

## Фактори захисту інформаційної безпеки авіатранспортного комплексу

УДК 004.398.75

Дмитро Чирва, Дмитро Волокітін,  
Іван Басюк, Світлана Ковтун<sup>1</sup>,  
Тетяна Приходько

*Національний авіаційний університет, <sup>1</sup>svt.kovtun@gmail.com*

Цілий ряд взаємопов'язаних між собою причин може призвести до порушення безпеки функціонування інформаційної системи авіатранспортного комплексу. У випадку дійсної реалізації потенційних загроз і, як наслідок, виникнення деструктивних процесів системам інформаційної безпеки завдається руйнівний вплив. В результаті функціонування інформаційної системи порушується та пошкоджуються основні сервіси безпеки: конфіденційність, цілісність, доступність, що може призвести до негативних наслідків. Опираючись на класифікацію ступенів пошкодження безпеки інформаційної системи в авіатранспортному комплексі, необхідно виробити обґрунтовані рекомендації щодо застосування заходів, спрямованих на ліквідацію наслідків зниження безпеки інформаційної системи.

За допомогою моделей нечітких даних (когнітивних моделей) можна вирішити досить широке коло завдань, пов'язаних з прогнозуванням і підтримкою прийняття рішень та створенням реальних моделей погано формалізованих процесів. Можливість формалізації чисельно невимірних факторів та можливість використання нечіткої, суперечливої інформації є найбільшою перевагою даних моделей над іншими.

Щоб побудувати когнітивну модель нечітких множин, об'єкт дослідження зазвичай представляють у вигляді орієнтованого графа. В якості такої моделі при оцінці комплексної безпеки системи (KBS) може бути прийнятий кортеж:

$$KBS = \langle G, QL, E \rangle \quad (1)$$

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

$$G = \langle \{GF\}; \{GD_j\} \rangle \quad (2)$$

де  $\{GF\}$  – безліч вершин графа (факторів або концептів в термінології НКМ);  $\{GD_j\}$  – безліч дуг, що з'єднують  $i$ -ую і  $j$ -ую вершини (безліч причинно-наслідкових зв'язків між концептами; при цьому дуги розташовані так, що початку дуги відповідає вершина нижнього рівня ієрархії (рангу), а кінця дуги – вершина рангу, на одиницю меншого);  $GF_0 = K$  – коренева вершина, що відповідає рівню комплексної безпеки в цілому (інтегральним критерієм безпеки – цільовим концепту);  $QL$  – набір якісних оцінок рівнів кожного фактору в ієрархії;  $E$  – система відносин переваги одних факторів іншим за ступенем їх впливу на заданий елемент наступного рівня ієрархії. Така система, як було показано вище, дозволяє визначити узагальнені на випадок уподобання/байдужості факторів по відношенню один до одного ваги

Фішберна для кожної дуги  $GD_j$ . Ваги Фішберна відображають той факт, що системі спадної уподобання  $N$  альтернатив найкращим чином відповідає система, що знижується за правилом арифметичної прогресії ваг. Тому ці ваги представляють собою раціональні дробу, в знаменнику яких стоїть сума  $N$  перших членів натурального ряду (арифметичної прогресії з кроком 1), а в чисельнику – убутий на одиницю елементи натурального ряду, від  $N$  до 1 (наприклад,  $3/6, 2/6, 1/6$ ). Таким чином, перевага по Фішберну виражається в убуванні на одиницю чисельника раціональної дробу вагового коефіцієнта слабшої альтернативи. Стан системи з точки зору безпеки можна охарактеризувати матрицею  $B$ , рядки якої складаються з елементів  $(K_i, F_i, V_i, T_i, S)$ , де  $K_i$  в довільний момент часу  $t$  може бути знайдено за формулою:  $K(t) = K_i(0) + F^* V_i(t/T_i)$  (3).

Показники міри критичності негативних наслідків  $S_i$  фактично являють собою ваги, з якими приватні критерії безпеки  $K_i$  впливають на комплексний показник безпеки системи в цілому, який, як було показано вище, може бути знайдений в результаті мультиплікативної згортки приватних критеріїв  $K_i$ .

Узагальнений приклад графа для комплексної оцінки безпеки інформаційної системи представлений на рис.2. Через  $Z\{1,2,3,\dots\}$  позначені превентивні заходи захисту (механізми забезпечення безпеки), покликані зменшити уразливості інформаційної системи авіатранспортного Узагальнений приклад графа для комплексної оцінки безпеки інформаційної системи представлений на рис.2. Через  $Z\{1,2,3,\dots\}$  позначені превентивні заходи захисту (механізми забезпечення безпеки), покликані зменшити уразливості інформаційної системи авіатранспортного комплексу  $UZ\{1,2,3,\dots\}$ ,  $UG\{1,2,3,\dots\}$  – загрози безпеці системи,  $K\{1,2,3,\dots\}$  – приватні показники рівня безпеки за відповідним критерієм,  $K$  – комплексний (інтегральний) показник безпеки інформаційної системи авіатранспортного комплексу.

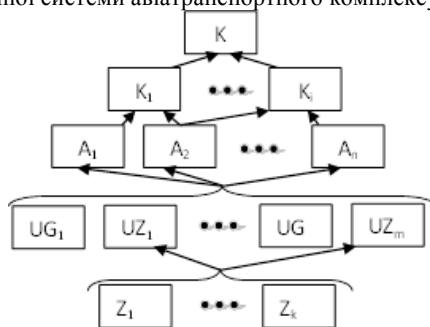


Рис.1. Вплив факторів захисту на інформаційну безпеку авіатранспортного комплексу

Потрібно сказати, що даний зв'язний граф не є деревом, оскільки не виконується вимога відсутності простих циклів. Це обумовлено тим, що чинники, які перебувають на нижньому рівні ієрархії, можуть одночасно впливати на кілька факторів більш високого рівня. Наприклад, застосування превентивних заходів захисту від однієї уразливості може одночасно усунути і яку-небудь іншу або привести до появи нової уразливості. Деякі атаки можуть викликати зміну відразу декількох приватних критеріїв безпеки (іноді в протилежному напрямку).

Таким чином можна зробити наступні основні висновки:

1. Інформаційна безпека авіатранспортного комплексу – поняття комплексне і не може розглядатися як проста сума складових її частин. Ці частини взаємозв'язані і взаємозалежні, кожна частина критично значима.
2. Оцінка рівня безпеки завжди відносна. Спроби безпосередньо приписати цій оцінці чисельне значення в більшості випадків безперспективні в плані подальшої інтерпретації результатів.
3. Для оцінки рівня комплексної безпеки інформаційної системи авіатранспортного комплексу доцільно використовувати приведену когнітивну модель.

*Науковий керівник – д.т.н., професор Козловський В.В.*