УДК 004:623

В.С. Чередниченко, кандидат технічних наук
П.В. Анахов, аспірант Інституту геохімії навколишнього середовища НАН та МНС України

ОЦІНЮВАННЯ ЖИВУЧОСТІ АВТОМАТИЗОВАНОЇ СИСТЕМИ КЕРУВАННЯ ЕФЕКТИВНІСТЮ ЗБРОЇ

З метою визначення чинників небезпеки, на основі аналізу класів загроз безпеці автоматизованої системи керування (АСК), виконано оцінювання ефективності зброї. Для оцінювання живучості АСК, яка вирізняється не передбаченими умовами нормальної експлуатації обставинами непереборної сили, запропоновано обернене до оцінювання ефективності зброї рішення.

Ключові слова: *автоматизована система керування, класи загроз безпеці, чинники небезпеки, ефективність зброї.*

С целью определения факторов опасности, на основе анализа классов угроз безопасности автоматизированной системы безопасности (АСУ), выполнено оценивание эффективности оружия. Для оценивания живучести АСУ, которая отличается непредусмотренными условиями нормальной эксплуатации обстоятельствами непреодолимой силы, предложено обратное к оцениванию эффективности оружия решение.

Ключевые слова: *автоматизированная система управления, классы угроз безопасности, факторы опасности, эффективность оружия.*

For the purpose of the definition of factors of danger, on the basis of the analysis of classes of threats to the safety of the automated system of safety an estimation of weapon efficiency is carried out. For an estimation of survivability of the automated safety system which differs with unforeseen conditions of normal operation by force majeure circumstances, the inverse solution to an estimation of the weapon efficiency is offered.

Keywords: *automated control system, classes of threats of safety, danger factors, efficiency of the weapon.*

У 2008 році фахівці фірми з інформаційної безпеки Websense (м. Сан-Дієго, США), базуючись на статистичних даних, зробили прогноз щодо перспектив розвитку ситуації з безпеки мережі Інтернет у найближчому майбутньому. У цілому експерти прогнозують подальшу криміналізацію глобальної мережі і швидку зміну тактик, яких вживають хакери, серед яких: веб-сервер-спам; атаки на "слабкі ланки"; інфікування легальних сайтів; крос-платформні атаки; атаки, орієнтовані на певні категорії користувачів; поліморфізм коду JavaScript; технології приховання даних і шифрування; атаки на кіберзлочинців; голосовий спам і голосовий фішинг.

Аналітики з головної науково-дослідної і дослідно-конструкторської Ліверморської національної лабораторії ім. Е. Лоуренса (м. Лівермор, США), яка займається розв'язанням проблем національної безпеки, дійшли висновку, що *проникнення* (термін установлено нормативним документом ДСТСЗІ СБУ НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу") до автоматизованих систем керування (АСК) виробничими процесами робить виробництво особливо уразливим при

нападах, оскільки дозволяє зловмисникам утримувати загрозу катастрофи, управляючи розвитком подій [1].

Об'єкти багатокористувацьких автоматизованих систем керування, зв'язок між якими здійснюється фізично (по мережевих з'єднаннях) і програмно (за допомогою механізму повідомлень), розподілені в просторі. Це визначає проблему зниження захищеності інформації, що циркулює в АСК, від проникнення до інформаційних ресурсів. Статистика атак дозволяє виділити три класи загроз безпеці АСК (рис. 1).

Порушення функціональних характеристик АСК
1. Клас загрози безпеці АСК: несанкціонований збір інформації про деякий сегмент мережі [2]. Ознака впливу загрози – прослуховування трафіку шляхом [3]: - несанкціонованого отримання інформації з обмеженим доступом; - розкриття змісту інформації з обмеженим доступом ІзОД (дешифрування). Функціональна характеристика захищеності АСК: конфіденційність інформації [2, 3].
2. Клас загрози безпеці АСК: генерування і впровадження нових об'єктів мережевої взаємодії у заздалегідь визначені сегменти мережі, з метою перехоплення управління мережевим пристроєм визначеного сегменту [2]. Ознака впливу загрози – порушення актуальності і несуперечності інформації, її захищеності від руйнації і несанкціонованої зміни шляхом [3]: - виведення з ладу, зміни режимів функціонування або несанкціонованим використанням носіїв інформації; - несанкціонованої модифікації ІзОД в середовищах її обробки, зберігання чи передачі. Функціональна характеристика захищеності АСК: цілісність інформації [2, 3].
3. Клас загрози безпеці АСК: вивід з ладу мережевого пристрою шляхом реалізації атак типу "відмова в обслуговуванні" [2]. Ознака впливу загрози – порушення можливості за прийнятний час одержати необхідну інформаційну послугу шляхом [3]: - несанкціонованого використання інформаційного ресурсу захопленням (неконтрольованим використанням, утриманням, занадто тривалим використанням) ресурсів і створення таким чином перешкод авторизованим користувачам у використанні цих ресурсів; - переводу ресурсу в режим штучної відмови (тривалої неможливості використання ресурсу за призначенням); - впливу природних чи штучних збоїв; - фізичного впливу на ресурс з метою виведення його з ладу чи зміни режимів його функціонування. Функціональна характеристика захищеності АСК: доступність інформації для її законних користувачів [2, 3].

Рис. 1. Класи загроз безпеці АСК

Представлені класи загроз описуються ознаками впливу, задачу забезпечення захищеності яких від порушень їх функціональних характеристик необхідно вирішувати.

М. Будько (Київське підприємство обчислювальної техніки та інформатизації, м. Київ) запропонував систему визначення ймовірності порушення функціональних властивостей автоматизованої системи керування, яка враховує класи загрози її безпеці [3]:

$$P_{пфх}=1-(1-q_1)\times(1-q_2)\times(1-q_3), \quad (1)$$

де q_i – ймовірність порушення захищеності конфіденційності інформації (захищеність інформації від несанкціонованого читання неуповноваженими особами, сутностей або процесів; поняття "сутність" означає, що взаємодія може відбуватись не тільки між людиною й інформаційною системою, але і між програмами, в якості яких виступають інтелектуальні агенти або віруси); q_2 – ймовірність порушення захищеності цілісності ресурсу (можливість виявлення будь-яких модифікацій, вставок або видалень, які впливають на коректність інформації, що зосереджена в інформаційному ресурсі); q_3 – ймовірність порушення захищеності доступності ресурсу (захищеність від неавторизованого використання ресурсу).

Метою цієї статті є визначення чинників небезпеки для АСК. Це дозволить виробити рекомендацій щодо протидії загрозам.

Ефективність зброї W оцінюється імовірністю виконання поставленого завдання у встановлений час. Типовим є випадок, коли виконання завдання можливе при значенні застосування зброї не менше деякої вибраної нижньої межі необхідного результату S_b [4]:

$$W=P\{S\geq S_b\}, \quad (2)$$

де S – можливий результат бойового застосування зброї; P – символ імовірності.

У той же час ефективність зброї визначається ієрархічною послідовністю вражаючих факторів (рис. 2), які так чи інакше впливають на захищену АСК.

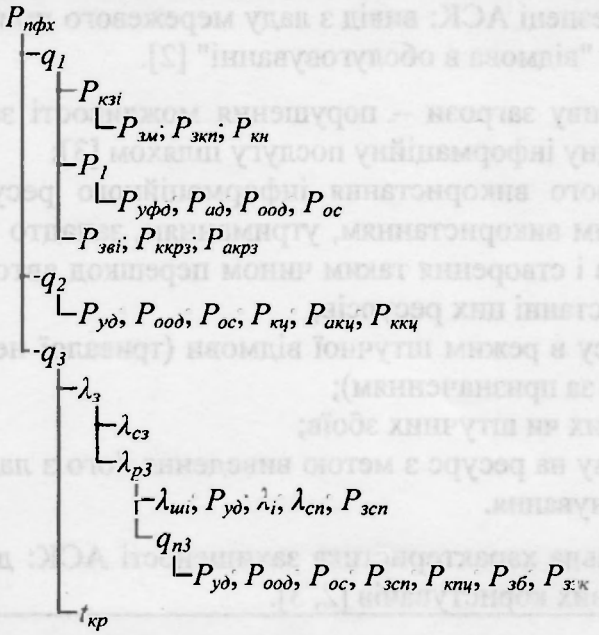

Рис. 2. Ієрархічна послідовність вражаючих факторів зброї нападу на АСК

Ймовірність порушення захищеності конфіденційності інформації q_1 розраховується за формулою [3]:

$$q_1=1-\{1-P_{кзі}[1-(1-P_1)(1-P_{зві})]\}[1-P_{ккрз}P_{акрз}]], \quad (3)$$

де $P_{кзі}=P_{зм}P_{зкп}P_{кн}$ – ймовірність подолання засобів криптографічного захисту інформації; $P_{зм}$ – ймовірність того, що порушник знає мову, якою інформація представляється; $P_{зкп}$ – ймовірність того, що порушник знає і може застосувати програмні засоби або апаратуру для криптографічного перетворення (для дешифрування закритої інформації); $P_{кн}$ – ймовірність того, що порушник має необхідні ключі (ключові набори) для такого перетворення; $P_1=P_{уфд}P_{ад}[1-(1-P_{ood})(1-P_{ос})]$ – ймовірність несанкціонованого отримання користувачем інформації при безпосередньому впливі; $P_{уфд}$ – ймовірність подолання порушником засобів управління фізичним доступом; $P_{ад}$ – ймовірність подолання порушником засобів адміністрування доступом; P_{ood} – ймовірність подолання засобів організаційного обмеження доступу; $P_{ос}$ – ймовірність подолання засобів охоронної сигналізації; $P_{зві}$ – ймовірність подолання засобів захисту від витоку інформації технічними каналами; $P_{ккрз}$ – ймовірність подолання неавторизованим користувачем засобів канального криптографічного захисту інформації у мережах електрозв'язку; $P_{акрз}$ – ймовірність подолання неавторизованим користувачем засобів абонентського криптографічного захисту інформації у мережах електрозв'язку.

Ймовірність порушення захищеності цілісності ресурсу q_2 розраховується за формулою [3]:

$$q_2=1-\{1-P_{уд}[1-(1-P_{ood})(1-P_{ос})]\}[1-P_{кц}][1-P_{акц}P_{ккц}], \quad (4)$$

де $P_{уд}$ – ймовірність подолання засобів управління доступом; P_{ood} – ймовірність подолання засобів організаційного обмеження доступу; $P_{ос}$ – ймовірність подолання засобів охоронної сигналізації; $P_{кц}$ – ймовірність подолання засобів контролю цілісності інформації відповідного вузла; $P_{акц}$ – ймовірність подолання засобів абонентського контролю цілісності інформації в мережах електрозв'язку; $P_{ккц}$ – ймовірність подолання засобів канального контролю цілісності інформації в мережах електрозв'язку.

Ймовірність порушення захищеності доступності ресурсу q_3 розраховується за формулою [3]:

$$q_3=1-(1+\lambda_3 t_{кр})\exp(-\lambda_3 t_{кр}), \quad (5)$$

де $\lambda_з=\lambda_{сз}+\lambda_{рз}$ – інтенсивність запитів на використання ресурсів АСК; $\lambda_{сз}$ – інтенсивність справжніх запитів; $\lambda_{рз}=(\lambda_{ш}P_{уд}+\lambda_i+\lambda_{сп}P_{кпц}P_{зсп})q_{пз}$ – результуюча інтенсивність загроз захищеному ресурсу; $\lambda_{ш}$ – інтенсивність штучних впливів через засоби управління доступом, під якими розуміються ті події, які є наслідком діяльності користувачів як авторизованих, так і неавторизованих, по відношенню до ресурсів АСК, які з якихось причин заборонені для цих користувачів; $P_{уд}$ – ймовірність подолання засобів управління доступом; λ_i – інтенсивність природних впливів, під якими розуміються потоки будь-яких подій, які здатні вивести АСК з ладу; $\lambda_{сп}$ – інтенсивність спеціальних впливів по технічним каналам; $P_{кпц}$ – ймовірність подолання засобів контролю та поновлення цілісності інформації

вузлів центрального, регіонального чи місцевого рівнів АСК; $P_{зсп}$ – ймовірність подолання засобів захисту від спеціального впливу на інформацію по технічним каналам; $q_{пз}=1-[1-P_{ид}[1-(1-P_{ood})(1-P_{oc})]][1-P_{зсп}P_{кпц}][1-P_{зб}P_{взк})]$ – ймовірність подолання засобів забезпечення доступності; $P_{ид}$ – ймовірність подолання засобів управління доступом; P_{ood} – ймовірність подолання засобів організаційного обмеження доступу; P_{oc} – ймовірність подолання засобів охоронної сигналізації; $P_{зсп}$ – ймовірність подолання засобів захисту від спеціального впливу на інформацію по технічним каналам; $P_{кпц}$ – ймовірність подолання засобів контролю та поновлення цілісності інформації вузлів центрального, регіонального чи місцевого рівнів АСК; $P_{зб}$ – ймовірність подолання засобів блокування засобів генерації безперервних запитів, спроб підбору паролів та ін.; $P_{взк}$ – ймовірність подолання засобів канального захисту інформації в телекомунікаційній мережі; $t_{кр}$ – середній час використання ресурсу.

У роботі А.В. Кострова [5], розглядаючи дію незалежних вражаючих факторів керованих снарядів ударно-вибухової дії, за умови єдиної шкали вимірювання функцій, вводиться поняття вагової функції збитку від i-го вражаючого фактора $0 \le \omega\left(\Delta\vec{r}\right) \in R < 1$:

$$\forall i \in \overline{1,n}\left\{W_i = \int_{-\infty}^{+\infty}\int\int \omega_i\left(\Delta\vec{r}\right)\varphi\left(\Delta\vec{r}\right)d\Delta\vec{r}\right\}, \quad (6)$$

де $\Delta\vec{r}$ – вектор промаху відносно точки прицілювання; $\varphi\left(\Delta\vec{r}\right) \in R$ – функція густини розподілу промаху відносно точки прицілювання.

Тоді ефективність зброї нападу на автоматизовану систему керування, за умови дії незалежних вражаючих факторів, при переході до більш простої фасетної класифікації вражаючих факторів, розраховуватиметься за формулою:

$$W = \bigvee_{\forall i \in 1,n}\left[1-\prod_{i=1}^{n}\left(1-P_i\{S\omega \ge S_b\}\right)\right], \quad (7)$$

де $\vee$ – символ диз'юнкції; П – символ добутку; $P_i\{S>S_b\}$ – імовірність порушення функціональних властивостей автоматизованої системи керування при дії i-го вражаючого фактора; n – кількість вражаючих факторів.

При розрахунках інженерних об'єктів за методом граничних станів виконується обернена до розрахунку ефективності зброї задача – встановлюються граничні стани ресурсів так, щоб ці стани не наступали при найсприятливіших поєднаннях вражаючих факторів і при найменших можливих значеннях стійкості ресурсів як апаратних, так і програмних:

$$xK^*<y, \quad (8)$$

де x – значення вражаючого фактора; y – значення критерію стійкості до дії вражаючого фактора; $K^*=\gamma_{lc}\gamma_n$ – коефіцієнт допустимих "ушкоджень" ресурсу; γ_{lc} – коефіцієнт сполучення навантажень, який розраховується за групами граничних станів (граничні стани першої групи визначають абсолютну непридатність ресурсів до експлуатації; граничні стани другої групи встановлюють непридатність

ресурсів до нормальної експлуатації, тобто до експлуатації без обмежень відповідно до технологічних або інших умов, передбачених нормами або завданнями на проектування); γ_n – коефіцієнт надійності ресурсу за відповідальністю.

Остаточно надійність системи N визначатиметься стійкістю системи до дії вражаючих факторів зброї і буде виглядати наступним чином:

$$N = \bigvee_{\forall i \in 1,n} \left[1 - \prod_{i=1}^{n} \left(1 - P_i \{ S\omega < S_b \} \right) \right], \qquad (9)$$

У роботі І.А. Рябиніна [6] визначається, що надійність як здатність системи зберігати властивості, необхідні для виконання заданого призначення, за нормальних (повсякденних) умов експлуатації протягом необхідного інтервалу часу. Здатність системи зберігати властивості, необхідні для виконання заданого призначення, при *форс-мажорних вражаючих діях, не передбачених умовами нормальної експлуатації* є живучістю системи.

Згідно зі ст. 263 Цивільного та ст. 218 Господарського кодексу України до надзвичайних і невідворотних за цих умов здійснення господарської діяльності події віднесено обставини *непереборної сили.*

З урахуванням зазначеного здатність АСК зберігати властивості, необхідні для виконання заданого призначення, за обставин непереборної сили (живучість автоматизованої системи керування) розраховується за формулою (9).

Висновки. Проникнення до автоматизованих систем керування (АСК) виробничими процесами робить виробництво особливо уразливим, оскільки дозволяє зловмисникам, які контролюють розвиток подій, утримувати стан небезпеки катастрофи. З метою визначення чинників небезпеки, на основі аналізу класів загроз безпеці АСК, виконано оцінювання ефективності зброї. Для оцінювання живучості АСК, яка вирізняється не передбаченими умовами нормальної експлуатації обставинами непереборної сили, запропоновано обернене до оцінювання ефективності зброї рішення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Gellman B.* Cyber-attacks by Al Qaeda feared / B. Gellman // Washington Post. – 2002. – June, 27. – P. A1.

2. *Остапенко Г.А.* Информационные операции и атаки в социотехнических системах / Г.А. Остапенко. – М. : Горячая линия – Телеком, 2007. – 134 с.

3. *Будько М.М.* Методи підвищення захищеності інформаційних ресурсів автоматизованих систем спеціального призначення та оптимізації структур систем їхнього технічного захисту : дис. ... канд. техн. наук : 05.13.21 / Будько Микола Миколайович. – К., 2002. – 162 с.

4. *Червонный А.А.* Вероятностные методы оценки эффективности вооружения / А.А. Червоный, В.А. Шварц, А.П. Козловцев, В.А. Чобанян ; под ред. проф. А.А. Червоного. – М. : Воениздат, 1979. – 95 с.

5. *Костров А.В.* Дискретная модель определения ущерба, наносимого объектам в социогенной чрезвычайной ситуации / А.В. Костров // Проблемы безопасности при чрезвычайных ситуациях. Обзорная информация. – М. : ВИНИТ. – 1999. – Вып. 6. – С. 50–75.

6. *Рябинин И.А.* Надежность и безопасность структурно-сложных систем / И.А. Рябинин. – СПб. : Политехника, 2000. – 248 с.

Отримано 20.04.2011