УДК 004.056.5

Голобородько М.Ю., к.т.н., с.н.с.[1];
Курченко О.А., к.т.н., доцент[2];
Кирись О.С.[2]

[1] - Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського;
[2] - Державний університет телекомунікацій

Методи числової оцінки рівня захищеності інформації у сегменті корпоративної інформаційної системи

Резюме. У статті оцінюється рівень інформаційної безпеки підприємства. Використано ймовірносно-статичний підхід, при якому не враховується динаміка зміни значень ймовірностей загроз і уразливості інформації в часі. Оцінюються також апріорні очікувані значення ймовірності порушення захищеності інформації.

Ключові слова: інформаційна безпека, система захисту інформації, оцінювання рівня захищеності інформації.

Методы числовой оценки уровня защищенности информации в сегменте корпоративных информационной системы

Резюме. В статье оценивается уровень информационной безопасности предприятия. Используя вероятностно-статистический подход, при котором не учитывается динамика изменения значений вероятностей угроз и уязвимости информации во времени. Оцениваются также априорные ожидаемые значения вероятности нарушения защищенности информации.

Ключевые слова: информационная безопасность, система защиты информации, оценка уровня защищенности информации.

Methods numerical evaluation level security of information in the segment corporate information systems

Resume. This paper evaluated the level of enterprise information security using static probabilistic approach, which does not take into account the dynamics of changes in the values of the probability of threats and vulnerabilities in time. Evaluated as expected a priori probability of breach of information security.

Keywords: information security, information protection system, evaluation of information security.

Постановка проблеми. Для забезпечення ефективного функціонування підприємство має підтримувати належний ступінь інформаційної безпеки, необхідною умовою чого є систематичне проведення відповідної діагностики.

Аналіз останніх досліджень і публікацій. Багато вчених як в Україні, так і в країнах ближнього і далекого зарубіжжя займаються питаннями, пов'язаними із забезпеченням належного рівня інформаційної безпеки підприємств. Вагомий внесок щодо вирішення цієї проблеми зробили С. Ілляшенко, Т. Клєбанова, Д. Ковальов, О. Кравчук, Є. Олєйников, В. Пономарьов, Н. Реверчук та інші [1-5]. Проте, на думку більшості фахівців, ймовірносно-статичний підхід до оцінки рівня інформаційної безпеки підприємства ще не в достатній мірі розроблений.

Метою статті є синтез методу оцінки рівня захищеності інформації (ризику порушення інформаційної безпеки) в сегменті корпоративної інформаційної системи, який надасть змогу порівняння різних комплексів засобів захисту.

Виклад основного матеріалу дослідження. Оцінка рівня захищеності інформації здійснюється на основі вимог положень уніфікованої концепції захисту, а також обґрунтованого підходу до оцінки необхідного рівня захищеності при проектуванні та в процесі експлуатації системи захисту інформації (СЗІ) [1]. При цьому бажано використовувати кількісні показники рівня захищеності.

У процесі аналізу і оцінювання ризиків встановлюється ступінь адекватності засобів захисту (ЗЗ), що використовуються, існуючим

загрозам. Властивості "захищеність інформації" кожного ЗЗ, що входять до СЗІ, в сукупності визначає загальну захищеність інформації у СЗІ в цілому.[5] Наявність уразливості ЗЗ може призвести до порушення захищеності, тобто здійсненню загрози, тому при вирішенні завдань захисту інформації першорядне значення має кількісна оцінка уразливостей засобів захисту. Оскільки вплив на інформацію різних деструктивних факторів значною мірою є випадковим, то в якості кількісної міри уразливості найбільш доцільно застосувати ймовірність порушення захищеності інформації.

Визначення значень ймовірностей загроз і уразливостей є основною проблемою при отриманні кількісної оцінки ризику порушення інформаційної безпеки. Відомо, що застосування методів класичної теорії ймовірностей допустимо при повторюваності дослідів та однаковості умов. Ця вимога в складних системах, якими є СЗІ, зазвичай, не виконується. Відповідно до одного з принципів системного аналізу – принципу невизначеності – для дослідження системи необхідно врахувати певний перелік невизначеностей і випадковостей. Оскільки складні відкриті системи не підкоряються імовірнісним законам, в них слід оцінити найгірші ситуації, відповідно до методу гарантованого результату, який пропонується використовувати при оцінці ймовірностей загроз.

Приймається, що значення В якості показника захищеність інформації m-го ЗЗ приймається величина $P_{бт}$. Тут $P_{бт}$ – це суб'єктивна ймовірність виявлення і блокування засобом захисту несанкціонованих дій, тобто теоретична очікувана ефективність бар'єру.

Очевидно, що ймовірність порушення захищеності $P^n_{бт}$ доповнює $P_{бт}$ до одиниці, тобто

$$P^n_{бт} = 1 - P_{бт}, \qquad (1)$$

де $P^n_{бт}$ – ймовірність порушення захищеності інформації, або ймовірність уразливості m -го ЗЗ (ймовірність подолання бар'єру).

Пропонується ймовірносно-статичний підхід, при якому не враховується динаміка зміни значень ймовірностей загроз і уразливостей в часі та оцінюються апріорні очікувані значення ймовірностей порушення захищеності інформації.

Особливістю даного підходу є отримання чисельних значень суб'єктивних ймовірностей на основі використання як часткових показників захищеності технічних характеристик і можливостей засобів захисту, декларованих розробниками. Вирішується задача отримання чисельної оцінки узагальненого показника якості засобу захисту.

Для отримання чисельної оцінки узагальненого показника якості засобу захисту пропонується використовувати теорію нечітких множин. Для оцінки засобів захисту за кожним критерієм нижнього ієрархічного рівня формуються функції приналежності. При цьому використовуються методи побудови функцій приналежності, засновані на формалізації та інтеграції нечітких даних, сформованих експертом в процесі оцінювання параметрів реальних засобів захисту. Формулюються відповідні правила, що дозволяють обробляти складні з'єднання. Перевагою такого способу є відносно висока об'єктивність.

Даний метод оцінювання рівня захищеності інформації базується на трирубіжній моделі захисту, що розроблена для об'єкта захисту, архітектура якого відповідає основним рекомендованим принципам безпеки.

Відомо, що рівень захищеності і відносний ризик доповнюють один одного до одиниці. Пропонується розраховувати рівень захищеності η за формулою

$$\eta = 1 - \overline{R} = 1 - \sum_s \frac{C_s}{C_\Sigma} \cdot P_s, \qquad (2)$$

де $\overline{R}$ – відносний ризик;

C_s – частка вартості інформаційних ресурсів, які захищаються в сегменті s;

s – номер сегмента;

S – число сегментів;

*P*s – результуюча ймовірність загроз інформаційному середовищі сегмента;

C_Σ – сумарний неприйнятний збиток;

$\frac{C_s}{C_\Sigma}$ – коефіцієнт небезпеки сукупності загроз в s -му сегменті, який визначається як відношення частки вартості інформаційних ресурсів, які захищаються в сегменті s до сумарного неприйнятного збитку.

Оцінка рівня захищеності інформації здійснюється шляхом кількісної оцінки ймовірностей реалізації каналів несанкціонованого доступу.

Для оцінки ймовірності порушення захищеності підмножиною порушників $\{K'\}$ по підмножині можливих каналів несанкціонованого отримання інформації $\{J'\}$ для сегмента s використовується співвідношення

$$P_{S\{J'\}\{K'\}} = 1 - \prod_{J'} \left(1 - P^{(\text{бб})}_{sjk}\right) \prod_{K'} \left(1 - P^{(\text{бб})}_{sjk}\right), \qquad (3)$$

в якому приймається

$$P_{sjk}^{(б)зов} \subset P_{sjk}^{(б)}, P_{sjk}^{(б)вн} \subset P_{sjk}^{(б)},$$

де $P_{sjk}^{(б)вн}, P_{sjk}^{(б)зов}$ – вірогідність несанкціонованого отримання інформації, що обробляється в s-му сегменті, що має точки виходу в глобальну мережу, виділені канали зв'язку та для якого можливі віддалені атаки через периметр, відповідно, внутрішнім і зовнішнім порушником (зловмисником).

З урахуванням трирубіжної моделі захисту $P_{sjk}^{(б)зов}$ обчислюється за формулою [3]:

$$P_{sjk}^{(б)зов} = 1 - \prod_{l=1}^{3} (1 - P_{sjkl}^{зов}), \quad (4)$$

де $P_{sjkl}^{зов}$ – ймовірність несанкціонованого отримання зловмисником або зовнішнім порушником інформації, що обробляється в s-му сегменті, в разі подолання відповідного кордону захисту *l*.

Імовірність $P_{sjkl}^{зов}$ залежить від чотирьох факторів і визначається залежністю

$$P_{sjkl}^{зов} = P_{skl}^{д} \cdot P_{sjkl}^{н} \cdot P_{sjl}^{к} \cdot P_{sjl}^{и}, \quad (5)$$

де $P_{sjkl}^{зов}$ – імовірність спроби доступу зловмисника або зовнішнього порушника до *l-го* рубежу захисту;

$P_{sjkl}^{н}$ – ймовірність подолання зловмисником або зовнішнім порушником *l-го* рубежу захисту;

$P_{sjl}^{к}$ – ймовірність наявності трафіку з сегменту s через *l -й* рубіж захисту (залежить від технології обробки інформації на об'єкті захисту, ймовірність можна прийняти рівною частоті роботи каналу);

P_{sjl}^{I} – ймовірність наявності інформації *s -го* сегмента, яка має бути захищена, в трафіку в момент подолання зовнішнім порушником *l -го* рубежу захисту (залежить від технології обробки інформації на об'єкті захисту).

Внутрішній порушник у процесі реалізації каналів несанкціонованого доступу повинен подолати два рубежі захисту.

Тоді ймовірність несанкціонованого отримання інформації, що обробляється в сегменті s, внутрішнім порушником обчислюється за формулою:

$$P_{sj}^{(б)вн} = 1 - \prod_{l=1}^{2} (1 - P_{sjl}^{вн}), \quad (6)$$

де $P_{sl}^{вн}$ – ймовірність несанкціонованого доступу внутрішнім порушником до інформації, що обробляється в *s -му* сегменті, в разі подолання відповідного кордону захисту *l* .

З перерахованих ймовірностей, що входять до формули для розрахунку $P_{sjl}^{вн}$ і $P_{sjkl}^{зов}$, одна з ймовірностей, а саме $P_{sjkl}^{н}$, залежить від якості використовуваних в системі засобів захисту та кількості бар'єрів на рубежі захисту. Якщо порушнику необхідно подолати *M* бар'єрів на рубежі захисту, то ймовірність його вдалої атаки визначається як добуток:

$$P_{sjkl}^{n} = \prod_{m=1}^{M} P_{бm}^{n} = \prod_{m=1}^{M} (1 - P_{бm}) \quad (7)$$

Варто зазначити, що для отримання інформації, необхідної для розрахунку наведених показників, обов'язковою умовою є наявність системи моніторингу діяльності інформаційної служби підприємства.

Висновок.. Запропоновано метод оцінки рівня захищеності інформації (ризику порушення інформаційної безпеки), в якому ймовірності уразливостей оцінюються з використанням механізму нечіткого логічного висновку на основі даних про технічні характеристики засобів захисту. Адекватність методу не залежить від наявності або відсутності достовірних статистичних даних по інцидентах інформаційної безпеки, що дозволяє забезпечити застосовність методу на стадіях розробки та експлуатації СЗІ, порівняти різні комплекси засобів захисту в кількісному вираженні.

СПИСОК ЛІТЕРАТУРИ.

1. Ілляшенко, С.М. Економічний ризик [Текст]: навч. посіб. 2-ге вид., доп., перероб. / С.М. Ілляшенко – К.: Центр навчальної літератури,2004. – 220с.
2. Поспелов Д.А. Нечеткие множества в моделях управления и искусственного интеллекта. -М. :Наука, 1986-312с.
3. Курило А.П., Зефиров С.Л., Голованов В.Б - Аудит информационной безопасности. - БДЦ-Пресс, 2006- 103с.
4. Разработка метода и функциональной модели численной оценки риска нарушения информационной безопасности и уровня защищенности информации на основе вероятностно-статического подхода / И.В. Машкина, С.Н. Алекса // Известия Южного федерального университета. Технические науки. Ростов, 2008. № 8. С. 47 – 54.
5. Системный подход к анализу уровня защищенности в системах защиты информации / И.В. Машкина, М.Б. Гузаиров // Безопасность информационных технологий. М. : МИФИ, 2007. №3. С. 58 – 64.