(табл. 6 и 7). Кроме того, как видно из сравнения данных для сплошной и перфорированной пленок (образцы 1.9 и 3.2), перфорирование экрана практически не снижает эффективность экранирования.

Необходимо отметить, что каждый из использованных методов осаждения покрытий – магнетронный и электродуговой, имеют определенные преимущества и приоритеты. Так, при электродуговом напылении, скорость осаждения покрытий, при всех прочих равных условиях (давление в рабочей камере, состав пленок, тип подложки и т. д.), примерно в 3 раза выше, чем при магнетронном напылении, что значительно повышает производительность процесса. Размер зерна осажденных пленок в случае магнетронного напыления значительно меньше, что имеет значение при осаждении проводящих прозрачных пленок. Отсюда следует, что магнетронный метод осаждения, несмотря на свою универсальность, предпочтителен лишь при напылении покрытий на оптически прозрачные элементы экранов, а электродуговой – может быть использован для экранирования элементов конструкций сложной объемной формы, таких как корпуса процессоров, дисплеев, клавиатуры и т. п.

На основании представленных результатов можно заключить, что оптимальным вариантом экранирующего покрытия для конструктивных элементов ПЭВМ является однослойные алюминиевые пленки толщиной 30–50 мкм. Осажденные на конструктивные элементы ПЭВМ пленки алюминия имеют необходимую равномерность и толщину покрытия, коррозионную стойкость, высокий уровень адгезии к полистиролу, способность к эксплуатации подложки на изгиб и позволяют обеспечить достаточный уровень экранирования. Однако из-за самопассивации алюминиевых пленок окислом алюминия возникает проблема так называемых «стыков» при сборке составных частей комплексов ПЭВМ. Данная проблема может быть решена путем осаждения на поверхность защитного покрытия из алюминия тонкой пленки никеля, либо путем локального осаждения в требуемых местах цинка.

Литература. 1. Маркин А. В. Безопасность излучений от средств электронно-вычислительной техники: домыслы и реальность // Зарубежная радиоэлектроника. – 1989. – № 12. – с. 102 – 124. 2. Князев Л. Н., Кечнев Б. В. Конструирование радиоэлектронной и электронно-вычислительной аппаратуры с учетом электромагнитной совместимости. – М.: Радио и связь, 1989. – 244 с. 3. Крылов Т. В., Юрченкова А. И. Защита от электромагнитных излучений. – М.: Сов. радио, 1972. – 216 с. 4. Конструирование экранов и СВЧ – устройств/ А. М. Чернушенко, Б. В. Петров, Л. Г. Малорацкий и др.; Под ред. А. М. Чернушенко. – М.: Радио и связь. 1990.– 352 с. 5. Бондарь Е. А., Мачулянский А. В. Динамическая поляризуемость ультрадисперсных частиц никеля// Оптика и спектроскопия. – 1990. – Т. 69. – вып. 4. – с. 876–880.

УДК 681.321;322:621.395

МОДЕЛЬ АУДИТУ БЕЗПЕКИ СИСТЕМИ ТЕХНОЛОГІЧНОГО УПРАВЛІННЯ ТЕЛЕКОМУНІКАЦІЙНИМИ МЕРЕЖАМИ

Микола Тардаскін, Володимир Кононович, Андрій Севостьяненко*

Одеський регіональний центр технічного захисту інформації ВАТ "Укртелеком"

**Одеська національна академія зв'язку*

Анотація: **Розглядаються алгоритми та часові характеристики моделі аудиту безпеки інформації в системах технологічного управління телекомунікаційними мережами.**

Summary: **The algorithm and time characteristics of information security audit model for the Telecommunication Management Network (TMN) are considered.**

Ключові слова: **Аудит безпеки, система технологічного управління, інформація, реєстрація.**

I Вступ

Системи управління та аналізу телекомунікаційних мереж безповоротно набули характеру комп'ютерних мереж і, відповідно, методи прямого впливу на ці системи також будуть комп'ютерні. Згідно з міжнародними рекомендаціями [1, 2] аудит безпеки – це незалежний перегляд та дослідження системних даних, протоколів і подій для перевірки адекватності управління системою, для забезпечення відповідності між встановленою політикою та діючими процедурами, для виявлення порушень безпеки і для цілеспрямованого вдосконалення політики та процесу функціонування системи. Аудит безпеки систем технологічного управління (СТУ), зупинка яких викликає переривання процесу управління, дозволяє також враховувати дії суб'єктів, контролювати правильність використання ресурсів, виявляти спроби пошкодити систему. Механізми аудиту безпеки хоча і не здатні безпосередньо запобігати порушенням безпеки, виконують важливі функції запису

та аналізу подій, що трапляються в системі, сприяють правильній реакції на ситуації порушення безпеки системи шляхом зміни робочих процедур. При виникненні неприпустимої загрози безпеці, коли параметри системи перевищують встановлені межі, в системі генерується сигнал тривоги.

В даній статті проведено аналіз шестирівневої моделі реалізації послуг аудиту та тривожної сигналізації системи технологічного управління [3–5], а також процесів, що відбуваються в ній, як реакції на дії порушника. При умові припущення щодо незалежності кожної з подій в системі виводиться ймовірнісний закон, що пов'язує ці події.

II Ієрархічна модель реалізації послуг аудиту

Серед множини процедур аудиту можна виділити робочі фази, кожна з яких характеризується своєю тривалістю:

t_1 – визначення події, що стосується безпеки системи;

t_2 – прийняття рішення щодо запису події або генерації тривожної сигналізації;

t_3 – опрацювання прийнятого рішення, тобто створення повідомлень аудиту безпеки або тривожної сигналізації;

t_4 – аналіз та оцінка, згідно з заздалегідь визначеними критеріями, події, що стосується безпеки системи, а також визначення реакції на подію, тобто послідовності дій;

t_5 – накопичення (збирання) розподілених в системі записів в журнали реєстрації аудиту (security audit trail);

t_6 – формування звіту із записів журналів реєстрації аудиту;

t_7 – архівація, тобто переміщення записів в журналах реєстрації аудиту.

Усі наведені вище фази не розділені за часом, тобто можуть перекриватись, тривати одночасно.

На рис. 1 наведено ієрархічну модель послуг аудиту та тривожної сигналізації в СТУ, що будується згідно з рекомендаціями ITU-T X.816 [1].

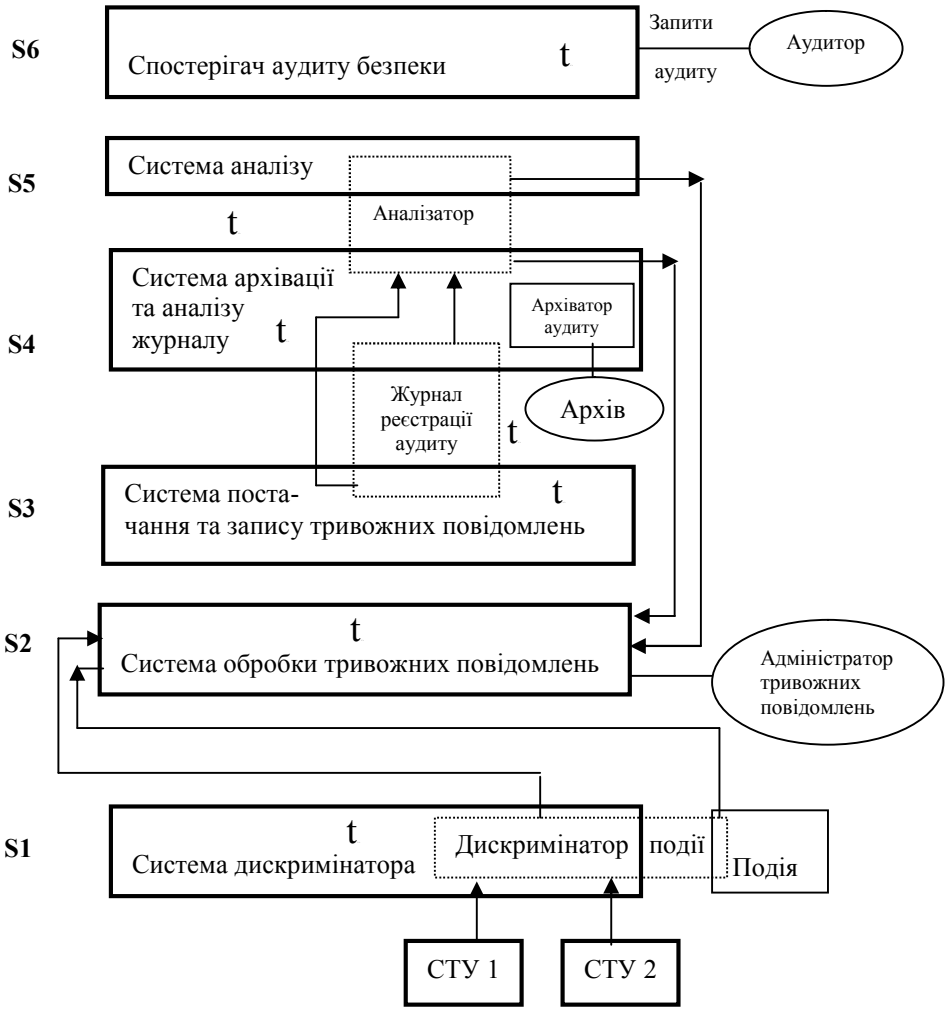

Рисунок 1 – Модель реалізації послуг аудиту та тривожної сигналізації в СТУ

На найнижчому рівні S1 відбувається, згідно з заздалегідь визначеними критеріями, визначення подій, що стосуються безпеки СТУ, та реакції на події. При прийнятті рішення вхідними параметрами дискримінатора події є тип події, що стосується безпеки, час доби та деякі особливі характеристики об'єкта – чинника події. Вихідною реакцією дискримінатора є повідомлення про дію у відповідь на подію, генерування тривожної сигналізації та повідомлення аудиту безпеки.

На рівні S1 відсутні можливості ведення стеження та аналізу подій, тому тривожні повідомлення направляються до S2, а повідомлення аудиту безпеки – до S3 для подальшого включення до журналів реєстрації аудиту. Журнал реєстрації аудиту містить дані, що збираються та потенційно використовуються для полегшення аудиту безпеки.

На рівні S3 відбувається поновлення (update) журналів реєстрації аудиту, забезпечується (для рівня S6) доступ до журналів реєстрації та до їх архівів з можливістю сортувати та вибирати потрібні записи журналів згідно з заздалегідь визначеними критеріями з подальшим занесенням цих записів до звіту безпеки. При формуванні звітів з безпеки інформації ці критерії враховуються при обробленні інформації, що міститься в одному чи більше журналах реєстрації аудиту. Рішення приймається на основі таких параметрів: тип аудит-запису; тип події, що стосується безпеки; тривалість події, що розглядається; тип об'єкту, інформація, котра потрібна для прийняття рішення. Кінцеве рішення видається у вигляді списку вибраних записів.

На рівні S4 відбувається архівація записів журналу реєстрації та пошук потрібних записів в архівах.

Програмне забезпечення (ПЗ) рівня S5 здійснює аналіз записів журналів реєстрації, а також архівних записів, згідно з визначеними критеріями, а також пересилає сигнали тривоги до S2 при перевищенні певних граничних значень параметрів системи або визначених умов роботи системи, що можуть трактуватись як ненормальні.

Критерії в даному разі визначають, яким чином аналізатор аудиту буде обробляти записи журналів реєстрації. В загальному випадку аналіз записів журналу реєстрації аудиту відбувається шляхом оцінки частоти появи подій та типу подій до того, як буде визначено реакцію системи на подію. Прийняття рішення базується на таких параметрах події: тип, частота появи, тривалість. Після ретельного аналізу події визначається, яка дія потрібна у відповідь.

Участь операторів у процесі аудиту передбачається на двох рівнях. Аудит-адміністратор здійснює загальне управління аудитом, а оперативне управління покладається на адміністратора тривожних повідомлень.

III Динаміка реалізації послуг аудиту

Складемо граф, що ілюструє послідовність виконання рівнями моделі своїх функцій при порушенні безпеки СТУ (рис. 2). Система дискримінатора рівня S1 визначає подію, що трапилась в системі або іншій СТУ і, якщо ця подія стосується безпеки, інформує про це систему обробки тривожних повідомлень на рівні S2. Система постачання та запису тривожних повідомлень рівня S3 взаємодіє з вищими рівнями S4 та S5, де відбувається архівація та аналіз сформованих повідомлень аудиту безпеки. Рівень S6 взаємодіє з рівнем S3 при створенні звітів безпеки. Результати роботи рівнів S4 та S5 передаються до системи обробки тривожних повідомлень, яка сповіщає про результати аналізу адміністратора тривожних повідомлень та відповідає на запити аудитора (рівень S6). За результатами обробки та аналізу інформації виноситься певне рішення щодо реакції системи.

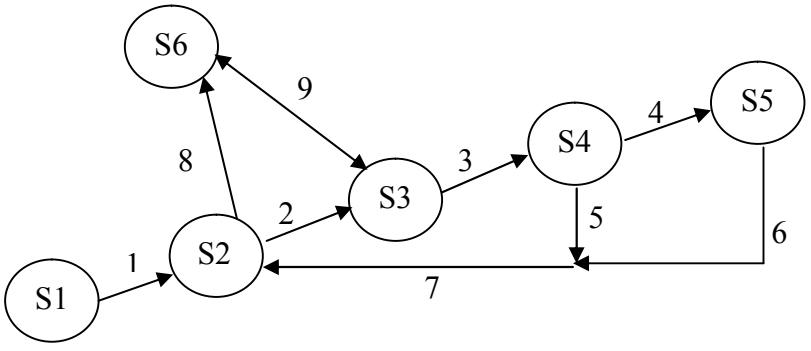

Рисунок 2 – Послідовність дій рівнів моделі реалізації послуг аудиту та тривожної сигналізації в СТУ як реакція на дії зловмисника, що стосуються безпеки системи

У СТУ передбачається як розміщення функцій безпеки в межах певного компонента системи, так і розподіл їх між компонентами системи. Особливості побудови системи впливають на спосіб інсталяції функцій безпеки. В реальних системах досить поширеним є спосіб дублювання функцій шляхом розміщення їх в різних кінцевих системах та групування функцій.

Для проведення дієвої політики аудиту безпеки важливою є здатність до неперервної перевірки адекватності засобів контролю параметрів системи та гнучкого реагування на результати перевірок. Цей процес базується на ретельному аналізі записів та нових повідомлень журналу реєстрації аудиту, що можуть надходити як від самих аудит-повідомлень, так і від інших журналів реєстрації аудиту. При аналізі подій, що трапились у системі, використовуються механізми фільтрації повідомлень за певними критеріями, наприклад, в залежності від часу доби, за типом самої події чи об'єкту – чинника події тощо. З точки зору управління ці фільтри можуть бути визначені як керовані об'єкти з певними специфічними параметрами, властивостями та поведінкою.

Наприклад, в необслуговуваній кінцевій системі аудит безпеки може мати такі інстальовані функції: диспетчер аудиту (audit dispatcher), запис аудиту (audit recorder), провайдер аудиту (audit provider), аналізатор аудиту (audit analyser). Можуть бути згруповані такі важливі для аудитора безпеки функції як перегляд журналу регістрації та аналізатор аудиту.

Остаточне рішення щодо запису певної події до журналу реєстрації аудиту або включення тривожної сигналізації приймає аудит-адміністратор, процес або особа, до обов'язків якого, насамперед, належить вибір серед усіх подій в системі таких, що стосуються безпеки. Цей процес відбувається в рамках політики аудиту безпеки, яка визначає комплексні загальні правила збирання, запису та аналізу важливих для системи подій.

Передбачається наявність засобів контролю критичних параметрів середовища телекомунікаційного об'єкту (зменшення пропускної спроможності каналів, падіння якості передавання, зміни температури, відчинення дверей, вікон чи люків тощо) або комбінації таких засобів. Робочі станції в СТУ мають вмонтовані програмно-апаратні засоби для автентифікації користувача, керування доступом, захисту системної пам'яті та пам'яті, що містить ПЗ системи забезпечення безпеки СТУ. Але вони залишаються уразливими до атак, вірусів, несанкціонованого доступу та пов'язаними із ними погрозами. В реальних СТУ для забезпечення служб аудиту, реєстрації та спостереження діють механізми реєстрації інформації щодо сеансів користувачів, фіксації будь-яких змін прав користувачів для керування доступом, реєстрації використання критично важливих файлів та їх модифікації, реєстрації використання інструментів керування трафіком, що циркулює в СТУ, а також використання засобів аудиту.

IV Базові кількісні характеристики

Розглянемо дії порушника безпеки СТУ та реакцію системи на його дії. Вважається, що порушник знає функціональні особливості СТУ, має високий рівень знань в області програмування й обчислювальної техніки, проектування й експлуатації автоматизованих інформаційних систем, досвід роботи з технічними засобами, знає структуру, функції і механізми дії засобів захисту, їхні сильні і слабкі сторони. Припустимо, що має місце спроба порушника отримати доступ до баз даних, архівів або зони керування засобами забезпечення безпеки СТУ. При цьому атака може бути безумовною, або відбуватись після настання очікуваної події на атакованому об'єкті, або за запитом від атакованого об'єкта.

Послідовність подій, що характерна для несанкціонованого доступу (НСД) у загальному вигляді може бути описана такими кроками:

1. Віддалене підключення порушника до лінії, що з'єднує комп'ютерну мережу, на якій базується СТУ та всі інші зовнішні мережі;
2. Спроба порушника підібрати або зламати пароль входу до комп'ютерної мережі СТУ (всього N спроб). Тут і далі фіксування всіх подій відбувається на рівні S1;
3. Фіксування спроби порушника підібрати або зламати пароль входу до комп'ютерної мережі СТУ;
4. Спроба порушника підібрати або зламати пароль входу до певного сервера або робочої станції комп'ютерної мережі СТУ;
5. Фіксування спроби порушника підібрати або зламати пароль входу до певного сервера або робочої станції комп'ютерної мережі СТУ;
6. Несанкціоновані дії, що стосуються безпеки СТУ;
7. Фіксування несанкціонованих дій, що стосуються безпеки СТУ, технічними та програмними засобами системи. Всі події в системі записуються, спрацьовує тривожна сигналізація (працюють рівні S2, S3). Відбувається аналіз та оцінка дій порушника на рівні S4. Після аналізу та класифікації події, що пов'язана з безпекою, реакцією СТУ на дії порушника можуть бути дії з впорядкування інциденту, резервування та дії, спрямовані на відновлення працездатності системи.

8. Вихід з об'єкту;
9. Фіксування виходу з об'єкту;

Впорядкування інциденту полягає у зменшенні потенційно небезпечних наслідків події, що стосується безпеки СТУ, з використанням засобів впорядкування інциденту і ресурсів для попередження операторів.

Резервування має гарантувати коректне закінчення сеансу роботи сервера або робочої станції з подальшим відновленням нормальних робочих параметрів.

Відновлення має забезпечити правильне та швидке відновлення нормальної роботи СТУ після перерви в її роботі за мінімальний можливий проміжок часу згідно з пріоритетом важливості для функціонування.

Конкретні загрози визначають організаційні заходи щодо забезпечення безпеки СТУ.

Кроки 3, 5, 7, 9 (фіксування подій) залежать від відповідних попередніх кроків. Дійсно, якщо подія не відбулась, вона не може бути зафіксованою. Розглянемо кроки 1, 2, 4, 6, 8, які навпаки, є незалежними випадковими величинами X_1, X_2, ..., X_n, (n=5). Припускаємо, що їх тривалості однаково розподілені за показниковим законом з параметром λ. Розподіл частості випадкових величин Y_1 описується законом Пуасона з параметром a.

Знайдемо закон розподілу та числові характеристики випадкової величини послідовності подій в СТУ:

$$Z = \sum_{i=1}^{Y} X_i \tag{1}$$

Закон розподілу суми $\sum_{i=1}^{n} X_i$ являє собою закон Ерланга (n–1)-го порядку з параметром λ :

$$f^{(n)}(x) = \frac{\gamma(\lambda x)^{n-1}}{(n-1)!} e^{-\lambda x}, \ (x > 0). \tag{2}$$

Згідно з формулою повної ймовірності густина розподілу випадкової величини z буде:

$$\varphi(z) = \sum_{n=1}^{\infty} f^{(n)}(z) P_n = \sum_{n=1}^{\infty} \frac{\lambda(\lambda z)^{n-1}}{(n-1)!} e^{-\lambda x} \frac{a^{n-1}}{(n-1)!} e^{-a} = \lambda e^{-\lambda x - a} \sum_{k=0}^{\infty} \frac{(\lambda z a)^k}{(k!)^2} \text{ при } z > 0. \tag{3}$$

Ця густина може бути виражена через модифіковану циліндричну функцію

$$I_0 = \sum_{k=0}^{\infty} \frac{(x/2)^{2k}}{(k!)^2} : \tag{4}$$

$$\varphi(z) = \lambda e^{-\lambda z - a} I_0\left(2\sqrt{\lambda z a}\right) \text{ при } z>0.$$

Припустимо, що $Y=n$. Тоді умовне математичне очікування:

$$M[Z_n] = M\left[\sum_{i=1}^{n} X_i\right] = n m_x. \tag{5}$$

Повне математичне очікування:

$$m_z = M[z] = \sum_{n=1}^{N} n m_x P_n = m_x m_y, \text{ де } m_y = \sum_{n=1}^{N} n P_n. \tag{6}$$

Отже,

$$M[z] = m_x m_y = \frac{a+1}{\lambda}. \tag{7}$$

При тій же умові $Y=n$ знайдемо умовний другий початковий момент:

$$M[Z_n^2] = M\left[\left(\sum_{i=1}^{n} X_i\right)^2\right] = \left[\sum_{i=1}^{n} X_i^2 + 2\sum_{i=j} X_i X_j\right] = n D_x + n_x^2 m_x^2, \tag{8}$$

де $D_x = D[x_i] = \int_{-\infty}^{\infty} (x - m_x)^2 f(x) dx.$

Другий початковий момент випадкової величини z:

$$a_{2z} = M\left[Z^2\right]\sum_{n=1}^{N} M\left[Z_n^2\right]P_n = \sum_{n=1}^{N}\left(nD_x + n^2 m_x^2\right)P_n = D_x m_y + m_x^2 a_{2y} a_{2z}, \quad (9)$$

де $D_{2y} = \sum_{n=1}^{N} n^2 P_n = D_y + m_y^2.$

Дисперсія випадкової величини *z:*

$$D_z = a_{2z} - a_z^2 = D_x m_y + m_x^2 a_{2y} = D_x m_y + m_x^2 D_y. \quad (10)$$

Маємо остаточно

$$D[z] = D_x m_y + m_x^2 D_y = \frac{a+1}{\lambda^2} + \frac{a}{\lambda^2} = \frac{2a+1}{\lambda^2}. \quad (11)$$

V Висновки

Надані результати дають змогу вирішувати задачі обчислення числових характеристик процесу аудиту на основі статистики елементарних подій, знаходження періодичності перегляду і аналізу даних в залежності від важливості даних та ефективного використання продуктивності мережі.

Література: 1. Recomendation CCITT X.800. Security architecture for open systems interconnection for CCITT applications. Geneva.1991. 2. ITU-T recomendation X.816. Information technjlogy – Open System Interconnection – Security frameworks for Open systems: Security audit and alarms framework. 3. Кононович В. Г., Голобородько Д. В. Методи та засоби захисту від несанкціонованого доступу в системі управління мережами електрозв'язку України // – К.: Зв'язок, № 2, 1999, с. 13–16. 4. Кононович В. Г., Севостьяненко А. О. Середовище потенційних порушників в системі технологічного управління телекомунікаційними мережами. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", – К., 2000. С. 142–147. 5. Тардаскін М. Ф., Кононович В. Г. Аспекти політики безпеки системи управління телекомунікаційними мережами. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", № 2, 2001. С 234–239. 6. Домарев В. В. Защита информации и безопасность компьютерных систем. – К.: Изд. «ДиаСофт», 1999. – 480 с.