗМІСТ

ВСТУП

Актуальність теми дослідження. В наш час інформаційно-комунікаційні системи, зазвичай, являються доволі масштабними та мають досить складну і унікальну архітектурну побудову.

Зростання загальної кількості способів та форм шкідливих впливів на інформаційно-комунікаційні системи як у комерційному секторі, так і державних організаціях, що відображено у звітах різноманітних компаній сфери інформаційної безпеки, що стало відповідним каталізуючим фактором покращення засобів та методів відповідного захисту наявної інформації. В наш час на перший план почали виходити відповідні системи керування відповідними подіями, які реєструються від різних засобів захисту інформації та елементів інформаційно-комунікаційних систем.

Крім головних засобів інформаційного захисту, для прикладу, таких як антивірусні програми, системи виявлення атак, міжмережеві екрани, засоби розмежування відповідного доступу в приміщення, також можливим є використання певних додаткових засобів – аналізаторів журналів подій, сканерів захищеності, SIEM-систем тощо. Враховуючи вище викладене має місце досить актуальна проблема дієвого аналізу та обробки наданої ними інформації щодо відповідних порушень мережевої безпеки. Загальна гострота даної проблеми обумовлена наступними причинами:

– різницею відповідних форматів звітів про одне й те саме порушення, що утворюються різними засобами (для проведення автоматизації відповідного процесу діагностування потрібно певні відомості про події приводити до одного єдиного формату);

– відповідною складністю завдання визначення взаємозв'язку подій;

– існуванням розподілених та прихованих у часових межах подій безпеки тощо.

Однак при цьому оперативність прийняття відповідного рішення стосовно реагування на виявлений комп'ютерний інцидент безпосередньо залежить від дієвості та правильності процесу діагностики.

Актуальність теми пов'язана з тим, що в останні роки різко зросла кількість можливих способів впливу на конфіденційність, цілісність і доступність інформації, що обробляється в приватних і корпоративних мережах. Причин цього явища кілька. Перш за все, зросла кількість вразливостей, які щодня виявляються в програмному забезпеченні інформаційних систем. З ускладненням систем інформаційної безпеки з'являються все більш витончені методи проникнення в систему за допомогою програмного забезпечення. В наш час основними напрямками захисту інформації є: забезпечення доступності необхідної інформації з будь-якої точки мережі, забезпечення її конфіденційності і цілісності.

Метою роботи є проведення комплексного дослідження особливостей використання методів реалізації «Журналу подій» в інформаційно-комунікаційних системах.

Об’єктом дослідження є інформаційно-комунікаційні системи.

Предметом дослідження Прогнозування втручання у роботу інформаційно-комунікаційних системах на основі аналізу «Журналу подій» в інформаційно-комунікаційних системах.

Відповідно до мети, предмету та об’єкту визначенні наступні завдання дослідження:

– визначити сутність поняття інформаційно-комунікаційних систем;

– надати характеристику інформаційним ресурсам ІКС;

– з’ясувати особливості та призначення «Журналу подій»;

– проаналізувати особливості роботи журналу подій;

– встановити особливості очищення «Журналу подій» в ІКС;

– обґрунтувати важливість використання «Журналу подій» на сучасному етапі.

Методи дослідження обрано на підставі визначених у роботі мети та завдань, із огляду на об’єкт і предмет дослідження. Методологічну основу становлять загальнонаукові та спеціальні методи пізнання. Зокрема, догматичний метод, системно-функціональний метод, метод аналізу та синтезу, абстрагування, систематизації, табличний та ілюстративний методи.

Практичне значення роботи полягає в тому, що її результати можуть бути використані в діяльності системних адміністраторів для виявлення різного виду загроз в інформаційно-комунікаційних системах на підприємстві.

Структура роботи. Робота складається зі вступу, трьох розділів, висновків та списку використаних джерел.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ВИЗНАЧЕННЯ СУТНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

1.1. Поняття інформаційно-комунікаційних систем

З початку розвитку технологій інформаційного спрямування у всьому цивілізованому світі збільшується усвідомлення усіх переваг, що може безпосередньо надати організаційній структурі інформаційно-комунікаційна система. Саме тому актуальними є питання розробки дієвих інформаційно-комунікаційних систем, що б працювали ефективно з ресурсами інформаційного спрямування, що являється досить актуальним в наш час.

Для визначення сутності поняття інформаційно-комунікаційної системи необхідно встановити, що собою являє дана система в загальному. Під поняттям «система» в загальному необхідно розуміти певну множину інформатизаційних сутностей та відповідних взаємозв'язків між ними [9, с. 510].

У відповідності із існуючим законодавством нашої держави, інформаційно-телекомунікаційна система являє собою певну множину телекомунікаційних та інформаційних систем, що в результаті опрацювання відповідної інформації працюють як одне ціле [7].

Відповідно до чинного українського законодавства передбачається кілька визначень поняття «інформаційної системи»:

– організаційно-технічна система, в котрій реалізована відповідна технологія інформаційної обробки із застосуванням програмних та технічних засобів [8, с. 18].

– система обробки відповідних даних певними накопичувальними засобами, обробки, зберігання та їх знаходження та відтворення.

Дані означення не протирічать, а навпаки доповнюють одне-одного. Для прикладу останнє визначення слугує певним уточненням того, яку саме інформаційну обробку може здійснювати інформаційна система.

Головне призначення інформаційно-комунікаційної системи (ІКС) це відповідне забезпечення комунікації та відповідної обробки інформаційних ресурсів організаційної структури.

ІКС відображає нагальну потребу покращення відповідних комунікацій в організації. Інформаційно-комунікаційна система безпосередньо забезпечує відповідний потік необхідної інформації в усіх напрямках організаційної структури. Структурну модель ІКС запропонувала С.А. Мезенцева [10]. Модель такої системи представлена на рисунку 1.1.

Рисунок 1.1. Структурна модель інформаційно-комунікаційної системи управління.

Блок вхідної інформації є приймачем інформації, як із зовнішнього, так і з внутрішнього середовища організації. Блок обробки і аналізу інформації виконує функції декодування, систематизації, узагальнення, порівняння та верифікації. Блок синтезу пропозицій генерує звіти, висновки, тенденції, проекти. Блок вихідної інформації виконує функції кодування, підготовки службової документації, розподілу інформації по каналах зворотного зв'язку.

Розглянемо як проводиться класифікація ІКС. Її можна здійснювати за великою кількістю критеріями. Так класифікація за відповідним критерієм функціональної повноти має наступний вигляд [9, с. 512]:

1. ІКС, що безпосередньо задовольняють потреби інформаційного характеру – системи інформаційного спрямування. Дані системи безпосередньо забезпечують відповідний користувацький доступ (клієнтів, персоналу, тощо) до відповідних інформаційних джерел. Вони мають забезпечувати пошук, зберігання інформації, захищений та швидкий доступ.

2. ІКС, безпосередньо призначені для того, щоб забезпечувати відповідну підтримку бізнес-процесів (системи інформаційно-аналітичного спрямування). Прикладом даних бізнес-процесів є транзакції, що проводять банківські установи .

3. ІКС, безпосередньо призначені для керування організаційною структурою, тобто системи управління автоматизованого характеру. Вони призначенні для безпосереднього забезпечення проведення автоматизації документообігу, комунікацій, контролю за здійсненням розпоряджень та наказів, тощо.

4. Системи інтелектуалізованого характеру, до котрих належать системи експертного характеру, системи оцінки прогнозування результатів рішень в управлінській сфері та ефективності, тощо. Дані системи безпосередньо забезпечують реалізацію певних окремих інтелектуальних людських функцій.

В ІКС слід виокремлювати деякі складові частини (рис. 1.2).

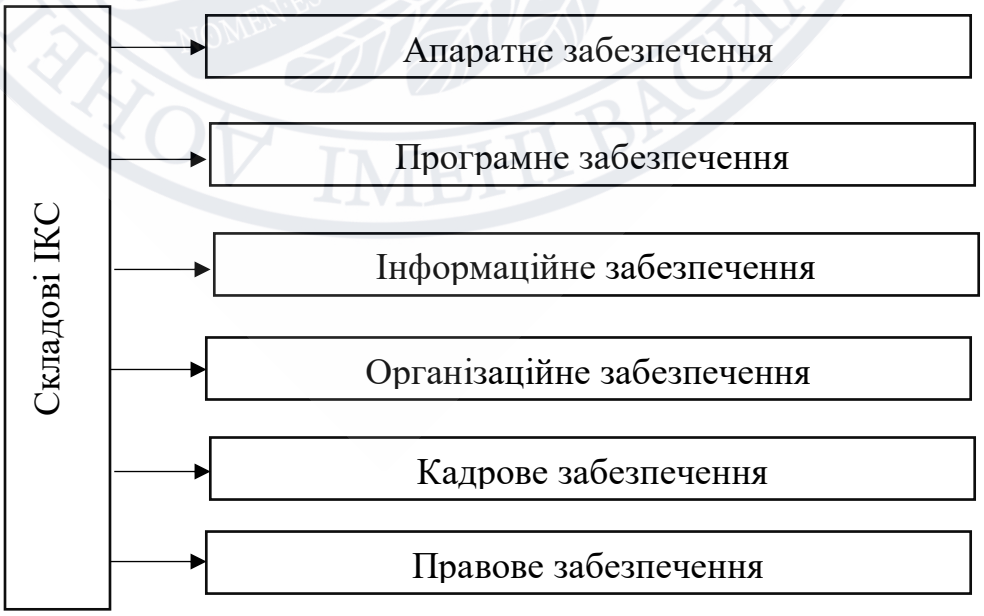

Рис. 1.2. Складові частини ІКС

Більш детально розглянемо кожну виділену частину.

Апаратне забезпечення (англ. hardware) це механічні та електронні частини обчислювального апарату, що входять до загального складу мережі або системи (дані які безпосередньо опрацьовує система та програмне забезпечення).

Власне під забезпеченням програмного спрямування ІКС слід розуміти певну множину документальних та програмних засобів для експлуатації та створення відповідної систем для обробки даних з використанням сучасної обчислювальної техніки. В залежності від реалізованих функцій все програмне забезпечення можна умовно розподілити на дві досить значні групи, а саме: системне та прикладне ПЗ [8, с. 19].

За власною суттю інформаційне забезпечення це множина нормативної бази, форм документів та відповідних рішень, які реалізовані стосовно об’ємів, розміщення та форм існування відповідної інформації, що застосовується в інформаційній системі.

Власне організаційне забезпечення являє собою певну множину засобів та методів роботи персоналу, що експлуатує відповідну систему.

Забезпечення кадрами це множина відповідних засобів та методів, проведення та організації навчання відповідного персоналу конкретно прийомам роботи з ІКС. Основною ціллю забезпечення кадрами являється відповідна підтримка працездатності ІКС та майбутнього її розвитку.

Правове забезпечення це множина норм права, що визначають відповідний юридичний статус системи.

Відповідну класифікацію ІКС є можливість також здійснювати відповідно до територіальної ознаки:

– інтегровані середні;

– локальні (системи для малого бізнесу);

– великі інтегровані (глобальні) системи [13].

Відповідно до способу організації ІКС поділяються на:

– клієнт-серверні;

– файл-серверні;

– на основі інтернет-технологій.

Можна зробити висновок, що головне призначення інформаційно-комунікаційної системи це забезпечення відповідної обробку інформаційних ресурсів організаційної структури та комунікації.

1.2. Характеристика інформаційних ресурсів ІКС

Однією із головних складових частин системи інформаційно-комунікаційного спрямування являються відповідні інформаційні ресурси. Відповідна інформація, дані та знання являються певними абстрактними об'єктами [5]. Для безпосередньої роботи із ними потрібна їх матеріалізація у вигляді відповідних ресурсів інформаційного змісту. Відповідно до законодавства нашої держави відповідний інформаційний ресурс це множина певних документів в системах інформаційного характеру (архівах, бібліотеках, банках даних) [6].

Документ це певним чином упорядкована множина інформації, даних та знань, що надає відповідні можливості передачі, доступу, обробки, тощо. Для прикладу таким документом може бути безпосередньо фільм, паперовий документ, комп'ютерний файл, тощо [9, с. 516].

Основним середовищем для зберігання відповідних документів являються відповідні системи інформаційно-комунікаційного спрямування, що забезпечують безпосередній доступ до інформації, до її обробки та обміну. Дана система не обов'язково має бути повністю комп'ютеризована.

Інформаційні ресурси можна класифікувати за наступними ознаками [8, с. 18]:

1. Приналежністю відповідного ресурсу до деякої організаційно-технологічної системи (для прикладу, ЗМІ, бібліотечної мережі, корпоративної системи);

2. Відповідним способом виділення певних об'єктів обліку (документи, твори, бази даних, видання, сайти, інтернет-сторінки, тощо);

3. Призначенням ресурсу (освіта, масова інформація, особиста переписка, бізнес, тощо)

4. Змістом ресурсу:

– тематичним;

– об'єктним;

– функціональним;

5. Видовим складом ресурсу (видами документів);

6. Джерелом інформації:

– закордонне чи національне;

– неофіційне або офіційне, тощо;

7. Правовим ресурсним статусом (об'єкти інтелектуальної власності, публічні документи, таємні документи, спам, тощо);

8. Структурним ресурсним типом, що враховує:

– можливість програм від відділення даних та представлення;

– кодування;

– формати.

9. Відкритістю ресурсу (з обмеженим доступом чи відкритий);

10. Загальним рівнем структурованості:

– неструктуровані;

– структуровані.

11. Носієм та способом поширення;

12. Мовою ресурсу;

Разом з тим, інформаційні ресурси мають низку наступних характеристик:

1. Характеристики відповідної продуктивності:

– час реакції;

– пропускна здатність;

– час затримки.

2. Характеристики відповідної надійності;

3. Характеристики розширюваності;

4. Характеристики маштабованості;

5. Повна вартість володіння;

6. Характеристики прозорості.

Власне загальну вартість володіння ресурсу інформаційного спрямування можна визначити не лише (і не стільки) вартістю вже використаних під час його створення програмних та апаратних засобів, а й відповідною вартістю інформації, що вже в нього закладена.

Інформаційні комп'ютеризовані ресурси можна розділити на наступні головні види:

– бази даних;
– файлові системи;
– сховища інформації;
– колектори інформації;
– web-ресурси.

Відповідні системи файлів є найбільш простим і найбільш поширеним типом ресурсів інформації. Вони дають змогу зберігати інформацію, дані та відповідні знання довільної структури та довільного типу.

База даних – це відповідний інформаційний ресурс, який дає змогу більш впорядковане зберігати відповідні дані по групі об'єктів, що мають певний однаковий набір деяких властивостей. Для прикладу бази даних: Microsoft SQL Server, FoxPro та інші. Відповідна класифікація баз даних здійснюється за наступними критеріями:

1. Відповідно до характеру інформації, що зберігається:

– документальні (архіви);
– фактографічні (картотеки).

2. Відповідно до способу збереження даних:

– централізовані (зберігаються лише на одному єдиному комп'ютері);

– розподілені (застосовуються в глобальних та локальних комп'ютерних мережах);

3. Відповідно до структури організації відповідних даних:

– табличні (реляційні);

– ієрархічні,

– об'єктні.

Необхідно відмітити, що під час розробки сучасних систем часом доречно застосовувати БД із змішаною структурою [11].

Інформаційні сховища застосовуються для зберігання відповідної інформації – даних з окресленими взаємозв'язками між ними. Вони являють собою відповідні системи, що, спираючись на бази даних (чи другі ресурси) надають відповідним користувачам відповідним чином підготовану інформацію. Отже, сховища інформації потрібно застосовувати саме там, де потрібно одержувати не певні окремі дані в значній кількості а вирішувати задачі аналітичного спрямування, безпосередньо пов'язані з відповідною обробкою значної кількості різнорідних даних з різноманітних джерел інформації.

Інформаційні колектори застосовуються для безпосереднього зберігання відповідних знань. Таким прикладом відповідного інформаційного колектора може слугувати бібліотечна система GreenStone, яку було розроблено в університеті Вайкато в Новій Зеландії в рамках потужного Проекту по розробці та створенню бібліотек з цифровими даними. Дані системи на пряму призначені для відповідного зберігання неструктурованої інформації, що спричиняє до низки їх особливостей.

Web-ресурси являють собою ресурси, що зберігаються на різних складових частинах, розподілених у мережі гетерогенного характеру. Відповідним прикладом даного ресурсу являється всесвітня мережа Internet. Головною перевагою цього типу ресурсу являється відповідне забезпечення

та надійність зручного доступу. Значним недоліком являється складність організації пошуку та управління.

Під час проведення розробки ІКС вагомим завданням являється відповідна організація пошуку в ресурсах значної кількості інформації. Слід виокремити наступні методи пошуку:

1. Повний перебір.
2. Класифікація.
3. Індексація.
4. Тегування.

Так, метод повного перебору являється одним єдиним методом, що можна використати для пошуку у інформаційних неструктурованих ресурсах, таких, для прикладу, як система файлів. Сутність його полягає в безпосередньому перегляді всіх наявних документальних джерел.

Основним недоліком цього методу є значний час знаходження інформації. Дієвість даного методу насамперед безпосередньо залежить саме від того, наскільки зберігає упорядковано інформацію відповідний користувач (наскільки він знає, де потрібно шукати). Основною перевагою даного методу являється те, що його використання не потребує відповідної попередньої інформаційної обробки.

Метод індексації ґрунтується на присвоєнні відповідним документам (чи атрибутам документів) деяких індексів. Ці індекси здатні бути певним чином впорядковані, що дає змогу доволі швидко здійснювати пошук потрібного документа. Цей метод застосовується для інформаційних структурованих ресурсів.

Пошуковий метод з використанням класифікації ґрунтується у відповідному визначенні деякої ієрархічної структури класів певних документів. Кожен документ відноситься до деякого класу. Прикладом може стати універсальний десятковий класифікатор (УДК). Основним недоліком даного підходу являється те, що для знаходження за відповідним класифікатором потрібно вміти більш точно знаходити, до якого саме класу

віднести деяку інформацію. Разом з тим, доволі часто відповідна інформація здатна бути безпосередньо віднесена до кількох областей знань. Для розв'язання даної порobленої ситуації в системі Yahoo було запропоновано слідуючий підхід – вказівники на відповідні підрозділи класифікатора додаються до других підрозділів. Проте в загальному підсумку ми одержуємо досить хаотичну систему [14].

Тегування ґрунтується на тому, що кожному окремо взятому документу автор у відповідність ставить набір тегів (ключових слів), що визначають його основний зміст. Основним недоліком даного підходу являється певна неоднозначність стосовно визначення основних ключових слів.

Основною модифікацією підходу, що було запропоновано Ширкі [14] є те, що теги визначають користувачі системи. В даному випадку кілька найбільш часто застосованих тегів мають коректно описувати весь документ. Проте це не позбавляє тегування його головного недоліку – різні люди є схильні застосовувати різні терміни для опису одних і тих самих понять.

Останнім часом було розпочато розробку таких засобів для оптимізації пошуку по файловій системі ПК, які дозволяють замінити повний перебір на швидший метод пошуку (Google Desktop Search). Головний принцип роботи даних засобів ґрунтується на індексації відповідних файлів на жорсткому диску. Отже, файлова система структурується. Головним недоліком даних засобів являється те, що вони на пряму підтримують певне обмежене число форматів, так як для того, щоб індексувати тільки ті значення, за якими доречно вести пошук (і відповідно одержати список індексів прийнятного розміру), потрібно знати саму файлову структуру.

Досить часто пошук відповідної інформації проводиться ієрархічно, іншими словами ведеться пошук в результатах пошуку що був перед цим. У даних випадках відповідний пошук буде здійснюватися значно швидше, якщо зберігати відповідні проміжні пошукові результати. Отже можна не розпочинати спочатку пошук. Проте даний підхід досить складно використати у певних системах пошуку, так як він потребує відповідних ресурсів

додаткового змісту. Власне саме тому доволі часто ієрархічний пошук здійснюється простим додаванням нової умови до попередніх.

Застосування класифікації, індексації та тегування потребує первинної інформаційної обробки. Дана обробка включає в себе відповідний аналіз інформації з ціллю проведення її безпосередньої класифікації. Отже, неструктуровану інформацію слід деяким чином структурувати. Аналіз документів може здійснюватися за відповідним змістом чи за діями користувачів. Аналіз за відповідними діями користувачів дає змогу визначити, наскільки саме документ безпосередньо відповідає визначеним для нього основним класам чи словам. Таким прикладом може стати індексація web-ресурсів так званими роботами систем пошуку. Дані роботи проводять оцінку релевантності відповідних сторінок. Для проведення фільтрування «небажаних» сторінок є можливість застосовувати сервіси, що дають змогу користувачам відмічати їх, так що в майбутньому вони зовсім не будуть включатися в пошук.

ВИСНОВКИ ДО ПЕРШОГО РОЗДІЛУ

Інформаційна система це організаційно-технічна система, в котрій реалізована відповідна технологія інформаційної обробки із застосуванням програмних та технічних засобів. Головне призначення інформаційно-комунікаційної системи це забезпечення відповідної обробку інформаційних ресурсів організаційної структури та комунікації.

Інформаційні ресурси класифікуються за такимим ознаками: приналежністю відповідного ресурсу до деякої організаційно-технологічної системи; відповідним способом виділення певних об'єктів обліку; призначенням ресурсу, змістом ресурсу; видовим складом ресурсу, джерелом інформації; правовим ресурсним статусом; структурним ресурсним типом; відкритістю ресурсу; загальним рівнем структурованості; носієм та способом поширення та мовою ресурсу.

РОЗДІЛ 2. ПРИКЛАДНІ АСПЕКТИ ВИЗНАЧЕННЯ ОСОБЛИВОСТЕЙ МЕТОДІВ РЕАЛІЗАЦІЇ «ЖУРНАЛУ ПОДІЙ» В ІКС

2.1. Актуальність реєстрації та аналізу подій безпеки

Підсистеми реєстрації подій безпеки є на сьогоднішній день важливими і невід'ємними компонентами систем забезпечення інформаційної безпеки практично в будь-який мережевий операційній системі. Реєстрацію подій безпеки також часто називають аудитом подій безпеки. Можливості реєстрації подій безпеки реалізовані в мережевих операційних системах і прикладному програмному забезпеченні. Однак, відчутний ефект від використання засобів аудиту досягається лише тоді, коли зареєстровані дані про події безпеки можуть бути проаналізовані. Тільки в цьому випадку стає можливим своєчасне виявлення шкідливих впливів на елементи мережевої інформаційної системи – комп'ютери, програмне забезпечення, що передають і зберігають дані тощо.

Наявність підсистем реєстрації подій безпеки є однією з основних вимог, які присутні у всіх сучасних стандартах і керівних документах з інформаційної безпеки комп'ютерних систем. Зазначені стандарти також визначають класи подій, що підлягають реєстрації. Вимоги до наявності засобів реєстрації подій безпеки відносяться до технічних вимог, тому вони, як правило, виконуються виробниками базового програмного забезпечення, використовуваного для побудови мережевих інформаційних систем.

Регулярний аналіз зареєстрованих подій безпеки зазвичай відносять до організаційних заходів, що є основною причиною недостатньої уваги виробників програмного забезпечення до проблем організації оперативного аналізу подій безпеки в мережі. Іншими словами, для того, щоб атестувати програмне забезпечення мережевої інформаційної системи на відповідність вимогам стандартів безпеки зазвичай досить реалізувати в ній лише засоби реєстрації подій безпеки.

Облік типових обсягів даних про події безпеки, а саме сотні і тисячі записів в день на одному комп'ютері в мережі, дозволяє стверджувати, що при відсутності спеціальних автоматизованих програмних засобів аналіз подій безпеки стає малоефективним. З цієї причини і обслуговуючий персонал мережевих інформаційних систем часто зневажливо ставиться до завдань аналізу зареєстрованих даних про події безпеки.

Все це в значній мірі знижує ефективність реєстрації подій безпеки, яка дає можливість виявити помилки і недоліки в реалізації політики безпеки мережевої інформаційної системи до того, як вони будуть використані в цілях зловмисників.

Засоби управління доступом, існуючі в програмному забезпеченні кожної мережевої інформаційної системи часто не можуть забезпечити безпеку в повній мірі, оскільки вони не призначені для запобігання некваліфікованим або зловмисним діям зі сторони користувачів які мають необхідні повноваження доступу. Своєчасний аналіз подій безпеки дозволяє оперативно виявляти небезпечні ситуації, що виникають внаслідок недостатньо суворого розмежування доступу і вживати заходів протидії.

Під час налаштування засобів управління доступом можуть бути допущені помилки, які найчастіше важко помітити при тестуванні, проте ці помилки стають помітні коли виникають проблеми з мережевою інформаційною системою. Своєчасний аналіз подій безпеки дозволяє виявити такі помилки до того, як вони стануть причиною порушення безпеки.

Таким чином, оперативний аналіз зареєстрованих подій безпеки в комп'ютерній мережі дозволяє підвищити захищеність мережевої інформаційної системи від різних загроз інформаційній безпеці за рахунок своєчасного виявлення вразливостей в системі захисту інформації та політики безпеки.

2.1. Особливості та призначення «Журналу подій»

Журнал подій Windows (англ. Windows Event log) – це досить детальний запис системних повідомлень, тобто повідомлень від систем безпеки та прикладних повідомлень, що безпосередньо зберігаються в операційній системі Windows, що застосовується системними адміністраторами для проведення діагностики системних проблем та прогнозування проблем в майбутньому [12].

За допомогою використання даного інструменту можна досить легко з'ясувати причину неполадок. Однак, для його застосування необхідно володіти спеціальними знаннями.

Операційна система та відповідні програми застосовують дані журнали подій для проведення безпосереднього запису важливих програмних та апаратних дій, що адміністратор здатен застосовувати для усунення безпосередніх проблем з операційною системою. ОС Windows безпосередньо відслідковує певні конкретно визначені події у власних файлах журналу, такі для прикладу, як управління безпекою, встановлення додатків, операції із відповідного налаштування системи при самому першому запуску, а також помилки або проблеми.

Кожна конкретно визначена подія у відповідному записі журналу містить таку інформацію [2]:

1. Журнал подій: містить ім'я журналу подій, в котрому виникла певна подія;

2. Джерело події : процес чи програма, яка генерувала відповідну подію. Для прикладу, усі події виходу та входу з системи походять із джерела безпеки. В даному випадку і джерело подій, і журнал подій мають одне ім'я, проте являються окремими полями;

3. Ідентифікатор події: унікальний ідентифікатор події, на основі котрого джерело провело генерування відповідної події. Ідентифікатори подій не являються унікальними між джерелами, проте постійно унікальні в межах

власного джерела. Ідентифікатор події не є особливим для кожної окремо взятої події, а тільки для кожної події деякого типу. Для прикладу, всі події блокування записів обліку Windows розташовуються в журналі безпеки із відповідним ідентифікатором події та джерелом захисту;

4. Тип події: це відповідне поле, яке описує відповідний тип події, що відбулася, і може бути корисним для визначення того, який саме 0тип діяльності створив відповідну подію;

5. Категорія події: розподіляє відповідні події на певні конкретні групи в залежності від самого типу події. Для прикладу, події категорії Logon / Logoff мають декілька ідентифікаторів подій, що належать до категорії;

6. Час/Дата: дата та час відповідної події застосовуються для обрахунку загальної кількості конкретної події в будь-який момент часу на протязі дня в будь-який конкретно визначений день тижня. Власне день тижня застосовується через те, що користувач можете мати більшу кількість запитів на вхід у визначений час у середу, ніж у неділю;

7. Ідентифікатор сервера: унікальний ідентифікатор для кожного сервера. Він є доволі корисним, щоб безпосередньо допомогти адміністратору зв’язати сповіщення з певним сервером, щоб безпосередньо визначити, де з’явилася проблема;

8. Ідентифікатор користувача: логін користувача.

Відповідні записи журналу подій безпосередньо зберігаються у відповідному ключі реєстру: *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog* [17].

Цей ключ містить певні підключі, які мають назву файлів журналу. За замовчуванням є присутніми:

– файл відповідного журналу додатків – для служб та застосунків;

– файл безпекового журналу – для подій аудитної системи;

– файл журналу системи – для подій драйверів певних пристроїв.

Наявна відповідна можливість створювати певні додаткові журнали. Для кожного джерела подій в журналі створюється певний окремий підключ. Події

від кожного джерела здатні безпосередньо включатися в окрему для кожного джерела категорію. Події мають відноситися до одного із п'яти встановлених типів (табл. 2.1) [3].

Таблиця 2.1

Типи подій

Тип	Опис
Інформація	Події вказують на важливі та рідкісні операції, які були успішними
Попередження	Події, що вказують на виникаючі проблеми, що не потребують швидкого втручання, проте здатні призвести до помилок в подальшому майбутньому. Прикладом даного роду подій може слугувати вичерпання всіх наявних ресурсів.
Помилка	Події безпосередньо вказують на значні проблеми, що досить часто спричиняють втрату самої функціональності чи безпосередньо даних. Для прикладу, це може бути неможливість запуску певної служби під час завантаження.
Вдалий аудит	Події безпеки, що трапилися при вдалому зверненні до відповідних ресурсів, що проходять аудит. Для прикладу, це може бути успішний вхід в саму систему.
Невдалий аудит	Події безпеки, що мають місце при досить неуспішному зверненні до самих ресурсів, що безпосередньо проходять аудит. Таким прикладом може безпосередньо служити відповідна спроба відкрити певний файл, не маючи відповідних прав доступу.

Безпосередньо сам запис про певну подію включає в себе наступне: тип події, ідентифікатор події, категорію події, додаткові, особливі для певної події, двійкові дані та масив рядків. Кожне з визначених джерел подій має зареєструвати власний файл-повідомлення, в котрому буде зберігатися рядок безпосередньо опису ідентифікаторів повідомлень, параметрів та категорій.

Сам рядок опису здатен містити відповідне місце для вставки рядків з масиву, зазначеного під час запису відповідної події. Додаткові дані ніяким чином не інтерпретуються відповідною програмою перегляду подій і показуються в текстовому та шістнадцятковому форматі [4].

Власне журнал подій безпеки Windows, збирає основні події, безпосередньо пов’язані із самою безпекою відносно логінів облікових

записів, використання та створення привілеїв, реєстрації процесів, безпосередньо пов’язаних із загальною безпекою, а також перезавантаження даної системи [20].

Події, що зафіксовані системою Windows, визначені в аудитній, котру можна використати глобально в межах відповідної доменної мережі Windows за допомогою визначення політики аудиту для різних груп машин. Дані події мають доволі передбачувані ознаки на основі відповідного типу події та в залежності від активної аудитної політики. Разом з тим, переважна більшість атрибутів являються так званими категоричними мітками, для прикладу такими, які встановлюють певний конкретний тип привілей або входу, що застосовується самим процесом.

Для більш кращого розуміння самого контексту передусім проведемо опис доменних служб Active Directory, що пропонують відповідні послуги системним адміністраторам налаштовувати та зберігати відповідні ресурси та користувачів в домені Windows.

Комп'ютери в організації безпосередньо підписані на саму мережу, а записи облікового змісту самих користувачів надаються працівникам для входу на дані комп’ютери. У випадку Windows, дана мережа має назву – домену Windows. Active Directory (AD) – служба каталогів, яка була пропонована

Microsoft, що надає відповідні способи розповсюдження та зберігання всіх даних, безпосередньо пов’язаних із керуванням самим доменом [19]. Контроль доступу за рахунок ролі реалізований через групи, що безпосередньо визначають привілеї, надані обліковій частині даної групи. В AD безпосередньо зберігається інформація про всі групи та акаунти (рис 2.1).

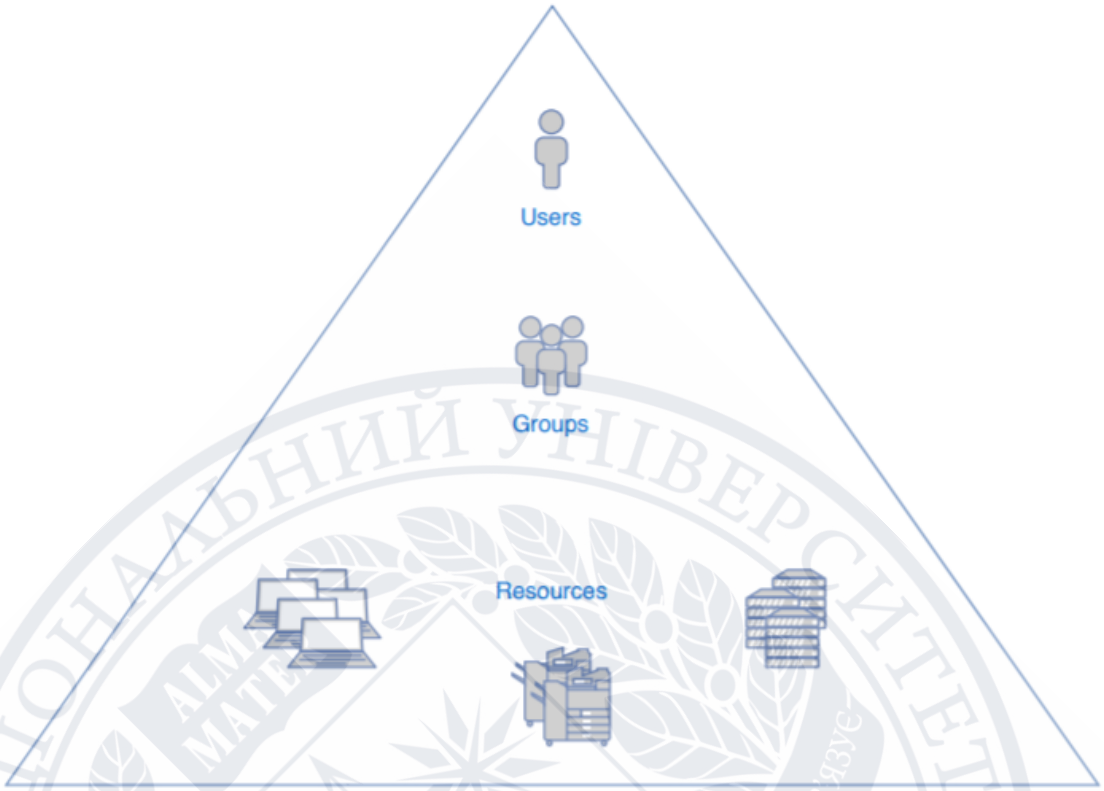

Рис. 2.1. Active Directory

У відповідному домені Windows наявні два головні типи відповідних облікових записів: облікові записи користувачів, які дають людям відповідну увійти в комп'ютерні акаунти і домен для керування ресурсами. Комп'ютерні акаунти та облікові записи користувачів адмініструються однаково та є відповідною частиною груп для керування їх привілеями. Сам контролер домену перебуває там саме, де і Active Directory. Контролери домену – це відповідні сервери, які відповідальні за надання відповідної інформації про каталог у всьому домені, а отже, також перевіряють облікові дані [4].

Можна дійти висновку, що для того, щоб простежити застосуванням дії та привілеїв, які були виконані відповідними користувачами, операційна система Windows пропонує журнал подій, що містить в своєму складі три стандартних типи журналів подій:

1. журнал програми (Application);
2. журнал безпеки (Security);
3. системний журнал (System);

Кожен окремо взятий журнал фіксує власні типи подій. Приклад такого опису події доступу до самого об'єкта можна зустріти в наступному повідомленні із самого журналу безпеки (рис. 2.2):

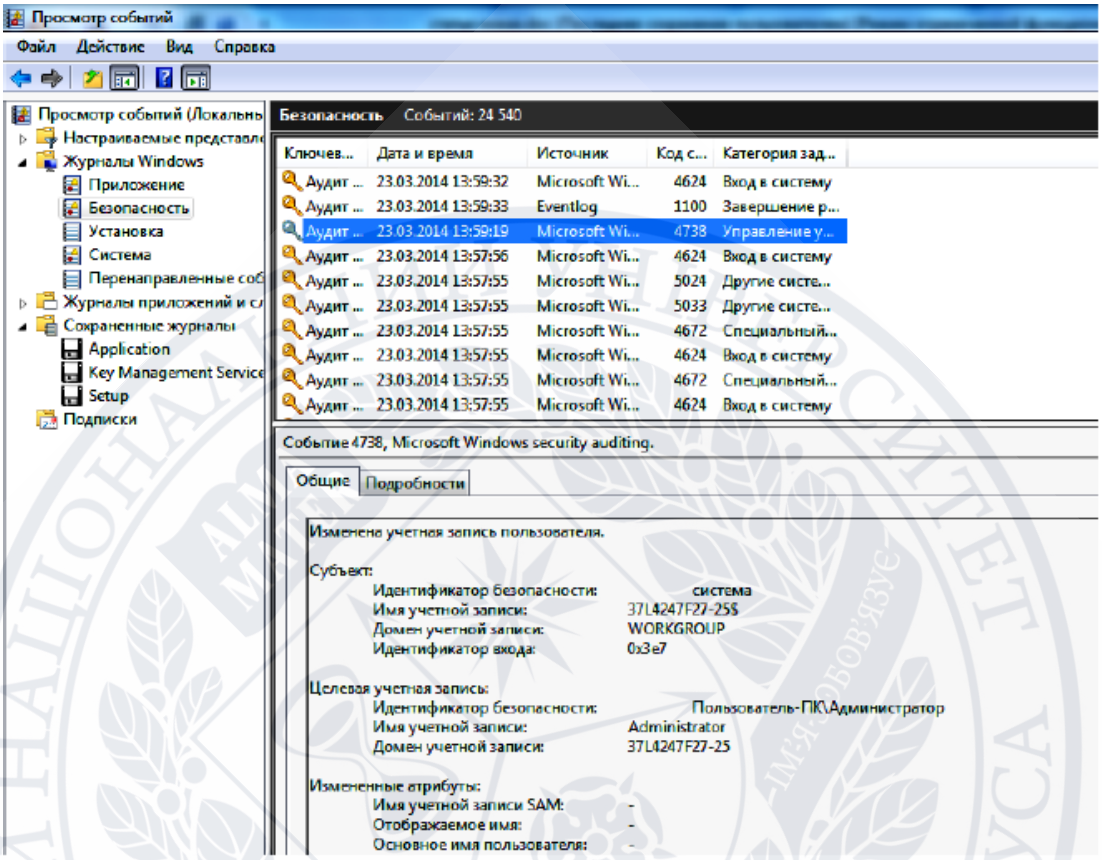

Рис. 2.2. Приклад опису події доступу до об'єкта

Відповідні записи подій програми містять інформацію журналу діагностики про встановлені програми, а структура та повідомлення журналу безпосередньо залежать від самого джерела програми. В системному журналі також безпосередньо реєструються відповідні діагностичні події. І система, і події програми містять в основному певний текстовий опис діагностичного запису всіх подій.

2.2. Особливості роботи журналу подій

У вкладці Журнал подій містить два таких розділи: Журнал та Параметри. Безпосередньо для того, щоб перейти до самого розділу, необхідно натиснути лівою клавішою миші на самій його назві в лівій частині

самого вікна.

Закладка Параметри розділена на дві частини наступним чином: зліва розташований відповідний перелік дій, що будуть вестись і відслідковуватися в журналі, праворуч – загальний перелік відповідних дій, що в журналі подій показуватися не будуть.

Для того, щоб провести налаштування списку дій, які будуть вестися у журналі, необхідно використовувати кнопки зі стрілками.

У відповідному полі Кількість днів збереження журнала необхідно вказати загальну кількість днів, на протязі котрих журнал буде безпосередньо збирати та зберігати відповідну історію проведених в самі системі операцій. Після закінчення визначеного періоду журнал безпосередньо очищається, і відлік відповідних подій розпочинається спочатку. Для відповідного зберігання внесених даних, необхідно натиснути кнопку Зберегти. Для відміни вже внесених даних необхідно натисніть кнопку Відмінити [5].

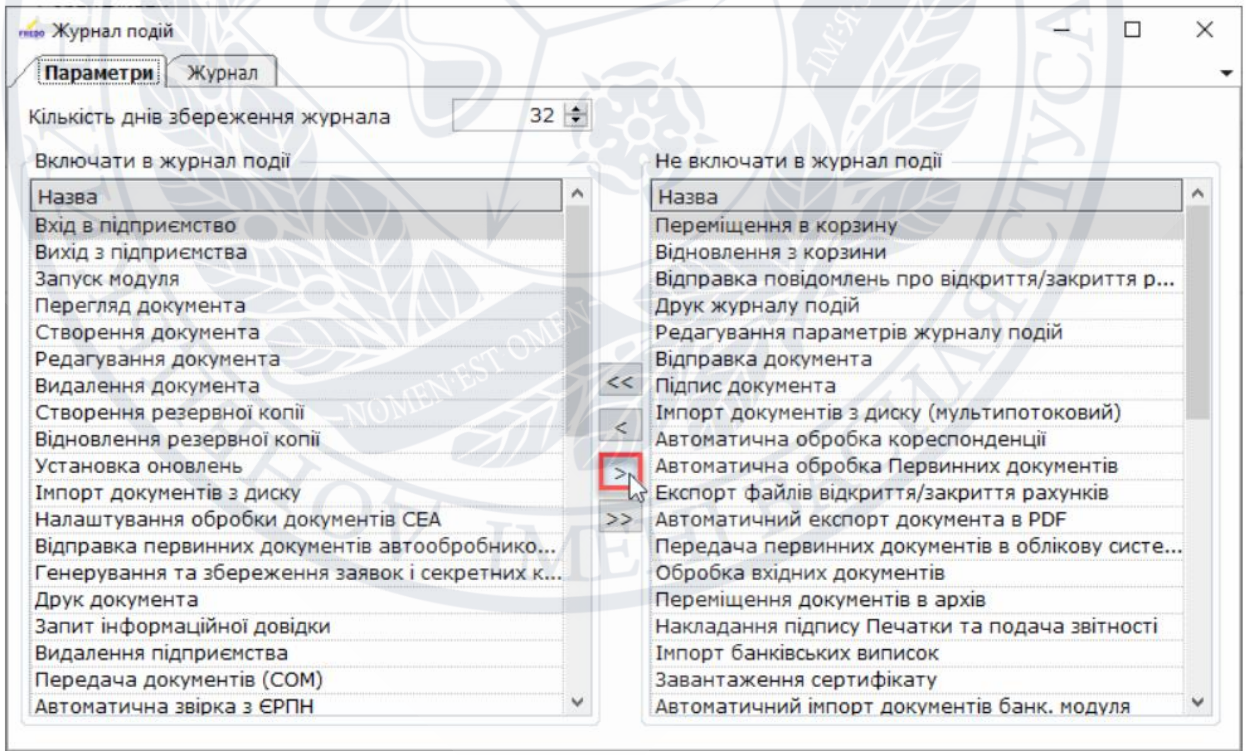

Рис. 2.3. Закладка Параметри

В закладці Журнал відображається вміст журналу подій.

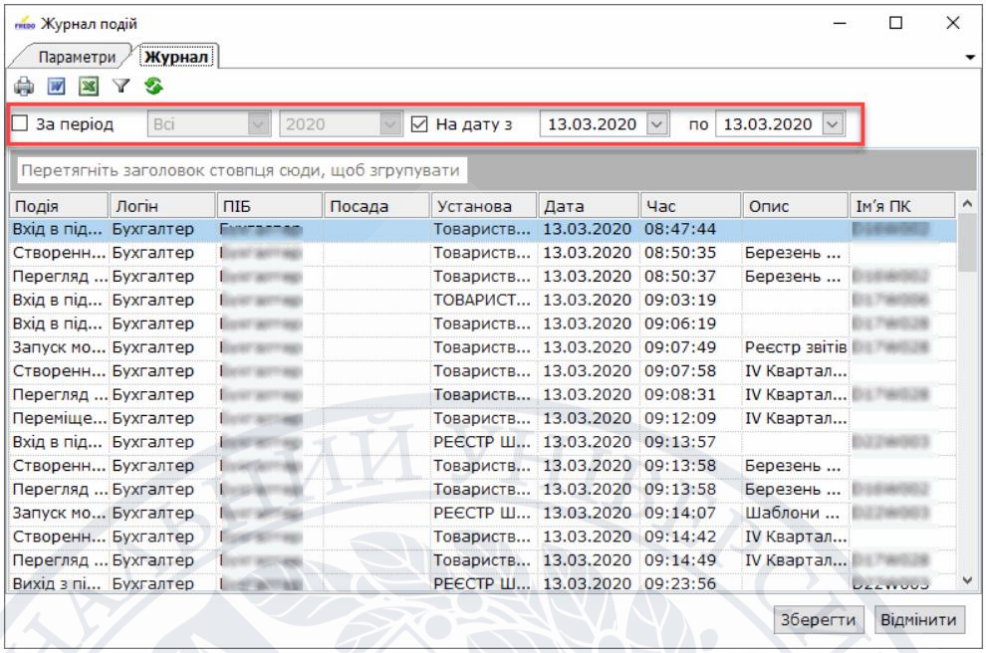

Рис. 2.4. Закладка Журнал

За замовчуванням, у самому Журналі відображаються відповідні події у вигляді певного списку. Дані події показано у хронологічному порядку – так на самому початку списку розміщенні відповідні події, що відбулись самими першими. Для кожної окремо визначеної події в певних окремих колонках збереженні такі дані:

Подія – назва події;

ПІБ – прізвище, ім'я та по батькові користувача;

Логін – логін, під яким користувач був зареєстрований у системі;

Установа – установа, з якою пов'язана подія;

Посада – посада користувача;

Дата – дата, на яку відбулась подія;

Опис – опис події;

Час – час події;

Ім'я ПК – назва ПК, з якого здійснювалась операція [4].

Власне для того, щоб провести відсортовування записів у списку, необхідно натиснути лівою клавіші миші на самій назві колонки. Відповідні записи будуть відсортовані за алфавітом (для текстових значень) або за зменшенням чи зростанням (для числових даних).

Для проведення налаштування відтворених подій по відповідних датах необхідно обрати відповідний спосіб вибору певних даних, визначивши відповідну відмітку:

За період – відтворення даних за заданий період часу, обрати тип періоду: всі чи певний окремо взятий місяць, обрати рік для показу відповідних даних;

На дату – необхідно встановити дату початку та закінчення часового періоду.

За замовчуванням, у фільтрі встановлено відображення даних на поточну дату.

За допомогою кнопок панелі інструментів можна виконати операції:

 Роздрукувати дані Журналу.

 Зберегти дані Журналу у вигляді файлу Word.

 Зберегти дані Журналу у вигляді файлу Excel.

 Встановити фільтр для перегляду даних. Якщо фільтр встановлено, кнопка змінює вигляд на  . Щоб відмінити фільтр, натисніть кнопку ще раз.

 Оновити дані Журналу.

Можна налаштувати перегляд Журналу у розрізі певних даних, наприклад, згрупувати події за установами, або за датами чи посадою користувача [5].

Для цього встановіть курсор миші на заголовку колонки, по даним якої необхідно згрупувати події. Натисніть та утримуйте ліву кнопку миші, перетягніть заголовок колонки на область, що містить напис "Перетягніть заголовок стовпця сюди, щоб згрупувати". Відображення даних розділу Журнал набуде вигляду (на прикладі групування по Даті):

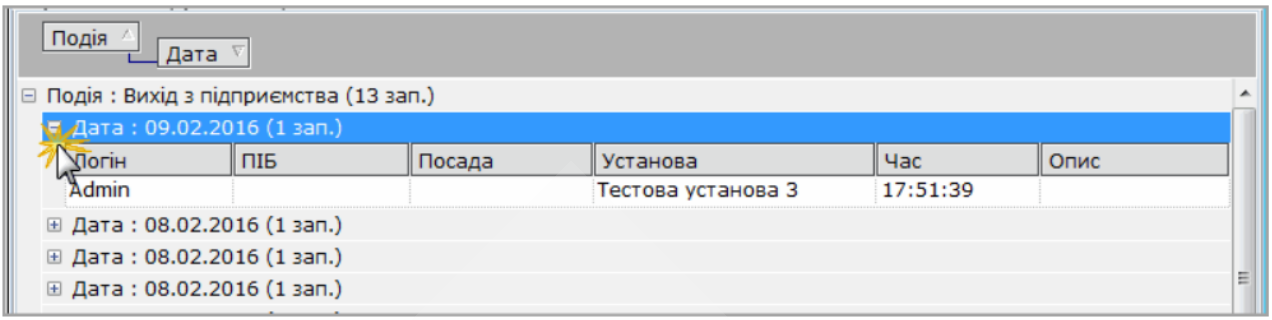

Рис. 2.5. Групування по Даті

Для того, щоб переглянути дані для деякої окремої дати, необхідно натиснути на позначку «+». Тоді відкриється відповідний список подій, які мали місце на обрану дату. Групування відповідних даних по других параметрах проводиться аналогічно.

Отже, є можливість здійснити відповідну побудову ієрархічного списку загального перегляду даних, іншими словами, провести групування даних за кількома головними параметрами.

Власне для того, щоб провести видалення самої гілки ієрархічного списку, чи безпосередньо повернутися до самого відображення відповідних даних загальним списком, необхідно перетягнути саму назву колонки, за котрою згруповано дані, до таблиці подій.

Налаштування відповідних відображення даних, які здійсненні користувачем в Журналі, зберігаються. При слідуючому запуску програми дані в Журналі будуть показані у тому ж вигляді, який був налаштований на час закінчення роботи самої програми.

2.3. Особливості очищення «Журналу подій» в ІКС

Журнал подій безпосередньо служить для збереження історії подій в системі з ціллю контролю дій самих користувачів.

Щоб безпосередньо запустити сам «Журнал подій» найбільш простим способом є наступний – ввести в пошуковій стрічці Windows фразу «перегляд подій». Проте якщо відключене індексування, то ніякого результату не буде. В

такому випадку потрібно відкрити «Панель управління» та безпосередньо перейти до розділу з назвою «Адміністрування», в котрому і розміщений необхідний пункт.

Із самого початку, даний інструмент було розроблено для адміністраторів, котрим необхідно на постійній основі вести відповідний моніторинг за станом серверів, знаходити помилки, причини їх прояву [3]. Не потрібно хвилюватися, якщо з комп'ютером все добре, проте в подіях є деяка кількість попереджень. Це досить нормальне явище навіть для оптимізованого ПК. Навіть незначні збої, які ми можемо не помітити, будуть внесені до «реєстру». Так що, не варто переживати з цього приводу. Велике число користувачів вважають, що не потрібно звичайним користувачам занурюватися в тему, що їм не потрібна. На нашу думку, даний інструмент може бути корисним у певних ситуаціях. Для прикладу, перед користувачем з'являється «синій екран смерті» чи система само по собі перезавантажується. Чому таке відбувається? Відповідь на дане питання можна знайти у відповідному журналі подій. У випадку якщо збій викликаний оновленням відповідного драйвера, то буде встановлено з яким обладнанням виникають проблеми і які є шляхи виходу із критичною ситуації. Для того, щоб простіше було здійснювати пошук потрібного звіту, необхідно запам'ятати більш точний час появи критичної ситуації. Ще одним із важливих моментів являється запис процесу безпосереднього завантаження ОС (указується продовжуваність, час та початок закінчення).

Разом з тим, можна безпосередньо прив'язати до вимикання ПК необхідність введення причини, що пізніше буде відображена безпосередньо в самому журналі. Це є досить хорошою практикою безпосередньо для самих власників серверів, для яких важливими являються будь-які деталі. Для проведення очищення журналу існує три способи, через вже створений виконуваний *.bat (називаємо його «батник») файл або через cmd консоль або через консоль PowerShell. Представимо всі три приклади реалізації [5].

Метод 1: через bat файл. Створюємо текстовий файл і вставляємо в нього

код, який представлений в таблиці 2.2. Далі перейменовуємо відповідне розширення txt bat, і все готове до безпосереднього запуску.

Таблиця 2.2

Створення текстового файлу

1	@echo off
2	FOR /F «tokens=1,2*» %%V IN (‘bcdedit’)
3	DO SET adminTest=%%V
4	IF (%adminTest%)==(Access) goto the End
5	for /F «tokens=*» %%G in (‘wevtutil.exe el’)
6	DO (call :do_clear «%%G»)
7	goto the End
8	:do_clear
9	echo clearing %1
10	wevtutil.exe cl %1
11	goto: eof
12	: the End

Досить важливим є пам’ятати, що запускати файл необхідно від імені самого адміністратора, для цього необхідно натиснути на файл правою клавішою миші і вибрати «запустити як адміністратор».

Метод 2: через командний рядок cmd.

Запускаємо командний рядок для цього натискаємо правою кнопкою миші на меню пуск і обираємо запустити консоль від імені самого адміністратора. В консоль вставляємо наступний код: for /F «tokens=*» %1 in (‘wevtutil.exe el’) DO wevtutil.exe cl «%1». Чекаємо не багато і всі звіти стають порожніми.

Метод 3: через PowerShell. Запускаємо PowerShell від імені адміністратора і вводимо наступну команду: wevtutil el | Foreach-Object {wevtutil cl «$_»}

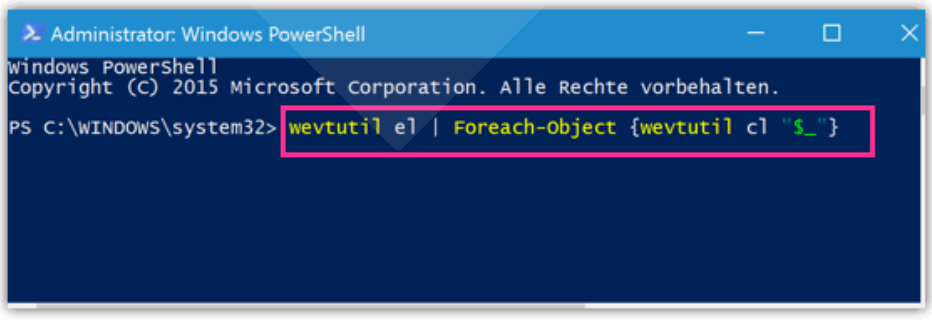

Рис. 2.6. Використання PowerShell

Далі тиснемо: Enter.

В кінці вийде помилка, не потрібно лякатися. Це нормально. Журнал подій буде очищений. На рисунку 2.6 показано, як можна призначити певну задачу до події. Тобто, якщо щось відбувається, то включається обробник і починається виконання зазначеного завдання.

ВИСНОВКИ ДО ДРУГОГО РОЗДІЛУ

Журнал подій Windows (англ. Windows Event log) – це детальний запис системних повідомлень, повідомлень від систем безпеки та прикладних повідомлень, що зберігаються в операційній системі Windows, який використовується адміністраторами для діагностики системних проблем та прогнозування майбутніх проблем. За допомогою цього інструменту можна легко визначити причину неполадок. Щоправда, для його використання необхідні спеціальні знання.

Вкладка Журнал подій містить два розділи: Параметри та Журнал. Для того, щоб перейти до розділу, натисніть лівою кнопкою миші на його назві у лівій частині вікна. Закладка Параметри розділена на дві частини: ліворуч міститься перелік дій, які будуть відстежуватись і вестись в журналі, праворуч - перелік дій, що в журналі подій відображатись не будуть. Налаштування відображення даних, виконані користувачем у Журналі, зберігаються. При наступному запуску програми дані у Журналі буде відображено у тому ж вигляді, який був налаштований на момент завершення роботи програми.

Для очищення журналу є три способи, через створений виконуваний *.bat (називаємо його «батник») файл або через cmd консоль або через консоль PowerShell.

РОЗДІЛ 3. ВАЖЛИВІСТЬ ВИКОРИСТАННЯ ЖУРНАЛУ ПОДІЙ НА СУЧАСНОМУ ЕТАПІ

Безпосередня реалізація «Журналу подій» це доволі важлива операція як сучасного етапу розвитку ІКС так і майбутнього, оскільки детальний аналіз журналів подій дає змогу запобігти несправності в роботі системи та встановити причини їх появи. Для прикладу, коли в журналі наявне відповідне попередження про те, що драйверу диска вдається записати будь-який сектор тільки після декількох спроб, то, можливо, цей сектор скоро стане непридатним для використання.

Власне журнали можуть також допомогти у розв’язані питань, безпосередньо пов'язаних із роботою відповідних додатків. Для прикладу, коли певна програма аварійно закінчила роботу, у відповідному журналі додатків, досить часто, присутні відповідні записи щодо тих події, що безпосередньо призводять саме до цього.

Читання журналів подій це щоденний обов'язок системних адміністраторів та програмістів. Досить часто і звичайному користувачеві перегляд даних журналів може досить сильно полегшити власне життя, зробивши спілкування із комп’ютером під керуванням Windows більш продуктивним та приємним.

Підсистеми реєстрації відповідних подій безпеки є в наш час невід'ємними та важливими компонентами загальної систем забезпечення відповідної інформаційної безпеки по факту в будь-який мережевий операційній системі. Реєстрацію відповідних подій безпеки також часто називають так званим аудитом подій безпеки. Відповідні можливості реєстрації подій безпеки реалізовані у відповідних мережевих операційних системах та прикладному програмному забезпеченні. Проте, доволі відчутний ефект від застосування засобів аудиту безпосередньо досягається тільки у том випадку, коли дані, що зареєстровані про події безпеки можуть бути

проаналізовані. Лише в даному випадку є можливість вчасно виявити виникаючі шкідливі впливи на відповідні складові інформаційної мережевої системи – комп'ютери, програмне забезпечення, що передаються і зберігаються дані тощо.

Існування відповідних підсистем реєстрації подій безпеки являється одним із головних вимог, які наявні у всіх новітніх стандартах та керівних документах з безпеки інформації відповідних комп'ютерних систем. Встановлені стандарти також визначають відповідні класи подій, які підлягають безпосередній реєстрації. Вимоги до існування засобів реєстрації подій безпеки більшою мірою можна віднести до вимог технічного характеру, власне саме тому вони, зазвичай, реалізовані відповідними виробниками основного програмного забезпечення, яке використовується для відповідної побудови інформаційних мережевих систем.

Постійний аналіз вже зареєстрованих подій безпеки досить часто відносять до заходів організаційного характеру, що є головною основною причиною недостатньої уваги виробників програмного забезпечення до проблем організації оперативного аналізу подій безпеки в мережі. Іншими словами, для того, щоб атестувати програмне забезпечення мережевої інформаційної системи на відповідність вимогам стандартів безпеки зазвичай досить реалізувати в ній лише кошти реєстрації подій безпеки.

Облік типових обсягів даних про події безпеки, а саме сотні і тисячі записів в день на одному комп'ютері в мережі, дозволяє стверджувати, що при відсутності спеціальних автоматизують програмних засобів аналіз подій безпеки стає малоефективним. З цієї причини і обслуговуючий персонал мережевих інформаційних систем часто зневажливо ставиться до завдань аналізу зареєстрованих даних про події безпеки.

Все це у великій мірі зменшує дієвість відповідної реєстрації подій безпеки, що дає змогу знайти недоліки та помилки в реалізації політики безпеки мережевої інформаційної системи до того, як вони будуть використані в зловмисних цілях.

Засоби керування доступом, існуючі в програмному забезпеченні кожної інформаційної мережевої системи досить часто не здатні забезпечити відповідну безпеку у повному обсязі, по причині того, що вони не призначені для запобігання зловмисних чи некваліфікованих дій зі сторони користувачів, які мають потрібні повноваження доступу. Вчасно реалізований аналіз подій безпеки дає змогу досить оперативно визначити небезпечні ситуації, які з'являються в результаті недостатньо суворого розмежування доступу і вжитих заходів протидії.

Під час проведення налаштування засобів керування відповідним доступом можуть бути безпосередньо допущені певні помилки, що доволі часто важко помітити під час проведення тестування, однак дані помилки стають помітні під час не правильної роботи інформаційної мережевої системи. Вчасно проведений аналіз подій безпеки дає змогу такі помилки вже до того, як вони стануть загальною причиною порушення самої безпеки.

Отже, оперативний аналіз вже зареєстрованих подій безпеки в комп'ютерній мережі дає змогу збільшити загальну захищеність мережевої інформаційної системи від різноманітних загроз інформаційній безпеці за рахунок вчасного встановлення відповідних вразливостей в системі політики безпеки та захисту інформації.

Власне аудит системи безпеки забезпечує проведення спостереження за різноманітними подіями, безпосередньо торкаючись відповідної безпеки самої операційної системи. Відтворення системних подій потрібне для встановлення зловмисників та відповідних спроб поставити під загрозу дані системи. Загальним прикладом події, яка безпосередньо підлягає аудиту, являється невдала спроба доступу.

Найбільш загальними типами подій для аудиту є:

- доступ до таких об'єктів, як папки та файли;
- керування обліковими записами груп, програм, Інтернет-ресурсів;
- вхід користувачів в систему і вихід з неї
- доступ і робота з процесами.

В процесі проведення аудиту подій, що безпосередньо пов'язані із безпекою, створюється журнал безпеки, в котрому є можливість перегляду даних події. Власне саме тому дана система аудиту являється незамінним засобом забезпечення відповідної інформаційної безпеки.

Можна дійти висновку, що журнал подій це доволі цінний інструментарій для проведення відповідного контролю якості безпосередньо зробленої роботи та відповідної безпеки мережі, в майбутньому і сьогодні, що досить часто застосовується не досить дієво через відповідну складність читання логів та їх об’єму. Керування логами подій та їх безпосереднє зберігання потребують структурованого підходу.

Для системного застосування Журналу безпеки можна запропонувати розробити деяку структуру системи моніторингу подій безпеки.

Розробка структури системи аналізу подій безпеки і розподіл функцій між її компонентами повинні проводитися з урахуванням основних вимог до системи. Можна сформулювати наступні вимоги, які безпосередньо впливають на саму структуру системи:

1. Система має обробляти відповідні дані про події безпеки, що беруться на пряму із самого журналу аудиту кінцевої множини комп'ютерів в мережі.

2. Відповідні результати обробки подій безпеки мають зберігатися в єдиній базі даних подій безпеки.

3. Загальні функції системи мають бути розподілені між відповідними компонентами, що працюють на різних комп'ютерах мережі.

Запропоновану структуру системи, що задовольняє відповідним зазначеним вимогам, представимо на рис 3.1.

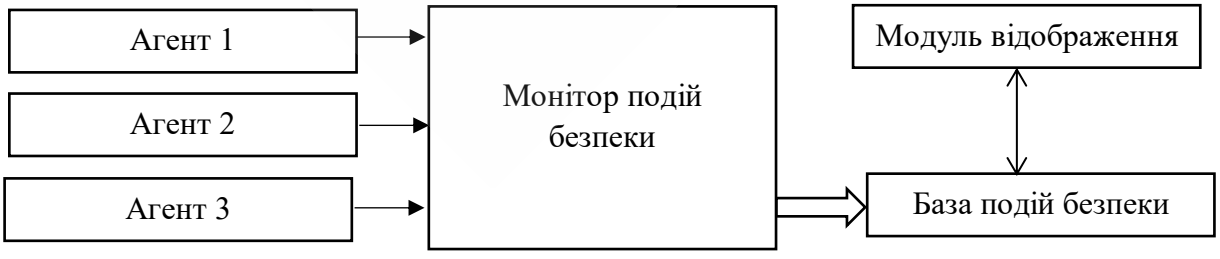

Рис. 3.1. Структура системи моніторингу подій безпеки

Більш детальніше проаналізуємо основне призначення і головні функціональні компоненти системи.

Власне агенти представленої системи працюють на комп'ютерах мережі та витягають відповідні дані про події безпеки і направляють їх до монітора подій безпеки для безпосередньої обробки.

Відповідні агенти системи можуть здійснювати власні функції такими двома головними способами, а це означає можна виокремити два головних можливих варіанти реалізації функцій агентів:

1. Активні агенти. Агенти даного типу безпосередньо направляють нові дані монітора подій безпеки в міру їх виявлення в журналах аудиту.

2. Пасивні агенти. Агенти даного типу безпосередньо надають монітору відповідні дані про події безпеки за відповідним запитом, реалізуючи, практично, функції сервісів віддаленого доступу безпосередньо до журналів аудиту комп'ютерної мережі.

Пасивні ж агенти, здатні забезпечувати як певне послідовне, так і довільне прочитання відповідних даних з журналів аудиту. Існування відповідної можливості довільного прочитання даних значно спрощує і пришвидшує відповідні процедури вибірки та пошуку нових даних. Ефективність та складність здійснення довільного читання журналів аудиту безпосередньо залежить від загального способу зберігання подій в них. Широко розповсюдженим текстовий формат відповідного зберігання подій ускладнює завдання довільного читання даних у порівнянні зі структурованими форматами.

Монітор подій безпеки (МПБ) – це головний модуль системи, що безпосередньо забезпечує обробку даних про певні події безпеки, які потрапляють з комп'ютерів мережі. Головні етапи, алгоритми і методи обробки подій безпеки проаналізуємо далі. МПБ розв’язує завдання фільтрації та автоматизованого аналізу надходячих подій відповідно із заданими правилами та їх збереження в головній базі даних подій безпеки. Отже, МСБ розв’язує велику частину завдань системи, забезпечуючи при цьому виявлення

ознак загроз безпосереднього порушення інформаційної безпеки в комп'ютерній мережі та оповіщення персоналу, що є відповідальним за безпеку в самій мережі.

Безпосередньо модуль відображення слугує для дослідження і відображення результатів роботи монітора подій безпеки.

Отже, монітор подій безпеки являється головним модулем системи, який розв'язує переважну кількість завдань, які існують перед самою системою моніторингу подій безпеки, за допомогою взаємодії з другими компонентами системи. Проводячи узагальнення, слід відмітити, що сам монітор подій безпеки має дієво розв'язувати одне з головних завдань системи – надійно та швидко проводити обробку подій безпеки. Дієвість розв'язання даного завдання великою мірою залежить від самої організації процесу обробки подій безпеки, самої структури монітора подій безпеки, розподілу функцій обробки подій безпеки між самим монітором подій безпеки і агентами системи, що працюють на комп'ютерах мережі. Дієвість відповідної обробки подій також безпосередньо залежить від загальних алгоритмів та методів, які виконують різноманітні етапи обробки подій безпеки.

Обов'язковою складовою методики має бути аудит критично необхідних процесів та об'єктів операційної системи, таких для прикладу як:

- реєстр Windows;
- кореневий системний каталог Windows, його підкаталоги;
- кореневе системне сховище System Volume Information;
- системні файли;
- проби входу в систему;
- об'єкти автозапуску;
- зміна облікових політик;
- інші критичні процеси і об'єкти.

Найбільш розповсюдженим місцем розташування виконуваних файлів шкідливого програмного забезпечення являється системний кореневий

каталог Windows, в результаті чого потрібно здійснювати аудит змін файлів в цьому каталозі, а саме на предмет виникнення нових виконуваних файлів.

Робота шкідливого програмного забезпечення досить часто супроводжується відповідним записом власних параметрів до самого реєстру операційної системи, особливо в гілку автозапуску.

Робота шкідливого програмного забезпечення безпосередньо торкається системних файлів, дописуючи шкідливий код в вихідний код файлу. В результаті цього відбувається зміна розміру та контрольної суми файлів, що заражені.

Сам процес обробки даних аудиту подій безпеки, отримуваних від будь-якого з джерел – журналів аудиту комп'ютерів мережі, може бути описаний узагальненим алгоритмом.

Відповідно до даного алгоритму, під час обробки даних аудиту подій безпеки необхідно виокремлювати чотири головні етапи.

1. Витяг даних з журналу аудиту.
2. Формалізація даних.
3. Аналіз і фільтрація подій безпеки.
4. Оповіщення про виявлені загрози і запис подій безпеки в базу даних подій безпеки.

Безпосередньо сам витяг даних з відповідного журналу аудиту ґрунтується у здійсненні операції читання даних з файлу журналу аудиту в певний буфер. Конкретні дії, що потрібно виконати на даному етапі безпосередньо залежать від загального способу організації зберігання подій безпеки в журналах аудиту. Нинішні засоби аудиту подій безпеки застосовують два головних підходи для організації зберігання подій безпеки в файлах журналів аудиту – зберігання подій в структурованих файлах і зберігання подій в текстових файлах, де кожна окрема текстова рядок задає окрема подія. У тому випадку, коли відповідні дані вдало отримані, то далі їх потрібно формалізувати, іншими словами перетворити ці дані до таких структур, які застосовуються в системі для подання подій. Оскільки, тільки

лічені дані про відповідні події безпеки представлені в такому форматі, в котрому вони зберігаються в журналі аудиту, то потрібно їх безпосередньо перетворити до структури, зручної для майбутнього подання в процесі обробки в системі. Саме для цього досить часто потрібно виокремити з масиву відповідної інформації певні окремі події і значення деяких полів даних структур, що задають події.

В загальному сам процес проведення відповідного аналізу зареєстрованих подій безпеки характеризується потребою розв’язання таких головних завдань:

1. Об'єднання подій, одержаних з різних джерел, для прикладу таких, що були зареєстровані на різних комп'ютерах інформаційного мережевого середовища.

2. Усунення надмірності журналу аудиту.

3. Пошук подій, що відповідають деяким умовам.

4. Обробка подій «вручну».

5. Класифікація зареєстрованих подій безпеки.

6. Оповіщення персоналу, відповідального за безпеку, про факти виявлення особливо важливих подій.

Під час проведення об'єднання відповідних подій в один єдиний журнал системні події утворюють журнал, що безпосередньо експортується в текстовий файл. Журнал являє собою опис подій, розділений символом-роздільником. При експорті роздільником є символ **«.** Власне текстовий формат відповідного зберігання даних дає змогу відповідним розробникам засобів аудиту істотним чином спростити відповідні операції запису даних аудиту у відповідні журнали аудиту. Обробка та перегляд відповідних даних аудиту в текстовому форматі також являються досить простими процедурами. Для цього потрібно провести відповідний розбір рядків текстового файлу журналу аудиту і виокремити в них значення певних полів запису про саму подію. Основним недоліком являється те, що при текстовому способі відповідного зберігання даних аудиту неможливим стає проведення

довільного читання даних із самого журналу аудиту, оскільки відповідні дані можуть бути безпосередньо прочитані лише послідовно.

Відповідне усунення надмірності самого журналу аудиту, іншими відповідне скорочення числа всіх подій для майбутньої обробки на основі «білого» та «чорного» списків.

Як було вже сказано раніше, віруси під час проникненні утворюють відповідні ключі і файли реєстру, що на основі досліджень, які були проведені ТОВ «Доктор Веб» та Лабораторією Касперського, і зібраної статистки дають змогу скласти відповідний список ключів та файлів реєстру, найбільш часто створюваних чи модифікованих відповідними програмами-шкідниками. Дана статистика, на постійній основі оновлювана, здатна бути відповідною основою для «чорного» списку, що використовується для безпосереднього пошуку відповідних подій, які на пряму стосуються даних файлів та ключів.

Так же само, для чималого зменшення загального числа подій необхідно застосовувати «білий» список. «Білий список» необхідно створювати із довірених додатків та безпосередньо доповнювати під час інсталяції нової програми.

Результатом використання «чорного» і «білого» списків має стати формування відповідних списків несанкціонованих подій, санкціонованих подій і подій, призначених для майбутньої обробки.

Пошук подій, які відповідають певним умовам. При необхідності провести сортування за такими критеріями як Дата / Час.

Обробка подій «вручну» полягає в перегляді та аналізі окремих подій адміністратором. На підставі знань адміністратора про систему, в якій здійснюється аудит, і його досвіду адміністратор виносить рішення про приналежність аналізованого події до одного з класів. Виділимо три класи: санкціоновані події, несанкціоновані події і «сумнівні» події. «Сумнівні» події – це ті події, щодо яких не можна зробити однозначного висновку є вони санкціонованими чи ні. Такі події вимагають перевірки із застосуванням додаткових засобів.

При віднесення події до одного з класів, визначається, до якого об'єкту відноситься подія (якщо категорія події – Аудит доступу до об'єктів), проводиться пошук всіх подій, що трапилися з цим об'єктом, і віднесення знайдених подій до того ж класу.

Класифікація зареєстрованих подій безпеки

На підставі попередніх пунктів складається три списки подій:

– список несанкціонованих подій, складений з подій, визначених «чорним» списком і відібраних адміністратором;

– список санкціонованих подій, складений з подій, визначених «білим» списком і відібраних адміністратором;

– список «сумнівних» подій.

ВИСНОВКИ ДО ТРЕТЬОГО РОЗДІЛУ

Журнали подій можуть допомогти у розв’язані питань, безпосередньо пов'язаних із роботою відповідних додатків. Для прикладу, коли певна програма аварійно закінчила роботу, у відповідному журналі додатків, досить часто, присутні відповідні записи щодо тих події, що безпосередньо призводять саме до цього.

Реалізація «Журналу подій» це важлива операція як сучасного етапу розвитку ІКС так і майбутнього, адже ретельний аналіз журналів подій допомагає запобігти неполадкам в роботі системи і визначити причини їх виникнення. Наприклад, якщо в журналі присутнє попередження про те, що драйверу диска вдається записати будь-якої сектор тільки після декількох спроб, то, можливо, цей сектор скоро стане непридатним для використання.

ВИСНОВКИ

В результаті проведеного дослідження нами були встановлені наступні важливі висновки:

1. Проаналізовано особливості роботи журналу подій. Вкладка Журнал подій містить два розділи: Параметри та Журнал. Налаштування відображення даних, виконані користувачем у Журналі, зберігаються. При наступному запуску програми дані у Журналі буде відображено у тому ж вигляді, який був налаштований на момент завершення роботи програми.

2. Встановлено особливості очищення «Журналу подій» в ІКС. Для очищення журналу є три способи, через створений виконуваний *.bat (називаємо його «батник») файл або через cmd консоль або через консоль PowerShell.

3. Обґрунтовано важливість використання «Журналу подій» на сучасному етапі. Реалізація «Журналу подій» це важлива операція як сучасного етапу розвитку ІКС так і майбутнього, адже ретельний аналіз журналів подій допомагає запобігти неполадкам в роботі системи і визначити причини їх виникнення.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Грибков А. Н. Информационно-управляющие системы многомерными технологическими объектами: теория и практика : монографія. Тамбов : Изд-во ФГБОУ ВО «ТГТУ», 2016. 164 с.

2. Для чого потрібен журнал подій Windows 10. URL: http://fastping.com.ua/2018/04/28/dlya-chogo-potriben-zhurnal-podij-windows-10/ (дата звернення: 29.11.2020)

3. Журнал подій. URL: https://fredo.com.ua/help/admlogs.htm (дата звернення: 25.11.2020)

4. Журнал событий Windows 10. Зачем нужен и как пользоваться. URL: https://zen.yandex.ru/media/poznyaevru/jurnal-sobytii-windows-10-zachem-nujen-i-kak-polzovatsia-5ca5f6793dd2f700b3b0cffa (дата звернення: 02.12.2020)

5. Журнал событий windows. URL: https://mysitem.ru/kompyuter/288-zhurnal-sobytij-windows.html (дата звернення: 25.11.2020)

6. Про Національну програму інформатизації: Закон України від 4 лютого 1998 року № 74/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/74/98-вр#Text (дата звернення: 28.11.2020)

7. Про захист інформації в інформаційно- телекомунікаційних системах: Закон України 5 липня 1994 року № 80/94-ВР URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 23.11.2020)

8. Маслянко П.П. Проблеми і технології продукування інформаційних ресурсів. Всеукраїнська науково-практична конференція «Сучасні тенденції розвитку інформаційних технологій і науці, освіті, економіці», Луганськ, 11-14 грудня 2006. С. 16 – 18

9. Маслянко П.П. Концепція інформатизації корпоративних структур. Наукові вісті НТУУ «КПІ». 2003, №3 с 510-525.

10. Может ли журнал событий Windows стать увлекательным чтением? URL: http://wintech.net.ru/windows-xp/winxp-admin/47-mozhet-li-zhurnal-sobytiy-windows-stat-uvlekatelnym-chteniem.html (дата звернення: 02.12.2020)

11. Сиротюк О. Особенности проектирования современных баз данных / www.computerworld.com.ua (дата звернення: 25.11.2020)

12. Технологии управления журналами событий. URL: https://www.osp.ru/winitpro/2007/06/4473876 (дата звернення: 22.11.2020) (дата звернення: 25.11.2020)

13. Черненко М., Слепцов С. Принципы классификации управленческих информационных систем // Корпоративные системы – 2004 №1 (дата звернення: 17.11.2020)

14. Баймакова И. А. Обеспечение защиты персональных данных: методическое пособие: учебное пособие / Т. А. Биячуев. Санкт-Петербург: СПб ГУ ИТМО, 2004. 161 с.

15. Игнатьев В. А. Информационная безопасность современного коммерческого предприятия. Старый Оскол: ТНТ, 2005. 448 с.

16. Мельников В. П. Информационная безопасность и защита информации. Москва: Издательский центр «Академия», 2008. 336 с.

17. Романец Ю. В. Защита информации в компьютерных системах и сетях. Москва: «Радио и связь», 2006. 328 с.

18. Скрипкин, К. Г. Экономическая эффективность информационных систем. Москва: ДМК Пресс, 2016. 256 с.

19. Чипига А. Ф. Информационная безопасность автоматизированных систем: учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. Безопасности. Москва: Гелиос АРМ, 2010. 336 с.

20. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей [Текст] : учеб. Пособие. Москва: «ФОРУМ»: ИНФРА-М, 2008. – 416 с.

21. Ярочкин В. И. Информационная безопасность: учебник для студентов вузов. Москва : Академический Проект, 2008. 544 с.

22. Clay Shirky Ontology is Overrated: Categories, Links, and Tags. URL: https://oc.ac.ge/file.php/16/_1_Shirky_2005_Ontology_is_Overrated.pdf (дата звернення: 28.11.2020)