Юдин Александр Константинович, доктор технических наук, профессор. Член экспертного и научно-методического совета Министерства образования и науки Украины в области «Информационная безопасность». Член-корреспондент Академии Связи Украины. Лауреат Государственной премии Украины в области науки и техники. Директор института компьютерных информационных технологий, заведующий кафедрой компьютеризованных систем защиты информации Национального авиационного университета.

Yudin Alexander Konstantinovich, D. of Engineering, professor. Member of expert and scientifically-methodical advice of Department of education and science of Ukraine in an area «Informative security». Corresponding member of Academy of Connection of Ukraine. Laureate of the State bonus of Ukraine in area of SciTech. Director of institute of computer information technologies, manager by the department of the computerized systems for information the National Aviation University.

Бучик Сергій Степанович, кандидат технічних наук, доцент, начальник кафедри автоматизованих систем управління Житомирського військового інституту імені С. П. Корольова.
E-mail: s_stbu@ukr.net

Бучик Сергей Степанович, кандидат технических наук, доцент, начальник кафедры автоматизированных систем управления Житомирского военного института имени С.П. Королева.

Buchyk Sergii, PhD in Eng., chief of department of automated control the system the Zhitomir Military Institute of the name of S.P. Korolyova.

УДК 004.056.5

ВИЗНАЧЕННЯ АКТУАЛЬНИХ ЗАГРОЗ БЕЗПЕЦІ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ

Сергій Гончар

З метою вирішення задач по забезпеченню безпеки інформації автоматизованих систем управління технологічними процесами приведено узагальнену модель процесу захисту інформації. Здійснено дослідження та аналіз взаємодії системи захисту інформації і дестабілізуючих факторів таких як, загрози, сприятливі умови для реалізації цих загроз, уразливості. Показано, що актуальність загрози безпеці інформації пропорційна ймовірності реалізації даної загрози та коефіцієнту її небезпеки. отримано вирази для визначення ймовірності реалізації загроз безпеці інформації та коефіцієнта їх небезпеки. Приведено метод визначення актуальних загроз безпеці інформації в автоматизованих системах управління технологічними процесами та сформульовано вихідні дані, які для цього необхідні.

Ключові слова: *загроза, безпека інформації, автоматизовані системи управління, уразливості, метод, модель.*

Вступ. На сьогоднішній день автоматизовані системи управління технологічними процесами (АСУ ТП), які включають в себе системи диспетчерського управління і збору даних, системи розподіленого управління та інші конфігурації систем управління використовуються в різних сферах промислового сектору, і кількість таких систем постійно зростає. До таких систем належать атомні і гідроелектростанції, нафто- і газопроводи, національні мережі розподілу електроенергії, транспортні системи національного і світового рівня, загальнодержавні системи зв'язку, галузеутворюючі підприємства тощо, тобто об'єкти критичної інфраструктури [1].

Очевидно, що в умовах сучасного надзвичайно інтенсивного розвитку інфраструктури провідних країн світу існує багато об'єктів критичної інфраструктури, виведення з ладу яких може призвести до надзвичайних ситуацій, пов'язаних із загибеллю людей, екологічними катастрофами, заподіянням великих матеріальних, економічних збитків тощо.

Багато держав, в першу чергу економічно розвинуті, вдосконалюють методи та способи використання інформаційних технологій і засобів для деструктивних впливів на інформаційні системи об'єктів критичної інфраструктури. При цьому, складна організація автоматизованих систем управління технологічними процесами і вимоги безперервності технологічних процесів призводять до того, що базові компоненти систем управління (індустріальні протоколи, операційні системи, системи управління базами даних тощо) старіють, не оновлюються, і їх уразливості не усуваються досить тривалий проміжок часу. Дані щодо усунення уразливостей в автоматизованих системах управління технологічними процесами

станом на перший квартал 2015 року приведені на рис. 1 [2].

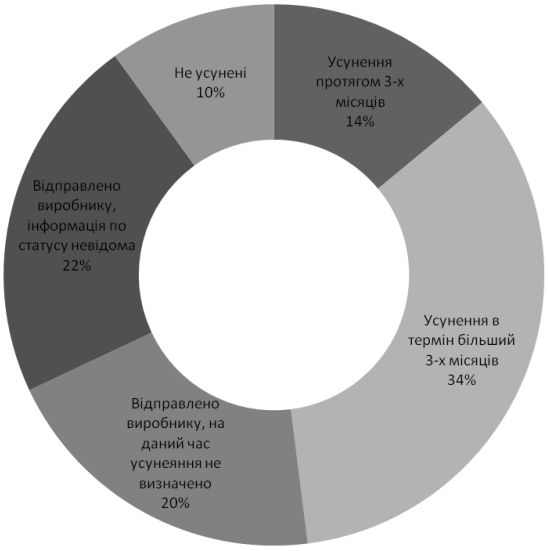

Рис. 1. Статистика усунення уразливостей АСУ ТП

Аналіз статистики усунення уразливостей, рис. 1, свідчать, що тільки 14% уразливостей були усунені в термін до трьох місяців, 34% уразливостей усувалися у термін більше трьох місяців, а інші 52% уразливостей або не усунені, або виробник не повідомляє термін усунення.

Враховуючи викладене вище, можна зазначити, що в сучасних реаліях, безпеку об'єктів критичної інфраструктури необхідно розглядати в новому ракурсі, а саме: разом з класичними заходами безпеки, необхідно забезпечувати безпеку інформації.

Постановка проблеми. На відміну від традиційних систем інформаційних технологій, в автоматизованих системах управління технологічними процесами існує досить тісний взаємозв'язок автоматизованих систем з фізичними процесами і виконавчими пристроями [1]. Тому, порушення безпеки інформації в автоматизованих системах управління технологічними процесами може призвести до наслідків у промисловому секторі, особливо у випадку автоматизованих систем управління небезпечними виробничими циклами або систем життєзабезпечення. Можливі збитки від реалізації таких загроз окрім фінансових втрат будуть включати ризики репутації і ризики, пов'язані із втратою здоров'я та життя людей, а також ризики виникнення екологічних катастроф. Навіть поодиноке порушення функціонування автоматизованих систем управління технологічним процесом може призвести до катастрофічних наслідків.

Враховуючи зазначене, небезпека загрози в автоматизованих системах управління технологічними процесами із множини загроз буде визначатися оцінкою можливих наслідків від її реалізації з позиції впливу на функціонування автоматизованих систем управління технологічними процесами, а рівень тяжкості таких наслідків – коефіцієнтом небезпеки даної загрози.

Однак, не кожна загроза може бути реалізована в той відрізок часу, який розглядається. Для реалізації загрози необхідно наявність уразливостей системи захисту і наявність для цього сприятливих умов. Наявність приведених факторів підвищує ймовірність реалізації загроз безпеці інформації [3].

Крім того, в залежності від умов і режимів функціонування автоматизованої системи управління технологічними процесами відбувається зміна як самих загроз безпеці інформації, так і їх актуальності.

Таким чином, кожна загроза характеризується ймовірністю її реалізації і нанесеними нею збитками [4]. Тобто, показник актуальності загрози в АСУ ТП буде пропорційний ймовірності реалізації даної загрози та коефіцієнту її небезпеки.

Враховуючи зазначене, для своєчасного та адекватного реагування на загрози безпеці інформації в автоматизованих системах управління технологічними процесами необхідне визначення актуальності даних загроз.

Матеріали і результати досліджень. З метою проведення дослідження та аналізу взаємодії дестабілізуючих факторів (загрози, сприятливі умови реалізації цих загроз, уразливості) і системи захисту інформації, яка запобігає впливу даних факторів, розглянемо узагальнену модель процесу захисту інформації, рис. 2.

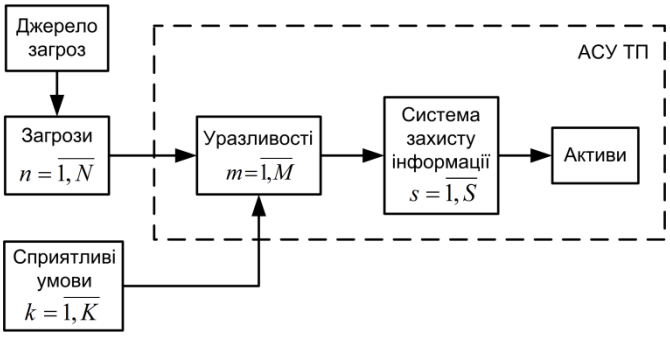

Рис. 2. Узагальнена модель процесу захисту інформації АСУ ТП

Так, потенційний порушник безпеки інформації з допомогою деякого джерела загроз створює множину загроз безпеці інформації АСУ ТП $n=\overline{1,N}$, кожна з яких може бути реалізована через одну або декілька уразливостей з множини

$m=\overline{1,M}$. При цьому, як уже зазначалося, актуальність кожної n-тої загрози характеризується ймовірністю її реалізації і нанесеними нею збитками.

Ймовірність реалізації загрози може бути представлена у вигляді матриці [5], як взаємозв'язок загроз безпеці інформації, уразливостей, через які дані загрози можуть бути реалізовані та сприятливих для цього умов:

$$P(R)=\left[P(R_{nm})\right]. \qquad (1)$$

де елементи матриці $P(R_{nm})$ визначаються з виразу:

$$P(R_{nm})=\sum_{k=1}^{K}P(R_{nm}\mid Q_k)P(Q_k), \qquad (2)$$

де $P(R_{nm}\mid Q_k)$ – ймовірність реалізації n-ї загрози з використанням m-ї уразливості при умові наявності сприятливих умов Q_k, де $n=\overline{1,N}$ – множина загроз; $m=\overline{1,M}$ – множина уразливостей; $P(Q_k)$ – ймовірність наявності сприятливих умов.

Як зазначають деякі автори [4], збитки, завдані n-ою загрозою можуть визначатися в абсолютних одиницях: економічних втратах, часових втратах, об'ємі втраченої або пошкодженої інформації і т.п. Однак, з практичної точки зору це зробити досить складно, особливо на ранніх етапах проектування системи захисту інформації. Тому пропонується [4] замість абсолютного збитку використовувати відносний збиток, який по суті і буде являти собою ступінь небезпеки n -ї загрози для інформаційної системи – коефіцієнт небезпеки n-ї загрози H_n. Тобто, коефіцієнт небезпеки загрози буде являти собою відношення величини збитку, який виникає від деструктивних дій в результаті реалізації цієї загрози, до його максимального (неприйнятного) значення. Таким чином, коефіцієнт небезпеки загрози є відносною величиною і,тому, не залежить від виду збитку. Коефіцієнт небезпеки може бути визначений експертним шляхом в припущенні, що всі загрози для інформаційної системи складають повну групу незалежних подій.

Коефіцієнти небезпеки деструктивних дій пропонується визначати експертним шляхом. Для цього необхідно визначити перелік можливих деструктивних дій щодо порушення конфіденційності, цілісності, доступності та неспростовності інформації, після чого здійснити оцінку коефіцієнтів небезпеки кожної деструктивної дії при реалізації загроз в залежності від наслідків, до яких може призвести дана деструктивна дія.

Основними категоріями впливу деструктивних дій в автоматизованих системах управління технологічними процесами є:

- фізичний вплив – включає в себе безліч прямих наслідків аварій автоматизованих систем управління технологічними процесами. Найважливішими потенційними наслідками є такі, які можуть призвести до травм і загибелі людей. Інші наслідки включають втрату майна (включаючи дані) і потенційні збитки навколишньому середовищу;
- економічні впливи – наслідки другого порядку від фізичних впливів, що є похідними від аварій автоматизованих систем управління технологічними процесами. Фізичний вплив може призвести до наслідків для системи, що, у свою чергу може нанести більший економічний збиток підприємству чи організації. У великих масштабах, ці наслідки можуть негативно позначитися на місцевому, регіональному, національному рівнях, а можливо і для глобальної економіки;
- соціальні впливи – наслідки другого порядку, які є похідними від втрати державної або громадської довіри в організації.

Враховуючи приведені вище категорії впливу порушення безпеки інформації в автоматизованих системах управління технологічними процесами можливо навести перелік наслідків цих впливів:

- порушення національної безпеки;
- сприяння вчиненню акту тероризму;
- втрата або скорочення виробництва;
- травми або смерть людей;
- пошкодження обладнання;
- викид (витікання, випаровування) або крадіжка небезпечних матеріалів;
- екологічні збитки;
- кримінальні або цивільно-правові зобов'язання;
- втрата приватної або конфіденційної інформації;
- втрата іміджу бренду або довіри клієнтів.

Слід зазначити, що елементи приведеного переліку не є незалежними. Очевидно, що один з наслідків може призвести до іншого.

Взаємозв'язок між загрозами безпеці інформації та основними можливими деструктивними діями приведений на рис. 3 [6].

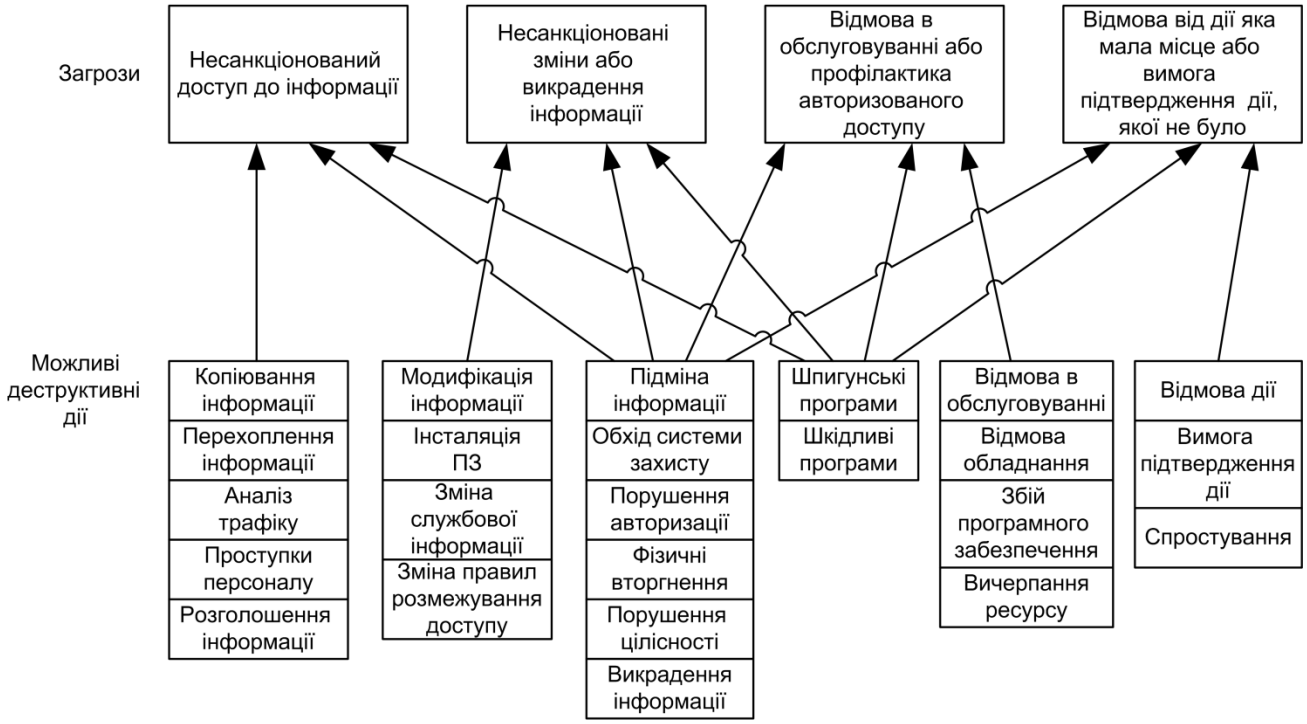

Рис. 3. Взаємозв'язок між загрозами та деструктивними діями

Взаємозв'язок між загрозами і деструктивними діями, які виникають в результаті реалізації цих загроз можливо представити у вигляді матриці:

$$G = [g_{dn}], \tag{3}$$

де $d = \overline{1, D}$ – множина можливих деструктивних дій; $n = \overline{1, N}$ – множина загроз.

Елементи g_{dn} матриці (3) набувають значення 1, якщо n-та загроза призводить до реалізації d-ї деструктивної дії, і набувають значення 0 – в протилежному випадку.

Нехай h_d – коефіцієнт небезпеки виконання d-ї деструктивної дії, де $d = \overline{1, D}$ – множина можливих деструктивних дій.

Тоді, враховуючи, що у випадку реалізації n-ї загрози може мати місце декілька деструктивних дій, коефіцієнт небезпеки n-ї загрози буде визначатися наступним чином:

$$H_n = \sum_{d=1}^{D} h_d \cdot g_{dn}, \tag{4}$$

де h_d – коефіцієнт небезпеки виконання d-ї деструктивної дії і визначається за рівнем тяжкості наслідків даного виконання; g_{dn} – коефіцієнт, який визначається, як елемент матриці (3).

Деструктивні дії спрямовані на те, щоб спричинити шкоду активам. Активом являється деяка сутність, цінна для особистості, організації або держави.

Активи автоматизованих систем управління технологічними процесами можуть бути класифіковані за видами наступним чином [7]: фізичні, логічні, людські. Розглянемо в загальному вигляді кожний з видів активів.

Фізичні активи включають в себе будь-які фізичні компоненти або групи компонентів, які належать організації. В автоматизованих системах управління технологічними процесами вони включають в себе системи управління, фізичні компоненти мережі передачі інформації або будь-які інші фізичні об'єкти, які певним чином залучені до процесів управління та аналізу виробничих процесів.

Логічні активи можуть включати в себе інтелектуальну власність, алгоритми, спеціальні знання, або інші інформаційні елементи, які містять в собі здатність функціонування організації або інноваційної діяльності. Крім того, ці види активів можуть включати в себе суспільну репутацію, довіру покупця, або інші заходи, які, у разі їх пошкодження, безпосередньо впливають на виробничий процес. Логічні активи можуть бути у формі особистої пам'яті, документів, інформації, що міститься на фізичному або електронному носіях інформації. Логічні активи можуть також включати в себе результати тестів, нормативних даних, або будь-яку іншу інформацію, яка розглядається як конфіденційна або приватна. Втрата

логічних активів часто викликає значну шкоду організації і на тривалий час.

Активи автоматизованих систем управління технологічними процесами є особливою формою логічних активів. Вони містять логіку автоматизації, яка приймає участь у виконанні виробничих процесів. Ці процеси надзвичайно залежать від повторного або безперервного виконання чітко визначених подій. І тому, нанесення шкоди цим активам, наприклад видалення або несанкціонована модифікація, може призвести до втрати цілісності або доступності безпосередньо до самого процесу.

Людські активи включають у себе людей, знання, а також теоретичні і практичні навички, якими вони володіють, і які пов'язані з їх виробничою діяльністю. Вони можуть включати в себе необхідні сертифікати або важливі навички, необхідні для дій під час надзвичайних ситуацій.

З метою мінімізації небезпеки, спрямованої на активи застосовується система захисту інформації, яка являє собою систему із набором властивостей – множиною функцій захисту інформації $s = \overline{1,S}$.

Завдяки функціям захисту інформації система захисту інформації в автоматизованих системах управління технологічними процесами повинна реагувати на події, пов'язані із забезпеченням безпеки інформації. Тобто, система захисту інформації має протиставляти певні функції захисту інформації кожній події, спрямованій на порушення захисту інформації, наприклад: оцінка реальної можливості прояву порушення безпеки інформації; виявлення фактів їх прояву; вжиття заходів щодо запобігання їх впливу на об'єкт захисту; виявлення, локалізація і ліквідація наслідків впливу на об'єкт захисту. Методи реалізації зазначених функцій можуть бути: організаційні, програмні, апаратні і ін. [8].

Виходячи із приведеного можна зазначити, що система захисту інформації повинна володіти функціями захисту інформації $s = \overline{1,S}$, які спрямовані на повну або часткову компенсацію загроз для активів автоматизованих систем управління технологічними процесами.

Контрзаходи, які впроваджуються для захисту активів АСУ ТП повинні враховувати різні типи загроз і можливих деструктивних дій, які можливі в результаті реалізації цих загроз.

Враховуючи викладене вище, можливо відмітити, що для визначення актуальності загроз необхідні наступні вихідні дані:

- перелік джерел загроз;
- перелік загроз безпеці інформації $n = \overline{1,N}$;
- перелік уразливостей, через які можлива реалізація загроз $m = \overline{1,M}$;
- перелік сприятливих умов для реалізації загроз $k = \overline{1,K}$;
- перелік можливих деструктивних дій $d = \overline{1,D}$;
- коефіцієнти небезпеки виконання деструктивних дій h_d;
- взаємозв'язок між загрозами і деструктивними діями g_{dn};
- взаємозв'язок між загрозами, уразливостями і сприятливими умовами $P(R_{nm} \mid Q_k)$.

Висновки. З метою вирішення задач по забезпеченню безпеки інформації автоматизованих систем управління технологічними процесами приведено узагальнену модель процесу захисту інформації.

Здійснено дослідження та аналіз взаємодії системи захисту інформації і дестабілізуючих факторів таких як, загрози, сприятливі умови реалізації цих загроз, уразливості.

Показано, що актуальність загрози безпеці інформації пропорційна ймовірності реалізації даної загрози та коефіцієнту її небезпеки.

Приведено вирази для визначення ймовірності реалізації загроз безпеці інформації та коефіцієнта їх небезпеки.

Приведено метод визначення актуальних загроз безпеці інформації в автоматизованих системах управління технологічними процесами та сформульовано вихідні дані, які для цього необхідні.

Визначення актуальності загроз безпеці інформації дасть змогу здійснювати своєчасне та адекватне реагування на дані загрози в автоматизованих системах управління технологічними процесами.

ЛІТЕРАТУРА

[1]. Гончар С.Ф. Особенности обеспечения кибербезопасности индустриальных систем управления : тези доповідей міжнародної науково-практичної конференції «Проблеми та перспективи розвитку енергетики, електротехнологій та автоматики в АПК», Київ, – 2013. – С. 36-37.

[2]. Исследование: уязвимости промышленных систем управления в 2014 году // [Електронний ресурс]. – Режим доступу: http://habrahabr.ru/company /pt / blog /258039/.

[3]. Мохор В. В. Построение оценок рисков безопасности информации на основе динамического множества актуальных угроз / В. В. Мохор, А. М. Богданов, О. Н. Крук, В. В. Цуркан // Збірник наукових працьІнституту проблем моделювання

в енергетиці ім. Г. Є. Пухова. – К.: ІПМЕ ім. Г. Є. Пухова НАН України, 2010. – Вип. 56. – С. 87-99.
[4]. Домарев В.В. "Безопасность информационных технологий. Методология создания систем защиты" – К.: ООО "ТИД "ДС", 2002. – 688 с.
[5]. Гончар С.Ф. Аналіз ймовірності реалізації загроз захисту інформації в автоматизованих системах управління технологічним процесом // Захист інформації. – 2014. – том 16, № 1. – С. 40-46.
[6]. 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.
[7]. Industrial communication networks – Network and system security: IEC 62443-1-1. – Part 1-1: Terminology, concepts and models.
[8]. Антонюк А.А., Боровская Е.Н., Суслов В.Ю. Модель угроз информации в защищенных автоматизированных системах // Безопасность информации. – 2001. – № 2. – С. 17-22.

REFERENCES

[1]. Gonchar S.F. Features of cybersecurity industrial control systems : Materials of International Scientific Conference "Problems and prospects of power engineering, electrotechnology and automation in agriculture", 2013, pp. 36-37.
[2]. Research: vulnerabilities of industrial control systems in 2014 // [Electronic resource]. – Access mode: http://habrahabr.ru/company/pt/blog/258039/.
[3]. Mokhor V.V. Building a risk assessment of information security based on dynamic set of actual threats / V.V. Mokhor, A.M. Bogdanov, O.N. Kruk, V.V. Tsurkan // Collection of scientific works Institute of Modelling Problems in Power Engineering, 2010, № 56, P. 87-99.
[4]. Information technology – Security techniques – Information security risk management: BS ISO/IEC 27005:2008.
[5]. Gonchar S.F. Analysis of probability of threats to information security in industrial control systems // information security, 2014, vol. 16, № 1, P. 40-46.
[6]. Guide to Industrial Control Systems (ICS) Security: NIST Special Publication 800-82. – Recommendations of the National Institute of Standards and Technology.
[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]. Industrial communication networks – Network and system security: IEC 62443.– Part 3.

ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕСАМИ

С целью решения задач, связанных с обеспечением безопасности информации в автоматизированных системах управления технологическими процессами приведена обобщенная модель процесса защиты информации. Выполнены исследования и анализ взаимодействия системы защиты информации и дестабилизирующих факторов таких как, угрозы, благоприятные условия для реализации этих угроз, уязвимости. Показано, что актуальность угрозы безопасности информации пропорциональна вероятности реализации данной угрозы и коэффициенту её опасности. Приведены выражения для определения вероятности реализации угроз безопасности информации и коэффициента её опасности. Приведен метод определения актуальных угроз безопасности информации в автоматизированных системах управления технологическими процессами и сформулированы исходные данные, необходимые для этого.
Ключевые слова: угроза, безопасность информации, автоматизированные системы управления, уязвимости, метод, модель.

DETERMINING OF THE RELEVANCE THREATS OF INFORMATION SECURITY IN INDUSTRIAL CONTROL SYSTEMS

In order to solve problems related to the information security in the industrial control systems shows a generalized model of information security. The studies and analysis of the interaction between the system of information security and destabilizing factors such as threats, favorable conditions for the realization of these threats, vulnerabilities are realized. It was shown that the relevance of the information security threats is proportional to the probability of the threat and the ratio of its danger is show. Expressions for the determination of the likelihood of threats to information security and the coefficient of its danger are given. A method for determining the actual information security threats in the automated process control systems, and formulated the initial data needed for this are given.
Index terms: threat, information security, industrial control systems, vulnerability, method, model.

Гончар Сергій Феодосійович, кандидат технічних наук, заступник начальника державного науково-дослідного інституту спеціального зв'язку та захисту інформації, докторант Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.
E-mail: sfgonchar@gmail.com.
Гончар Сергей Феодосьевич, кандидат технических наук, заместитель начальника государственного научно-исследовательского института специальной связи и защиты информации, докторант Института проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины.
Gonchar Sergii, PhD in Eng., Deputy Chief of State Research Institute for Special Telecommunication and Information Protection, doctoral student of Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine (Kyiv, Ukraine).