УДК 004.056.5

МОДЕЛЬ ІМОВІРНИХ ДЕСТРУКТИВНИХ ДІЙ ПЕРСОНАЛУ АСУ ТП В УМОВАХ НАЯВНОСТІ ДЕСТАБІЛІЗУЮЧИХ ВПЛИВІВ В АСПЕКТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

С. Ф. Гончар, канд. техн. наук

Державний НДІ спеціального зв'язку та захисту інформації

sfgonchar@gmail.com

Наведено модель імовірних деструктивних дій обслуговуючого персоналу АСУ ТП за умови наявності зовнішніх та/або внутрішніх дестабілізуючих впливів. Дано рекомендації щодо забезпечення інформаційної безпеки АСУ ТП в аспекті навмисних деструктивних дій обслуговуючого персоналу.

Ключові слова: модель; інформаційна безпека; дестабілізуючий вплив; деструктивні дії; персонал.

Model of possible destructive actions of personnel of industrial control systems provided availability of external and/or internal destabilizing influences is given. Recommendations for information security of industrial control systems in terms of intentional destructive actions of personnel are given.

Keywords: model; information security; destabilizing effects; destructive actions; personnel.

Вступ

На сьогодні інформаційна безпека держави визначається, в тому числі, рівнем інформаційної безпеки існуючих складних людино-машинних систем управління об'єктами технічних, технологічних, організаційних і економічних комплексів країни — автоматизованих систем управління технологічними процесами (АСУ ТП) [1; 2].

Якщо спочатку зазначені системи були у вигляді окремого комп'ютера із власними операційними системами і мережами, то розвиток і поширення інформаційних технологій, глобалізація інформаційно-телекомунікаційних мереж дало можливість забезпечувати управління виробничою діяльністю в режимі реального часу, здійснювати дистанційний моніторинг систем управління технологічним процесом, підвищити безпеку підприємства і персоналу, зменшити витрати на експлуатацію.

Однак, ціною цих переваг являється підвищена уразливість до нового типу загроз інформаційної безпеки АСУ ТП — злому і порушення режимів функціонування ключових об'єктів, які відповідають за управління та забезпечення безпеки об'єктів критичної інфраструктури, до яких можна віднести: атомні і гідроелектростанції, нафто- і газопроводи, національні мережі розподілу електроенергії, транспортні системи національного і світового рівня тощо. Від інформаційної безпеки систем управління такими об'єктами залежить не тільки прибуток компаній, але й національна безпека.

Постановка проблеми

Забезпечення інформаційної безпеки, що вміщує які основні складові духовно-світоглядну, архетипічну, соціально-моральну, психічну, інтелектуальну і психофізіологічну безпеку, являє собою актуальну військово-політичну, наукову і соціально-економічну проблему [3].

На думку деяких фахівців [4; 5], наукове вирішення даної проблеми повинно базуватися на дослідженні відповідних інформаційних відносин активних компонентів указаних систем, якими є обслуговуючий персонал, з відповідними активними компонентами конфронтуючих систем і між собою.

Інформаційні відносини активних об'єктів у різних інформаційних середовищах (природних, штучних, гібридних) повинні включати відносини інформаційного відокремлення (ізоляції та захисту) і взаємодії (суперництво та співробітництво). Крім того, деякі автори [6] висловлюють думку, що на даний час все більше зростає роль людського фактору на інформаційну безпеку АСУ ТП при недостатній кількості методів і засобів його оцінки та захисту.

Засоби і методи, які наразі розробляються (наприклад, метод інженерної психології) дають змогу зменшити рівень помилкової інформації, але не досліджують проблему в цілому, у тому

числі не проводять оцінку і захист, як від випадкових, так і від умисних деструктивних дій обслуговуючого персоналу.

При цьому, людський фактор є одночасно і необхідним елементом людино-машинних систем управління і джерелом загроз інформаційній безпеці таких систем.

Отже, основними об'єктами інформаційно-психологічного впливу в АСУ ТП є обслуговуючий персонал і особа, яка приймає рішення щодо управління процесами в той чи іншій предметній галузі [6].

У складних людино-машинних системах управління персоналу доводиться приймати ті чи інші рішення. При цьому, на адекватність прийнятих рішень персоналом у таких системах можуть впливати такі фактори [5]: зовнішні та внутрішні дестабілізуючі впливи, нестійкість рішення при великій кількості альтернатив, тривалість часового інтервалу для прийняття рішення.

Враховуючи викладене, можна зазначити, що важливим завданням є прийняття адекватних рішень обслуговуючим персоналом у різних інформаційних середовищах і відносинах. Для цього актуальним є отримання моделі ймовірних деструктивних дій персоналу АСУ ТП в умовах наявності дестабілізуючих впливів в аспекті інформаційної безпеки.

Матеріали і результати досліджень

Кількість альтернатив і тривалість часового інтервалу для прийняття рішення буде залежати від технологічних особливостей конкретної системи і вплив даних факторів може призвести до ненавмисних помилкових дій персоналу.

Водночас, дія зовнішніх та/або внутрішніх дестабілізуючих впливів може призвести до навмисних деструктивних дій персоналу. Загальна схема дії таких чинників показана на рис. 1.

Розглянемо більш детально, що собою являє кожний з наведених чинників.

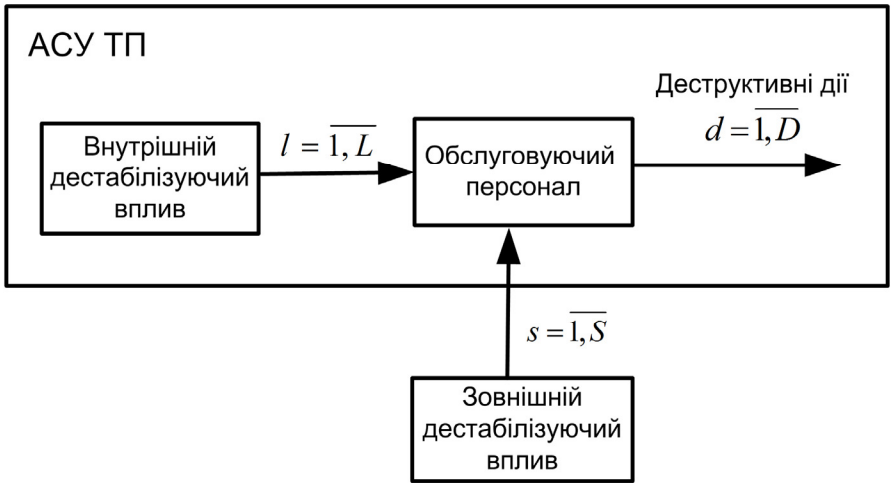

Рис. 1. Загальна схема дії чинників в АСУ ТП

Під зовнішнім дестабілізуючим впливом $s=\overline{1,S}$ будемо розуміти множину загроз реалізації інформаційно-психологічного впливу на обслуговувальний персонал АСУ ТП. Такі впливи матимуть дезорієнтацію, дезінформацію, дезорганізацію, придушення, руйнування тощо. Виділяють п'ять відповідних груп засобів, які мають бути застосовані для інформаційно-психологічного впливу на персонал людино-машинних систем управління [4]:

– засоби масової інформації, агітаційно-пропагандистські засоби;

– психотронні засоби;

– електронні засоби: радіоелектронні, оптикоелектронні, електронно-обчислювальні засоби і засоби комп'ютерних інформаційних технологій;

– лінгвістичні засоби;

– психотропні засоби.

Множина факторів внутрішнього дестабілізуючого впливу $l=\overline{1,L}$ являє собою множину людських потреб, через захищеність яких може розкриватися забезпечення інформаційної безпеки людино-машинних систем управління, а саме [4]:

– вітальні (природні): їжа, одяг, житло, відпочинок, комфорт, екологія тощо;

– самоактуалізаційні (пізнавальні): активність, навички, уміння, діяльність, ініціатива, дослідницький пошук тощо;

– інтелектуальні (наукові): освіта (знання), виховання, мислення, цінна інформація, самосвідомість, істина тощо;

– психічні (естетичні): прив'язаність, спорідненість, чиста совість, піднесеність тощо;

– соціальні (групові): спілкування, засоби спілкування, увага до себе, спільна діяльність тощо;

– самореалізувальні (індивідуальні): творчість, самовдосконалення, самоповага, повага з боку інших, визнання, досягнення успіху і високої оцінки, службове зростання тощо;

– духовні (етичні): щастя, свобода совісті, цілісність світогляду, доброта, честь тощо.

Отже, стан інформаційної безпеки персоналу АСУ ТП визначається двома основними чинниками: інформаційно-психологічною задоволеністю людських потреб персоналу і дестабілізую чими (навмисними або випадковими) інформаційно-психологічними та інформаційно-технічними впливами.

Множиною деструктивних дій $d = \overline{1, D}$ з боку обслуговуючого персоналу відносно технічної компоненти будуть дії, спрямовані на порушення конфіденційності, цілісності, доступності та неспростовності інформації в АСУ ТП, тобто виникнення загрози інформаційної безпеки.

Загрози можуть бути реалізовані різними типами деструктивних дій.

Взаємозв'язок між загрозами і можливими деструктивними діями наведено на рис. 2 [7].

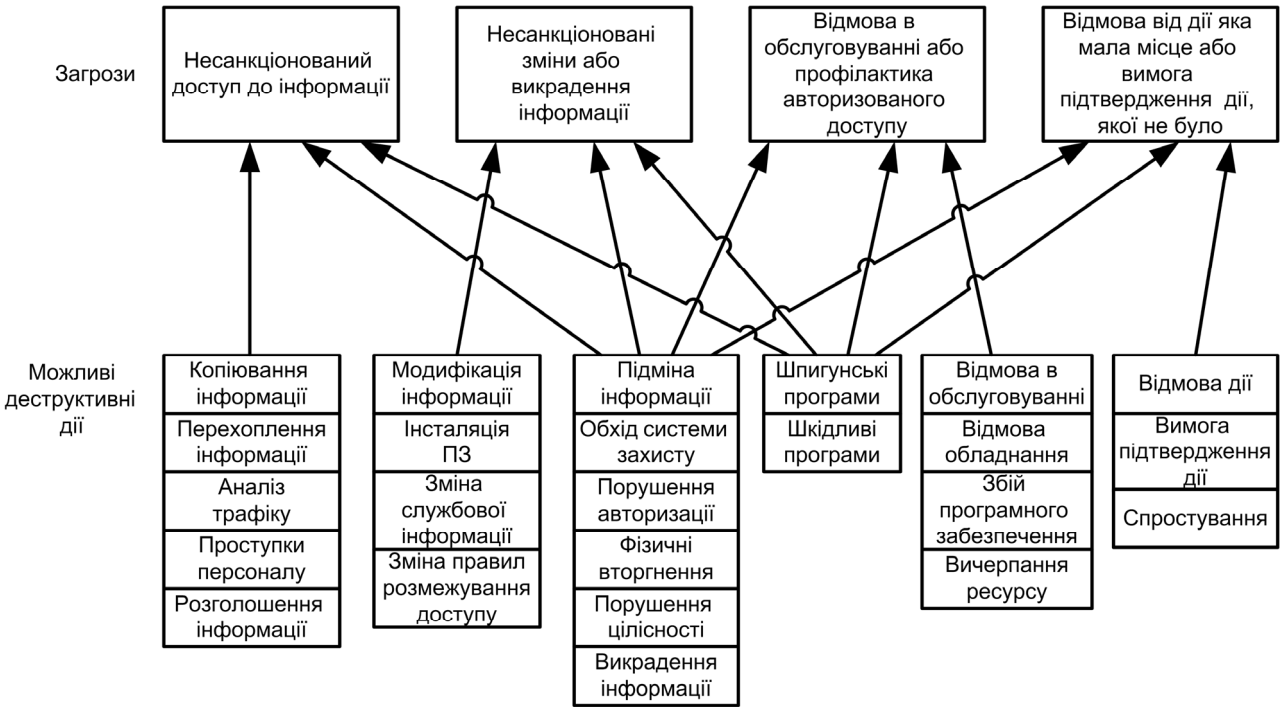

Рис. 2. Взаємозв'язок між загрозами і деструктивними діями

Як бачимо з рис. 2, загрози інформації можна класифікувати за результатом їх впливу на інформацію. В результаті реалізації загроз інформації є порушення інформаційної безпеки, тобто — порушення конфіденційності, цілісності доступності інформації і відповідальності.

Розрізняють чотири типи загроз безпеки інформації:

- несанкціонований доступ до інформації;
- несанкціоновані зміни або викрадення інформації;
- відмова в обслуговуванні або профілактика авторизованого доступу;
- відмова у відповідальності.

Таким чином, конфіденційність буде забезпечуватись, якщо дотримуються встановлених правих доступу до системи, цілісність — якщо дотримуються встановлених правил модифікації інформації або її видалення, доступність — якщо зберігається можливість доступу до системи або модифікації інформації відповідно до встановлених правил упродовж будь-якого певного (малого) проміжку часу. Загрози, реалізація яких призводить до втрати інформацією якої-небудь з названих властивостей, відповідно є загрозами конфіденційності, цілісності або доступності інформації. Загрози для автоматизованих систем управління технологічними процесами можуть виходити з різних джерел: навмисних (терористичні групи, промислові шпигуни, невдоволені працівники, зловмисники), ненавмисних (складність системи, людські помилки, аварії, відмови обладнання), природних (стихійні лиха, кліматичні умови тощо). Однак, ми розглядаємо загрози, які можуть виходити від імовірних навмисних деструктивних дій обслуговуючого персоналу за умови наявності деструктивних впливів.

Очевидно, що обслуговуючий персонал складається з індивідів, кожний з яких здатний здійснювати хороші або погані вчинки, бачити себе зі сторони спостерігача, усвідомлювати відповідні відчуття за здійсненні вчинки.

Найпростішу модель, яка описує поведінку такого індивіда, його готовність до дій, можна подати у вигляді імплікації [3]:

$$I = J \to Z = F(Z, J), \qquad (1)$$

де Z — дія зовнішніх та/або внутрішніх дестабілізуючих впливів; J — усвідомлення індивідом своїх дій відносно до дії дестабілізуючих впливів.

Нехай $P(I)$ — імовірність здійснення індивідом деструктивних дій; $P(I|Z)$ — імовірність здійснення індивідом деструктивних дій за умови дії зовнішніх та/або внутрішніх дестабілізуючих впливів; $P(Z)$ — імовірність дії зовнішніх та/або внутрішніх дестабілізуючих впливів.

Очевидно, що кожен із зовнішніх дестабілізуючих впливів з множини $s = \overline{1,S}$ може діяти одночасно з кожним із внутрішніх дестабілізуючих впливів з множини $l = \overline{1,L}$. Тоді, враховуючи основні властивості ймовірності [8], імовірність дії дестабілізуючих впливів буде визначатися з виразу:

$$P(Z) = \begin{Vmatrix} \left[P(s_1) + P(l_1) - P(s_1 l_1)\right] & \cdots & \left[P(s_1) + P(l_L) - P(s_1 l_L)\right] \\ \vdots & \ddots & \vdots \\ \left[P(s_S) + P(l_L) - P(s_S l_L)\right] & \cdots & \left[P(s_S) + P(l_L) - P(s_S l_L)\right] \end{Vmatrix}, \qquad (2)$$

де $P(s)$ — імовірність дії зовнішніх дестабілізуючих впливів; $P(l)$ — імовірність дії внутрішніх дестабілізуючих впливів; $P(sl)$ — імовірність одночасної дії зовнішніх та внутрішніх дестабілізуючих впливів.

Тоді, ймовірність здійснення індивідом деструктивних дій, спрямованих на порушення інформаційної безпеки, буде визначатися з виразу:

$$P(I) = \left\| P(I \mid Z_{sl}) P(Z_{sl}) \right\|, \qquad (3)$$

де $P(I|Z_{sl})$ — імовірність здійснення індивідом деструктивних дій при умові дії s-го зовнішнього впливу та l-го внутрішнього впливу; $P(Z_{sl})$ — імовірність дії s-го зовнішнього впливу та l-го внутрішнього впливу і визначається з виразу (2).

Аналіз виразу (3) показує, що відсутність навмисних деструктивних дій з боку обслуговуючого персоналу, тобто забезпечення інформаційної безпеки АСУ ТП буде виконуватися за умови $P(I|Z_{sl}) = 0$ або $P(Z_{sl}) = 0$.

Висновки

Наведена модель імовірних деструктивних дій обслуговуючого персоналу АСУ ТП за умови наявності зовнішніх та/або внутрішніх дестабілізуючих впливів. Аналіз наведеної моделі показує, що для забезпечення інформаційної безпеки АСУ ТП в аспекті навмисних деструктивних дій обслуговуючого персоналу необхідно:

– забезпечити відсутність зовнішнього дестабілізуючого інформаційно-психологічного впливу на персонал;

– забезпечити, по можливості, задоволення потреб персоналу, через захищеність яких може розкриватися забезпечення інформаційної безпеки людино-машинних систем управління;

– здійснювати заходи, спрямовані на запобігання здійснення ймовірних деструктивних дій персоналом за наявності дестабілізуючих впливів.

ЛІТЕРАТУРА

1. *Мохор В. В*. Наставления по кибербезопасности (ISO/IEC 27032:2012) / В. В.Мохор, А. М. Богданов, А. С. Килевой. — К..: ООО «ТриК», 2013. — 129 с.

2. *Гончар С. Ф*. Шляхи удосконалення державної політики забезпечення інформаційної безпеки критичної інфраструктури України : матеріали круглого столу «Державне реагування на загрози національним інтересам України: актуальні проблеми та шляхи їх розв'язання». — К. : НАДУ, 2014. — С. 92–95.

3. *Лефевр В. А*. Алгебра совести / В. А. Лефевр; [пер. с англ. В. Лефевр и Е. Юдиной]. — М. : Когито-Центр, 2003. — 426 с.

4. *Ловцов Д. А*. Управление безопасностью эргасистем / Д. А. Ловцов, Н. А. Сергеев; под ред. Д. А. Ловцова. — 2-е изд. испр. и доповн. — М. : РАУ-Университет, 2001. — 224 с.

5. *Силов В. Б*. Принятие стратегических решений в нечеткой обстановке / В. Б. Силов. — М. : ИНПРО-РЕС, 1995. — 228 с.

6. *Емелин В. И.* Методы и модели оценки и обеспечения информационной безопасности автоматизированных систем управления критическими системами: дис. … доктора техн. наук : 05.13.19 / Вадим Иванович Емелин. — СПб., 2012. — 238 с.

7. *Power* systems management and associated information exchange — Data and communications security: IEC 62351-1. — Part 1: Communication network and system security — Introduction to security issues.

8. *Теория* вероятностей и математическая статистика. Базовый курс с примерами и задачами / [А. И. Кибзун, Е. Р. Горяинова, А. В. Наумов, А. Н. Сиротин]. — М. : ФИЗМАТЛИТ, 2002. — 224 с.

Стаття надійшла до редакції 21.07.2015