DOI:**10.33099/2311-7249/2020-37-1-103-106**

УДК: 004.94.355

Олександр Валерійович Крайнов *(кандидат технічних наук, доцент)*
Марина Федорівна Маланчук *(кандидат економічних наук)*
Роман Іванович Грозовський

Національний університет оборони України імені Івана Черняховського, Київ, Україна

МЕТОДИКА ОЦІНКИ ЕФЕКТИВНОСТІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІВ ВІЙСЬКОВОГО УПРАВЛІННЯ

Питання безпеки інформації – важлива частина концепції впровадження нових інформаційних технологій в військову справу. "Той, хто володіє достовірною і повною інформацією, – той володіє ситуацією, а той, хто володіє ситуацією, – той здатен управляти нею у своїх інтересах, а той, хто здатен управляти, – той здатен перемагати". Тому захист інформації у інформаційному середовищі органів управління військами на теперішній час є дуже актуальною проблемою, яка потребує свого вирішення.

Захист інформації в органах військового управління має низку особливостей порівняно з загальновідомими концепціями. Це обумовлено, з одного боку, специфікою роботи штабів, як носіїв таємниць державного та військового характеру, з іншого – типовим організаційно-штатною структурою з відповідними ній постійними чітко встановленими функціями. Сучасна концепція інформаційної війни також передбачає широке використання спеціальних засобів боротьби в інформаційному просторі. Це і обумовлює актуальність проблеми захисту інформації.

Ключові слова: *автоматизована інформаційна система; інформаційно-аналітичне забезпечення; орган військового управління; ефективність.*

Вступ

Постановка проблеми. Комплексна система захисту інформації (КСЗІ) є сукупністю методів і засобів, об'єднаних єдиним цільовим призначенням, які забезпечують необхідну ефективність захисту інформації в автоматизованих інформаційних системах (АІС) органів військового управління.

Комплексність системи захисту інформації досягається охопленням всіх можливих загроз і узгодженням між собою різнорідних методів і засобів, що забезпечують захист всіх елементів АІС [3].

При побудові комплексної системи захисту інформації (КСЗІ) виділяють дві групи вимог до захищеності АІС [1,2], які повинні враховуватися – формалізовані вимоги і вимоги, які формулюються на підставі існуючої статистики загроз. Неможливість в загальному випадку формалізувати вимоги другої групи не дозволяє і формалізувати порівняльний аналіз систем захисту, віднесених до одного класу захищеності (відповідно до класифікації нормативних документів).

Зокрема, дві системи захисту, віднесені до одного класу захищеності, можуть принципово розрізнятися за своїми можливостями. При цьому необхідно відзначати, що у разі передбачуваної ідентичності реалізації формалізованих вимог, для них найважливішою характеристикою стає рівень кваліфікації їх розробників.

Припущення ідентичності звичайно не відповідає дійсності, оскільки в нормативних документах не вказується, яким способом повинен бути реалізований кожний механізм захисту. Тому існуючі системи додаткового захисту, віднесені до одного класу захищеності, принципово розрізняються і в реалізації формалізованих вимог. Питання оцінки ефективності і питання проектування КСЗІ тісно пов'язані, оскільки в їх основі лежить єдиний математичний апарат рішення відповідної оптимізаційної задачі.

Аналіз остатніх досліджень і публікацій. Проблематиці захисту інформації в АІС приділяють увагу багато вчених як в Україні, так і за кордоном. Особливо гостро на сьогодні, з урахуванням умов постійної конкуренції не лише між недержавними структурами, а і структурами, які містять державні інформаційні ресурси, точиться боротьба за інформацію. Тому її захист завжди актуальний. Принципи побудови КСЗІ, загальні принципи інформаційної безпеки в АІС розглядали такі фахівці у сфері захисту інформації, як В. М. Богуш, М. В. Грайворонський, О. А. Довидьков, В. Г. Кривуца, В. Ф. Шаньгин, О. Г. Корченко, Г. Ф. Конахович, В. Г. Грибунін та інші вчені.

Таким чином, **метою статті є** удосконалення науково-методичного апарату оцінювання ефективності комплексної системи захисту інформації автоматизованих інформаційних систем органів військового управління.

Виклад основного матеріалу дослідження

Розглянемо загальний підхід щодо оцінки ефективності КСЗІ та визначимо критерії і параметри оптимальної системи захисту.

Оцінку захищеності системи Z будемо здійснювати кількісно залежно від вартості інформації, що захищається, ймовірності злому, вартості КСЗІ, продуктивності системи:

$$Z = f\left(C_{інф},\ P_{взл},\ Ц_{ксзі},\ П\right),$$

де: $C_{інф}$ – вартість інформації;

$P_{взл}$ – ймовірність взлому;

$Ц_{ксзі}$ – вартість КСЗІ;

$П$ – продуктивність системи.

Оптимізаційна задача полягає в функції вартості інформації при забезпеченні максимального рівня захищеності (якщо захищається і ймовірність злому) при мінімальній вартості системи захисту і мінімальному впливу її на продуктивність системи:

$$Z^{opt} = \max Z\left(C_{інф},\ P_{взл},\ Ц_{ксзі},\ П\right)/$$

При цьому слід зазначити, що крім необхідного забезпечуваного рівня захищеності, повинен враховуватися ще ряд досить суттєвих характеристик системи. Наприклад, обов'язково повинен враховуватися вплив КСЗІ на завантаження обчислювального ресурсу об'єкту, що захищається.

На практиці найбільш часто оцінка рівня захищеності проводиться використовуючи теорію ризиків. Ризик (R) – це потенційні втрати від загроз захищеності:

$$R(p) = C_{інф} P_{взл}.$$

По суті, параметр ризику тут вводиться як мультиплікативна згортка двох основних параметрів захищеності.

З другого боку, можна розглядати ризик як втрати в одиницю часу:

$$R(\lambda) = C_{інф} \lambda_{взл}$$

де: $\lambda_{взл}$ – інтенсивність потоку зломів (під зломом розуміємо вдалу спробу несанкціонованого доступу до інформації).

Ці дві формули пов'язані наступним співвідношенням:

$$P_{взл} = \frac{\lambda_{взл}}{\Lambda},$$

де: Λ – загальна інтенсивність потоку несанкціонованих спроб доступу зловмисника до інформації.

Розглянемо основний критерій захищеності та загальне рішення задачі проектування оптимальної КСЗІ.

В якості основного критерію захищеності можна використовувати коефіцієнт захищеності (D), що показує відносне зменшення ризику в захищеній системі в порівнянні з незахищеною системою.

$$D = \left(1 - \frac{R_{зах}}{R_{незах}}\right) \times 100\% \qquad (1)$$

де: $R_{зах}$ – ризик в захищеній системі;

$R_{незах}$ – ризик в незахищеній системі.

Таким чином, в даному випадку задача оптимізації виглядає таким чином:

$$\begin{cases} D\left(C_{інф},\ P_{взл}\right) \to \max; \\ Ц_{ксзі} \to \max; \\ П_{ксзі} \to \max. \end{cases}$$

Для вирішення цієї задачі зведемо її до однокритеріальної за допомогою введення обмежень. В результаті отримаємо:

$$\begin{cases} D\left(C_{інф},\ P_{взл}\right) \to \max; \\ Ц_{ксзі} \le Ц_{зад}; \\ П_{ксзі} \ge П_{зад}. \end{cases}$$

де: $Ц_{зад}$ і $П_{зад}$ – задані обмеження на вартість КСЗІ та продуктивність системи.

Цільова функція вибрана виходячи з того, що саме вона відображає основне функціональне призначення системи захисту – забезпечення безпеки інформації.

Продуктивність системи $П_{ксзі}$ розраховується із застосуванням моделей і методів теорії масового обслуговування і теорії розкладів (залежно від того, захищається система оперативної обробки чи реального часу). На практиці можливо завдання обмеження по продуктивності (вплив на завантаження обчислювального ресурсу системи, що захищається) не безпосередньо у вигляді необхідної продуктивності системи, а як зниження продуктивності ($dП_{ксзі}$) АІС від встановлення системи захисту. В цьому випадку задача оптимізації виглядатиме таким чином:

$$\begin{cases} D\left(C,\ p\right) \to \max; \\ Ц_{ксзі} \to \min; \\ dП_{ксзі} \to \min, \end{cases}$$

або після зведення її до однокритерійної:

$$\begin{cases} D\left(C,\ p\right) \to \max; \\ Ц_{ксзі} \le Ц_{зад}; \\ dП_{ксзі} \le dП_{зад}, \end{cases}$$

де: $Ц_{зад}$ і $dП_{зад}$ – задані обмеження на вартість КСЗІ і зниження продуктивності.

Саме такий принцип зведення задачі до однокритеріальної доцільний, оскільки в будь-якому технічному завданні на розробку КСЗІ вказується, якою мірою система захисту буде впливати на продуктивність системи. Як правило, впровадження системи захисту не повинне знижувати продуктивність системи більш ніж на 10%. Крім того, звичайно вводиться обмеження на

вартість системи захисту.

Якщо розраховане значення коефіцієнта захищеності D не задовольняє вимогам до системи захисту, то в допустимих межах можна змінювати задані обмеження і вирішити задачу методом послідовного вибору уступок. При цьому задається приріст вартості і зниження продуктивності:

$$Ц^{*}_{зад} = Ц_{зад} \Delta Ц,$$

$$Ц^{*}_{зад} = П_{зад} - \Delta П, \text{ або } П^{*}_{зад} = dП_{зад} + \Delta dП.$$

У такому вигляді задача розв'язується внаслідок реалізації ітераційної процедури шляхом відсіювання варіантів, що не задовольняють обмежувальним умовам, і подальшому вибору з тих, що залишилися варіанту з максимальним коефіцієнтом захищеності.

Визначимо коефіцієнт захищеності через параметр загроз. В цих умовах задаємо наступні величини:

ω – кількість видів загроз, що впливають на систему;

C_i – вартість (втрати) від злому і-того виду;

λ_i – інтенсивність потоку зломів і-того виду, відповідно;

Q_i – ймовірність появи загроз і-того виду в загальному потоці спроб несанкціонованого доступу до інформації:

$$Q_i = \frac{\lambda_i}{\Lambda};$$

P_i – ймовірність відбиття загроз і-того виду системою захисту.

Відповідно, коефіцієнт втрат від зломів системи захисту визначається:

$$R(p) = \sum_{1}^{\omega} R_i(p) = \sum_{1}^{\omega} C_i P_{взл_i}$$

де: $R_i(p)$ – коефіцієнт втрат від злому і-того типу та показує, які в середньому втрати припадають на один злом і-того типу.

Для незахищеної системи $P_{загр_i} = Q_i$, для захищеної системи $P_{загр_i} = Q_i(1 - p_i)$.

Коефіцієнт втрат від зломів системи захисту в одиницю часу відповідно визначається:

$$R_i(\lambda) = \sum_{1}^{\omega} R(\lambda) = \sum_{1}^{\lambda} C_i \lambda_{взл_i}$$

де: $R_i(\lambda)$ – коефіцієнт втрат від зломів і-того типу в одиницю часу.

Для незахищеної системи $\lambda_{загр_i} = \lambda_i$; для захищеної системи $\lambda_{загр_i} = \lambda_i(1 - p_i)$.

Відповідно, з (1) маємо:

$$D = 1 - \frac{\sum_{1}^{\omega} C_i Q_i (1 - p_i)}{\sum_{1}^{\omega} C_i Q_i} = 1 - \frac{\sum_{1}^{\omega} C_i \lambda_i (1 - p_i)}{\sum_{1}^{\omega} C_i \lambda_i}.$$

Якщо у якості вихідних параметрів задана ймовірність появи загроз Q_i, тоді коефіцієнт захищеності зручно рахувати через ймовірності появи загроз. Якщо ж в якості вихідних параметрів задані інтенсивності потоків загроз λ_i, тоді коефіцієнт захищеності рахується через інтенсивність.

Висновки й перспективи подальших досліджень

Загрози інформаційному простору не залишаються незмінними в часі. Бурхливий розвиток інформаційних технологій та засобів обробки та удосконалення систем захисту аналогічно впливає і на розвиток засобів атак та удосконалення методів їх проведення. Свідченням цього є постійний ріст кількості загроз вірусного характеру в глобальній мережі. Це вимагає створення динамічних систем захисту адаптивних відповідно змін зовнішнього оточення інформаційних систем.

В сучасних умовах безпека інформаційних ресурсів може бути забезпечена тільки комплексною системою захисту інформації. Комплексна система захисту інформації повинна бути: безперервною, плановою, цілеспрямованої, конкретної, активної, надійною. Система захисту інформації повинна спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування не тільки в повсякденних умовах, але і в умовах ведення бойових дій.

В умовах сучасної інформаційної та кібервійни, яка ведеться проти нашої країни, забезпечення безпеки АІС органів військового управління має стати державним завданням.

Література

1. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. Санкт-Петербург: Наука и техника, 2004.-384с. **2. Мельников В.А**. Защита информации в компьютерных системах. М.: Финансы и статистика: Электроинформ, 1997.-368с. **3.** Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНОВ ВОЕННОГО УПРАВЛЕНИЯ

Александр Валериевич Крайнов *(кандидат технических наук, доцент)*
Марина Федоровна Маланчук *(кандидат экономических наук)*
Роман Иванович Грозовский

Национальный университет обороны Украины имени Ивана Черняховского, Киев, Украина

Вопрос безопасности информации - важная часть концепции внедрения новых информационных технологий в военном деле. "Тот, кто владеет достоверной и полной информацией - тот владеет ситуацией, а тот, кто владеет ситуацией, - тот способен управлять ею в своих интересах, а тот, кто способен управлять, - тот способен побеждать". Поэтому защита информации в информационной среде органов управления войсками в настоящее время является очень актуальной проблемой, требующей своего решения.

Защита информации в органах военного управления имеет ряд особенностей по сравнению с общеизвестными концепциями. Это обусловлено, с одной стороны, спецификой работы штабов, как носителей тайн государственного и военного характера, с другой - типичным организационно-штатной структуре с соответствующими ней постоянными установленными функциями. Современная концепция информационной войны также предусматривает широкое использование специальных средств борьбы в информационном пространстве. Это и обусловливает актуальность проблемы защиты информации.

Ключевые слова: *автоматизированная информационная система; информационно-аналитическое обеспечение; орган военного управления; эффективность.*

METHODOLOGY FOR ESTIMATING THE EFFECTIVENESS OF AN INTEGRATED INFORMATION PROTECTION SYSTEM FOR AUTOMATED INFORMATION SYSTEMS OF MILITARY MANAGEMENT BODIES

Oleksandr Krainov *(Candidate of technical sciences, associate professor)*
Maryna Malanchuk *(Candidate of Economic Sciences)*
Roman Hrozovskyi

National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine

The issue of information security is an important part of the concept of introducing new information technologies in military affairs. "The one who possesses reliable and complete information - the one who owns the situation, and the one who owns the situation - that is able to manage it in his own interests, and the one who is able to manage - that is able to win." Therefore, the protection of information in the information environment of military command and control agencies is currently a very urgent problem that needs to be addressed.

Information security in military command and control has a number of features compared to well-known concepts. This is due, on the one hand, to the specifics of the work of staffs as carriers of state and military secrets, and on the other, to a typical organizational and staff structure with corresponding permanent functions. The modern concept of information warfare also provides for the widespread use of special means of combat in the information space. This determines the urgency of the problem of information security.

Key words: *automated information system; information and analytical support; military command body; efficiency.*

References

1. Scheglov A.Yu. Zaschita kompyuternoy informatsii ot nesanktsionirovannogo dostupa. Sankt-Peterburg: Nauka i tehnika, 2004.-384s. **2. Melnikov V.A.** Zaschita informatsii v kompyuternyih sistemah. M.: Finansyi i statistika: Elektroinform, 1997.-368s. **3.** Zakhyst informaciji v avtomatyzovanykh systemakh upravlinnja : navchaljnyj posibnyk / Uklad. I. A. Piljkevych, N. M. Lobanchykova, K. V. Molodecjka. – Zhytomyr : Vyd-vo ZhDU im. I. Franka, 2015. – 226 s.