УДК 621.392

О.Г. Пузиренко

Генеральний штаб Збройних Сил України, Київ

МАТЕМАТИЧНА МОДЕЛЬ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Представлено математичну модель визначення відносного показника загроз інформаційній безпеці держави, на основі методу експертних оцінок. В роботі розглядаються джерела загроз у інформаційно-телекомунікаційних системах спеціального призначення на основі яких визначаються основні показники, що критично впливають на інформаційну безпеку держави. Запропонований підхід до якісних оцінок комплексних інформаційних загроз дозволяє практично оцінювати стан інформаційної безпеки за кожною сферою національної безпеки.

***Ключові слова**: захист інформації, інформаційно-телекомунікаційні системи, загрози інформаційної безпеки.*

Вступ

Постановка проблеми в загальному вигляді. Анализ останніх досліджень і публікацій. На етапі розвитку Збройних Сил України, під час побудови сучасної системи управління Збройних Сил України, захист від загроз інформаційної безпеки в інформаційно-телекомунікаційних системах спеціального призначення набуває важливого значення.

Інформаційно-телекомунікаційні системи спеціального призначення являють собою комплекс інформаційних та телекомунікаційних засобів, призначених для обробки та обміну усіма видами інформації, яка циркулює безпосередньо у Збройних Силах України.

Звичайно, виникають питання захисту інформації в інформаційно-телекомунікаційних системах спеціального призначення від загроз інформаційної безпеки.

Насамперед, в загальному контексті, загрози інформаційної безпеки – сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері.

Сучасні системи управління створюються і функціонують за безпосередньою допомогою інформаційно-телекомунікаційних засобів і технологій. Протиправні дії в комп'ютерно-телекомунікаційному середовищі вже сьогодні реально загрожують національній безпеці держави, оскільки можуть порушити керування державними та військовими структурами.

До основних чинників, [1] що формують джерела загроз у інформаційно-телекомунікаційних системах спеціального призначення, відносяться:

– соціально-економічні:

низький рівень комп'ютерної культури персоналу, який безпосередньо обслуговував інформаційно-телекомунікаційні системи, за достатньої кваліфікації вітчизняних комп'ютерних злочинців, що здійснюють несанкціоноване втручання в комп'ютерні мережі;

відсутність у широкого загалу фінансових можливостей для придбання ліцензованого програмного забезпечення;

недостатня увага з боку держави до проблем інформатизації, незважаючи на потенційну економічну рентабельність національного сегменту Інтернету;

– організаційно-правові:

відставання вітчизняного законодавства в інформаційної галузі від розвинутих країн в умовах спільного існування в єдиному інформаційному просторі;

порушення прав інтелектуальної власності щодо вітчизняних інформаційних технологій і засобів їхнього захисту від несанкціонованого доступу;

посилення можливостей для негативного інформаційного впливу на людину, суспільство і державу за допомогою нових комп'ютерно-телекомунікаційних засобів і технологій, що постійно розвиваються і поширюються;

– технологічні:

можливість перехоплення електронної пошти, паролів і файлів за допомогою легкодоступних для зацікавлених користувачів програмно-технічних засобів;

відсутність ефективної політики безпеки комп'ютерних мереж і необхідних програмно-технічних засобів для обмеження доступу до конфіденційної інформації в базах даних та ін.;

Тому передувати впровадженню механізмів захисту має класифікація та оцінка загроз інформаційної безпеки в інформаційно-телекомунікаційних системах спеціального призначення. **Метою даної роботи** є побудова математичної моделі загроз інформаційної безпеки, їх оцінка та аналіз.

Основна частина

Існують наступні головні причини й передумови для виникнення і реалізації загроз у вітчизняної інформаційно-телекомунікаційної сфері:

– діючи та створювані в системі управління Збройними Силами України бази даних (адміністративного, фінансового, кадрового та іншого характеру), які не мають належного нормативно-правового забезпечення й не відповідають вимогам інформаційної безпеки;

– відсутня державна система засекречування, кодування та шифрування інформації в комп'ютерно-інформаційному середовищі;

– в інформаційно-телекомунікаційних системах широко використовуються закордонні програмно-технічні засоби, в основному застарілих версій і не завжди ліцензовані, що особливо небезпечно для систем управління;

– законодавчо не визначені функції моніторингу та регулювання українського сегменту Інтернету, що перешкоджає ефективному виявленню, попередженню, локалізації та нейтралізації комп'ютерної злочинності.

У цих умовах зростають можливості для порушення конфіденційності, цілісності й доступності інформації в інформаційно-телекомунікаційних системах.

Таким чином, класифікувати інформаційно-телекомунікаційні загрози можна за наступними ознаками [2]:

а) за джерелами:

антропогенні: несанкціоновані дії зовнішніх користувачів, у т.ч. розвідувальних та інших спецслужб, кримінальних структур, недобросовісних партнерів і конкурентів; ненавмисні або навмисні дії обслуговуючого і адміністративного персоналу, програмістів, внутрішніх користувачів, у т.ч. служб інформаційної безпеки;

техногенні: неякісні програмно-технічні засоби, а також засоби зв'язку і сигналізації; мережі енергопостачання і транспортування, що можуть призвести до зникнення або коливання електроживлення, та, як наслідок, до відмов і збоїв програмно-технічних засобів, а також до електромагнітних опромінювань і наводок, витоку інформації через канали зв'язку;

природні: магнітні, електромагнітні, радіоактивні та інші впливи; руйнівні стихійні явища.

б) за об'єктами:

збір даних;
передача даних;
накопичення даних;
обробка даних;
форматування даних;
пошук даних;
надання даних.

в) за засобами:

втручання людини: несанкціонований доступ до пристроїв зберігання, обробки та передачі інформації; крадіжка інформаційних носіїв, псування програмно-технічних засобів і т.д.;

апаратно-технічне втручання: порушення цілісності інформації за допомогою електромагнітного опромінювання комп'ютерного обладнання; радіоелектронне заглушення каналів передачі інформації;

інформаційно-програмне втручання: використання завантажувальних, файлових і заражуючих вірусів; введення програмних закладок для отримання, модифікації чи знищення інформації та ін.;

г) за методами:

порушення конфіденційності інформації: перехоплення конфіденційної інформації з каналів зв'язку за допомогою електронних засобів; вплив на парольно-ключові засоби захисту в системах обробки та передачі інформації, в тому числі крадіжка програмних чи апаратних ключів або засобів криптографічного захисту;

порушення цілісності інформації: навмисне змінювання інформації, що зберігається в комп'ютерної системі чи передається від однієї системи до іншої; втрата інформації внаслідок знищення, пошкодження чи крадіжки машинних або інших носіїв;

порушення працездатності комп'ютерної системи: несанкціонована чи некоректна зміна режимів роботи системних компонентів, що призводить до отримання неправильних результатів, відмов обладнання, затримки в інформаційному обслуговуванні.

д) за наслідками:

читання сторонню особою інформації з відеотерміналу під час відсутності авторизованого користувача на робочому місці;

крадіжка машинних носіїв інформації (дискет, компакт-дисків, флеш пам'яті тощо);

підключення до комп'ютерного обладнання спеціальних апаратних засобів для копіювання інформаційного чи програмного забезпечення з подальшим їхнім вилученням;

використання спеціальних радіоелектронних пристроїв для перехоплення електромагнітних випромінювань від комп'ютерного обладнання;

порушення конфіденційності інформації шляхом її передачі каналами зв'язку без шифрування або з неправильним адресуванням;

перехоплення зашифрованої інформації під час її проходження з'єднувальними лініями або спільною шиною;

зовнішні загрози, що спричиняються несанкціонованими користувачами та проявляються через перехоплення інформації, її модифікацію або знищення, формування фальшивих чи хибних сповіщень, їхню переадресацію.

Відповідно до Доктрини інформаційної безпеки України [4], основні реальні та потенційні загрози в конкретних умовах нинішнього історичного періоду структуруються у воєнній сфері національної безпеки в наступні комплекси:

порушення встановленого регламенту збирання, обробки, зберігання і передачі інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України;

несанкціонований доступ до інформації ресурсів, незаконне збирання та використання інформації з питань оборони;

реалізація програмно-математичних заходів з метою порушення функціонування інформаційних систем у сфері оборони України;

перехоплення інформації в телекомунікаційних мережах, радіоелектронне глушіння засобів зв'язку та управління;

інформаційно-психологічний вплив на населення України, у тому числі на особовий склад військових формувань, з метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби.

Для структурованих вище ознак комплексних інформаційних загроз практичне (емпіричне) їхнє оцінювання можливе за показниками, що представлені в табл. 1.

Таблиця 1

Оцінка показників загроз інформаційній безпеці

Сфера національної безпеки	Показники	Емпіричні оцінки
Воєнна сфера	Кількість виявлених фактів порушення встановленого регламенту збирання, обробки, зберігання і передачі інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України	Випадків/ рік
	Кількість встановлених спроб несанкціонованого доступу до інформаційних ресурсів з питань оборони	Випадків/ рік
	Кількість виявлених програмно-математичних заходів з метою порушення функціонування інформаційних систем у сфері оборони України	Випадків/ рік
	Кількість виявлених фактів перехоплення інформації в телекомунікаційних мережах, радіоелектронного глушіння засобів зв'язку та управління	Випадків/ рік
	Кількість встановлених випадків інформаційно-психологічного впливу на особовий склад військових формувань з метою послаблення їхньої готовності до оборони держави та погіршення іміджу військової служби	Випадків/ рік

Після здійснення емпіричних оцінок показників вони мають бути співставленні з їхніми критичними значеннями у різних сферах національної безпеки. Критичні значення представляють граничні межі, порушення яких призводить до деградації чи суттєве послаблення безпеки об'єктів захисту. В результаті цього можливі значні матеріальні, моральні та інші втрати.

Проведені дослідження [3] вказують, що втрата системою у життєвому циклі більше ніж 1/3 власних ресурсів, як правило, призводить до загибелі цієї системи. Для того, щоб система була життєздатною, в неї має залишатися не менше 2/3 її життєзабезпечуючих ресурсів. Враховуючи ці закономірності доцільно в якості граничних значень запропонованих показників визначити 1/3 для їх абсолютних значень та 33% – для відносних. Перевищення цих граничних значень свідчитиме про незворотні негативні процеси у сфері інформаційної безпеки держави, що зрештою призведуть до її повної деградації або занепаду.

В якості квантифікації показників комплексних інформаційних загроз використовується метод експертних оцінок. Експертне оцінювання здійснюється за кожним показником воєнної сфери національної безпеки Ψ_i, де $i \in \{1,k\}$, що характеризується відповідним набором показників ψ_{ij}, де $j = 1,2,3,\ldots$. Кожний показник ψ_{ij} оцінюється за допомогою шкали важливості та шкали значень.

Перша шкала характеризує ступінь важливості показника ψ_{ij} і передбачає присвоєння йому експертом відповідного рангу φ_{ij}:

$$\varphi_{ij} = \begin{cases} 5 - \text{украй важливий;} \\ 4 - \text{дуже важливий;} \\ 3 - \text{важливий;} \\ 2 - \text{не дуже важливий;} \\ 1 - \text{неважливий.} \end{cases}$$

Друга шкала відображає відносну величину показника ψ_{ij}, що експертно оцінюється певним значенням δ_{ij}:

$$\delta_{ij} = \begin{cases} 5 - \text{максимальне;} \\ 4 - \text{вище за середнє;} \\ 3 - \text{середнє;} \\ 2 - \text{нижче середнього;} \\ 1 - \text{мінімальне.} \end{cases}$$

Експертне оцінювання проводиться наступним чином. Спочатку, на основі емпіричних оцінок показників загроз, експертами за шкалою важливості здійснюється присвоєння кожному з них відносного рангу φ_{ij}.

Після цього здійснюється експертна оцінка за шкалою значень δ_{ij}, яка визначає внесок кожного показника в загальну характеристику стану відносної сфери національної безпеки. Далі розраховуються відносні значення показників загроз λ_{ij} за співвідношенням:

$$\lambda_{ij} = \lfloor \delta_{ij} / \varphi_{ij} \rfloor \le 1, \qquad (1)$$

де $i \in \{1,k\}$, $j = 1,2,3,\ldots$.

Відносні значення показників визначають ступінь небезпеки кожної загрози у будь-якій сфері національної безпеки Ψ_i. Загальний стан інформаційної безпеки в цілому у кожній сфері доцільно оцінювати за мінімальним значенням усіх її показників ψ_{ij}.

Таким чином, емпіричні значення показників комплексних інформаційних загроз перетворюються у відносну форму. Таким чином оцінюються узагальнені відносні показники загроз для кожної сфери Ψ_i національної безпеки:

$$\Psi_i = \sum_j \alpha_{ij} \lambda_{ij}, \qquad (2)$$

де α_{ij} – нормуючий ваговий коефіцієнт ($0 \le \alpha_{ij} \le 1$), що визначається експертним шляхом для кожного показника в окремій сфері.

Відповідно, узагальнений відносний показник загроз інформаційній безпеці в цілому Ω визначатиметься як лінійно зважена сума узагальнених відносних показників усіх сфер національної безпеки:

$$\Omega = \sum_{i=1}^{k} \beta_i \Psi_i, \qquad (3)$$

де β_i – нормуючий ваговий коефіцієнт і-тої сфери інформаційної безпеки ($0 \le \beta_i \le 1$), що також визначається шляхом експертної оцінки [5].

Таким чином, узагальнюючий відносний показник загроз інформаційній безпеці у воєнній сфері визначатиметься співвідношенням:

$$\Psi_i = \alpha_{11}\lambda_{11} + \alpha_{12}\lambda_{12} + \alpha_{13}\lambda_{13} + \\ + \alpha_{14}\lambda_{14} + \alpha_{15}\lambda_{15}. \qquad (4)$$

Відповідно формується матриця оцінок показників інформаційних загроз (табл. 2), яка дозволяє практично оцінити стан інформаційної безпеки у воєнній сфері національної безпеки.

Таблиця 2

Матриця оцінок показників інформаційних загроз у воєнній сфері

Сфера національної безпеки	Емпіричні оцінки	Оцінки за шкалою значень	Оцінки за шкалою важливості	Відносні значення показників	Вагові коефіцієнти
Ψ_1	ψ_{11}	δ_{11}	φ_{11}	λ_{11}	α_{11}
	ψ_{12}	δ_{12}	φ_{12}	λ_{12}	α_{12}
	ψ_{13}	δ_{13}	φ_{13}	λ_{13}	α_{13}
	ψ_{14}	δ_{14}	φ_{14}	λ_{14}	α_{14}
	ψ_{15}	δ_{15}	φ_{15}	λ_{15}	α_{15}

Висновки

Слід зауважити, що запропонований підхід до квантифікації комплексних інформаційних загроз та розроблена математична модель загроз інформаційної безпеки в інформаційно-телекомунікаційних системах дозволяє:

практично оцінювати стан інформаційної безпеки за кожною сферою національної безпеки;

цілеспрямовано формувати і розвивати моніторинг зовнішніх і внутрішніх загроз інформаційній безпеці на основі системи показників цих загроз;

більш обґрунтовано приймати рішення щодо підвищення рівня інформаційної безпеки за всіма сферами національної безпеки.

У рамках розробленої моделі доцільно провести подальші дослідження за наступними напрямами:

розробка методів і засобів системного моніторингу загроз інформаційній безпеці, що дозволяють не лише контролювати, а й підтримувати такий стан інформаційної безпеки, за якого її показники перебуватимуть у допустимих межах;

визначення взаємозв'язків відносних показни-

ків загроз інформаційній безпеці за всіма сферами національної безпеки;

обґрунтування вибору нормуючих вагових коефіцієнтів для оцінювання стану інформаційної безпеки в цілому.

Аналіз стану інформаційної безпеки в Україні показує, що її рівень не відповідає сучасним вимогам, зокрема:

нормативно-правова база у цій сфері характеризується фрагментарністю, неповнотою вимогам і несистемністю;

у структурі державного управління відсутній центральний орган, уповноважений і відповідальний за захист національних інтересів від комплексних інформаційних загроз.

відсутнє науково-методичне забезпечення стратегії і тактики ведення інформаційного протиборства за національні інтереси [6].

В сучасних умовах держава неспроможна ефективно протидіяти комплексним інформаційним загрозам і системно вирішувати завдання інформаційного протиборства.

Для якісного вдосконалення системи захисту національного інформаційного простору необхідно першочергово реалізувати такі завдання:

створити чи визначити в структурі державного (військового управління) управління окремий орган, уповноважений і відповідальний за моніторинг і прогнозування зовнішніх і внутрішніх інформаційних загроз, а також за координацію численних і розміщених організацій щодо захисту і протидії цим загрозам;

розробити і впровадити єдину державну політику інформаційної безпеки і відповідно вдосконалити нормативно-правову базу на засадах гармонізації інформаційних прав, свобод і відповідальності людини, суспільства і держави;

запровадити незалежне суспільне телебачення і радіомовлення для наповнення національного інформаційного простору незаангажованими альтернативними повідомленнями і аналітичними експертними оцінками щодо актуальних міжнародних і внутрішніх подій;

розробити науково-методичне забезпечення стратегії і тактики ведення інформаційної боротьби за національні інтереси;

підвищити ефективність системи відбору і підготовки кадрів для проведення експертиз і профілактичних заходів, впровадження сучасних методів і засобів захисту національного інформаційного простору.

Список літератури

1. Проблеми захисту інформаційного простору України: монографія / Під ред. В.П. Горбуліна, М.М. Биченка. – К.: ІПНБ РНБОУ, 2009. – 136 с.

2. Інформаційні впливи та операції. Теоретико-аналітичні нариси: монографія / О.В. Литвиненко – К.: НІСД, 2003. – 240 с.

3. Журавский В.С. Україна на шляху до інформаційного суспільства / В.С. Журавский – К.: Азимут-Україна, 2008. – 120 с.

4. Баховець О.Б. Передумови становлення інформаційного суспільства в Україні / О.Б. Баховець – К.: Політехніка, 2011. – 140 с.

5. Петрік В.М. Соціально-правові основи інформаційної безпеки / В.М. Петрік, А.М. Кузьменко – К.: Росава, 2007. – 497 с.

6. Кормич Б.А. Інформаційна безпека: організаційно-правові основи / Б.А. Кормич. – К.: Кондор, 2012. – 384 с.

Надійшла до редколегії 14.09.2014

Рецензент: д-р техн. наук проф. Г.В. Пєвцов, Харківський університет Повітряних Сил імені Івана Кожедуба, Харків.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

О.Г. Пузыренко

Представлена математическая модель определения относительного показателя угроз информационной безопасности государства, на основе метода экспертных оценок. В работе рассматриваются источника угроз в информационно-телекоммуникационных системах специального назначения на основе которых определяются основные показатели, которые критически влияют на информационную безопасность государства. Предложенный подход к качественным оценкам комплексных информационных угроз разрешает практически оценивать состояние информационной безопасности за каждой сферой национальной безопасности.

Ключевые слова: *защита информации, информационно-телекоммуникационные системы, угрозы информационной безопасности.*

MATHEMATICAL MODEL OF INFORMATION SECURITY THREATS IN INFORMATION AND TELECOMMUNICATION SYSTEMS SPECIAL PURPOSE

O.G. Puzyrenko

A mathematical model for determining the relative indicator of threats to the information security of the state, on the basis of expert assessments. The paper considers the source of threats to information and telecommunication systems for special purposes on the basis of which identifies the major factors that critically affect the information security of the state. The proposed approach to qualitative estimates of complex information threats solves almost assess the state of information security in every sphere of national security.

Keywords: *information security, information and telecommunication systems, information security threats.*