

информационной безопасности развития и лидерства, энергетической, экономической и других безопасностей. Оно должно включать нормативно-правовые, психологические и технологические приемы и средства обеспечения.

В индивидуальном плане наиболее эффективной мерой противодействия энергоинформационным влияниям является экранирование человека от воздействия излучений. Экраны выполняются в виде одежды из металлизированных тканей, экранирования помещений. В уникальную металлизированную одежду – халаты, жилеты или пояса –, защищающие от вредного электромагнитного излучения, станут в ближайшем будущем одеваться работники компьютерных служб, врачи физиокабинетов, летчики, военные, нефтяники и все те, кто подвергается излучению. Суперткань представляет собой тканую основу, на которую нанесено несколько слоев различных металлов.

Кроме пассивных средств противодействия энергоинформационным воздействиям применяются активные средства.

Однако, самыми эффективными средствами противодействия представляются внесистемные политические средства – правовое регулирование использование процессов энергоинформационного воздействия в рамках международного сотрудничества.

V Выводы

Проведен обзор состояния проблем энергосбережения в информационных системах и энергоинформационных воздействий на человека. Представлены эвристические модели и задачи энергетической безопасности общества и энергоинформационной безопасности человека.

Направлениями дальнейших исследований могут быть разработка математически и/или имитационных моделей процедур обеспечения безопасности.

Література: 1. Есауленко Алексей. Синдром энергодефицита в информационной индустрии // *Сети*, № 2, 2007 (<http://www.osp.ru/nets/2007/02/3945207>). 2. Севериновский Евгений, Олейник Тарас. IDF Spring, 2006: какими будут компьютеры следующих лет // *Компьютерное обозрение*, 30 марта, 2006 (<http://itc.ua/23815>). 3. Ефременко Д. В. Введение в оценку техники. Изд-во МНЭПУ, - М.: 2002. – С. 188. (<http://www.vusnet.ru/biblio/archive/efremenko%5Fvvedenie/default.aspx>). 4. Закон України. «Про основи національної безпеки України». В редакції від 15.12.2005 р. 5. Лозовик Ю. Э., Попов А. М. Свойства и нанотехнологические применения нанотрубок // *Успехи физических наук*. Т. 177, № 7, 2007. – С. 786 – 799. 6. Методика информационной безопасности. Под рук. авторского коллектива академика Ю. С. Уфимцева. – Издательство «Екзамен», 2004. – С. 544. 7. Кучерявий А. Е., Кучерявий Е. А. От Е-России к U-России: Тенденции развития электросвязи // *Электросвязь*, № 5, 2005. С. 10 – 12. 8. ITU-T Recommendation X.1081. The telebiometric ITU-T Recommendation X.1081. The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics. – 22 с. 9. Кононович І. В., Кононович Ю. В. Телебіометрика та сенсорні мережі. Вибір топології телекомунікацій. // *Сб научных трудов Четвертого семинара “Информационные системы и технологии”* (Приложение к журналу «Холодильная техника и технологии»), 19-20 октября 2006 года, – Одесса, 2006. С. 28 - 35. 10. Махов С. А. Устойчивое развитие с точки зрения технологического императива. // *ИПИМ им. М. В. Келдыша. Препр. № 63*, Москва, 2006. – С. 20. 11. Форрестер Дж. Мировая динамика. – М.: Наука, 1978. – С. 287. 12. Табунчиков Ю. А. Строительные концепции XXI века в области теплоснабжения и климатизации // *Сборник материалов Международной научно-технической конференции «Теоретические основы теплогазоснабжения и вентиляции»*. – М.: 2005. (<http://tgvmgsu.ru>).

УДК 681.3.06

АНАЛІЗ ЧУТЛИВОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДО ЗМІНИ ЕФЕКТИВНОСТІ РЕАЛІЗАЦІЇ ЗАГРОЗ ТА КОЕФІЦІЄНТІВ МІЦНОСТІ МЕХАНІЗМІВ ЗАХИСТУ

Олексій Новіков, Андрій Родіонов

Національний технічний університет України "КПІ"

Анотація: На основі логіко-імовірнісного методу для опису структурно-складних систем запропоновано алгоритм аналізу чутливості системи захисту інформації до зміни параметрів механізмів захисту та ефективності реалізації загроз у системі.

Summary: Based on logical-and-probabilistic method for complex system, have proposed method and

algorithm for sensitivity of information security system analysis.

Ключові слова: Інформаційна безпека, система захисту, механізми захисту, чутливість.

I Вступ

Сучасні інформаційно-комунікаційні системи складаються з багатьох компонентів, є розподіленими та інтероперабельними. Для забезпечення конфіденційності, доступності, цілісності та спостереженості інформації, яка в них обробляється, створюється комплексна система захисту інформації. Системи захисту інформації притаманні ті самі властивості складності, що і основній системі. При цьому, система захисту інформації не є статичним об'єктом, а може змінюватися під час експлуатації. Також може змінюватись модель загроз безпеці, і до складу системи включатись (або видалятися) додаткові механізми захисту.

Тому необхідним є проведення періодичного аналізу системи захисту інформації з метою забезпечення захищеності на заданому рівні безпеки та своєчасної реакції на зміну ефективності загроз.

Задачі аналізу систем безпеки інформації вирішувались у ряді робіт. У першу чергу це стосується механізмів криптографічного захисту, де розглядаються задачі аналізу стійкості криптографічних алгоритмів [1].

У [2] виконується спроба застосувати системний аналіз до систем захисту інформації. У [3] за допомогою функції чутливості аналізується вплив дестабілізуючих факторів на ступінь захищеності системи.

Актуальною залишається задача аналізу чутливості системи захисту до зміни параметрів міцності механізмів захисту, та чутливості системи захисту до зміни рівнів загроз безпеці. В результаті, ґрунтуючись на отриманих даних, можна виконати оптимізацію системи захисту інформації.

Метою даної роботи є розробка та дослідження методу і алгоритму аналізу чутливості існуючої системи захисту до зміни параметрів механізмів захисту та ефективності реалізації загроз у системі.

II Постановка задачі аналізу чутливості системи захисту інформації

Для опису рівня захищеності інформаційної системи скористаємось логіко-імовірнісним методом для опису структурно-складних систем. У [4] отримане рекурентне співвідношення, що визначає ймовірність збереження захищеності інформації для абстрактної системи з відкритою архітектурою для довільного числа рівнів протоколів і загроз інформації, можливих для даної системи:

$$P(E, K, M) = \prod_{i=1}^L P_i(M) = \prod_{i=1}^L \left(\prod_{j=1}^N (1 - E_{ij}) + \sum_{j=1}^N \left[E_{ij} \prod_{k=1}^{j-1} (1 - E_{ik}) \left(\sum_{k=1}^j M_{ik} K_{ik} \prod_{l=k+1}^j (1 - M_{il} K_{il}) \right) \right] \right), \quad (1)$$

де $L \in \mathbb{Z}$ – кількість загроз інформації, включених до множини загроз;

$N \in \mathbb{Z}$ – кількість рівнів стека протоколів інформаційної системи;

$E_{ij} \in [0,1]$ – показник ефективності реалізації i -ї загрози на протоколі j -го рівня;

$M_{ij} \in \{0,1\}$ – параметр, який визначає наявність або відсутність механізму захисту від i -ї загрози, реалізованого на протоколі j -го рівня (наявність або відсутність цих механізмів захисту визначає структуру системи захисту);

$K_{ij} \in [0,1]$ – коефіцієнт міцності механізму захисту від i -ї загрози, реалізованого на протоколі j -го рівня.

Показники ефективності загроз (E_{ij}) можуть бути отримані статистичними або експертними методами, ґрунтуючись на аналізі й типах різних атак та загроз, найбільш поширених в інформаційних системах.

Значення коефіцієнтів міцності (K_{ij}) можуть бути отримані методом, запропонованим у роботі [6] (обчислення оптимальних значень коефіцієнтів міцності механізмів захисту інформації, які забезпечують ймовірність збереження захищеності системи не нижче заданого граничного значення).

Виходячи зі співвідношення (1), ймовірність збереження захищеності системи визначається структурою системи захисту інформації, коефіцієнтами міцності механізмів захисту та ефективністю реалізації загроз. При зміні кожної з цих складових рівень захищеності системи буде змінюватися.

Таким чином, для існуючої системи захисту інформації, що може бути описана співвідношенням (1), визначимо чутливість системи до зміни ефективності реалізації загроз та чутливість системи до зміни міцності механізмів захисту.

III Функції чутливості системи захисту інформації

Математична постановка задачі полягає в знаходженні функції чутливості за параметрами моделі (1), які відповідають за міцність механізмів захисту та ефективність реалізації загроз.

Функція чутливості (чи коефіцієнти впливу параметрів) визначаються як частинна похідна за відповідними параметрами системи [7].

Функція чутливості системи до зміни міцності механізмів захисту визначимо як частинну похідну за відповідним коефіцієнтом міцності від ймовірності збереження захищеності системи:

$$\frac{\partial P(K)}{\partial K_{ij}} = \frac{\partial P_i(K)}{\partial K_{ij}} \prod_{k=1}^{i-1} P_k(K) \prod_{l=i+1}^L P_l(K),$$

де

$$\frac{\partial P_i(K)}{\partial K_{ij}} = M_{ij} \sum_{k=j}^N E_{ik} \prod_{l=1}^{k-1} (1 - E_{il}) \prod_{l=1}^{j-1} (1 - M_{il} K_{il}) \prod_{l=j+1}^k (1 - M_{il} K_{il});$$

Функція чутливості системи до зміни ефективності реалізації загроз визначимо як частинну похідну за відповідним показником ефективності реалізації загроз від ймовірності збереження захищеності системи:

$$\begin{aligned} \frac{\partial P(E)}{\partial E_{ab}} = & \left(\prod_{i=1, i \neq a}^L \left[\prod_{j=1}^N (1 - E_{ij}) + \sum_{j=1}^N \left(E_{ij} \prod_{r=1}^{j-1} (1 - E_{ir}) \left(\sum_{r=1}^j M_{ir} K_{ir} \prod_{l=r+1}^j (1 - M_{il} K_{il}) \right) \right) \right] \right) * \\ & * \left[-1 \prod_{j=b+1}^N (1 - E_{aj}) + \left(\prod_{r=1}^{b-1} (1 - E_{ar}) \right) * \left(\sum_{r=1}^b M_{ar} K_{ar} \prod_{l=r+1}^b (1 - M_{al} K_{al}) \right) - \right. \\ & \left. - \sum_{j=b+1}^N \left\langle E_{aj} \prod_{r=1, r \neq b}^{j-1} (1 - E_{ar}) \left(\sum_{r=1}^j M_{ar} K_{ar} \prod_{l=r+1}^j (1 - M_{al} K_{al}) \right) \right\rangle \right] \end{aligned}$$

Отриманні після обчислень значення функцій чутливості будуть показувати ступінь впливу кожного з параметрів на рівень захищеності системи.

IV Обчислювальний експеримент

Як вхідні дані для обчислення значень функцій чутливості візьмемо результати, отримані в [5, 6].

У [5] у результаті розв'язку задачі оптимального синтезу отримана структура механізмів захисту інформації. У [6] запропоновано алгоритм, за яким для цієї структури визначили оптимальні значення коефіцієнтів міцності, які забезпечують імовірність збереження захищеності системи не нижче заданого граничного рівня.

Загрози та ефективності їх реалізації є наступними: $E = E_{1,1} = 0.3$ – перехоплення інформації та викриття її змісту (*information sniffing*); $E_{1,2} = 0.05$ – відмова в обслуговуванні (*DoS-атака*); $E_{1,3} = 0.15$ – неавторизований доступ (*unauthorized access*); $E_{1,4} = 0.4$ – порушення цілісності інформації (*violation of information integrity*); $E_{2,1} = 0.05$ – підміна джерела інформації (*spoofing of information traffic*); $E_{2,2} = 0.35$ – порушення цілісності інформації (*violation of information integrity*); $E_{2,4} = 0.6$ – неавторизований доступ (*unauthorized access*).

В результаті виконання алгоритму з [6] отримаємо наступні значення коефіцієнтів міцності для відповідних механізмів захисту: $K = K_{1,1} = 0.78$ – шифрування даних (*data encoding*); $K_{1,2} = 0.26$ – фільтрація запитів (*filtration*); $K_{1,3} = 0.22$ – автентифікація (*authentication*); $K_{1,4} = 0.14$ – цифровий підпис (*digital signature*); $K_{2,1} = 0.68$ – строга маршрутизація (*routing*); $K_{2,2} = 0.56$ – перевірка контрольних сум (*checksum*); $K_{2,4} = 0.23$ – контроль доступу (*access control*).

У результаті обчислень значень функцій чутливості з вхідними даними, наведеними вище, отримуємо наступні результати: чутливість системи захисту до зміни коефіцієнтів міцності (рис. 1); чутливість системи захисту до зміни ефективності реалізації загроз (рис. 2).

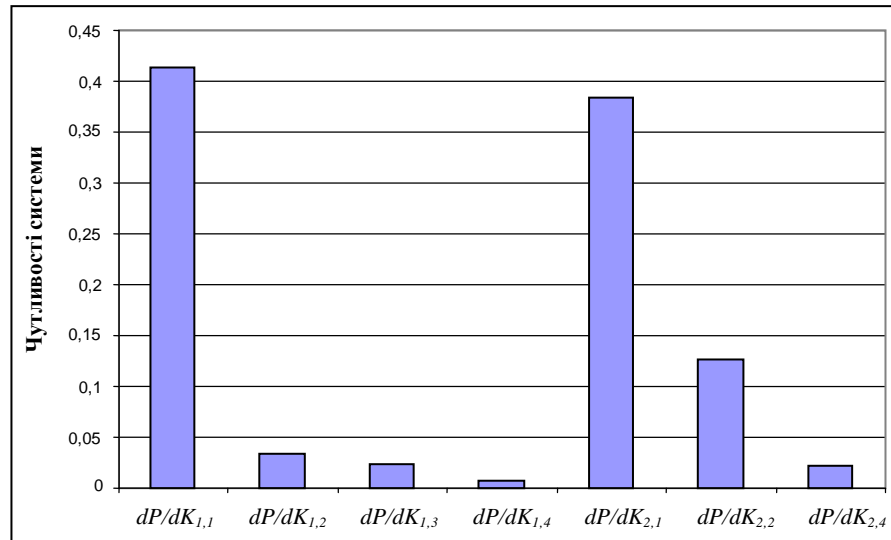


Рисунок 1 – чутливості системи захисту до зміни коефіцієнтів міцності

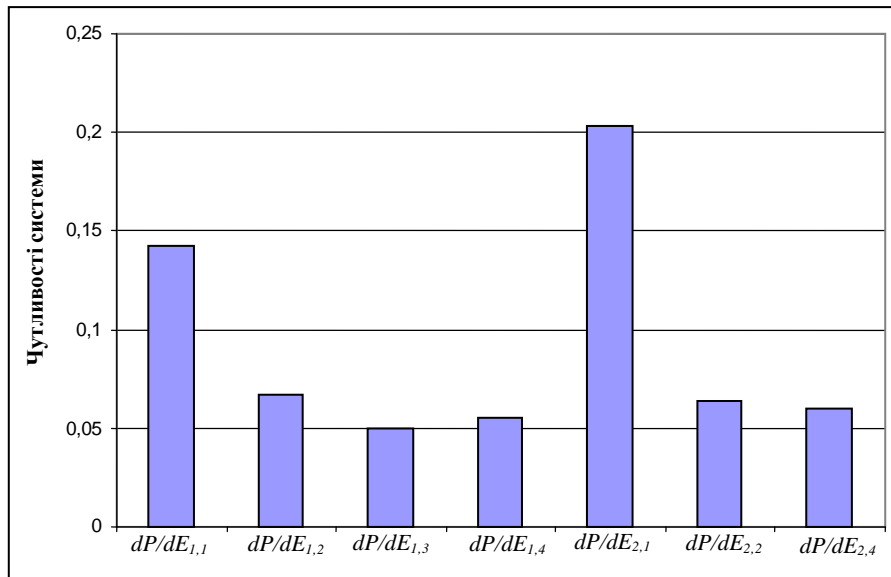


Рисунок 2 – чутливість системи захисту до зміни ефективності реалізації загроз

V Інтерпретація результатів

Чутливість системи захисту до коефіцієнтів міцності показує важливість відповідного механізму захисту та його коефіцієнту міцності для збереження ймовірності захищеності системи.

Чутливість системи захисту до зміни ефективності реалізації загроз показує вплив відповідної загрози на систему захисту інформації. У цьому випадку зниження коефіцієнтів чутливості буде сприяти збільшенню стійкості системи.

Таким чином, за допомогою збільшення коефіцієнту міцності відповідного механізму захисту можна зменшити чутливість системи захисту до збільшення ефективності реалізації загрози, на нейтралізацію якої направлений даний механізм. Але це має сенс робити там, де коефіцієнти чутливості до загроз є найбільш високими.

VI Висновки

Грунтуючись на даному методі можна знаходити найбільш критичні для системи захисту механізми захисту. Також можна моделювати відмови механізмів захисту та зміни впливу ефективності реалізації загроз на систему захисту інформації.

Даний метод може використовуватися експертами під час проведення аудиту системи захисту

інформації для подальшої оптимізації її структури.

Література: 1. Брюс Шнайер. Прикладная криптография, 2-е издание. Триумф. 2002 г. - 816 с. 2. А. А. Шелупанов. А. А. Шумский. Системный анализ в защите информации. Гелиос АРВ, 2005 г.- 224 с. 3. Г. А. Остапенко. Информационные операции и атаки в социотехнических системах. Горячая Линия-Телеком, 2007 -134 с. 4. О. Новіков, А. Тимошенко. Побудова логіко-ймовірностної моделі захищеної комп'ютерної системи. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001.- Вип. 3. – с. 101 – 105. 5. Ю. Ю. Боня, О. М. Новіков. Синтез систем захисту інформації з мінімальною вартістю механізмів захисту. Проблеми керування та інформатики. 2006, № 3. – с. 147–156. 6. О. М. Новіков, А. М. Родіонов, А. О. Тимошенко. Оптимальний синтез параметрів системи захисту інформації. Наукові вісті КПП. 2007, № 4. – с. 146-151. 7. П. Эйкхофф. Основы идентификации систем управления. Мир, 1975.