УДК 004 к.т.н., доц. **Петров А.О.** (СНУ ім. В. Даля)

МЕТОДОЛОГІЯ ОЦІНЮВАННЯ РІВНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

У статті запропонована нова методологія процесу оцінювання рівня захищеності інформації, засновану на сучасному науковому базисі. Процес оцінювання захищеності інформації представлене як аналіз і оцінювання ризиків, у результаті чого оцінюється оптимальність використовуваних або планованих засобів захисту адекватно існуючим погрозам. У статті формулюється проблема одержання чисельної оцінки показника ефективності засобу захисту інформації. Чисельне оцінювання полягає в зіставленні узагальненому показнику ефективності засобу захисту – захищеність інформації - одного числа.

Ключові слова: інформаційна безпека (ІБ), нечіткі множини, рівень захищеності, імовірність, загроза.

Вступ. Методологія повинна містити кількісні алгоритми аналізу й синтезу систем захисту та керування ними в процесі функціонування. Тому одним з основних положень концепції захисту повинна бути вимога обґрунтованого підходу до оцінювання у кількісному вираженні необхідного рівня захищеності на об'єкті захисту в мінливих умовах його функціонування.

Науковий аналіз проблеми одержання чисельної оцінки ризику порушення ІБ і рівня захищеності інформації припускає визначення ключових термінів даної проблематики: захищеність інформації, керування ризиками, та імовірності загроз.

Керування ризиками (рівнем захищеності) – це процес усунення або зменшення імовірності подій, потенційно здатних негативно впливати на ресурси інформаційної системи, за рахунок вибору контрзаходів за умови прийнятної вартості захисту. Ціль керування полягає в тому, щоб зменшити ризики до рівнів, установлених уповноваженим для цього особою, що ухвалюють розв'язок про припустиме значення відносного ризику. Процес керування ризиками містить у собі аналіз, оцінювання ризиків і вибір належних контрзаходів [1] у рамках організаційно-технічного керування ЗІ. Аналіз ризиків – це виявлення потенційних загроз, що впливають на рівень можливого збитку.

Процес оцінювання величини ризиків при проектуванні СЗІ містить у собі: визначення цінності ресурсів, вивчення загроз і вразливостей, вибір параметрів для їх опису та одержання оцінок імовірностей по цих параметрах, оцінок теоретичної ефективності контрзаходів і очікуваного збитку, визначення його прийнятності.

У процесі аналізу та оцінювання ризиків встановлюється ступінь адекватності використовуваних або планованих наборів засобів захисту існуючим загрозам.

Основна частина.Визначимо зміст поняття «захищеність інформації». В [2] відзначається, що захищеність інформації не є властивістю певного кількості інформації на відміну від цінності, а залежить від характеристик функціонування системи захисту. Захищеність інформації ϵ властивістю засобу захисту досягати цільового ефекту, що полягає в недопущенні несанкціонованого доступу до програм, що захищаються даним і, при взаємодії із системою інформаційного нападу. Характеристика захищеності визначається об'єктивними (статистичними) або суб'єктивними (експертними) імовірностями досягнення засобами захисту відповідних цілей. У динамічних моделях захищеність інформації може змінюватися із часом і описується значеннями відповідних показників у фіксовані моменти часу. У динамічних завданнях показник захищеності показує виграш ЗЗ на даному тимчасовому інтервалі $[0, T]$, у статичних завданнях – очікуваний прогнозований виграш ЗЗ.

Стосовно до властивості захищеності інформації найпростіші властивості визначаються здатністю системи захисту досягати тієї або іншому ступеня відповідних елементарних цільових ефектів, що полягають у перешкоді системі нападу одержувати, руйнувати або блокувати інформацію.

Властивість захищеність інформації кожного ЗЗ, що входить у СЗИ, у сукупності визначає захищеність інформації в СЗИ в цілому. Таким чином відзначемо, що захищеність інформації буде являти собою комплексний показник – вектор, компоненти якого є показники кожного ЗЗ, що входить у СЗІ:

$$Z = \left\langle Z_{ЗЗ}, ..., Z_{ЗЗ_i}, ..., Z_{ЗЗ_n} \right\rangle, \quad (1)$$

де n – кількість ЗЗ, що входять у СЗИ; $Z_{ЗЗ_i}$ – показник захищеності інформації і-*го* ЗЗ; Z – комплексний показник захищеності інформації.

Показник захищеності необхідний для одержання кількісних оцінок при розв'язку прикладних завдань аналізу й синтезу СЗІ, керування ЗІ.

Наявність уразливості ЗЗ може привести до порушення захищеності, тобто до здійснення погрози. Відомо, що уразливість – це фактор об'єкта захисту, недолік якого-небудь засобу захисту або слабість системи захисту. Уразливість може бути результатом помилок на етапах виробітку вимог і проектування, при розробці або реалізації ЗЗ, або результатом, недотримання правил застосування й помилок, допущених у ході експлуатації. При розв'язку завдань захисту інформації першорядний значення має кількісна оцінка її уразливості. Оскільки вплив на інформацію різних факторів значною мірою є випадковим, то в якості кількісного заходу її уразливості найбільше доцільно застосувати імовірність порушення захищеності інформації P_I.

Неясність способу визначення значень імовірностей погроз і уразливостей є основною проблемою при кількісному оцінюванні ризиків порушення ІБ. У зв'язку з ростом складності інформаційних систем, участю людини в процесах керування, обробки й передачі інформації, функціонування сучасних інформаційних систем характеризується великим ступенем невизначеності, випадковості, нестабільності, впливом зовнішніх і внутрішніх збурювань. Усі ці фактори обмежують використання класичних математичних методів і точних моделей, заснованих на застосуванні теорії імовірності. Це обумовлене також або відсутністю, або недоліком інформації про функціонування компонентів інформаійної системи. Крім того, при проектуванні системи захисту статистичний дані про ймовірності погроз і уразливостей відсутні [3].

Відповідно одному із принципів системного аналізу – принципу невизначеності – у процесі дослідження системи необхідний облік невизначеностей і випадковостей, однак складні відкриті системи не підкоряються імовірнісним законам. У таких системах можна оцінити «найгірші» ситуації й розгляд проводити для них. Цей спосіб звичайно називається методом гарантованого результату. Він застосовний, коли невизначеність не описується апаратом теорії ймовірностей, його слід використовувати при оцінці ймовірностей погроз.

Імовірність реалізації погрози для деякого ресурсу залежить від технічних можливостей для реалізації й привабливості ресурсу.

Для одержання чисельних оцінок імовірності порушення захищеності пропонується використовувати поняття нечіткості і суб'єктивної ймовірності. З поняттям нечіткості пов'язані класи, у яких існують градації ступеня приналежності, що займають проміжні значення між повною приналежністю й повною неприналежністю об'єктів до певного класу. Відзначемо нечіткий характер приналежності засобів захисту до множини ЗЗ, за допомогою яких можуть бути виявлені й блоковані несанкціоновані дії. На відміну від об'єктивної імовірності – поняття, застосовуваного при аналізі результатів великої кількості спостережень, що мали місце в минулому, або отриманих при аналізі відносної частоти появи якої-небудь події в загальному числі спостережень, під суб'єктивною ймовірністю є через захід упевненості експерта в тому, що подія буде мати місце. Вона погоджується з функцією корисності.

Значення показника засобу захисту захищеність інформації $P_б$ – це суб'єктивна ймовірність виявлення й блокування засобом захисту несанкціонованих дій, тобто теоретична очікувана ефективність бар'єра.

Очевидно, імовірність порушення захищеності P_I доповнює $P_б$ до одиниці, тобто

$$P_I = 1 - P_б, \qquad (2)$$

де P_I – імовірність порушення захищеності інформації, або ймовірність уразливості m-го засобу захисту.

Правильність виконання засобом захисту своїх функцій, перевірка відповідності реальних і декларованих функціональних можливостей і контроль відсутності недекларованих оцінюються в ході сертифікаційних випробувань. При експлуатації засобу захисту необхідно здійснювати перевірку показника «захищеність» для того, щоб вчасно виявити уразливість у випадку її виникнення та вжити заходів до її усунення або зменшити її шкідливі наслідки. Властивість захищеності інформації кожного засобу захисту, що входить у СЗІ, у сукупності визначає захищеність інформації в ІС у цілому.

В імовірнісне статичному підході не враховується динаміка зміни значень імовірностей погроз і уразливостей у часі, оцінюються апріорні очікувані значення показників засобів захисту «захищеність інформації» і ймовірностей порушення захищеності.

Одержання чисельних оцінок суб'єктивних імовірностей виявлення й блокування засобами захисту несанкціонованих дій з використанням механізму нечіткого логічного виводу/ У процесі розв'язку завдання оцінювання показника захищеності інформації ЗЗ виникають перешкоди для побудови точних моделей на основі класичних математичних методів.

Подібні завдання, які не піддаються строгій формалізації, може розв'язати експерт із використанням суб'єктивних вистав.

Суб'єктивна ймовірність того, що ЗЗ може бути віднесене до безлічі засобів захисту, за допомогою яких можуть бути виявлені й блоковані несанкціоновані дії, – це імовірнісний захід, який може бути отримана експертним шляхом. Для одержання суб'єктивних імовірностей $P_{бт}$ у роботі використовується тісний зв'язок між $P_{бт}$ і корисністю ЗЗ.

Оцінка значень суб'єктивних імовірностей $P_{бт}$ повинна бути вільна від сваволі. Приватні показники захищеності повинні мати ясний фізичний зміст і бути взаємозалежними. Тому особливістю пропонованого в роботі підходу є одержання чисельних оцінок суб'єктивних імовірностей $P_{бт}$ на основі об'єктивних технічних характеристик і можливостей засобів захисту, декларируемых їх розроблювачами.

Методи оцінювання ЗЗ розділяються на якісні й кількісні. Якісні методи використовуються на початкових етапах моделювання. Із цією метою була розроблена система ієрархічних показників якості засобів захисту, що ставляться до наступних функціональних підсистем: VPN, IDS, антивірусний захист, мережний контроль доступу, виявлення вторгнень на хосте, розмежування доступу, резервне копіювання, ідентифікація й аутентификация. Кількісні методи використовуються на наступних етапах моделювання для кількісного аналізу кожного засобу захисту.

Якість – сукупність істотних властивостей засобу захисту, що обумовлюють його відповідність для використання по призначенню.

У роботі вирішується завдання одержання чисельної оцінки узагальненого показника якості ЗЗ. Чисельне оцінювання полягає в зіставленні узагальненому показнику якості засобу захисту – захищеність інформації - одного числа. Це завдання може бути вирішена безпосередньо за допомогою експертів.

Показник якості – це вектор показників істотних властивостей. Основною характеристикою якості є сукупність атрибутивних властивостей Срз, істотних для його

використання по призначенню, що характеризують ступінь його функціональної придатності.

Узагальненим показником якості ЗЗ є вектор:

$$Z_{\text{Захист ЗЗ}_i} = A_{\text{Захист ЗЗ}} =< A_{\text{Захист ЗЗ}_{11}}, A_{\text{Захист ЗЗ}_{12}}, \ldots A_{\text{Захист ЗЗ}_{1n}},$$

$$A_{\text{Захист ЗЗ}_{21}}, A_{\text{Захист ЗЗ}_{22}}, \ldots A_{\text{Захист ЗЗ}_{2m}} >$$

компоненти якого – показники його окремих властивостей, або частки показники якості. Розмірність вектора визначається числом обраних для аналізу істотних властивостей засобу захисту.

Приватні показники якості ЗЗ мають різні розмірності. Тому при утворі узагальненого показника якості ЗЗ – захищеність інформації – слід оперувати не з *показниками*», а з їхніми нормованими значеннями, що забезпечують приведення показників до одному масштабу, що необхідно для їхнього зіставлення.

Необхідна якість засобу захисту задається правилами, яким повинні задовольняти показники істотних властивостей, а перевірка їх виконання називається оцінюванням якості засобу захисту. Ефективність ЗЗ за критерієм – це приписування йому дійсне число, що характеризує його перевагу в порівнянні з іншими альтернативами щодо мети захисту.

Таким чином, для одержання розв'язків в області інформаційної безпеки пропонується використовувати математичний апарат нечітких множин. Розглянемо використання апарата нечітких множин для одержання чисельної оцінки узагальненого показника ефективності ЗЗ – захищеність інформації.

Формування функції приналежності засноване на аналізі впливу показника на показника більш високого рівня ієрархії на основі методу експертних оцінок, який припускає, що практичний досвід і знання експертів важко замінити дедуктивними побудовами формального характеру. Тому способам на експертній основі властиві відомі переваги в порівнянні з іншими, і вони інтенсивно синтезуються на даний момент часу. Суб'єктивні моменти в оцінку ефективності хоча й вносяться, але в непрямийо спосіб.

При формуванні функцій приналежності по двом групам критеріїв ефективності для засобів захисту, що ставляться до одній функціональній підсистемі, треба використовувати організовані в табличній формі відомості про технічні характеристики обраних для аналізу використовуваних сучасних програмних або апаратних ЗЗ.

Необхідно використовувати відомі методи побудови функції приналежності, засновані на формалізації й інтеграції нечітких даних, сформованих експертом у процесі оцінювання параметрів реальних засобів захисту. Внаслідок цього формулюються відповідні продукційні правила, що дозволять обробляти складні з'єднання.

Використання механізму нечіткого логічного виводу для чисельного оцінювання показника ефективності ЗЗ приводить до необхідності встановлення найбільш значимих приватнх показників захищеності – об'єктивних технічних характеристик засобів захисту, що входять в ієрархічну- структуру, розроблену для ЗЗ відповідної функціональної підсистеми.

Висновки і перспективи подальших розвідок у даному напрямку. Запропоновано методологію оцінювання рівня захищеності інформації у інформаційній системі, що полягають у тому, що необхідні для розрахунків чисельні значення імовірностей уразливостей пропонується одержувати з використанням експертних оцінок на основі відомостей про об'єктивні технічні характеристики засобів захисту, адекватність методу не залежить від наявності або відсутності достовірних статистичних даних по інцидентах ІБ, які відсутні на етапі проектування СЗІ, що дозволяє забезпечити оперативність оцінювання, можливість порівняння різних комплексів контрзаходів у кількісному вираженні й застосовність методу на стадії розробки СЗІ.

У наступних роботах буде дано більш докладне та розгронутий опис запропонованого методу.

ЛІТЕРАТУРА:
1. Машкина И.В., Гузаиров, М.Б. Интеллектуальная поддержка принятия решений по управлению защитой информации в критически важных сегментах информационных систем // Информационные технологии.№7. Приложение - 32 с.
2. Касперский, К. Компьютерные вирусы снаружи и изнутри. — СПб.: Питер, 2006. - 527 с.
Нестеренко, В.А. Статистические методы обнаружения нарушений безопасности в сети //Информационные процессы. - 2006. — т. 6. - Вып. 3.-С. 208-217.

Рецензент: д.т.н, проф. Хорошко В.О., професор кафедри безпеки інформаційних технологій Національного авіаційного університету**.**

к.т.н. Петров А.А.

МЕТОДОЛОГИЯ ОЦЕНКИ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМАХ

В статье предложена новая методология процесса оценивания уровня защищенности информации, основанную на современном научном базисе.Процесс оценивания защищенности информации представлено как анализ и оценивания рисков, в результате чего оценивается оптимальность используемых или планируемых средств защиты адекватно существующим угрозам. В статье формулируется проблема получения численной оценки показателя эффективности средства защиты информации. Численное оценивание состоит в сопоставлении обобщенному показателю эффективности средства защиты – защищенность информации - одного числа. Предложено использования аппарата нечетких множеств для получения численной оценки обобщенного показателя эффективности средства защиты информации.

Ключевые слова: информационная безопасность, нечеткие множества, уровень защищенности, вероятность, угроза.

Petrov A.

METODOLOGY OF SECURITY LEVEL EVALUATION IN THE INFORMATION AND COMMUNICATION SYSTEMS

The paper proposes a new methodology for the evaluation process is the level of information security, based on the modern scientific basis. The evaluation process is presented as information security analysis and assessment of risks, resulting in estimated optimally utilized or planned resources to adequately protect existing threats. We formulate the problem of obtaining the numerical evaluation of performance indicator means of information protection. Numerical evaluation is to compare the effectiveness of the generalized index of protection - protection of information - one number.

Suggested the use of fuzzy sets for the numerical evaluation of the generalized indicator of the effectiveness of protection of information.

Keywords: information security, fuzzy sets, the level of protection, the likelihood of the threat.