2. Простая развертываемость виртуальных систем требует постоянного контроля, поскольку «забытые» и не обновляемые системы могут являться точкой проникновения злоумышленников во внутреннюю сеть компании. К тому же, нельзя забывать об инсайдерских угрозах - необходимо правильно разграничивать права доступа персонала к информационным ресурсам, содержащих виртуальные системы. В больших масштабах нужно использовать специализированное ПО для контроля за ИТ-инфраструктурой и средства обнаружения вторжений.

3. Большое количество уязвимостей, найденных за последнее время в платформах виртуализации, говорит о том, что внимание хакеров к виртуальным системам в дальнейшем будет только расти. Поэтому, безусловно, необходимо тщательно следить за обновлениями платформ, точно так же, как и за обновлениями операционных систем.

Список литературы

1. *Гультяев А. К.* Виртуальные машины: несколько компьютеров в одном. — Питер, 2006.
2. *Стивен Браун.* Виртуальные частные сети.: Пер. с англ. - М.: Изд.дом «Лори», 2001.
3. *Крис Касперски.* Техника сетевых атак. Приемы противодействия.: Пер. с англ. - Том I. – Р. Изд.дом «СОЛОН», 2001.

У даній статті розглянуто питання забезпечення безпеки віртуального середовища, зроблено аналіз можливих загроз і запропоновано ряд рекомендацій для підтримки віртуальної інфраструктури в безпечному стані.

Ключові слова: віртуальне середовище, загрози, безпека.

В данной статье рассмотрен вопрос обеспечения безопасности виртуальной среды, сделан анализ возможных угроз и предложен ряд рекомендаций для поддержания виртуальной инфраструктуры в безопасном состоянии.

Ключевые слова: виртуальная среда, угрозы, безопасность.

In given article is considered the question of the virtual environment safety, is made the analysis of possible threats and is offered a number of recommendations for maintenance of a virtual infrastructure in a safe condition.

Key words: virtual environment, threats, safety.

Поступила 17.11.2009

УДК 004.621.391

к.т.н. Павлов І.М. (НТУУ «КПІ»)

ФОРМАЛЬНИЙ ОПИС ВПЛИВУ НЕБЕЗПЕЧНИХ ЗАГРОЗ НА СИСТЕМУ ЗАХИСТУ ІНФОРМАЦІЇ

Забезпечення захисту інформації на практиці проводиться в умовах випадкового або системного впливу будь-яких різних факторів (загроз), які, в цілому, систематизовані в стандартах. Причому стандарти, які прийняті в державі, та стандарти, якими керуються в світі – відрізняються як самим підходом до оцінки загроз так і системністю методології оцінки ефективності систем захисту інформації.

В статті [1] були розглянуті питання неформального підходу до методиці оцінки ефективності ескізного проектування комплексних систем захисту інформації. Були виділені в окремий етап та розглянуті основні підходи до аналізу як самої комп'ютерной системи, так і інформації, яка циркулює в цей системі, а також проаналізовані загрози по цілям застосування і визначені етапи подальшої оцінки ефективності комплексних систем захисту інформації під час ескізного проектування.

Метою цієї статті є загальний формальний опис небезпечних для комплексної системи захисту інформації загроз в інформаційно-телекомунікаційних системах.

На рис. 1 показано, як можна виділити загрози по цілям їх застосування для інформаційно-телекомунікаційної системи.

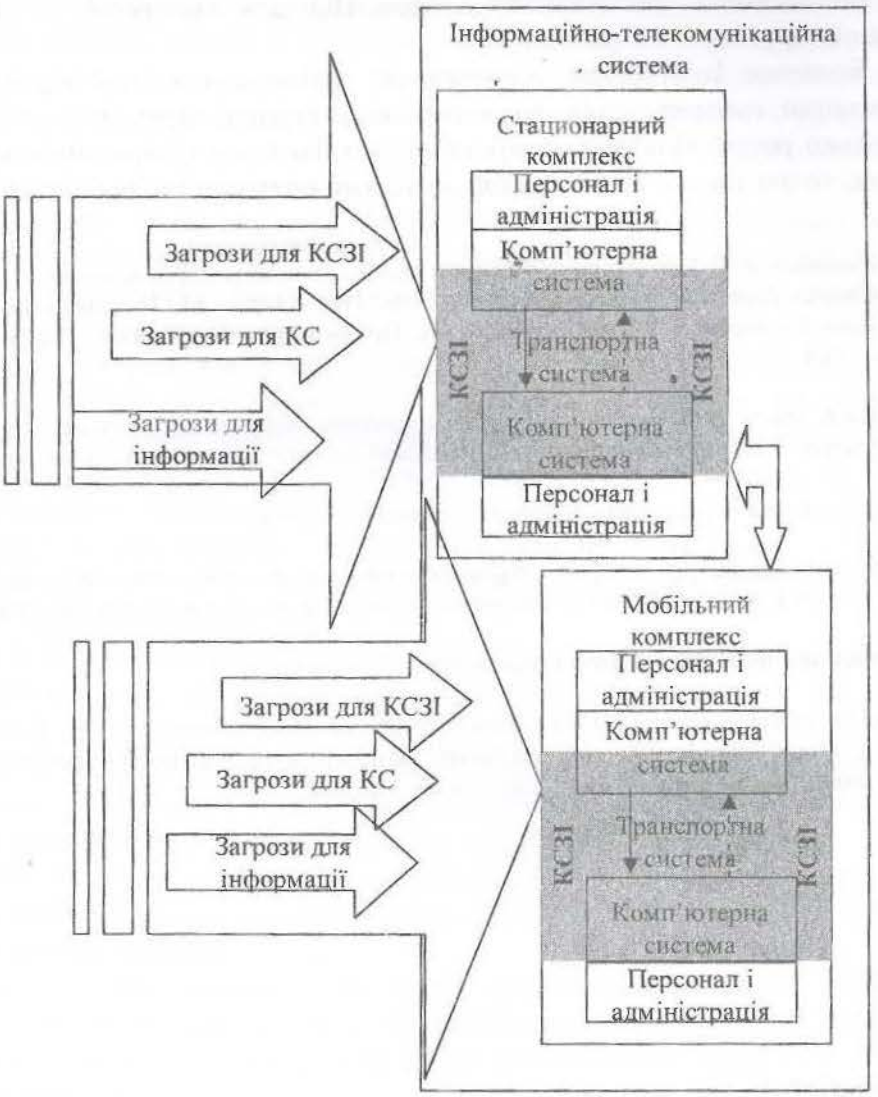

Рис. 1. Порядок впливу загроз на інформаційно-телекомунікаційну систему

Як показано на рис. 1., на інформаційно-телекомунікаційну систему (ІТС) впливають загрози для КСЗІ, для самої комп'ютерної системи та для інформації. Кожен клас загроз виконує свої задачі: задачі взлому системи захисту, задачі проникнення та дезорганізації комп'ютерної системи, задачі порушення конфіденційності, цілісності, доступності інформації. Причому загрози для стаціонарної компоненти ІТС надходять раніше, і в подальшому впливають на мобільну компоненту ІТС.

На рис. 2. наведена загальна структура роботи КСЗІ в ІТС, яка включає до себе систему впливу загроз на КСЗІ та систему протидії загрозам збоку КСЗІ [2].

Рис. 2. Порядок впливу загроз на інформаційно-телекомуікаційну систему

Розглянемо загальну математичну модель впливу загроз та процес протидії цим загрозам:

В загальному вигляді, полагається, що задані: множина загроз для інформації, які можуть виникати для інформаційно-телекомунікаційної системи та множина механізмів захисту (МЗ) за допомогою яких ці загрози можуть бути нейтралізовані. Причому для кожного співвідношення загрози та механізми захисту визначено число $r_1(i,j)$ – ефективність нейтралізації i –тим засобом захисту (МЗ) j –й інформаційної загрози.

Для побудови математичної моделі вводиться похібна $y(i,j)$, яка дорівнює 1, коли j-та інформаційна загроза блокується за допомогою і-того механізму захисту, та дорівнює 0 в іншому випадку.

За допомогою теорії графів побудуємо двухдольний граф $G(X,U)$, де $X = \bigcup X_i, i = 1,2$. Вершини множини в X_1 відповідають механізмам захисту, а вершини множини X_2 – відповідним інформаційним загрозам (рис.3). Кожен елемент (вершина) множини X_1 характеризується ефективністю по блокуванню інформаційних загроз X_2.

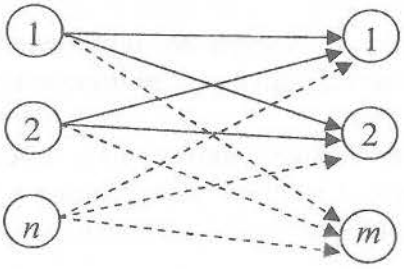

Рис. 3. Двухдольний граф впливу інформаційних загроз на механізми захисту

Кожній вершині множини X/X_2 надається вага, яка дорівнює ефективності блокування загроз *i*-тим МЗ, а кожній дузі (i,j)=1,0 (наявності або відсутності МЗ на шляху загроз), при обмеженнях затрат Q. Формально постановка задачі має наступний вигляд:

$$\sum_{j=1}^{m}\sum_{i=1}^{h} r_1(i,j)y(i,j) \Rightarrow \max \qquad (1)$$

При обмеженнях:

$$\sum_{i=x_j \in X_2}^{n} r_2(i) \times sign\sum y(i,j) \le Q, \forall x_j \in U, y(i,j) = 1{,}0, \qquad (2)$$

де $r_2(i)$ – затрати на встановлення *i*-го МЗ.

Коли необхідно мінімізувати затрати на встановлення МЗ від інформаційних загроз в ІТС при обмеженні рівня ефективності P, то формальна постановка задачі буде мати вигляд:

$$\sum_{i=1,j=1}^{hm}(i) \times sign\sum y(ij) \Rightarrow \min. \qquad (3)$$

$$\sum_{j=1,j=1}^{nn}\sum_{i=1,j=1}^{nm} r_1(ij)y(ij) / \sum(\max r_1(ij)) \le P, \forall x_j \in X_2, \sum y(ij) = 1, x_i \in X_1, y(ij) = 1{,}0. \qquad (4)$$

В цій моделі рахується, що найвищій рівень ефективності КСЗІ ІТС буде тоді, коли для нейтралізації кожної загрози буде вибраний МЗ з максимальною ефективністю. Найвищій рівень ефективності КСЗІ дорівнює сумі елементів в кожному стовбці матриці, яка будується на основі прокольного графа $G(X,U)$.

Необхідно враховувати, що вибір найбільш оптимального набору класичних МЗ в умовах зниження об'ємів ресурсів не гарантує того, що дана система дійсно буде ефективною. При цьому слід враховувати, що практичне застосування ефективних МЗ, а значить і створення ефективної КСЗІ ІТС стає можливим в випадку, коли вірогідність наступу ризиків нанесення фізичної навмисної шкоди ІТС є достатньо малою величиною [3]..

Розглянемо модель, яка дозволяє визначити вірогідність причинення шкоди ІТС при несанкціонованому доступі (НСД).

Захист від НСД будується на практиці як послідовність побудови бар'єрів у складі МЗ після успішного проникнення, яких, зловмисник отримує доступ до інформаційних ресурсів ІТС.

Порушник в стані проникнути в систему лише при умові, коли:

- йому стає відомо (будь-яким чином) побудова системи захисту, в частині вирішення цілей проникнення;
- порушник поспіває отримати доступ до інформаційних ресурсів до того, як система захисту зминеться (після чого перед порушником виникне проблема повторного преодолінння бар'єрів КСЗІ).

Обозначим через K_j номер бар'єра, який блокує доступ до інформації *J*-го типу. Тоді вірогідність того, що інформація J в процесі зберігання в базі даних не стане викривленою від НСД до моменту видачі користувачу $P_{\text{інф}j}$ визначається виразом:

$$P_{\text{інф}\_j} = 1 - \prod_{K_j=0}^{n} P_{nj}, \qquad (5)$$

де P_{nj} – вірогідність взлому бар'єра, n – кількість бар'єрів КСЗІ.

При умові вснування стаціонарних розподілів часу між сусідніми змінами параметрів КСЗІ і часу взлому КСЗІ, вірогідність взлому бар'єру існує, і дорівнює:

$$P_{\text{бар'єру}} = f\int_0^{\infty}(1-F_{\text{зміни}}(t))G_{\text{взлому}}(t)dt, \tag{6}$$

де $F_{\text{зміни}}$ – функція розподілу часу між сусідніми змінами параметрів бар'єру КСЗІ; f – величина, зворотна математичному очікуванню часу між сусідніми змінами параметрів системи захисту; $G_{\text{взлому}}$ – функція розподілу часу взлому бар'єру системи захисту:

$$P_{\text{бар'єру}} = \prod_{k=1}^{n} f\int_0^{\infty}(1-F_{\text{зміни}}(t))G_{\text{взлому}}(t)dt, \tag{7}$$

де k – номер бар'єру системи захисту; n – кількість бар'єрів системи захисту.

Можливих варіантів для функції розподілу часу між сусідними змінами параметрів системи захисту бар'єра $F_{\text{взлому}}$ може бути декілько:

Варіант 1. Параметри комплексної системи захисту змінюються через постійний інтервал часу, тобто $F_{\text{взлому}}$ є детермінованою:

$$P_{\text{бар'єру}} = \begin{cases} 0, t < f^{-1} \\ 1, t \geq f^{-1} \end{cases}. \tag{8}$$

Варіант 2. Інтервали часу між сусідніми змінами параметрів визначаються випадковим чином, наприклад, за допомогою генератора псевдовипадкової послідовності:

$$P_{\text{бар'єру}} = 1-\exp(-ft). \tag{9}$$

Можливі варіанти для функції розподілу часу взлому бар'єру системи захисту $F_{\text{взлому}}(t)$:

Варіант 1. Час взлому бар'єру системи захисту є постійним:

$$G_{\text{взлому}}(t) = \begin{cases} 0, t \leq g^{-1} \\ 1, t > g^{-1} \end{cases}. \tag{10}$$

Варіант 2. Розглянемо випадок, коли час взлому порушником бар'єру системи захисту невизначений:

$$G_{\text{взлому}} = 1-\exp(-gt), \tag{11}$$

де g – масштабний коефіцієнт, за допомогою якого можна враховувати важкість операцій, так і рівень підготовленості та технічна оснащеність порушника.

Відповідно вірогідність взлому всієї комплексної системи захисту буде визначатися на основі наступних значень, в залежності від часу взлому захисту інформації:

- у випадку, коли параметри системи захисту змінюються через постійний проміжок часу, а час взлому системи захисту є постійною величиною:

$$P_{\text{бар'єру}} = \begin{cases} 0, f \geq g \\ 1-f/g, f < g. \end{cases} \tag{12}$$

- зміна параметрів системи виконується через рівні проміжки часу, а час взлому бар'єра невідомий:

$$P_{\text{бар'єру}} = (1 - f/g)(1 - \exp(-g/f)). \quad (13)$$

- час між сусідніми змінами параметрів визначається випадковим чином, а час взлому бар'єра системи захисту є постійним:

$$P_{\text{бар'єру}} = \exp(-f/g). \quad (14)$$

- час між сусідними змінами параметрів визначається випадковим чином, час взлому бар'єрів невідомий:

$$P_{\text{бар'єру}} = g(g+f). \quad (15)$$

На рис. 4., надано схема створення небезпечних для системи захисту інформації загроз.

Рис. 4. Схема створення небезпечних для системи захисту загроз

Ефективність загрози для системи захисту інформації визначається коефіцієнтом небезпечності:

$$\beta_i = K_i B_i / C_i, \quad (16)$$

де K_i – коефіцієнт ступені реалізації загрози в КС, B_i – виграш порушника від реалізації, C_i – затрати порушника на підготовку та реалізацію загрози [4]..

На рис. 5., надано фрагмент схеми аналізу небезпечних загроз для системи захисту інформації, який може бути реалізований під час проектування систем захисту інформації.

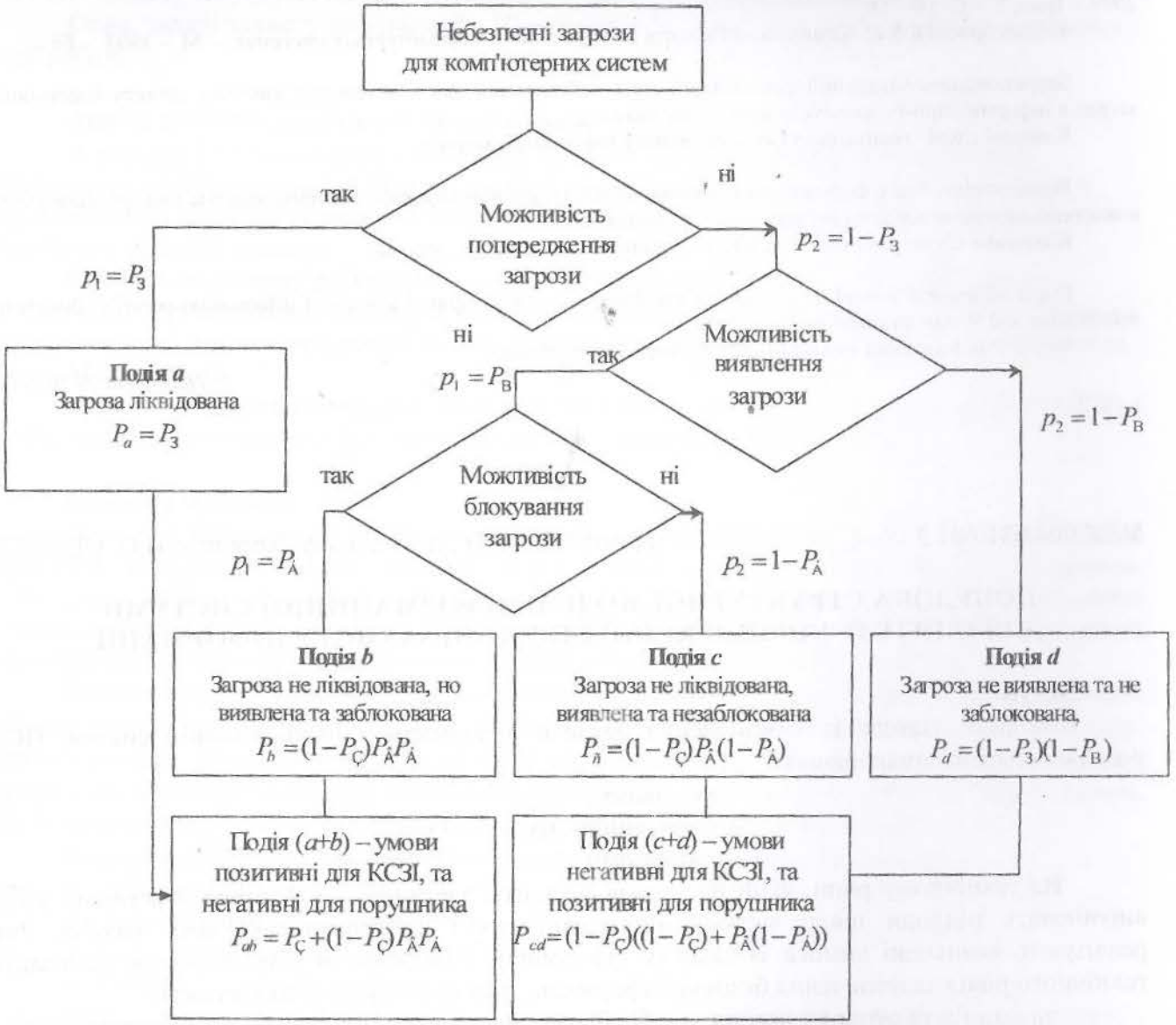

Рис. 5. Фрагмент схеми аналізу небезпечних загроз для системи захисту інформації

Висновки

Можливість попередження небезпечних для КСЗІ загроз може бути забезпечена ще на етапі проектування систем захисту інформації. Отримання попередніх формальних показників ефективності застосування загроз даст можливість розробникам закласти в систему захисту, яка проектується для конретної інформаційно-телекомунікаційної системи, показники, по яким в подальшому можливо оцінити ефективність розробляємої системи захисту інформації, а це є вагомий економічний фактор, який перед собою ставить кожен, хто приступає до проблеми створення системи захисту інформації.

Список літератури

1. *Павлов І.М.* Неформальний підхід в методиці оцінки ефективності ескізного проектування комплексних систем захисту інформації // Захист інформації. – К.: 2009. – № . – С..

2. *Павлов И.Н.* Проектирование систем защиты информации. Формальный подход // "Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні". – Київ, 2005. – Вып. 11. – С. 54 – 59.

3. *Табаков А.Б.* Разработка моделей оптимизации средств защиты информации для оценки страхования информационных рисков. // Научный журнал Кубанского государственного аграрного университета. – К. – 2009. - Вып. 2. – С. 14 – 18.

4. *Завгородний В.И.* Комплексная защита информации в компьютерных системах. – М. – 1994. – 86 с.

Запропоновано загальний формальний опис небезпечних для комплексної системи захисту інформації загроз в інформаційно-телекомунікаційних системах.

Ключові слова: комплексна система захисту інформації, загрози.

Предложено общее формальное описание опасных для комплексной системы защиты информации угроз в информационно-телекоммуникационных системах.

Ключевые слова: комплексная система защиты информации, угрозы.

Proposed general formal description of the dangerous for integrated system of information security, threats to information and telecommunication systems.

Key words: integrated system of information security, threats.

Надійшла 29.10.2009

УДК 004.681:681.3.06

Дмитренко О.П., д.т.н., проф. Хорошко В.О. (ДУІКТ)

ПОБУДОВА СТРУКТУРНОЇ МОДЕЛІ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ СИНТЕЗУ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Вступ

Комплекс заходів із забезпечення безпеки інформації в інформаційній системі (ІС) розглядається на трьох рівнях:

- правовому;
- організаційному;
- технічному.

На технічному рівні, який нас більш цікавить, забезпечення безпеки інформації у ІС виробляють підходи щодо застосування технічних і програмно-технічних засобів, які реалізують визначені вимоги із захисту інформації. Розглядаючи різні варіанти реалізації технічного рівня забезпечення безпеки інформації, слід враховувати такі аспекти:

- експлуатація та супроводження засобів блокування технічних каналів витоку інформації;
- керування доступом до інформації та механізмів, що реалізують послуги безпеки;
- перевірка і забезпечення цілісності критичних даних на на всіх стадіях їх обробки в ІС;
- резервне копіювання критичних даних, супроводження архівів даних і програмних засобів;
- відновлення роботи ІС після збоїв, відмов, насамперед систем із підвищеними вимогами до доступної інформації;
- захист програмних засабів окремих компонентів ІС і системи в цілому від несанкціонованого внесення доповнень і змін;
- забезпечення функціонування засобів контролю, у тому числі засобів виявлення технічних каналів витоку інформації.

Враховуючі аспекти захисту інформації при проектування комплексної системи захисту інформації (КСЗІ) формуються вимоги до системи, які поділяються на такі групи:

- вимоги щодо захисту від НСД (відповідно НДТЗІ 2.5-004-99);
- вимоги щодо захисту від витоку технічними каналами (відповідно НДТЗІ 2.5-005-99, НДТЗІ 2.5-008-02 та НДТЗІ 2.5-010-03).