6. Новиков, Д. А. Теория управления организационными системами [Текст] / Д. А. Новиков. — М.: МПСИ, 2005. — 584 с.
7. Цыпкин, Я. З. Частотные критерии робастной модальной линейных дискретных систем [Текст] / Я. З. Цыпкин, Б. Т. Поляк // Автоматика. — 1990. — № 5. — С. 4–11.
8. Мирошник, И. В. Нелинейное и адаптивное управление сложными динамическими системами [Текст] / И. В. Мирошник, В. О. Никифоров, А. Л. Фрадков. — СПб.: Наука, 2000. — 549 с.
9. Цыпкин, Я. З. Робастная устойчивость нелинейных дискретных систем при параметрической неопределенности [Текст] / Я. З. Цыпкин // Автоматика. — 1992. — № 4. — С. 3–9.
10. Левин, В. И. Интервальная математика и изучение неопределенных систем [Текст] / В. И. Левин // Информационные технологии. — 1998. — № 6. — С. 27–33.
11. Трахтенгерц, Э. А. Субъективность в стратегическом управлении [Текст] / Э. А. Трахтенгерц; под ред. Н. А. Абрамовой, К. С. Гинсберга, Д. А. Новикова // Человеческий фактор в управлении. — М.: КомКнига, 2006. — С. 408–438.

КЛАССИФИКАЦИЯ НЕОПРЕДЕЛЕННОСТЕЙ В УПРАВЛЕНИИ ОРГАНИЗАЦИОННО-ТЕХНОЛОГИЧЕСКИМИ ОБЪЕКТАМИ

Представлена классификация неопределенностей по разным признакам. Учитывая, что неопределенность порождает риск, предложенная классификация неопределенностей предоставит возможности определения и классификации рисков в процессе принятия управленческого решения в системах управления сложными организационно-технологическими объектами в различных отраслях промышленности, таких как пищевая, химическая, нефтеперерабатывающая.

Ключевые слова: неопределенность, риск, классификация, стратегическое управление, принятие решения.

Прокопенко Тетяна Олександрівна, *кандидат технічних наук, доцент, кафедра економічної кібернетики і маркетингу, Черкаський державний технологічний університет, Україна,* ***e-mail: tatianaalexandr@yandex.ru****.*

Прокопенко Татьяна Александровна, *кандидат технических наук, доцент, кафедра экономической кибернетики и маркетинга, Черкасский государственный технологический университет, Украина.*

Prokopenko Tatiana, *Cherkasy State Technological University, Ukraine,* ***e-mail: tatianaalexandr@yandex.ru***

УДК 004.58
DOI: 10.15587/2312-8372.2014.31870

Козловський В. В.,
Міщенко А. В.,
Сніжко В. В.

АЛГОРИТМ АНАЛІЗУ ТА УПРАВЛІННЯ КОМПЛЕКСНОЮ БЕЗПЕКОЮ НА ОСНОВІ КОГНІТИВНОГО МОДЕЛЮВАННЯ

В статті представлено алгоритм аналізу та управління комплексною безпекою, котрий був розроблений із застосуванням нечіткого когнітивного моделювання. Даний алгоритм дозволяє уніфікувати підходи до управління комплексною безпекою і приступити до розробки відповідних обчислювальних процедур і модулів, які можуть бути надалі використані при побудові систем захисту інформації.

Ключові слова: *інформаційна безпека, комплексна безпека, когнітивне моделювання, інформаційна система.*

1. Вступ

Вирішення питань забезпечення інформаційної безпеки та управління захистом інформації сьогодні стає життєво необхідним для існування і розвитку будь-якої сучасної організації.

Безпека — поняття комплексне і не може розглядатися як проста сума її складових частин. Ці частини взаємопов'язані і взаємозалежні [1]. Крім того, кожна частина критично значима. Отже, ніякі методи, які передбачають часткове ігнорування критеріїв безпеки (нехай і неявне) при комплексній оцінці безпеки неприйнятні. Тому розробка алгоритму, що дозволяє уніфікувати підходи до управління комплексною безпекою системи є актуальним завданням.

2. Аналіз літературних даних і постановка проблеми

Під безпекою розуміється стан і тенденції розвитку захищеності життєво важливих елементів системи від зовнішніх і внутрішніх негативних факторів. При цьому необхідно врахувати, що безпека — динамічна категорія, що має множинну предметність [2]. Діяльність щодо безпеки виникає в ході вирішення протиріччя між небезпекою і потребою управляти безпекою: передбачувати, запобігати, локалізовувати і усувати збитки від впливу загроз [3]. Комплексна оцінка рівня безпеки (КОРБ) не може бути більшою мінімальної оцінки, отриманої для різних аспектів системи [4].

Безпека не існує сама по собі, поза людським впливом. Вона забезпечується для людини і нею ж оцінюється. Тому, поняття безпеки має не тільки об'єктивну, але й суб'єктивну сторону, оскільки оцінка її рівня проводиться в кінцевому підсумку людиною [5]. Специфічними особливостями задачі створення систем захисту є [6]:

— неповнота вихідної інформації про склад і характер загроз;

— багатокритеріальність задачі, пов'язана з необхідністю врахування великої кількості локальних показників;

— наявність як кількісних, так і якісних показників, які необхідно враховувати при вирішенні завдань розробки та впровадження систем захисту;

— неможливість застосування класичних методів оптимізації [7].

Когнітивний аналіз об'єкта дослідження дозволяє [8]:

— прогнозувати напрямки розвитку системи (ситуації);

— виявити фактори, що впливають на розвиток ситуації;

— формалізувати процеси прийняття рішень;

— отримати як якісні, так і кількісні характеристики ситуації;

Оцінка інформаційних ризиків, котра базується на нечіткому когнітивному моделюванні дозволяє [9]:

— виявити найбільш небезпечні загрози та вразливості, що впливають на інформаційну систему;

— оцінити можливий збиток від дії загроз на інформаційну систему;

— адаптуватися до нових зовнішніх і внутрішніх загроз та технологій;

— дати ефективний і простий механізм прийняття рішень для служб, що займаються забезпеченням інформаційної безпеки.

Розробка алгоритму, який дозволить уніфікувати підходи до управління комплексною безпекою дозволить вирішити ряд питань пов'язаних з суб'єктивною стороною при аналізі та управлінні комплексною безпекою [10].

3. Мета та задачі дослідження

Мета дослідження — розробити алгоритм аналізу та управління комплексною безпекою, використовуючи когнітивний підхід.

Для досягнення поставленої мети необхідно:

1. Сформувати матрицю, котрою можна охарактеризувати рівень комплексної безпеки.
2. Сформувати матрицю превентивних заходів.
3. Сформувати матрицю, за допомогою якої буде формалізована реалізація превентивних заходів.
4. Представити оцінку комплексної безпеки системи у вигляді нечіткої когнітивної моделі.

4. Розробка алгоритму аналізу і управління комплексною безпекою

Сформулюємо математичну модель, що описує динаміку зміни рівня комплексної безпекою різних систем.

Назвемо рівнем комплексної безпеки системи (РКБС) оцінку, засновану на наборі показників і критеріїв, що характеризують стан системи в плані захищеності критичних для неї елементів.

Рівень комплексної безпеки системи можна охарактеризувати такою матрицею (матриця безпеки):

$$B=\begin{pmatrix} K_1 & F_1 & V_1 & T_1 & S_1 \\ K_2 & F_2 & V_2 & T_2 & S_2 \\ K_3 & F_3 & V_3 & T_3 & S_3 \\ -- & -- & -- & -- & -- \\ K_n & F_n & V_n & T_n & S_n \end{pmatrix},$$

де K_i — показник рівня безпеки по i -му критерію; F_i — тенденція змін i -го критерію (зростає, спадає, нейтральний); V_i — швидкість змін i -го критерію (наприклад: низька, нижче середнього, середня, вище середнього, висока); T_i — характерний для i -го критерію час, котрий дозволяє правильно інтерпретувати значення параметру V_i; S_i — степінь критичності негативних наслідків при реалізації ризиків, що погіршують значення i -го критерію.

Перший і четвертий стовпчик МБ характеризують поточний стан комплексної безпеки. Інші стовпці матриці відображають динаміку розвитку процесів і дозволяють будувати прогноз розвитку на майбутнє.

Необхідно проаналізувати основні загрози безпеці інформаційної системи, їх можна розділити на дві категорії: первинні і вторинні.

Ймовірності виникнення первинних загроз від нас не залежать. Однак сукупність превентивних заходів захисту дозволяє послабити вплив первинних загроз на рівень безпеки системи [11]. Цей факт може бути описаний за допомогою матриці превентивних заходів (МПЗ):

$$Z_j=\begin{pmatrix} z_{11} & z_{12} & z_{13} & z_{14} & z_{15} \\ z_{21} & z_{22} & z_{23} & z_{24} & z_{25} \\ -- & -- & -- & -- & -- \\ z_{n1} & z_{n2} & z_{n3} & z_{n4} & z_{n5} \end{pmatrix},$$

де $j=1,...,M$, де M — загальна кількість превентивних заходів.

Якщо все ж, незважаючи на превентивні заходи захисту, реалізація певної множини первинних загроз призвела до виникнення наслідків, то необхідно вжити заходів для їх локалізації та усунення.

Реалізація цих заходів може бути формалізована за допомогою матриці ліквідації наслідків (МЛН):

$$L=\begin{pmatrix} l_{11} & l_{12} & l_{13} & l_{14} & l_{15} \\ l_{21} & l_{22} & l_{23} & l_{24} & l_{25} \\ -- & -- & -- & -- & -- \\ l_{n1} & l_{n2} & l_{n3} & l_{n4} & l_{n5} \end{pmatrix}.$$

З первинними загрозами ми починаємо боротися ще до їх настання. У випадку з вторинними загрозами ми повинні не допустити їх, тобто і боротися з причинами, котрі їх викликають. Це принципова відмінність в блоках заходів, вплив яких формалізовано множиною матриць Z_j і матрицею L.

При побудові нечіткої когнітивної моделі (НКМ) об'єкт дослідження представляють у вигляді знакового орієнтованого графа [12]. В якості такої моделі при оцінці комплексної безпеки системи (КБС) може бути прийнятий:

$$KBS=<G, QL, E>,$$

де G — орієнтований граф, що має одну кореневу вершину і не містить петель і горизонтальних ребер в межах одного рівня ієрархії:

$$G=<\{GF_i\};\{GD_{ij}\}>,$$

де $\{GF_i\}$ — множина вершин графа (факторів або концептів в термінології НКМ); $\{GD_{ij}\}$ — множина дуг, що

з'єднують i -у і j -у вершини (множина причинно-наслідкових зв'язків між концептами; при цьому дуги розташовані так, що початку дуги відповідає вершина нижнього рівня ієрархії (рангу), а закінченню дуги — вершина рангу, на одиницю меншого); $GF_0 = K$ — коренева вершина, що відповідає рівню комплексної безпеки в цілому (інтегральному критерію безпеки — цільовому концепту); QL — набір якісних оцінок рівнів кожного фактору в ієрархії; E — система відношень переваги одних факторів над іншими за ступенем їх впливу на заданий елемент.

Загальний алгоритм аналізу та управління комплексною безпекою на основі нечіткого когнітивного моделювання можна представити в наступному вигляді:

1. Збір інформації про об'єкт захисту: ідентифікація активів і встановлення початкового рівня безпеки. У процесі ідентифікації слід розглянути основні характеристики активів: інформаційну цінність, чутливість активів до загроз, наявність захисних заходів. При цьому необхідно врахувати, що в числі факторів, що впливають на безпеку, особливе місце займають суб'єктивні фактори, які є найменш прогнозованими.

2. Вибір критеріїв, що характеризують стан різних сторін забезпечення безпеки, визначення їх прийнятного рівня.

3. Побудова когнітивної моделі у вигляді знакового-орієнтованого графа.

4. Розрахунок і аналіз рівня комплексної безпеки системи (РКБС).

5. Якщо РКБС не знаходиться в прийнятному діапазоні значень, то виробляються зміни у складі концептів, що беруть участь у побудові когнітивної моделі, у складі зв'язків між концептами, змінюються їх значення за допомогою введення захисних заходів.

Таким чином, процес забезпечення безпеки системи передбачає вирішення двох взаємопов'язаних завдань: пряма задача (аналіз стану системи) і оберненої задачі управління (вплив на систему).

При вирішенні першого завдання потрібно визначити значення критеріїв безпеки K_i та інтегрального критерію K при заданих значеннях всіх концептів, котрі впливають на них.

Якщо отримані значення знаходяться поза діапазоном прийнятності, то при вирішенні оберненої задачі необхідно підібрати такі керуючі впливи Z_j та L, які забезпечать повернення цільових критеріїв у безпечний діапазон.

Якщо існує не єдиний набір необхідних управляючих впливів, то на цьому етапі може виникнути задача оптимізації, що складається в знаходженні такої комбінації Z_j і L, яка забезпечує максимальний вплив на негативні фактори при заданих або мінімальних витратах на реалізацію способів і засобів захисту.

5. Висновки

У результаті проведених досліджень:

1. Сформовано матрицю безпеки, у котрій виділено показники рівня безпеки, тенденцію та швидкість змін, а також ступінь критичності негативних наслідків.

2. Визначено сукупність превентивних заходів захисту, що дозволяє послабити вплив первинних загроз на рівень безпеки системи.

3. Формалізована реалізація превентивних заходів за допомогою матриці ліквідації наслідків.

4. Розроблено алгоритм аналізу та управління комплексною безпекою системи.

Управління інформаційною безпекою значно спрощується і формалізується при використанні нечіткого когнітивного моделювання. Використання даного підходу сприяє вирішенню проблем, пов'язаних з суб'єктивною стороною в процесах аналізу інформаційних ризиків і загроз безпеці. Розроблений алгоритм дозволяє уніфікувати підходи до управління комплексною безпекою і приступити до розробки відповідних обчислювальних процедур і модулів, які можуть бути в подальшому використані при побудові систем захисту інформації.

Література

1. Гайдамакин, Н. А. Разграничение доступа к информации в компьютерных системах [Текст] / Н. А. Гайдамакин. — Э.: Урал, 2003. — 328 с.
2. Зегжда, Д. П. Основы безопасности информационных систем [Текст] / Д. П. Зегжда, А. М. Ивашко. — М.: Телеком, 2000. — 286 с.
3. Девянин, П. Н. Модели безопасности компьютерных систем [Текст] / П. Н. Девянин. — М.: Академия, 2005. — 144 с.
4. Корт, С. С. Теоретические основы защиты информации [Текст]: учеб. пособие / С. С. Корт. — М.: Гелиос, 2004. — 240 с.
5. Курило, А. П. Аудит информационной безопасности [Текст] / А. П. Курило, С. Л. Зефирова, В. Б. Голованов. — М.: БДЦ-пресс, 2006. — 304 с.
6. Садердинов, А. А. Информационная безопасность [Текст]: учеб. пособие / А. А. Сардердинов, В. А. Трайнев, А. А. Федулов. — М.: Дашковка, 2005. — 336 с.
7. Петренко, С. А. Управление информационными рисками. Экономически оправдана безопасность [Текст] / С. А. Петренко, С. В. Симонов. — М.: Пресс, 2005. — 384 с.
8. Борисов, В. В. Нечеткие модели и сети [Текст] / В. В. Борисов, В. В. Круглов, А. С. Федулов. — М.: Телеком, 2007. — 284 с.
9. Райков, А. Н. Интеллектуальные информационные технологии [Текст]: учеб. пособие / А. Н. Райков. — М.: МГИРЕА (ТУ), 2000. — 96 с.
10. Васильев, В. И. Анализ и управление информационной безопасностью вузов на основе когнитивного моделирования [Текст] / В. И. Васильев, Г. Т. Кудрявцева // Системы управления и информационные технологии. — 2007. — № 1, Т. 27. — С. 74–81.
11. Ажмухамедов, И. М. Управление информационной безопасностью региона на основе когнитивного моделирования [Текст] / И. М. Ажмухамедов // Вестник АГТУ. — 2010. — № 1. — С. 96–102.
12. Ажмухамедов, И. М. Моделирование на основе экспертных суждений процесса оценки информационной безопасности [Текст] / И. М. Ажмухамедов // Вестник АГТУ. — 2009. — № 2. — С. 101–109.

АЛГОРИТМ АНАЛИЗА И УПРАВЛЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТЬЮ НА ОСНОВЕ КОГНИТИВНОГО МОДЕЛИРОВАНИЯ

В статье представлен алгоритм анализа и управления комплексной безопасностью, который был разработан с применением нечеткого когнитивного моделирования. Данный алгоритм позволяет унифицировать подходы к управлению комплексной безопасностью и приступить к разработке соответствующих вычислительных процедур и модулей, которые могут быть в дальнейшем использованы при построении систем защиты информации.

Ключевые слова: информационная безопасность, комплексная безопасность, когнитивное моделирование, информационная система.

Козловський Валерій Валерійович, *доктор технічних наук, професор, завідувач кафедри систем захисту інформації, Національний авіаційний університет, Київ, Україна,* ***e-mail: vvk@zeos.net****.*
Міщенко Андрій Віталійович, *кандидат технічних наук, професор кафедри систем захисту інформації, Національний авіаційний університет, Київ, Україна,* ***e-mail: vvk@zeos.net****.*
Сніжко В'ячеслав Володимирович, *аспірант, кафедра систем захисту інформації, Національний авіаційний університет, Київ, Україна,* ***e-mail: bb_c@ukr.net****.*

 ISSN 2226-3780

Козловский Валерий Валериевич, *доктор технических наук, профессор, заведующий кафедрой систем защиты информации, Национальный авиационный университет, Киев, Украина.*
Мищенко Андрей Витальевич, *кандидат технических наук, профессор кафедры систем защиты информации, Национальный авиационный университет, Киев, Украина.*
Снижко Вячеслав Владимирович, *аспирант, кафедра систем защиты информации, Национальный авиационный университет, Киев, Украина.*

Kozlovskyi Valerii, *National Aviation University, Kyiv, Ukraine,* ***e-mail: vvk@zeos.net****.*
Mishchenko Andrii, *National Aviation University, Kyiv, Ukraine,* ***e-mail: vvk@zeos.net****.*
Snizhko Viacheslav, *National Aviation University, Kyiv, Ukraine,* ***e-mail: bb_c@ukr.net***

УДК 519.86:519.612
DOI: 10.15587/2312-8372.2014.31877

Зарубенко О. О.

ПОБУДОВА АЛГОРИТМУ АНАЛІЗУ РУКОПИСНОГО ТЕКСТУ

Проведено загальний аналіз роботи двох підходів розпізнавання рукописного тексту та на базі аналізу створено два відповідних алгоритми для отримання вірного результату на основі оффлайнового методу аналіза тексту. Наведено результативність розпізнавання даного типу тексту на поточний момент. Представлено загальний висновок по роботі двох алгоритмів.

Ключові слова: *рукописний текст, online метод, offline метод, розпізнання рукописного тексту, IRC.*

1. Вступ

При оформленні анкет, документів та інших ділових паперів в різних компаніях в основному використовується макет документу, в який заповнювач вносить потрібні дані вручну (рукописним/рукодрукованим текстом). Для ефективного використання цієї інформації дані потрібно занести до бази даних. Це можна зробити двома способами: або вручну користувачем, або автоматично програмою. Швидкість роботи користувача по занесенню даних залежить від його кваліфікації у роботі з базами даних, швидкості набору, можливості проаналізувати (розпізнати) написане заповнювачем, що свідчить про залежність більше від атрибутів користувача, ніж від можливостей програмного забезпечення. А при роботі з системою автоматичного розпізнання тексту і його аналізу, користувачеві потрібно лише сканувати потрібний документ і звіряти вихідні дані з даними на документі, коригуючи їх при необхідності.

На поточний момент найбільш актуальною можна вважати проблему розпізнавання рукописного тексту. Для таких текстів досягнута точність розпізнавання суттєво нижча, ніж для рукодрукованого тексту. Більш високі показники можуть бути досягнуті тільки з використанням контекстної та граматичної інформації. Наприклад, в процесі розпізнання шукати цілі слова в словнику легше, ніж намагатися проаналізувати окремі символи з тексту. Знання граматики мови може також допомогти визначити, чи є слово дієсловом або іменником. Форми окремих рукописних символів іноді можуть не містити достатньо інформації, щоб точно (більше 98 %) розпізнати весь рукописний текст. Це відбувається, тому що люди мають різний почерк, що навіть для людини він іноді є складним для розпізнанні (наприклад, почерк лікарів в рецептах та медичних книжках).

Точність роботи методів може бути виміряна кількома способами і тому може сильно варіюватися. Приміром, якщо зустрічається спеціалізоване слово «бетономішалка», яке не використовується для відповідного програмного забезпечення медичного закладу, при пошуку неіснуючих слів, помилка може збільшитися.

2. Аналіз літературних даних і постановка проблеми

На даний час поточним станом технологій розпізнання оптичного тексту є доволі точне розпізнавання символів у друкованому тексті (майже 100 %), у рукодрукованому (80–90 %), у рукописному (60–70 %) при чіткому зображенні, отриманому, наприклад, за допомогою сканування документів. Точність розпізнавання зображення останнього дуже низька, оскільки почерк індивідуальний для кожної людини і технологія начала досліджуватися в XXI віці [1–9]. Якість розпізнавання такого зображення може бути підвищенна тільки шляхом подальшого редагування людиною або внесення строгих форм заповнення тексту. Тобто загальна точність розпізнання відсканованого зображення буде варіюватися від 70 до 80 %, що не є добре адже ми будемо мати з десяток помилок на сторінці. Тобто така технологія може бути корисна лише у дуже обмеженому числі додатків.

Розпізнавання символів online іноді плутають з оптичним розпізнаванням символів. Але таке розпізнання часто залежить від зчитування руху курсора по екрану, де програма аналізує рух і виводить символ. Наприклад, у засобах online розпізнавання, розроблених для OS PenPoint та планшетного ПК (на даний час — для системи Android) для більш зручного вводу інформації за допомогою стілуса, можна визначити, з якого боку пишеться рядок: справа наліво або зліва направо. *Offline метод* — працює зі статичної формою подання тексту [10, 11].

Online системи для розпізнавання рукописного тексту останнім часом стали широко відомі в якості комерційних