Для профессионалов. – М., СПб., К.: "ИД Вильямс", 2008. – 928 с. 4. Petzold Charles.Programirowanie Microsoft WINDOWS w języku C#. – Warszawa: „RM", 2003. – 1161 s. 5. Powers Lars, Snell Mike. Microsoft Visual Studio – 2005. Księga eksperta. – Gliwice: „Helion", 2007. – 840 s. 6. Троэлсен Эндрю. Язык программирования C# и платформа .NET 2.0. – – М., СПб., К.: "ИД Вильямс", 2007. – 1168 с. 7. Schildt Herbert. C#. Kurs podstawowy. – Kraków:"Edittion 2000", 2002. – 638 с. 8. Овсяк В. Засоби еквівалентних перетворень алгоритмів / Овсяк В. // Доповіді національної академії наук України. – 1996. – №9. – С.83–89. 9. Овсяк В. АЛГОРИТМИ: аналіз методів, алгебра впорядкувань, моделі, моделювання / В. Овсяк. – Львів, 1996. – 132 с. 10. Овсяк В. АЛГОРИТМИ: методи побудови, оптимізації, дослідження вірогідності / В. Овсяк. – Львів: Світ, 2001. – 160 с. 11. Owsiak W., Owsiak A., Owsiak J. Teoria algorytmów abstrakcyjnych i modelowanie matematyczne systemów informacyjnych / Owsiak W., Owsiak A., Owsiak J. – Opole: Politechnika Opolska, 2005. – 275 s. 12. Ovsyak V.K. Computation models and algebra of algorithms / V.K. Ovsyak // Інформаційні системи та мережі: Вісник Нац. ун-ту "Львівська політехніка". – 2008. – № 621. – С.3 – 18.

УДК 004.22(0.23)

В. Лахно, А. Петров
Луганський національний аграрний університет,
кафедра економічної кібернетики

МОДЕЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНИХ СИСТЕМ ПІДПРИЄМСТВ З ВИКОРИСТАННЯМ ТЕОРІЇ ІГОР І МАРКІВСЬКИХ ПРОЦЕСІВ

Розглянуто питання моделювання системи захисту інформації, побудованої з використанням теорії ігор і теорії випадкових марківських процесів, за допомогою якої розглядається сукупність проектів систем захисту інформації, розраховуються вірогідність здійснення загроз для ресурсів корпоративних інформаційних систем і ризики за кожною загрозою, і на основі цих показників вибирається оптимальний проект.

The article deals with the issue of information security modeling system built using game theory and the theory of random Markov process, whereby a set of projects considered information security systems, calculate the probability of threats to corporate information systems resources and risks of each threat, and based on these indicators selected the best project.

Постановка проблеми

Найціннішою в корпоративних мережах суб'єктів господарської діяльності є інформація, яка становить інтерес для конкурентів. Про серйозність проблеми свідчить хоча б такий факт, що одна людина, що має доступ до серверу корпоративної мережі або бази даних, за незначний час може повністю паралізувати діяльність будь-якої компанії. Для цього достатньо ввести в програмне забезпечення системи всього декілька десятків рядків коду програми-вірусу. Якщо система не матиме спеціальних засобів захисту, то це загрожує як мінімум величезними економічними втратами.

Аналіз попередніх досліджень

У більшості вітчизняних і зарубіжних джерел вважають головною загрозою скоординовані напади хакерів на державні, корпоративні і приватні мережі одночасно з багатьох точок земної кулі. Такого роду напади характеризуються одночасним надсиланням мільйонів пакетів, великою

напруженістю мережного трафіку і приводять, як мінімум, до відмови в обслуговуванні видаленого комп'ютера. Декілька зловмисників можуть паралельно вести атаку на декілька вузлів, через що існуючим системам виявлення вторгнення набагато складніше ідентифікувати пакети, які передаються у межах скоординованого нападу. Більше того, при скоординованих нападах один з хакерів може здійснювати розвідку, тоді як інший здійснює напад [5]. Реалізація таких атак вимагає узгодження великої кількості атакуючих пакетів, які надходять з декількох вузлів [6].

Однією з основних цілей служби безпеки є захист цієї інформації від зовнішніх і внутрішніх комп'ютерних атак. Для виявлення атак необхідно використовувати системи моніторингу (системи виявлення атак), для перевірки достатності захисту й оцінювання її ефективності необхідно регулярно здійснювати перевірки на наявність загроз і за можливістю моделювати ці загрози.

Мета статті

У роботі запропоновано модель системи захисту, побудовану із використанням теорії ігор і теорії випадкових марківських процесів, за допомогою якої розглядається сукупність проектів систем захисту інформації (СЗІ), розраховуються вірогідність здійснення загроз для ресурсів корпоративних інформаційних систем (КІС) і ризики за кожною загрозою, і на основі цих показників вибирається оптимальний проект. Критеріями оптимальності є мінімальний ризик загроз інформації і мінімальна вартість проекту СЗІ при обмеженнях на решту показників.

Основний матеріал статті

Запропоновано загальну методику управління інформаційно-обчислювальним процесом для забезпечення інформаційної безпеки КІС (рис. 1).

У роботі зокрема розглянуто блоки моделі у вигляді гри між двома протиборчими сторонами: власник КІС і зловмисник.

Загалом гру можна описати функцією

$$b = (X, Y, Z), \tag{1}$$

де $X = \{x_i\}$ – безліч стратегій власника КІС, тобто можливі проекти побудови СЗІ; $Y = \{y_j\}$ – множина типів зловмисника, тобто деякі стратегії поведінки, властиві тому або іншому типу зловмисників; Z – функція корисності інформації для власника КІС.

Вірогідність зіткнення з певним типом зловмисника в КІС визначається розподілом вірогідності $P(y_j) = \{p_{y_j}\}$.

Матрицю виграшів H, власника КІС у цьому випадку можна подати так:

$$H = \{q(x_i, y_j)\}, \tag{2}$$

де $q(x_i, y_j)$ – виграш власника КІС при виборі ним і-ї стратегії і зіткненні із j-м типом зловмисника, у цьому випадку під виграшем розуміють деяку оцінку інформаційного ризику.

Для розрахунку також розглядається гра, задана функцією

$$b = (X, M, Z), \tag{3}$$

де $M = \{m_k\}$ – безліч загроз, які можуть бути реалізовані певним типом зловмисника.

Позначимо через A безліч номерів загроз інформації; PA – число можливих цілей порушника у захищеній КІС; D – безліч номерів засобів захисту, які можуть бути використані в системі захисту КІС; Bfa – безліч номерів загроз інформації, які реалізовані порушником у разі досягнення fa-ї мети; $N_l^{f_a}$ – безліч номерів засобів захисту, які потенційно можуть бути використані для протидії реалізації порушником fa-ї мети на l-му рубежі захисту (для нейтралізації m-ї загрози, що входить у ра-ту мету) (fa =1,2., PA; l= 1,2.,M).

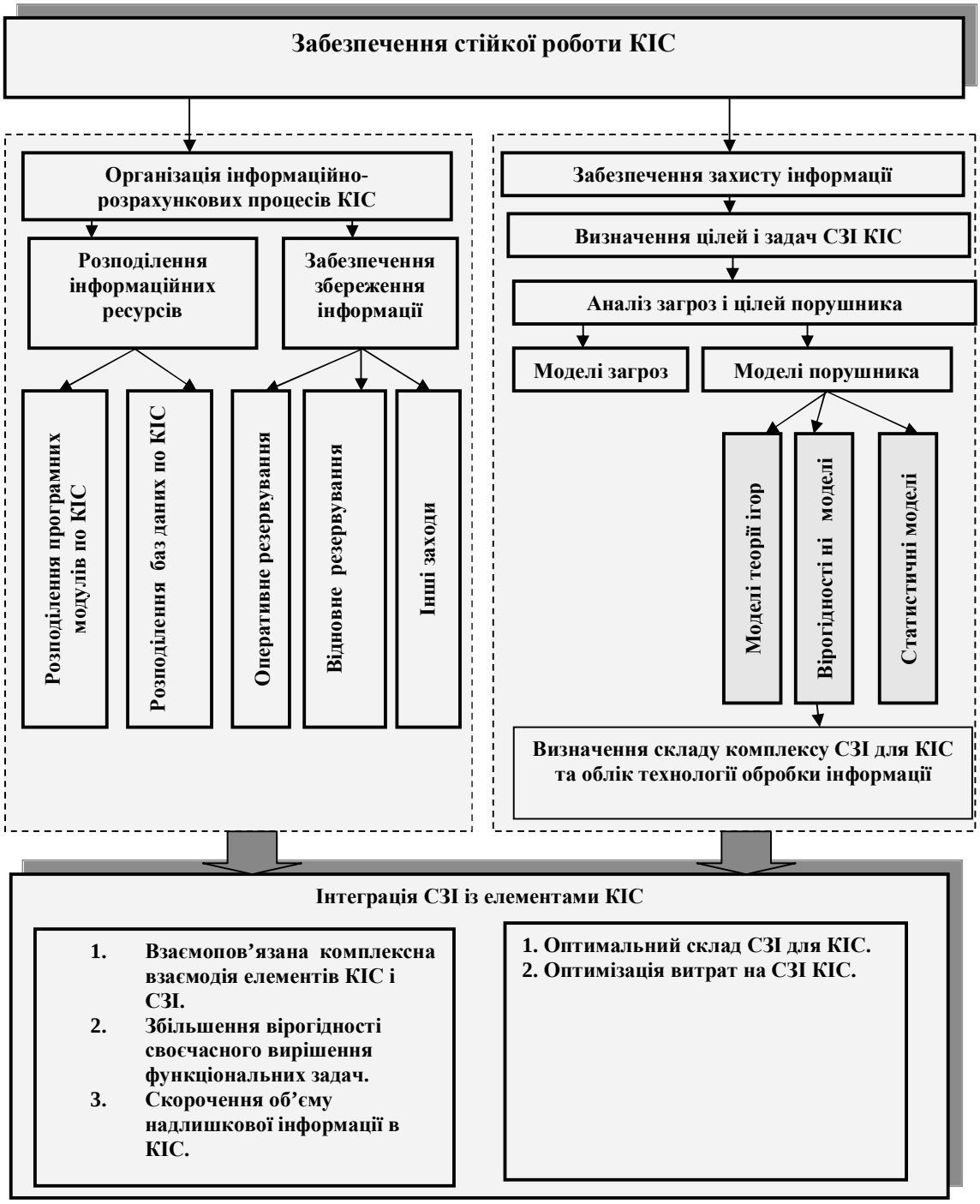


Рис. 1. Методика процесу забезпечення стійкості інформаційно-обчислювального процесу, збереження і захищеності інформації в КІС

Причому

$$B_{f_a} \subset PA,\ \bigcup_{f_a=1}^{PA} B_{f_a} = PA,\ n_{f_a} = \left|B_{f_a}\right| \ \text{и} \ \bigcup_{f_a=1}^{PA} \bigcup_{m \in B_{f_a}}^{n_{f_a}} N_l^{f_a} \subset D \ . \qquad (4)$$

У цьому випадку процес реалізації порушником кожної із своїх цілей можна подати у вигляді графу (рис. 2).

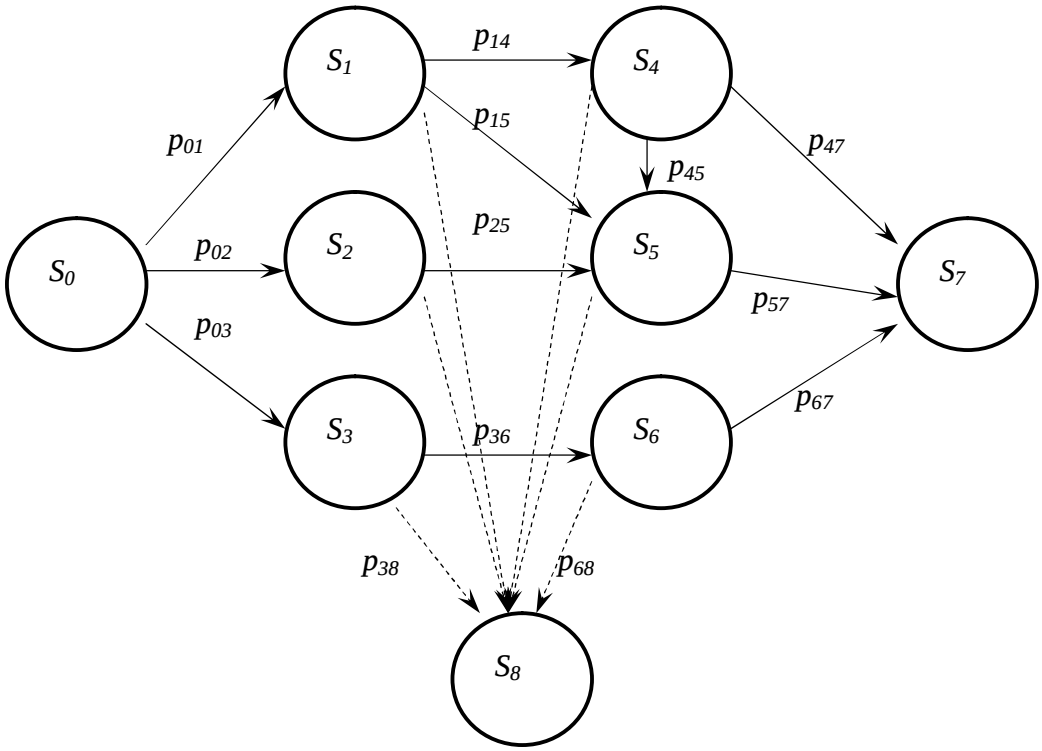


Рис. 2. Приклад графу станів КІС

Вершини графу є станами КІС, які відповідають спробам реалізації порушником деякої загрози інформації. Стан системи S0 є початковим, тобто таким, за якого жодна із загроз інформації не реалізована.

Стан Sj $\left(m \in B_{f_a}\right)$ відповідає спробі реалізації m-ї загрози. У разі її успішної реалізації здійснюється перехід до наступного стану системи, інакше (при штатному реагуванні СЗІ) – перехід до стану S_{n_f+1} (див. рис. 2). Стан $S_{n_{fa}}$ є кінцевим і відповідає досягненню порушником fa-ї мети (fa =1,2., РА). Дуги графу відповідають напрямам переходів між станами. Кожна дуга характеризується значенням вірогідності переходу між станами системи. Пунктиром позначені дуги, які відповідають переходу зі стану Si в стан $S_{n_{pa}+1}$.

Вірогідність вибору зловмисником певної загрози для реалізації розраховується як розподіл вірогідності $P(m_k) = \{p_{m_k}\}$.

Тоді матрицю виграшів G_j, $J = 1, J$ власника КІС у випадку гри з j-м типом зловмисника можна записати у вигляді:

$$G_j = \{q(x_i, m_{jk})\}, \tag{5}$$

де $q(x_i, m_{jk})$ – виграш власника КІС при виборі ним і-ї стратегії і виборі j-м типом зловмисника k-ї стратегії, зокрема під виграшем розуміємо ризик, розрахований за залежністю [1]:

$$q(x_i, m_{jk}) = P_{ijk}^{ug} \cdot C_k, \tag{6}$$

де P_{ijk}^{ug} – вірогідність реалізації k-ї загрози j-м типом зловмисника при і-му реалізованим проекті СЗІ; C_k – втрати від реалізації k-ї погрози.

Для розрахунку P_{ijk}^{ug} використовується модель подолання системи захисту (блок модель загроз, див. рис. 1).

Розглянемо як приклад модель атаки типу «Відмова в обслуговуванні», яка наведена у вигляді графу (рис. 3).

Модель є напівмарківським процесом з кінцевою безліччю станів

$$\{S\} = U \cup \{S1\} \cup T, \tag{7}$$

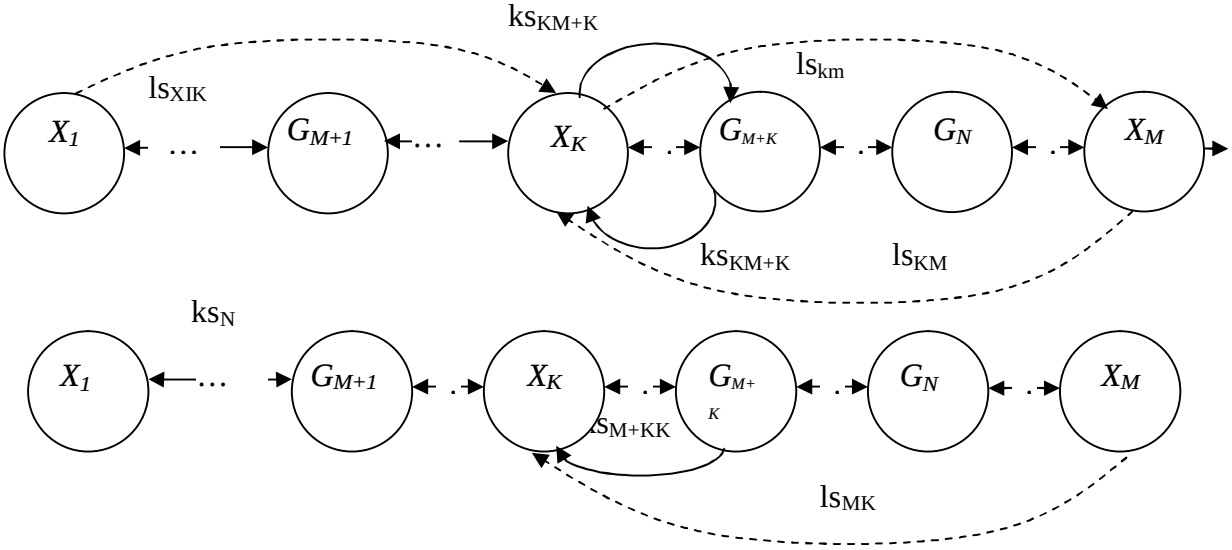
де U – зловмисник; $\{S1\}$ – множина вразливостей СЗІ; T – загроза КІС для j-го типу зловмисника.

Враховуючи специфіку модельованого процесу, всі стани є незворотними, а стан Т – поглинальним. Згідно з [2] напівмарківський процес визначається як східчастий випадковий процес $u(t), t \geq 0,$ з такими властивостями:

$u(t) = u_1 \quad [0, t_1]$;

$u(t) = u_2 \quad [t_1, t_2]$;

тощо.



$X = \{x_i \mid i = 1..M\}$ – множина хостів;

$G = \{g_i \mid j = M+1..N\}$ – множина маршрутизаторів КИС;

$KS = \{ks_{KL} \mid k = 1..N, L = 1..N\}$ – множина ліній зв'язку на мереженому рівні КІС

Рис. 3. Граф атаки типу «Відмова в обслуговуванні»

За фіксованої реалізації ланцюга Маркова $u_n = s_n, n \geq 1,$ тривалість перебування в певних станах (s1, s2, s3…) позитивна і незалежна, причому кожна з цих величин залежить лише від стану, в якому знаходиться процес, і від наступного стану.

У рамках цієї моделі час перебування в стані інтерпретується як час, необхідний зловмиснику на реалізацію a-ї загрози, за умови, що надалі він перейде до реалізації b-ї загрози.

Тоді можна задати такі функції розподілу часу перебування у стані:

$$P\{t_n - t_{n-1} < x \mid u_n = a, u_{n+1} = b\} = F_{ab}(x), n \geq 1, \tag{8}$$

де $F_{ab}(x)$ – матриця часу перебування системи у стані реалізації a-ї загрози за умови, що надалі вона перейде у b-й стан.

Крім того, задається початковий розподіл, що визначає, з якого стану зловмисник почне подолання СЗІ КІС, і матриця перехідної вірогідності, яка визначає вірогідність вибору шляху подолання СЗІ зловмисником.

Замість матриці перехідної вірогідності (p_{ab}) і матриці часів перебування можна задати лише функції [2]:

$$P_{ab}(x) = p_{ab} \cdot F_{ab}(x). \tag{9}$$

Функції $P_{ab}(x)$ мають таку інтерпретацію: якщо у певний момент часу зловмисник увійшов до стану реалізації a-ї уразливості, то з вірогідністю $P_{ab}(x)$ наступний його перехід відбудеться за час менший, ніж в стані реалізації b-ї загрози, або якщо b-й стан це стан T, то він перейде до реалізації загрози.

Згідно із [3], для опису часу, затрачуваного на виконання якої-небудь задачі, використовується логнормальний розподіл. Тобто функція розподілу часу перебування в стані $F_{ab}(x)$ описується логнормальним розподілом з певними параметрами.

Розв'язок шукають моделюванням напівмарківського процесу, який було описано вище. Моделювання проводиться до закінчення наперед заданого часу моделювання t^m, щоб визначити вірогідність P_t здійснення загрози за заданий час

$$P_t = E_T / E, \tag{10}$$

де ЕТ – кількість експериментів, в яких за час t^m було досягнуто стану Т; Е – загальна кількість експериментів;

Одержані в результаті моделювання величини P_t, для різних проектів СЗІ КІС, загроз і типів зловмисників, і є P_{ijk}^{ug}.

Після розрахунку всіх виграшів власника КІС в матрицях ігор $\{G_j\}$ в кожній матриці розраховується $\{q(x_i, y_j)\}$ – інформаційний ризик за і-м проектом СЗІ при зіткненні з j-м типом зловмисника. Він розраховується як:

$$q(x_i, y_j) = \sum_{k=1}^{n} q(x_i, m_{jk}) \cdot p(m_{jk}). \tag{11}$$

Для знаходження оптимального проекту СЗІ, тобто стратегії власника КІС, розглядається матриця Н.

Коли відомий розподіл вірогідності $P(y_j)$, власник КІС може скористатися байєсівською стратегією x_{bc} для оптимізації проекту, тобто:

$$Z(x_{bc} \mid P(y_j)) = \max(-1) \cdot Z(x_i \mid P(y_j)) = \max(-1) \sum_j q(x_i, y_j) \cdot p(y_j). \tag{12}$$

Фактично байесівська стратегія – це найкраща стратегія власника КІС в усередненій грі проти зловмисника.

У разі гри з невизначеністю, тобто з невідомим розподілом $P(y_j)$, для знаходження оптимальної стратегії власнику КІС фактично доводиться вибирати оптимальну стратегію експертним шляхом, при цьому можна скористатися одним з критеріїв: Вальда, Севіджа, Лапласа або Гурвіца [4].

Висновки

Описані моделі реалізації загроз КІС не тільки становлять самостійний практичний інтерес, але і є прикладом можливої формалізації опису інших програмних атак. Наведений підхід дає змогу перейти до кількісних процедур оцінювання можливостей реалізації загроз у корпоративних комп'ютерних мережах з урахуванням чинника часу, і тим самим підвищити обґрунтованість заходів, що проводяться у напрямі захисту інформації.

1. Петренко С.А. Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. – М.: ДМК Пресс, 2004. – 214 с. 2. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания. – М.: КомКнига, 2005. – 198 с. 3. Кельтон В., Лоу А., Имитационное моделирование. Классика CS. – 3-е изд. – СПб.: Питер; К.: Издательская группа BHV, 2004. – 480 с. 4. Протасов И.Д. Теория игр и исследование операций: Учеб. пособие. – М.: Гелиос АРВ, 2003. – 312 с. 5. http://www.ptsecurity.ru 6. http://www.whitehatsec.com/home/resource.